RODRIGO COLLI

ESTUDO DE VIABILIDADE DE UTILIZAÇÃO DE VPN PARA A INTERLIGAÇÃO DE REDES DE COMUNICAÇÃO DE DADOS BASEADAS EM LINKS ADSL

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

LAVRAS
MINAS GERAIS – BRASIL
2005

RODRIGO COLLI

ESTUDO DE VIABILIDADE DE UTILIZAÇÃO DE VPN PARA INTERLIGAÇÃO DE REDES DE COMUNICAÇÃO DE DADOS BASEADAS EM LINKS ADSL

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Área de Concentração:
Rede de Computadores

Orientador:
Prof. Rêmulo Maia Alves

Co-orientador:
Prof. Anderson Bernardo dos Santos

LAVRAS
MINAS GERAIS – BRASIL
2005

Ficha Catalográfica preparada pela Divisão de Processos Técnicos da Biblioteca Central da UFLA

Colli, Rodrigo

Estudo de Viabilidade de Utilização deVPN para a Interligação de Redes de Comunicação de Dados Baseadas em Links ADSL – Minas Gerais, 2005. 90 páginas.

Monografia de Graduação – Universidade Federal de Lavras. Departamento de Ciência da Computação.

1. Introdução. 2. Redes de Computadores. 3.TCP/IP. I. COLLI, R. II. Universidade Federal de Lavras. III. Título.

RODRIGO COLLI

ESTUDO DE VIABILIDADE DE UTILIZAÇÃO DE VPN PARA A INTERLIGAÇÃO DE REDES DE COMUNICAÇÃO DE DADOS BASEADAS EM LINKS ADSL

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 07 de Julho de 2005.

_____
Rafael de Magalhães Dias Frinhani

_____
Cristiane Xavier Figueiredo

_____
Prof. Anderson Bernardo dos Santos (Co-Orientador)

_____
Prof. DSc.Rêmulo Maia Alves (Orientador)

LAVRAS
MINAS GERAIS – BRASIL
2005

AGRADECIMENTOS

Agradeço acima de tudo à DEUS, por me guiar em todos os momentos da minha vida e principalmente nessa caminhada.

Aos meus pais, Walter e Tereza, e irmãos, Léo e Junior, por compartilharem comigo os melhores momentos e por me ajudarem nos momentos mais difíceis desses quatro anos de graduação.

Aos professores, Rêmulo e Anderson, que participaram ativamente e contribuíram para que este projeto fosse concluído.

Á todos meus colegas de trabalho e de república pela amizade e por me incentivarem e ajudarem neste projeto e em toda minha caminhada na UFLA.

À minha namorada, por dividir comigo grande parte dos meus momentos em Lavras e pela grande força e incentivo em todas as coisas que realizei e irei realizar.

Muito obrigado a todos!

RESUMO

Proposta de uma VPN para Interligação de Redes de Comunicação Baseada em Links ADSL

Com o explosivo crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação, associado a um grande aumento nas velocidades de acesso, esta passou a ser vista como um meio conveniente para a interligação de redes diferentes e geograficamente distantes.

Foi diante dessa realidade e da necessidade de uma solução com custos acessíveis que surgiu a idéia do projeto em questão, que trás uma solução interligação de redes remotas através de uma VPN sobre conexões de internet ADSL com IP dinâmico e válido, e com custos relativamente baixos para que estas empresas possam ter acesso a esta tecnologia.

Palavras-Chave: Rede de Computadores, *Virtual Private Network* (VPN), Segurança.

ABSTRACT

Proposal of a VPN for Interconnection of Nets of Communication Based on Links ADSL

With the explosive growth of the InterNet, the constant increase of its area of abrangência, and the expectation of a fast improvement in the quality of the medias, associate to a great increase in the access speeds, this passed to be seen as a convenient way for the interconnection of different and geographically distant nets.

It was ahead of this reality and the necessity of a solution with accessible costs that the idea appeared of the project in question, that backwards a solution interconnection of remote nets through a VPN on connections of InterNet ADSL with dynamic and valid IP, and with relatively low costs so that these companies can have access to this technology.

Keywords*: Computer Networks, Spanning Tree Protocol* (VPN)*,Security.*

SUMÁRIO

Página

LISTA DE FIGURAS

1 INTRODUÇÃO

Nos últimos anos, com a grande necessidade de compartilhamento de recursos (Internet, impressoras, sistemas), as Empresas e Instituições de todos os portes necessitam se conectar em rede local de computadores. Porém, na atualidade, ocorre uma grande necessidade de redes locais diferentes e distantes uma das outras, serem conectadas para que uma possa usufruir os recursos da outra e vice-versa.

Com o explosivo crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação, associado a um grande aumento nas velocidades de acesso, a Internet passou a ser vista como um meio conveniente para a interligação de redes diferentes.

No entanto, a passagem de dados pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio inseguro em um meio confiável. Com essa abordagem, o uso de VPNs (*Virtual Private Network*) sobre a Internet se torna viável e adequada.

A necessidade de se implantar um mecanismo de segurança eficiente em redes públicas é de extrema importância. Pois, para podermos trafegar dados numa rede pública, onde as informações estão desprotegidas, e estas podendo ser capturadas por pessoas não autorizadas, é extremamente importante a implementação de segurança através de um VPN. E como temos que transportar informações importantes e confidenciais sobre essa tecnologia, essa implementação se torna essencial.

As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou de outras redes públicas ou privadas para transferência de informações, de modo seguro, entre redes diferentes (que podem ser ou não geograficamente distantes) ou usuários remotos.

Este projeto consistirá na Interligação de duas redes remotas através de uma VPN baseada em conexões de internet ADSL com IP dinâmico e válido, tudo isso com o intuito de se obter uma solução de interligação de filiais para pequenas e médias empresas.

O Capítulo 2 faz uma abordagem dos conceitos básicos sobre redes de computadores e suas classificações.

O Capítulo 3 mostra as características da pilha de protocolos TCP/IP, bem como o endereçamento IP, máscara de sub-rede e encapsulamento de pacotes.

No Capítulo 4 é feita uma abordagem sobre segurança em redes. Neste capítulo serão mostrados aspectos de segurança, técnicas de ataque e métodos de defesa (firewall e criptografia).

O Capítulo 5 aborda os conceitos de Rede Privada Virtual (VPN) como os requisitos básicos para sua implantação, seus protocolos, tunelamentos e IPSec.

No Capítulo 6, será mostrada a metodologia para o desenvolvimento do projeto, como variáveis que devem ser analisadas e padrões que devem ser seguidos num projeto de VPN.

Finalmente, no Capítulo 7 os resultados do projeto em questão serão expostos e discutidos.

1.1 Objetivos

Este projeto tem como principal objetivo desenvolver um Estudo de Viabilidade de Utilização de VPN para a Interligação de Redes de Comunicação de Dados Baseadas em Links ADSL, definindo de parâmetros para dimensionamento de equipamentos e serviços de uma VPN, oferecendo solução de interligação de duas redes remotas, com a segurança implementada através de um Rede Privada Virtual (VPN) baseada em conexões ADSL, com o objetivo de se obter uma solução de interligação de filiais para pequenas e médias empresas.

2 REDES DE COMPUTADORES

Segundo Soares (1995), uma rede de computadores é formada por um conjunto de módulos processadores capazes de trocar informações e compartilhar recursos interligados por um sistema de comunicação.

Soares (1995) ainda explica que o sistema de comunicação vai se constituir de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

De acordo com Tanenbaum (1997), existem dois tipos de tecnologia de transmissão: as de redes de difusão e as redes ponto a ponto.As redes de **difusão** (*broadcasting*) têm apenas um canal de comunicação, compartilhado por todas as máquinas. As mensagens curtas, que em determinados contextos são chamadas de pacotes, enviadas por uma das máquinas são recebidas por todas as outras. Um campo de endereço dentro do pacote especifíca seu destinatário. Quando recebe um pacote, uma máquina analisa o campo de endereço. Se o pacote tiver sido endereçado à própria máquina, ela o processará; se for destinado a outra máquina, o pacote será ignorado.

As redes **ponto a ponto** consistem em muitas conexões entre pares individuais de máquinas. Para ir da origem ao destino, talvez um pacote desse tipo de rede tenha de visitar uma ou mais máquinas intermediárias. Como em geral é possível ter diferentes rotas com diferentes tamanhos, os algoritmos de roteamento desempenham um importante papel nas redes ponto a ponto. Embora haja algumas exceções, geralmente as redes menores tendem a usar os sistemas de difusão e as maiores, o sistema ponto a ponto.

2.1 Redes Locais

Jack (2003), de uma forma geral, define uma Rede Local ou LAN(*Local Area Network*) como sendo qualquer rede que conecta dois ou mais computadores ou dispositivos relacionados, localizados dentro de uma área geograficamente limitada (até poucos quilômetros).

De acordo com Tanenbaum (1997), as LANs têm um tamanho restrito, o que significa que o pior tempo de transmissão é limitado e conhecido com devida antecedência.

O conhecimento desse limite permite a utilização de determinados tipos de projetos que em outras circunstâncias seriam inviáveis, além de simplificar o gerenciamento da rede.

Segundo Jack (2003) as rede locais surgiram nos ambientes de institutos de pesquisa e universidades. O enfoque dos sistemas de computação que perduravam durante a década de 70, levava em direção à distribuição do poder computacional. Redes Locais surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região que possui distâncias entre 100m e 25km, embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias. Outras características típicas encontradas e comumente associadas às redes locais são as altas taxas de transmissão, de 0,1 à 100Mbps, e baixas taxas de erro, 1 bit em cada 10^8 a 10^{11} bits transmitidos (JACK, 2003).

2.2 Redes de Campus

Segundo Jack (2003), a definição de Rede de Campus nunca foi clara, mas uma bastante comum é a de um grupo de segmentos LAN localizados em um prédio ou grupo de prédios que estão interconectados de modo a formar uma rede. Estes segmentos LAN, tipicamente utilizam tecnologia Ethernet, Token Ring, FDDI ou ATM. O tamanho de uma Rede de Campus não é definido, mas ela começa a tomar forma à medida que sai de um edifício e se difunde por um perímetro que engloba diversos outros edifícios, como é o caso de um campus universitário.

Em 1990 as Redes de Campus Tradicionais surgiram como uma LAN que progrediu e cresceu de modo que foi necessária a sua segmentação apenas para mantê-la ativa e operando. Nesta época de rápida expansão, o tempo de resposta era uma preocupação secundária e era desejável apenas a garantia de que a rede estivesse funcionando (JACK, 2003).

Ainda segundo Jack (2003), o principal desafio do administrador de rede é fazer uma rede de campus funcionar eficientemente e efetivamente. Para alcançar este objetivo, é necessário conhecer a rede de campus tradicional, procurando entender as suas limitações, bem como aproveitar os benefícios das redes de campus emergentes.

2.3 Redes Geograficamente Distribuídas

Segundo Tanenbaum (1997), uma **rede geograficamente distribuída**, ou WAN (*Wide Area Network*), abrange uma ampla área geográfica, com freqüência um país ou continente. Ela contém um conjunto de máquinas (***hosts***) cuja a finalidade é executar as aplicações do usuário. Os *hosts* são conectados por uma sub-rede que tem a função de transportar mensagens de um *host* para o outro.

Na maioria das redes geograficamente distribuídas, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão (também chamadas de **circuitos**, **canais** ou **troncos**) transportam os bits entre as máquinas (TANENBAUM, 1997).

O mesmo autor afirma que os elementos de comutação são computadores, especializados, usados para conectar duas ou mais linhas de transmissão. Vamos chamar esses computadores de comutação de roteadores. A figura 2.1 mostra o esquema de uma Rede Geograficamente Distribuída.

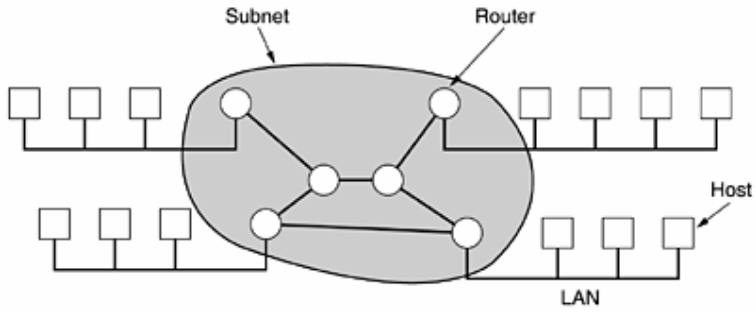

Figura 2.1: Rede Geograficamente Distribuída

2.4 Redes sem Fio

Redes sem fio, ou redes *wireless,* podem ser definidas como redes que utilizam o ar como meio de transmissão de dados, voz e vídeo.

A comunicação sem fio é atualmente uma das áreas mais ativas de desenvolvimento da tecnologia. Este desenvolvimento está sendo dirigido primeiramente pela transformação de um meio muito utilizado para a telefonia, suportando voz, em um meio para suportar outros serviços, tais como a transmissão do vídeo, imagens, texto, e dados.

Nos últimos cinco anos, o mundo vem se tornando cada vez mais móvel, com a telefonia celular e as redes de dados sem fios cada vez mais comuns. Em conseqüência, tipos tradicionais de rede de computadores têm se mostrado inadequado devido aos desafios proposto por nosso novo estilo de vida coletivo. Se usuários estão conectados a uma rede por meio de cabos físicos, seus movimentos serão muito reduzidos. As redes sem fio, entretanto, permite uma maior mobilidade do usuário e uma maior flexibilidade numa rede (Gast, 2002).

2.5 Protocolos

Segundo Torres (2001), **protocolo** é uma "linguagem" usada pelos dispositivos de uma rede de modo que eles consigam se entender, isto é, trocar dados e informações entre si. Para que todos os dispositivos de uma rede consigam conversar entre si, todos eles deverão estar usando uma mesma linguagem, isto é, um mesmo protocolo.

Um **protocolo** define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento (Kurose & Ross, 2003).

Kurose & Ross (2003) destaca que a Internet e as redes de computadores em geral utilizam amplamente os protocolos. Protocolos diferentes são usados para realizar diferentes tarefas de comunicação.

2.6 Padrão ADSL

O termo ADSL (*Asymmetric Digital Subscriber Line*) foi concebido em 1989 e não se refere a uma linha, mas a modems que convertem o sinal padrão do fio de telefone par-

trançado em um duto digital de alta velocidade. Os modems são chamados "assimétricos" porque eles transmitem dados da sua casa do cliente em uma velocidade menor do que recebe.

O sistema ADSL atinge velocidades altíssimas quando comparado a os sistemas de transmissão de dados atuais, permite transmissões de mais de 6Mbps (chegando ao máximo, hoje, a 9Mbps) de download, e chegando à 640kbps (máximo de 1 Mbps) para upload. Este padrão pode transformar a cadeia de informação pública já existente que é limitada a voz, texto e gráficos de baixa resolução para um sistema poderoso, onipresente capaz de trazer multimídia, incluindo, por exemplo, video-conferência, para a casa de todos.

Um novo cabeamento levaria décadas para atingir todos os assinantes, mas o sucesso destes serviços novos dependerá do alcance de todos os assinantes quanto possível durante os primeiros anos de sua implementação sem a troca do cabeamento já existente.

O padrão ADSL funciona com um modem colocado na sua casa enquanto um outro modem colocado na central telefônica. Estes dois modems estão permanentemente conectados. O modem divide digitalmente a linha telefônica em 3 canais separados. O primeiro canal é utilizado para transmissão de voz. O segundo canal é utilizado para o fluxo de informações no sentido usuário => rede (upstream) e o terceiro canal para o fluxo de dados no sentido rede => usuário (downstream). Esta técnica permite maiores velocidades porque raramente as pessoas fazem o mesmo número de uploads e downloads. Isto significa que o canal de downstrean pode ser mais largo sem afetar a velocidade de transmissão de dados.

2.7 Protocolo PPPoE

Diante das informações da seção anterior, surge a dúvida de porque em muitos casos é necessário usar um programa para se conectar à internet, se o ADSL permite uma conexão permanente usando unicamente o modem.

O ADSL por si só é um meio físico de conexão, que trabalha com os sinais elétricos que serão enviados e recebidos. Funcionando dessa forma, é necessário um protocolo para encapsular os dados de seu computador até a central telefônica. O protocolo mais utilizado para essa finalidade é o PPPoE (*Point-to-Point over Ethernet*).

O protocolo PPPoE trabalha com a tecnologia Ethernet, que é usada para ligar sua placa de rede ao modem, permitindo a autenticação para a conexão e aquisição de um endereço IP à máquina do usuário. É por isso que cada vez mais as empresas que oferecem ADSL usam programas ou o navegador de internet do usuário para que este se autentique. Com a autenticação, a identificação dos usuários conectados e o controle de suas ações pode ser feita com uma maior facilidade.

Os primeiros serviços de ADSL do país forneciam aos seus clientes um IP fixo e válido ao usuário, sem necessidade de usar o PPPoE, pois, na época, o protocolo PPPoE era novo (foi homologado em 1999) e ,conseqüentemente, pouco conhecido. Com isso, o usuário usava ADSL através de uma conexão direta do modem à central telefônica, sem necessidade de autenticar. Quando as empresas começaram a descobrir as vantagens do PPPoE, passaram a implantá-lo, pois este protocolo permitia à companhia ter mais controle sobre as ações do usuário.

O padrão ADSL brasileiro ainda inclui uma autenticação adicional, mesmo após a autenticação PPPoE, para liberar a conexão à internet. E esta autenticação é realizada por um provedor de acesso (UOL, Terra, UAI, etc.), onde do qual se contrata um serviço adicional, apenas para ser liberado o caminho entre o cliente e a internet.

3 TCP/IP

O conjunto de protocolos TCP/IP permite que computadores de todos os tamanhos, de diferentes fabricantes, rodando sistemas operacionais totalmente diferentes, possam se comunicar entre si. Iniciou-se na década de 60 como um projeto de pesquisa financiado pelo governo para redes de comutação, foi na década de 90 transformado no protocolo de redes mais utilizado na comunicação de computadores. O protocolo TCP/IP é essencialmente um sistema aberto na sua definição de conjunto de protocolos e muitas das suas implementações estão publicamente disponíveis (Stevens, 1993).

Protocolos de redes são normalmente desenvolvidos em camadas, onde cada camada é responsável por funções diferentes na comunicação. Uma suíte de protocolos ou um conjunto de protocolos, como o TCP/IP, é uma combinação de protocolos diferentes em cada camada, TCP/IP é normalmente considerado como um sistema de quatro camadas definidos como na Figura 3.1 a seguir:

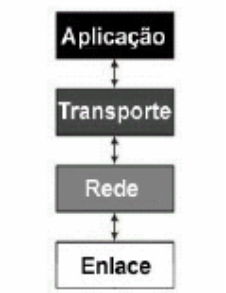

Figura 3.1: As camadas do conjunto de protocolos TCP/IP

Cada camada possui uma responsabilidade diferente (Stevens, 1993):

1. A camada de **Enlace**, às vezes chamada de Link de Dados (*Data Link*) ou simplesmente link, normalmente inclui o *driver* de dispositivo no sistema operacional e a sua interface de rede correspondente no computador. Juntos eles tratam todos os detalhes de hardware e a comunicação física com a mídia de transmissão utilizada;

2. A camada de **Rede** (às vezes chamada de camada Internet ou inter-rede) trata do movimento dos pacotes (ou datagramas) na rede. O roteamento de pacotes ocorre nesta camada. IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), e IGMP (*Internet Group Management Protocol*) fazem parte da camada de rede no suíte de protocolos TCP/IP;

3. A camada de **Transporte** determina o fluxo de dados entre os hosts, para a camada de aplicação localizada acima. Na suíte de protocolos TCP/IP existe dois protocolos de transporte diferentes: TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*).
    - **TCP** cuida do fluxo de dados confiável entre dois *hosts*. Ele se preocupa com tarefas do tipo: repartir dados que passam por ele vindos da camada de aplicação em pedaços de tamanho apropriado para a camada de rede, reconhecer pacotes recebidos ajustando *timeouts* para garantir o reconhecimento de pacotes que enviou, etc. Devido a este fluxo de dados confiável proporcionado pela camada de tranporte, a camada de aplicação pode ignorar estes detalhes.
    - **UDP**, por outro lado, fornece um serviço mais simples para a camada de aplicação. Ele apenas envia dados de um host para o outro, mas não garante que estes pacotes alcançarão o seu destino. Qualquer recurso de confiabilidade que seja desejado, precisa ser adicionado à camada de aplicação.

4. A camada de **Aplicação** cuida dos detalhes de uma aplicação em particular. Existem várias aplicações TCP/IP, algumas delas estão listadas abaixo:
    - Telnet, para conexão remota;
    - FTP (*File Transfer Protocol*), protocolo de transferência de arquivos;
    - SMTP (*Simple Mail Transfer Protocol*), para correio eletrônico;
    - SNMP (*Simple Network Management Protocol*)

Cada camada possui um ou mais protocolos para comunicação com seu par, localizados na mesma camada no *host* origem e no *host* destino. Um protocolo, por exemplo, permite que duas camadas TCP possam se comunicar, e outro protocolo permite que duas camadas IP possam se comunicar. Normalmente a camada de Aplicação é um processo do usuário enquanto as outras três camadas são usualmente implementadas no *kernel* (o sistema operacional). Outra diferença entre a camada de Aplicação e as outras três camadas, é que esta se preocupa com os detalhes da aplicação e não com o movimento dos dados através da rede. As outras três camadas não sabem nada a respeito da aplicação, mas cuidam de todos os detalhes da comunicação.

A figura 3.2 mostra um exemplo de quatro protocolos diferentes, cada um em sua camada específica. FTP é um protocolo da camada de Aplicação, TCP é um protocolo da camada de Transporte, IP é um protocolo da cada de Rede e o protocolo Ethernet opera na cama de Enlace (Stevens, 1993).

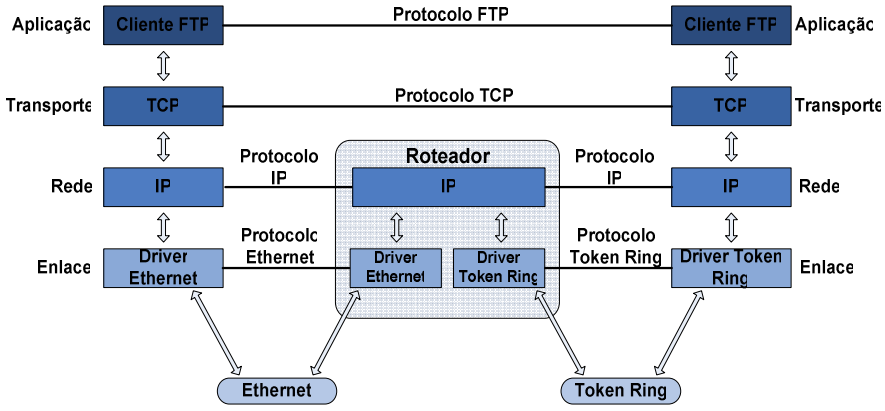

Figura 3.2: Protocolos em suas camadas

3.1 Endereçamento IP

Cada interface na Internet precisa ter um endereço único chamado endereço IP. Estes endereços são números de 32-bits. Em vez de utilizar endereços planos, o endereço IP utiliza o sistema hierárquico de endereços. A figura abaixo mostra cinco classes diferentes de endereços IP:

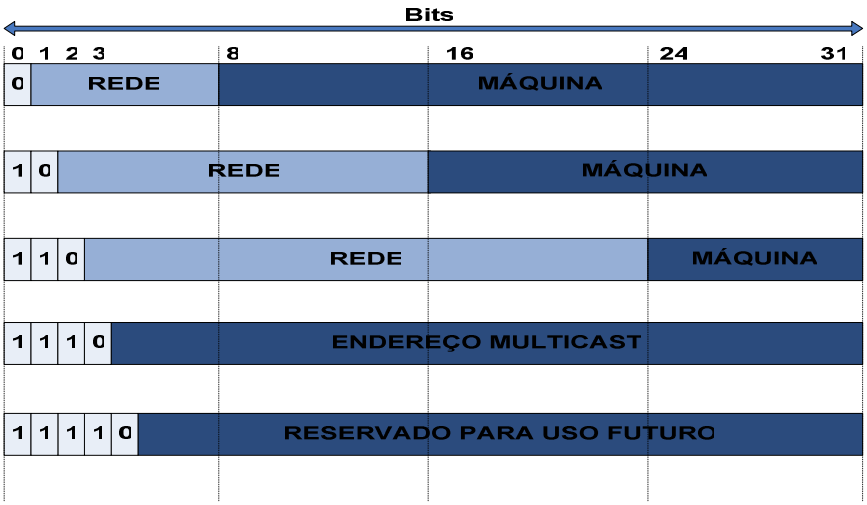

Figura 3.3: As cinco classes de endereçamento IP

Estes endereços de 32-bits são normalmente escritos em quatro números decimais, uma para cada byte do endereço. Para sabermos em que classe um endereço IP está localizado, devemos olhar o primeiro campo do endereço. A figura 3.4 abaixo mostra as diferentes classes, com o primeiro número em negrito.

Classe	Limite
A	**0**.0.0.0 à **127**.255.255.255
B	**128**.0.0.0 à **191**.255.255.255
C	**192**.0.0.0 à **223**.255.255.255
D	**224**.0.0.0 à **239**.255.255.255
E	**240**.0.0.0 à **247**.255.255.255

Figura 3.4: Faixa, por classe, de endereços IP

3.1.1 Máscara de sub-rede

Em adição para o endereços IP, um *host* também necessita conhecer quantos bits estão sendo utilizados para o ID da sub-rede e quantos bits são destinados à ID do host. Esta máscara possui uma faixa de 32-bits contendo bits 1 para o ID da rede e da sub-rede, e bits 0 para o ID do *host*.

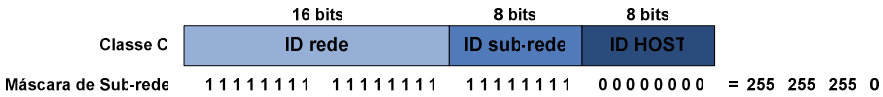

Figura 3.5: Exemplo de máscara de sub-rede classe C

Embora estes endereços IP sejam normalmente escritos em notação ponto-decimal, as máscara de sub-rede são freqüentemente escritas em hexadecimal, especialmente se seus limites não são limites de byte, e por esta razão a máscara de sub-rede é uma máscara bit.

3.1.2 Encapsulamento

Quando uma aplicação transmite um conjunto de dados usando a pilha de protocolos TCP/IP, o mesmo é enviado de cima para baixo na pilha de protocolos, passando por cada uma das camadas, antes de enviar um fluxo de bits através da rede. Cada camada acrescenta no começo dos dados que recebeu, um cabeçalho (às vezes também adiciona informações no final). A figura 3.6 mostra esse processo.

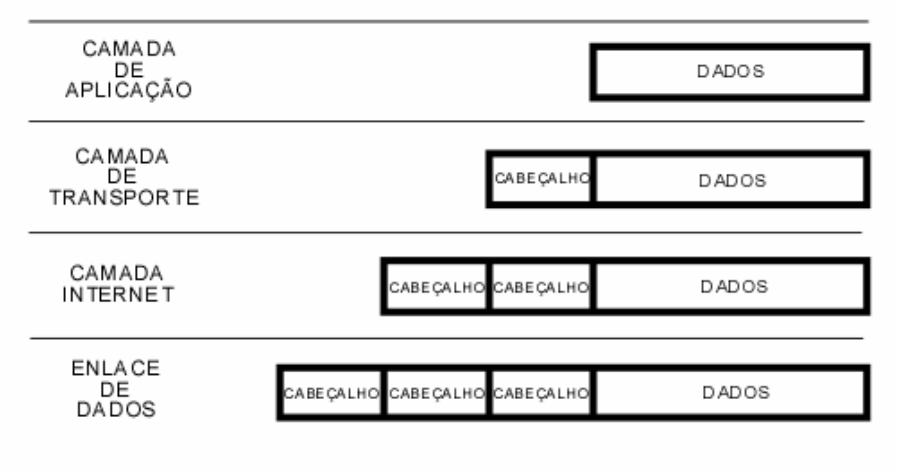

Figura 3.6: Encapsulamento de Dados

A unidade de dados que o protocolo TCP envia para o protocolo IP é chamado de segmento **TCP**. A unidade de dados que o protocolo IP envia para a interface de rede é chamado **datagrama IP**. O fluxo de bits que passa pela mídia de comunicação é chamado de **quadro** (Stevens, 1993).

3.2 Modelo de Referência OSI

Segundo Torres (2001), quando as redes de computadores surgiram, as soluções eram, na maioria da vezes, proprietárias, isto é, uma determinada tecnologia só era suportada por seu fabricante. Não havia a possibilidade de se misturar soluções de fabricantes diferentes. Dessa forma um mesmo fabricante era responsável por construir praticamente tudo na rede.

Para facilitar a interconexão de sistemas de computadores, a ISO (*International Standarts Organization*) desenvolveu um modelo de referência chamado OSI (*Open System Inter-connection*), para que os fabricantes pudessem criar protocolos a partir desse modelo. O modelo de protocolos OSI é um modelo de sete camadas, que é apresentado na Figura 3.7.

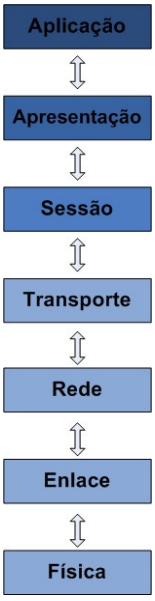

Figura 3.7: Modelo de Referência OSI

Na transmissão de um dado, cada camada pega as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada inferior. Esse processo é conhecido como encapsulamento.

3.2.1 Aplicação

A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá a informação através de rede. Por exemplo, se você quiser baixar o seu e-mail com seu aplicativo de e-mail, ele entrará em contato com a camada de aplicação do protocolo de rede efetuando este pedido.

3.2.2 Apresentação

A camada de Apresentação, também chamada de Tradução converte o formato de dado recebido pela camada de aplicação em um formato comum a ser usado na transmissão desse dados, ou seja, um formato entendido pelo protocolo usado. U exemplo comum é a conversão do padrão de caracteres quando, por exemplo, o dispositivo transmissor usa um padrão diferente do ASCII, por exemplo. Pode ter outros usos, como compressão de dados e criptografia.

3.2.3 Sessão

A camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação. Nesta sessão, essas aplicações definem como será feita a transmissão de dados e coloca marcações nos dados que estão sendo transmitidos. Se porventura a rede falhar, os computadores reiniciam a transmissão dos dados a partir da última marcação recebida pelo computador receptor.

3.2.4 Transporte

A camada de Transporte é responsável por pegar os dados enviados pela camada de Sessão e dividi-los em pacotes que serão transmitidos peã rede, ou, melhor dizendo, repassados para a camada de Rede.No receptor, a camada de Transporte [e responsável por pegar os pacotes recebidos da camada de Rede e remontar o dado original para envia-lo à camada de Sessão. Isso inclui controle de fluxo (colocar os pacotes recebidos em ordem, caso eles tenham chegado fora de ordem) e correção de erros, tipicamente enviando para o transmissor um informação de reconhecimento, informando que o pacote foi recebido com sucesso.

3.2.5 Rede

A camada de Rede é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, 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 de rede e prioridades.

3.2.6 Enlace

A camada de Enlace, ou Link de Dados, pega os pacotes de dados recebidos da camada de Rede e os transforma em quadros que serão trafegados pela rede, adicionando informações como o endereço da placa de rede de origem, o endereço da placa de rede de destino, dados de controle, os dados em si e o CRC.

3.2.7 Física

A camada física pega os quadros enviados pela camada de Link de Dados e os transforma em sinais compatíveis com o meio onde os dados deverão ser transmitidos. Se o meio for elétrico, essa camada converte os 0s e 1s dos quadros em sinais elétricos a serem transmitido pelo cabo. Se o meio for óptico, essa camada converte os 0s e 1s dos quadros em sinais luminosos e assim por diante, dependendo do meio de transmissão de dados.

4 SEGURANÇA EM REDES

Segundo Puttini (2000) inicialmente as redes foram projetadas com finalidade de pesquisa e o objetivo principal era permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo. Portanto, a interoperabilidade e não a segurança, foi enfatizada. Agora, com o crescimento da demanda comercial cada vez mais acentuado, a segurança passou a ser uma necessidade fundamental consistindo foco de discussão das pessoas envolvidas com a tecnologia de redes.

O alicerce da construção de um ambiente seguro consiste em saber o que precisa realmente ser protegido. Cada organização precisa proteger algo diferente, recursos ou informações, normalmente com graus de proteção diferenciados. Muitas vezes, uma informação é sigilosa para uma organização e para outra não (Puttini, 2000).

A finalidade de toda análise de segurança consiste em fundamentar a especificação de como os níveis de segurança desejados devem ser atingidos. Assim, depois de conhecer a ameaça, devem-se projetar mecanismos para prevenir, detectar ou recuperar-se de um ataque. Nesse sentido, são desenvolvidas diversas ferramentas para avaliação das vulnerabilidades das redes, bem como para sua proteção, onde se destacam técnicas de criptografia e softwares *firewalls* e *proxies*. Essas ferramentas possibilitam, além da proteção preventiva do sistema, a realização de auditorias que permitam identificar a ocorrência de ataques e rastrear a origem destes (Puttini, 2000).

4.1 Aspectos de Segurança

Segundo Monteiro (2002), a segurança em redes deve ser entendida segundo vários aspectos, dentre eles:

- **Autenticidade** – verifica se a pessoa com quem está se trocando informações sigilosas é realmente quem deveria ser;
- **Confidencialidade** – Limita o acesso a informações, geralmente através do uso de criptografia e controles de acesso (login e senha);
- **Integridade** – Assegura que os dados não serão alterados durante um transmissão;

- **Disponibilidade** – Mantém os recursos disponíveis, mesmo em caso de falhas, garante rápido restabelecimento dos mesmos;
- **Não repúdio** – Impede que uma entidade (computador, pessoa, etc.) envolvida em uma transação negue a sua participação no evento.

4.2 Técnicas de Ataque

4.2.1 *Denial of Service*

Segundo Strauch (1999), os ataques do tipo *denial of service* consistem em impedir o funcionamento de uma máquina ou de um serviço especifico. Quando ocorrem ataques a redes, geralmente seus usuários legítimos não conseguem mais acessá-las.

Denial of service não é um ataque propriamente dito, é um tipo de ataque, o qual inclui ataques como sobrecarga da rede, excessivos pedidos de abertura de conexão, etc. A Figura 4.1 faz uma ilustração deste ataque.

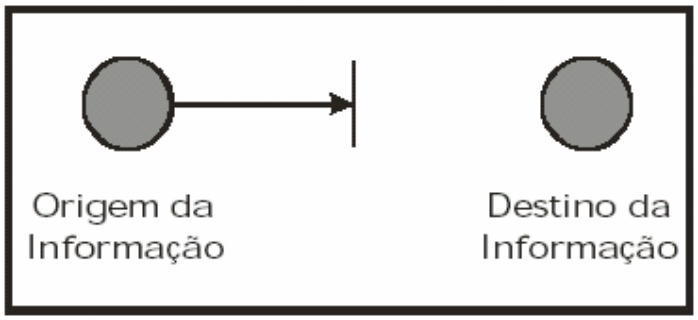

Figura 4.1: Ataque *Denial of service*

4.2.2 *Man in the middle*

De acordo com Vasquez & Schuber (2002), esse tipo de ataque tem como objetivo capturar o que está sendo transmitido sem que o sistema perceba, ou seja, ataca-se a confidencialidade das informações. No *man-in-the-middle* o invasor simula ser o parceiro de ambas as partes envolvidas na conexão assumindo a identidade de um usuário válido. A Figura 4.2 faz uma ilustração deste ataque.

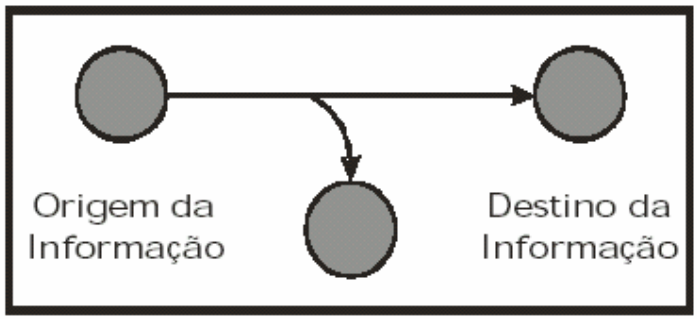

Figura 4.2: Ataque *man-in-the-middle*

4.2.3 *Replay*

Em algumas circunstâncias, o atacante pode pegar uma informação no caminho e enviar esta informação novamente de forma modificada, esse tipo de ataque é chamado de *replay* (Chandra et al, 2002).

Segundo Zwicky et al , (2000), existem dois tipos de *replay,* um que o atacante está habilitado a certas partes da informação e a outro onde o atacante apenas reenvia a informação inteira. A figura 4.3 ilustra esse tipo de ataque.

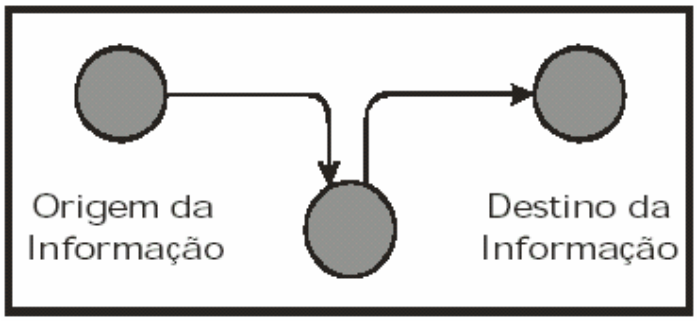

Figura 4.3: Ataque *replay*

4.2.4 *IP Spoofing*

Este ataque consiste em "mentir" o número IP da máquina, gerlamente trocando-o por um número IP qualquer, isto pode ser feito através de manipulação direta dos campos do cabeçalho. Quando um host A quer se conectar ao B, identificação é feita através do número IP que vai no cabeçalho, por isto, se o IP do cabeçalho enviado pelo host A for

falso (IP de um host C), o host B, por falta de outra forma de identificação acredita estar se comunicando com o host C (Strauch, 1999).

O *IP Spoofing* não é exatamente um forma de ataque, mas sim um técnica que é utilizada na grande maioria dos ataques, pois ele ajuda a esconder a identidade do atacante.

De acordo com Strauch (1999), através da técnica de IP falso, um atacante consegue atingir os seguintes objetivos: obtém acesso a máquinas que confiam no IP que foi falsificado, capturar conexões já existentes e burlar os filtros de pacotes dos *firewalls* que bloqueiam o tráfego baseado nos endereços de origem e destino. A figura 4.4 nos mostrará o funcionamento desse tipo de ataque.

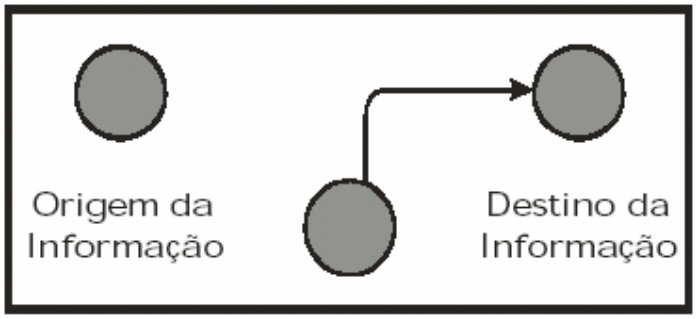

Figura 4.4: *IP Spoofing*

4.3 Firewall

Segundo Torres (2001), nos dias atuais praticamente todas as estruturas de segurança de redes dependem do conceito de *firewall.* A idéia original do *firewall* era isolar a sua rede interna da Internet, por completo. Como a Internet é uma rede que respira TCP/IP, não existe melhor forma de fazer isso do que "*escutar*" todo o tráfego TCP/IP endereçado para a sua rede interna, proviniente da Internet, e todo o tráfego para a Internet, proveniente da sua rede interna.

O objetivo dos firewalls é o de filtrar o que era permitido do que não era. Como regra geral, praticamente tudo era proibido, aos poucos, eram criadas regras permitindo a passagem do tráfego essencial.

Um *firewall* funciona analisando os cabeçalhos dos pacotes IP que passam através dele, com origem ou destino a uma das redes à qual ele quer proteger, supõe-se que as redes de origem e destino são diferentes.

Ao analisar o cabeçalho dos pacotes, o *firewall* consegue saber os protocolos usados e as portas de origem e destino do pacote. O *firewall* pode ainda analisar os endereços IP de origem e destino. Depois disso, ele faz uma comparação em um tabela de regras, analisando se o pacote pode prosseguir ou não. Se o pacote estiver permitido o *firewall* passa a agir como um roteador normal. Se este pacote não se enquadrar em nenhuma das regras , o *firewall* pode tomas duas decisões: recusar o recebimento do pacote (*deny*) ou descartá-lo (*drop*).

Quando um pacote é recusado, existe uma comunicação entre o *firewall* e o remetente do pacote, informando que a conexão foi cortada. No caso de um pacote descartado, essa comunicação não existe e o *firewall* simplesmente ignora qualquer comunicação vinda do remetente do pacote, fazendo parecer que o pacote simplesmente se perdeu (Torres, 2001).

De acordo com Scoot et al. (1999), os *firewalls* geralmente possuem duas funções principais para um administrador de rede. A primeira é controlar quais máquinas podem ver os serviços e com quais serviços essas máquinas podem conversar. A segunda controla quais máquinas na Internet um usuário interno pode ver, e quais serviços ele pode usar.

4.4 Criptografia

Segundo Scheneier (1996), a palavras criptografia vem do grego (Kryptos =escondido, oculto e Grafia = Escrita) e pode ser definida como a arte ou ciência de garantir a segurança de mensagens, de forma que apenas pessoas autorizadas a leiam. Ela garante confidencialidade, autenticidade, integridade e não-repúdio.

O processo de criptografia pode ser descrito da seguinte forma: um emissor gera a mensagem original chamada de texto plano e utilizando uma chave e um algoritmo de cifragem gera um texto cifrado, ou seja, incompreensível para quem não tem autorização de lê-lo. Ao chegar ao receptor, este texto passa pelo processo inverso, chamado decifragem, resultando no texto plano original, observado na figura 4.5.

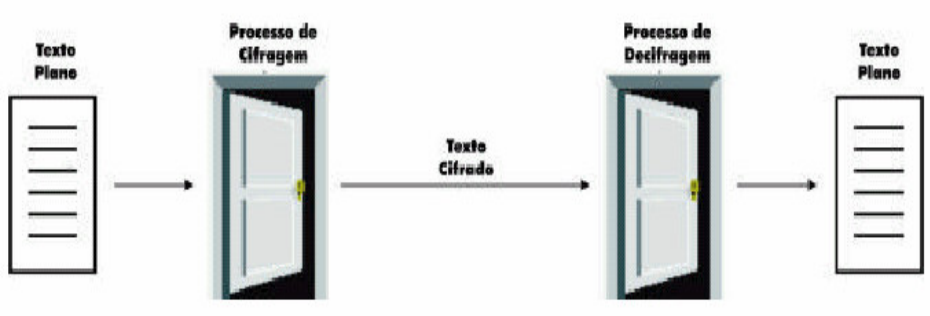

Figura 4.5: Processo de Cifragem e Decifragem

Uma chave é um combinação de bits, e quanto maior for esta combinação, maior será a segurança obtida. Dependendo do tipo de chave utilizada, a criptografia classifica-se em: Criptografia Simétrica e Criptografia Assimétrica (Vasques & Schuber, 2002).

4.4.1 Criptografia Simétrica

Segundo Chandra et al. (2002), os algoritmos chaves simétricas cifram e decifram dados usando uma única chave. Como mostrado na Figura 2.13, a chave e a mensagem do texto plano são passadas ao algoritmo de criptografia, produzindo a mensagem cifrada. O resultado pode ser emitido através de um meio seguro, permitindo somente um receptor que tenha a chave original para decifrar a mensagem que é feita passando a mensagem cifrada e a chave a um algoritmo do criptografia. Obviamente, a chave deve permanecer secreta para que este esquema seja eficaz.

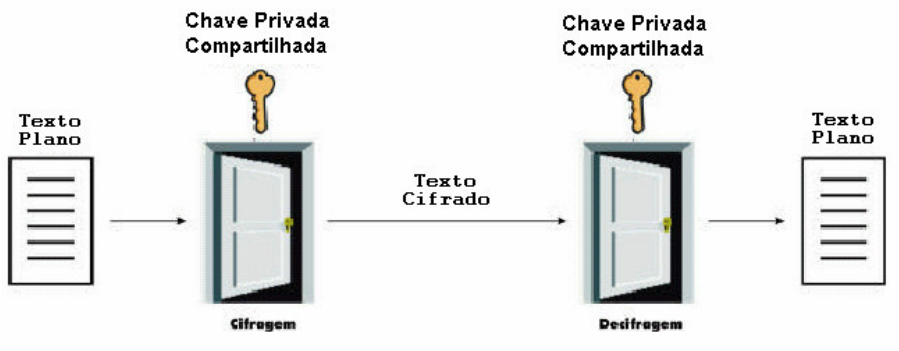

Figura 4.6: Processo de Criptografia Simétrica

A desvantagem preliminar da criptografia simétrica é que a chave deve remanescer secreta em todas as vezes. Em particular, trocar chaves secretas pode ser difícil, desde que você irá querer geralmente trocar chaves no mesmo meio esse que você irá usar a criptografia para proteger os dados. Enviar a chave antes que você o use a criptografia gera a possibilidade de um atacante gravar a chave antes que você comece mesmo a emitir dados (Chandra et al, 2002).

O triplo DES (geralmente escrito 3DES, ou algumas vezes DES3) é o algoritmo simétrico mais utilizado dentre vários como, *Data Encryption Standart* (DES – 56 bits), *Triple Data Encryption Standart* (3DES – 112 bits), *Advanced Encryption Standart* (AES – 128, 192 ou 256 bits), etc.

4.4.2 Criptografia Assimétrica

De acordo com Chandra et al, (2002), a criptografia Assimétrica ou criptografia de chave pública sugere uma solução ao problema da distribuição de chaves da criptografia simétrica. Na forma mais popular da criptografia assimétrica , cada parte tem duas chaves, uma que deve permanecer segredo (chave privada) e uma que pode livremente ser distribuída (chave pública). As duas chaves (pública e privada) têm um relacionamento matemático especial. A Figura 4.7 mostra o processo de criptografia assimétrica.

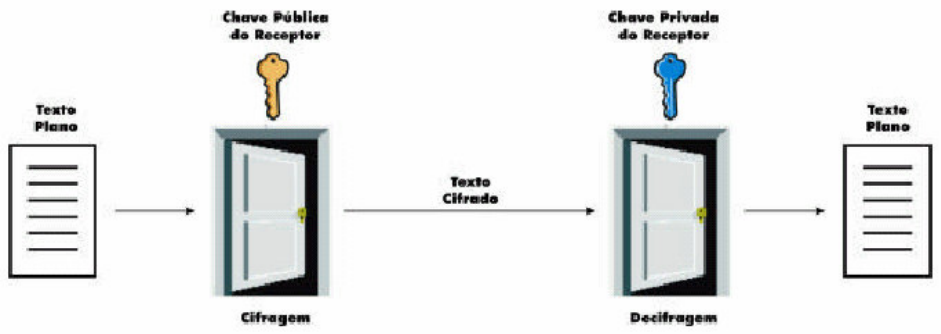

Figura 4.7: Processo de criptografia assimétrica

Por exemplo, para que uma pessoa chamada Alice envie uma mensagem para outra pessoa chamada Bob usando a criptografia assimétrica. Alice deve primeiramente ter a chave pública de Bob, então ela cifra a mensagem com a chave pública de Bob e a envia.

Uma vez cifrado, somente alguém que tem a chave privada de Bob pode descriptografar a mensagem (Chandra et al, 2002).

O RSA (*Rivest Shamir Adleman*) é o algoritmo assimétrico mais popular e este algoritmo possui chaves de 512, 768, 1024, 2048 bits

4.4.3 Função Hash

Dada uma mensagem original, a função hash tem como objetivo produzir um número. Conhecido como resumo, que representa de forma única esta mensagem. Um propriedade desta função, diz que o caminho inverso deverá ser computacionalmente inviável, ou seja, não poderá ser possível obter uma mensagem original através de um resumo, o que garante a integridade da mesma (Vasques & Schuber, 2002).

Segundo Chandra et al, (2002), os algoritmos mais utilizados que implementam a função hash são o MD5 (*Message Diggest 5*), onde o tamanho do resumo é de 128 bits, e o SHA-1 (*Secure Hash Algorithm 1*), onde o tamanho do resumo é de 160 bits.

4.4.4 Assinatura Digital

O principal benefício da criptografia assimétrica (a assinatura digital utiliza a chave publica e privada) é que ela fornece um método de assinaturas digitais. As assinaturas digitais permitem que o receptor da informação verifique a autenticidade da origem da informação, e também que a informação esta intacta. Assim, a assinatura digital assimétrica fornece a integridade e a autenticidade dos dados. Uma assinatura digital também fornece o não-repúdio dos dados, o que significa que ela previne que o remetente reivindique que ele realmente não enviou a informação.

Uma assinatura digital serve para mesma finalidade que uma assinatura escrita à mão. Entretanto, uma assinatura escrita a mão é fácil de falsificar. Uma assinatura digital é superior a uma assinatura escrita à mão, pois é quase impossível falsifica-la.

O processo de geração da assinatura utiliza a função hash para a obtenção do resumo do documento, que, em seguida, cifra-o com a chave privada do emissor e envia-o ao receptor. Este utilizará a chave pública do emissor para decifrar a mensagem e a função hash para reclacular o resumo do documento, comparando-o com o resumo recebido, segundo a Figura 4.8 (Vasques & Schuber, 2002).

figura 4.8: Processo de assinatura digital.

4.4.5 Certificado Digital

Um problema com a criptografia assimétrica é que os usuários das chaves públicas devem se assegurar de que estejam cifrando com a chave da pessoa correta. Em um ambiente onde chaves são trocadas livremente através de servidores públicos, os ataques são uma ameaça potencial.

O certificado digital simplifica a tarefa de verificar se uma chave pública pertence verdadeiramente ao proprietário pressuposto.

Um certificado é um formulário de credencial, exemplos podem ser sua carteira de habilitação, seu cartão de seguro social, ou sua certidão de nascimento. Cada um desses tem alguma informação que identifica você e alguma autorização que indica que alguma outra pessoa confirmou sua identidade.

Um certificado digital são dados que funcionam como o certificado físico. Um certificado digital é informação incluída com chave pública de uma pessoa que ajuda outras a verificar se uma chave é válida. Os certificados digitais são usados contra tentativas de substituir uma chave da pessoa para outros.

Um certificado digital consiste em três coisas: uma chave pública, um certificado de informação, e uma ou mais assinaturas digitais.

5 REDE PRIVADA VIRTUAL (VPN)

A idéia de utilizar uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas é denominada de *Virtual Private Network* (VPN) ou Rede Privada Virtual. As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas ou privadas para transferência de informações, de modo seguro, entre redes corporativas e usuários remotos (CHIN, 2004).

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de *links* dedicados de longa distância que podem ser substituídos pela Internet. As LANs podem, através de *links* dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet. Esta solução pode ser bastante interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. Outro fator que simplifica a operacionalização da WAN é que a conexão LAN-Intenet-LAN fica parcialmente a cargo dos provedores de acesso.

5.1 Aplicações para as VPNs

5.1.1 Acesso Remoto via Internet

O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da ligação local a algum provedor de acesso (*Internet Service Provider* - ISP). A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet. A Figura 5.1 ilustra este esquema.

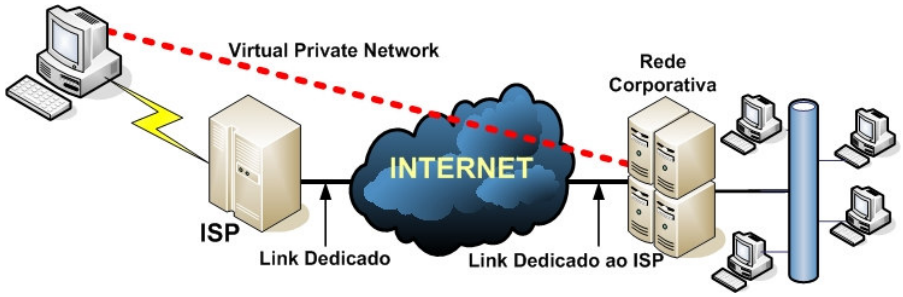

Figura 5.1: Acesso remoto via Internet

5.1.2 Conexão de LAN's via Internet

Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a WAN corporativa.

A depender das aplicações, também se pode optar pela utilização de circuitos discados em uma das pontas, devendo a LAN corporativa estar, preferencialmente, conectada à Internet via circuito dedicado local ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.

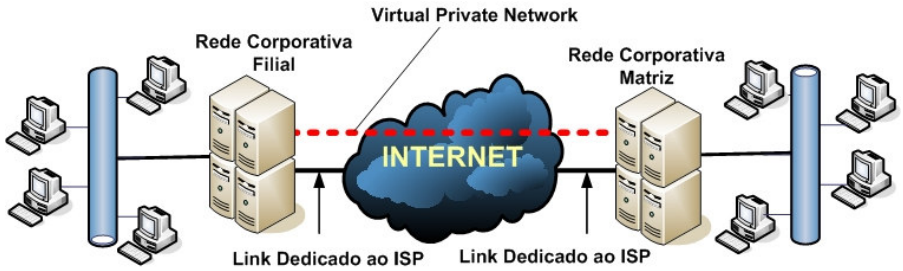

Figura 5.2: Conexões de LAN's via Internet

5.1.3 Conexões de computadores numa Intranet

Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução, apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa, uma vez que o roteador possibilitaria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva. Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada, assegurando a "confidencialidade" das informações. Os demais usuários não credenciados sequer “enxergarão” a rede departamental.

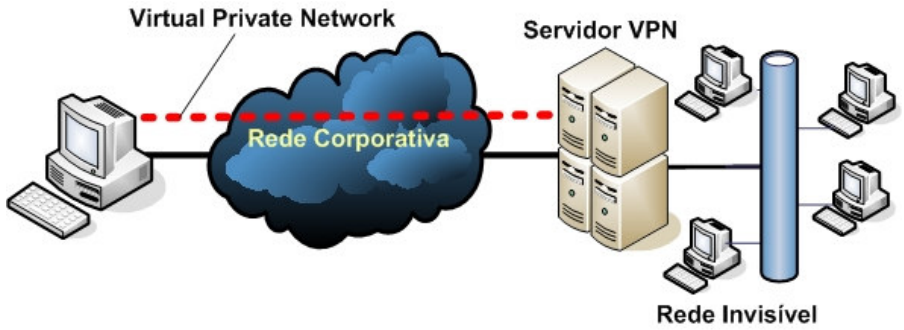

Figura 5.3: Conexão de computadores numa Intranet

5.2 Requisitos Básicos

No desenvolvimento de soluções de rede, é bastante desejável que sejam implementadas facilidades de controle de acesso para informações e recursos corporativos. A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interconexão de LANs de forma a possibilitar o acesso de filiais, compartilhando recursos e informações e, finalmente, assegurar privacidade e integridade de dados ao atravessar a Internet bem como a própria rede corporativa. A seguir são enumeradas características mínimas desejáveis numa VPN (Segundo CHIN, 2004):

- **Autenticação de Usuários**

  Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados (quem acessou, o quê, e quando foi acessado).

- **Gerenciamento de Endereço**

  O endereço do cliente na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

- **Criptografia de Dados**

  Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

- **Gerenciamento de Chaves**

  O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

- **Suporte a múltiplos protocolos**

  Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos padrão de fato usadas nas redes públicas, tais como IP (*Internet Protocol*), IPX (*Internetwork Packet Exchange*), etc.

5.3 Tunelamento

As redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior às VPNs. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a

ficar ilegível, caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino onde é desencapsulado e decriptografado, retornando ao seu formato original. Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

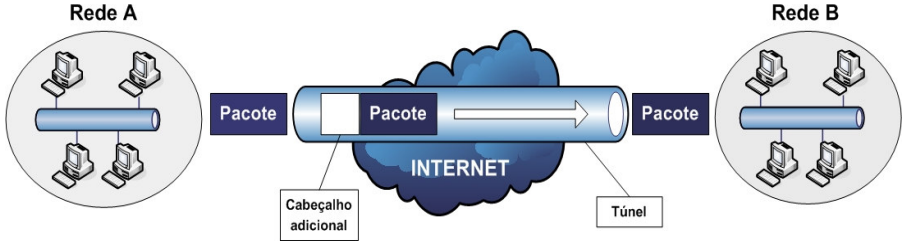

Figura 5.4: Tunelamento

Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote.

5.3.1 Protocolos de Tunelamento

Para se estabelecer um túnel é necessário que as suas extremidades utilizem o mesmo protocolo de tunelamento. O tunelamento pode ocorrer na camada 2 ou 3 (respectivamente enlace e rede) do modelo de referência OSI (*Open System Interconnection*).

Tunelamento em Nível de Enlace (nível 2)

O objetivo é transportar protocolos de nível 3, tais como o IP e IPX na Internet. Os protocolos utilizam quadros como unidade de troca, encapsulando os pacotes da camada 3 (como IP/IPX) em quadros PPP (*Point-to-Point Protocol*). Como exemplos podemos citar:

- **PPTP** (*Point-to-Point Tunneling Protocol*) da Microsoft permite que o tráfego IP, IPX e NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas como a Internet;

- **L2TP** (*Layer 2 Tunneling Protocol*) da IETF (*Internet Engineering Task Force*) permite que o tráfego IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto, tais como, IP, X25, Frame Relay, ATM;

- **L2F** (Layer 2 Forwarding) da Cisco é utilizada para VPN's discadas.

Tunelamento em Nível de Rede (Nível 3)

O tunelamento em nível de rede é feito pelo IP Security *Tunnel Mode* (IPSec) da IETF permite que pacotes IP sejam criptografados e encapsulados com cabeçalho adicional deste mesmo protocolo para serem transportados numa rede IP pública ou privada. O IPSec é um protocolo desenvolvido para IPv6 (*Internet Protocol version 6*), devendo, no futuro, se constituir como padrão para todas as formas de VPN caso o IPv6 venha de fato substituir o IPv4. O IPSec sofreu adaptações possibilitando, também, a sua utilização com o IPV4.

5.3.2 Funcionamento dos Túneis

Nas tecnologias orientadas à camada 2 (enlace), um túnel é similar a uma sessão, onde as duas extremidades do túnel negociam a configuração dos parâmetros para estabelecimento do túnel, tais como endereçamento, criptografia e parâmetros de compressão. Na maior parte das vezes, são utilizado s protocolos que implementam o serviço de datagrama. A gerência do túnel é realizada através protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada 3, não existe a fase de manutenção do túnel.

Uma vez que o túnel é estabelecido os dados podem ser enviados. O cliente ou servidor do túnel utiliza um protocolo de tunelamento de transferência de dados que acopla um cabeçalho preparando o pacote para o transporte. Só então o cliente envia o pacote encapsulado na rede que o roteará até o servidor do túnel. Este recebe o pacote, desencapsula removendo o cabeçalho adicional e encaminha o pacote original à rede destino. O funcionamento entre o servidor e o cliente do túnel é semelhante.

5.3.3 Protocolos x Requisitos de Tunelamento

Os protocolos de nível 2, tais como PPTP e L2TP, foram baseados no PPP, e, como conseqüência, herdaram muito de suas características e funcionalidades. Estas características e suas contrapartes de nível 3 são analisadas juntamente com alguns dos requisitos básicos das VPN's:

Autenticação do Usuário

Os protocolos de tunelamento da camada 2 herdaram os esquemas de autenticação do PPP e os métodos EAP (*Extensible Authentication Protocol*). Muitos esquemas de tunelamento da camada 3 assumem que as extremidades do túnel são conhecidas e autenticadas antes mesmo que ele seja estabelecido. Uma exceção é o IPSec que provê a autenticação mútua entre as extremidades do túnel. Na maioria das implementações deste protocolo, a verificação se dá a nível de máquina e não de usuário. Como resultado, qualquer usuário com acesso às máquinas que funcionam como extremidades do túnel

podem utilizá-lo. Esta falha de segurança pode ser suprida quando o IPSec é usado junto com um protocolo de camada de enlace como o L2TP.

Suporte a Token Card

Com a utilização do EAP, os protocolos de tunelamento de camada de enlace podem suportar uma variedade de métodos de autenticação, tais como senhas e cartões inteligentes (*smart cards*). Os protocolos de camada 3 também podem usar métodos similares, como, por exemplo, o IPSec que define a autenticação de chave pública durante a negociação de parâmetros feita pelo ISAKMP (*Internet Security Association and Key Management Protocol*)

Endereçamento Dinâmico

O tunelamento na camada 2 suporta alocação dinâmica de endereços baseada nos mecanismos de negociação do NCP (*Network Control Protocol*). Normalmente, esquemas de tunelamento na camada 3 assumem que os endereços oram atribuídos antes da inicialização do túnel.

Compressão de Dados

Os protocolos de tunelamento da camada 2 (enlace) suportam esquemas de compressão baseados no PPP. O IETF está analisando mecanismos semelhantes, tais como compressão de IP, para tunelamento na camada 3 (rede).

Criptografia de Dados

Protocolos de tunelamento na camada de enlace suportam mecanismos de criptografia baseados no PPP. Os protocolos de nível 3 também podem usar métodos similares. No caso do IPSec são definidos vários métodos de criptografia de dados que são executados durante o ISAKMP. Algumas implementações do protocolo L2TP utilizam a criptografia provida pelo IPSec para proteger cadeias de dados durante a sua transferência entre as extremidade do túnel.

Gerenciamento de Chaves

O MPPE (*Microsoft Point-to-Point Encryption*), protocolo de nível de enlace, utiliza uma chave gerada durante a autenticação do usuário, atualizando-a periodicamente. O IPSec negocia uma chave comum através do ISAKMP e, também, periodicamente, faz sua atualização.

Suporte a Múltiplos Protocolos

O tunelamento na camada de enlace suporta múltiplos protocolos o que facilita o tunelamento de clientes para acesso a redes corporativas utilizando IP, IPX, NetBEUI e outros. Em contraste, os protocolos de tunelamento da camada de rede, tais como IPSec, suportam apenas rede destino que utilizam protocolo IP.

5.3.4 Tipos de Túneis

Os túneis podem ser criados de 2 formas diferentes:

- **Túnel Voluntário** - um cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel.

- **Túnel Compulsório** - um servidor de acesso discado VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como cliente do túnel.

5.4 IPSec (*Internet Protocol Security*)

O IPSec é um protocolo padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em

outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.

Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser se forma conjunta ou separada, acordo com a necessidade de cada usuário:

- Autenticação e Integridade
- Confidencialidade;

Para implementar estas características, o IPSec é composto de 3 mecanismos adicionais:

- AH – Autentication Header;
- ESP – *Encapsulation Security Payload*
- ISAKMP – *Internet Security Association and Key Management Protocol.*

5.4.1 Negociação do nível de segurança

O ISAKMP combina conceitos de autenticação, gerenciamento de chaves e outros requisitos de segurança necessários às transações e comunicações governamentais, comerciais e privadas na Internet. Com o ISAKMP, as duas máquinas negociam os métodos de autenticação e segurança dos dados, executam a autenticação mútua e geram a chave para criptografar os dados.

Trata-se de um protocolo que rege a troca de chaves criptografadas utilizadas para decifrar os dados. Ele define procedimentos e formatos de pacotes para estabelecer, negociar, modificar e deletar as SAs (*Security Associations*). As SAs contêm todas as informações necessárias para execução de serviços variados de segurança na rede, tais como serviços da camada IP (autenticação de cabeçalho e encapsulamento), serviços das camadas de transporte, e aplicação ou auto-proteção durante a negociação do tráfego. Também define pacotes para geração de chaves e autenticação de dados. Esses formatos provêm consistência para a transferência de chaves e autenticação de dados que

independem da técnica usada na geração da chave, do algoritmo de criptografia e a mecanismo de autenticação.

O ISAKMP pretende dar suporte para protocolos de segurança em todas as camadas da pilha da rede. Com a centralização do gerenciamento dos SAs, o ISAKMP minimiza as redundâncias funcionais dentro de cada protocolo de segurança e também pode reduzir o tempo gasto durante as conexões através da negociação da pilha completa de serviços de uma só vez.

5.4.2 Autenticação e Integridade

A autenticação garante que os dados recebidos correspondem àqueles originalmente enviados, assim como garante a identidade do emissor. Integridade significa que os dados transmitidos chegam ao seu destino íntegros, eliminando a possibilidade de terem sido modificados no caminho sem que isto pudesse ser detectado.

O AH é um mecanismo que provê integridade e autenticação dos datagramas IP. A segurança é garantida através da inclusão de informação para autenticação no pacote a qual é obtida através de algoritmo aplicado sobre o conteúdo dos campos do datagrama IP, excluindo-se aqueles que sofrem mudanças durante o transporte. Estes campos abrangem não só o cabeçalho IP como todos os outros cabeçalhos e dados do usuário. No IPv6, o campo *hop-count* e o *time-to-live* (TTL) do IPv4 não são utilizados, pois são modificados ao longo da transferência.

5.4.3 Confidencialidade

Propriedade da comunicação que permite que apenas usuários autorizados entendam o conteúdo transportado. Desta forma, os usuários não autorizados, mesmo tendo capturado o pacote, não poderão ter acesso às informações nele contidas. O mecanismo mais usado para prover esta propriedade é chamado de criptografia.

O serviço que garante a "confidencialidade" no IPSec é o ESP - *Encapsulating Security Payload*. O ESP também provê a autenticação da origem dos dados, integridade da conexão e serviço *anti-reply*. A "confidencialidade" independe dos demais serviços e pode ser implementada de 2 modos - transporte e túnel. No primeiro modo, o pacote da

camada de transporte é encapsulado dentro do ESP, e, no túnel, o datagrama IP é encapsulado inteiro dentro do cabeçalho ESP.

6 MATERIAS E MÉTODOS

6.1 Tipo de Pesquisa

Inicialmente, o projeto consistiu numa pesquisa exploratória, onde foram feitas pesquisas e análises de serviços conexões de internet, de roteadores VPN, de custos de implantação e manutenção de uma VPN e das variáveis que influenciam na escolha dos equipamentos e serviços, para se chegar numa solução adequada. Esse tipo de pesquisa tem como objetivo, proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Outro objetivo desta pesquisa é o aprimoramento de idéias ou descobertas de intuições.

Quanto aos procedimentos técnicos de implantação do projeto em questão, a pesquisa teve um caráter de pesquisa-ação que é realizada a partir do envolvimento dos pesquisadores e representantes da situação de maneira cooperativa ou participava na ação ou na resolução dos problemas. A pesquisa ação consistiu basicamente na configuração dos roteadores e nos testes de estabilidade de conexão entre os mesmos.

6.2 Procedimentos Metodológicos

O estudo, análise e implantação do projeto foi realizado através de uma parceria no CIN-UFLA (Centro de informática – UFLA) e a Empresa Conecta Redes de Computadores, mais conhecida como Redes & Cia. A implantação do projeto foi realizada durantes os meses de abril e maio de 2005.

6.2.1 Descrição do Projeto

O Projeto em questão surgiu com a necessidade de uma solução para a interligação entre matriz e filiais de empresas com um baixo custo de instalação e manutenção. A utilização da Internet como infra-estrutura é apontada como solução viável e de baixo custo.

Quando se aproveita um link de Internet para o estabelecimento de uma VPN, eliminamos a necessidade de uma conexão dedicadas para a comunicação entre redes, o que reflete na redução de custos.

À partir dessa observação, observou-se a necessidade de custos de mensalidades de serviços de conexão com a internet mais baixos e equipamentos de menor porte e preço, ou seja, uma solução que pequenas e médias empresas poderiam ter acesso.

Após pesquisas de preços e soluções de equipamentos de serviços, definiu-se que o projeto consistiria na interligação de duas redes de computadores geograficamente separadas (localizadas na cidade de Lavras – Minas Gerais e denominadas REDE A e REDE B) através de uma VPN utilizando conexão de internet banda larga e roteadores VPN de pequeno porte.A figura 6.1 ilustra o cenário do projeto.

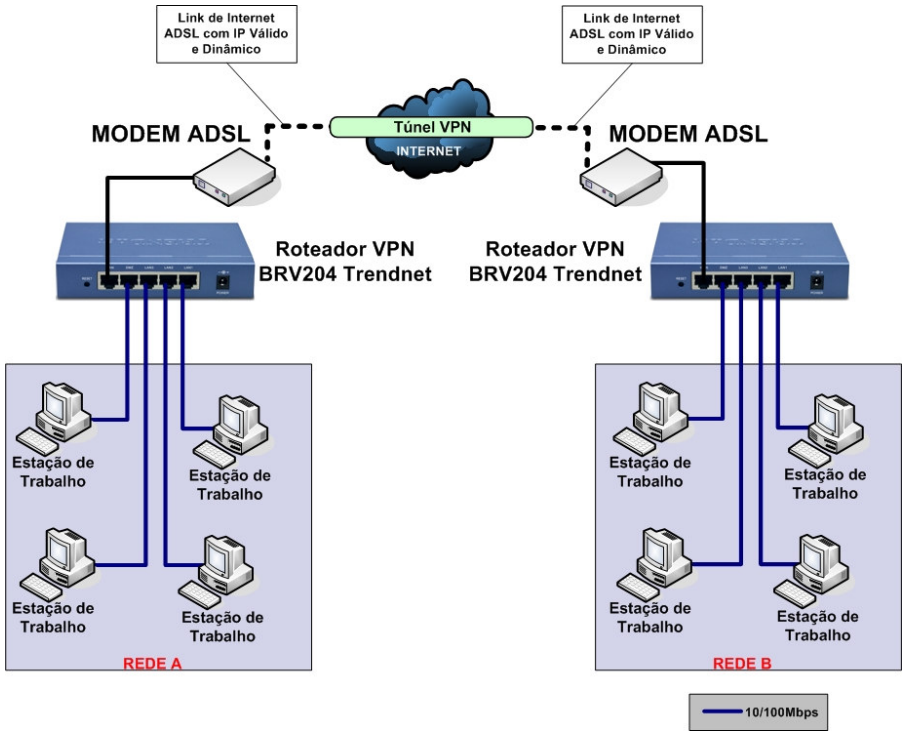

Figura 6.1 – Cenário do Projeto

Para definir a melhor solução a ser adotada, foi realizada uma série de etapas para a pesquisa, análise e implantação de uma solução VPN. Estas etapas podem ser vistas no fluxograma abaixo:

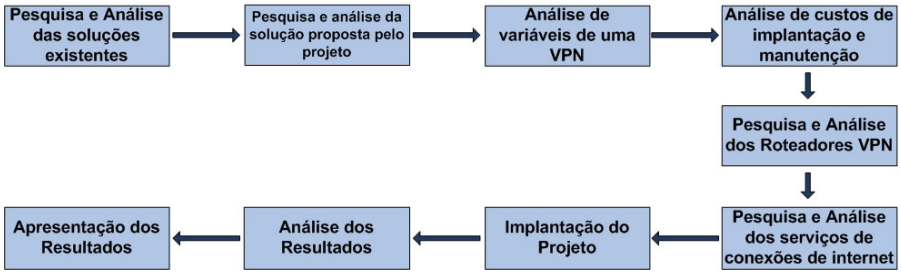

Figura 6.2 – Fluxograma do Projeto

6.2.2 Pesquisa e Análise das Soluções Existentes no Mercado

Na Primeira etapa do projeto foi realizada uma pesquisa de quais soluções para a interligação de filiais existem no mercado. Depois de encontrarmos alguns tipos de soluções, geralmente fornecidas por empresas de telefonia, essas foram analisadas com relação a velocidades de conexão, serviços oferecidos e principalmente os custos de mensalidades e alugueis de roteadores.

Ainda nessa primeira fase, também foram pesquisadas as necessidades das pequenas e médias empresas, e foi verificado que elas necessitam de serviços integrados. Por exemplo, no mesmo serviço de interligação de filiais devem estar incluídos também serviços como acesso a Internet. Tudo isso com custos relativamente baixos.

Nas pesquisas e análises descritas acima, verificou-se que nenhuma das soluções existentes no mercado possuíam recursos de serviços integrados somados a baixos custos de mensalidades e de aluguéis de roteadores.

6.2.3 Pesquisa e Análise da Solução Proposta pelo Projeto

A segunda etapa do projeto se resumiu na realização de pesquisas de soluções alternativas, pois as soluções existem no mercado não supririam as necessidades de baixos custos de mensalidades e manutenções.

Após várias pesquisas realizadas, definiu-se que uma solução que será proposta é uma solução baseada na interligação de filiais através de conexões de internet banda larga e na utilização de roteadores VPN SOHO (*Small Office Home Office*).

Com isso, resolve-se o problema da necessidade de serviços integrados, pois nesse caso pode-se fornecer serviço de interligação e o de conexão com a internet, com custos de mensalidades baixos e com desempenho semelhante aos serviços existentes no mercado.

6.2.4 Análise de Variáveis de um Projeto VPN

Por se referir um projeto de uma VPN deve-se ser considerado que os custos relativos ao mesmo envolvem aquisição de equipamentos (roteadores e modems), serviços de conexão (link de Internet) e mão de obra para a configuração de modems e roteadores.

Para planejar a implantação de uma VPN, é necessário fazer antes uma análise das necessidades do cliente, pois este planejamento depende de muitas variáveis, como:

- **O número de pontas que a VPN possuirá**

O cálculo de número de pontas de uma VPN é feito somando a ponta da matriz e o número de filiais a serem interligadas. A necessidade de sabermos a quantidade de pontas em uma VPN é extremamente importante pois este é o primeiro contato sobre o projeto, e, de acordo com o número de pontas, pode-se começar a definir algumas características que irão influenciar na escolha do link de internet, do roteador e da definição de custos adicionais para a implantação do projeto.

- **Distância entre as pontas;**

Esta variável influencia diretamente nos custos de mão de obra, pois, de acordo com a distância e o número de pontas que uma VPN terá, pode-se calcular quais os custos com deslocamento, hospedagem e alimentação da equipe que executará a configuração da VPN.

- **Serviços que serão compartilhados entre as redes;**

Os serviços compartilhados entre as redes (matriz-filial), influenciarão no estudo de fluxo de dados e nos custos de implantação de uma VPN, pois, de acordo com a quantidade de serviços a serem compartilhados entre as redes como, integração de sistemas e utilização de impressoras remotas, maior será o fluxo de dados e maior será o custo de implantação da solução.

- **Estudo do tráfego de dados entre as pontas da VPN;**

Antes de definirmos qual link será utilizado em cada ponta da VPN, é necessário o estudo do fluxo de dados entre as redes para saber quais tipos de dados serão transmitidos e de quais aplicações, quais os sistemas e serviços que serão compartilhados entre essas redes, etc.

Quanto maior o fluxo de dados maior deverá ser a taxa de transmissão do link de Internet, ocasionando um aumento nos custos de mensalidades desse serviço.

- **Link de Internet;**

Tendo conhecimento do número de pontas de uma VPN, quais serviços serão compartilhados entre as redes e de ter estudado tráfego de dados entre as pontas, já se tem as informações necessárias para a escolha do link de internet para cada ponta. Cada um desses links deve ter uma taxa de transmissão de dados suficiente para fornecer, além da interligação rápida e eficiente entre matriz e filiais, a conexão da rede interna de cada ponta com a Internet.

- **Roteador VPN;**

De acordo com o tráfego de dados entre as redes, com o número de hosts existentes em cada uma das pontas da VPN e com os serviços a serem compartilhados entre as redes, serão escolhidos os tipos de roteadores que serão utilizados em cada uma das pontas. Quanto maior o tráfego de dados, mais robusto os roteadores deverão ser, e consequentemente o custo para aquisição desses equipamentos será maior.

6.3 Pesquisa e Análise de Roteadores VPN

A quarta etapa do projeto em questão consistiu na pesquisas de alguns tipos de Roteadores VPN SOHO e na análise de funcionalidades e de custo/benefício desses roteadores.

Dentre os vários roteadores pesquisados podemos citar os seguintes modelos: XRT-401D (Planet), TW100-BRV204 (Trendnet), DI-804HV (D-Link) e o BEFVP41 (Linksys).

Após análises dos recursos fornecidos por estes roteadores e dos custos para aquisição dos mesmos, a roteador escolhido foi o TW100-BRV204 da Trendnet, pois este mostrou-se mais adequado, de acordo com suas características ténicas, para a proposta do projeto e com um custo bastante acessível. Veja abaixo a especificações do roteador TW100-BRV204:

Características do TW100-BRV204

- Suporta Cable/DSL modems com IP dinâmico, IP estático e tipos de conexões PPPoE, PPTP e L2TP;
- Compatível com Windows 95/98/ME/NT/200/XP, Unix e Mac OS;
- Suporta até 10 túneis IPSec;
- Suporta 100 (IPSec, L2TP, PPTP) sessões Pass-Through simultâneas;
- Suporta um servidor PPTP e 10 conexões clientes VPN;
- Possui Virtual Servers (Desvio de porta) e firewall que suporta até 60 regras;
- Possui controle de acesso de usuários;
- Possui roteamento estático e serviço de DNS dinâmico;
- Fácil configuração via web browser;

Especificações de Hardware do TW100-BRV204

Padrões:

- IEEE 802.3 (10-Base T), 802.3u (100-Base TX)

Protocolos:

- NAT, PPPoe, NTP, SMTP, HTTP, TFTP, DHCP, TCP/IP, PAP, CHAP, RIP, RIP2, DDNS.

WAN:

- 1 porta 10/100 Mbps (Internet)

LAN:

- 3 portas 10/100 Mbps Auto-MDIX

DMZ:

- 1 portas 10/100 Mbps Auto-MDIX

Especificações do Roteador TW100-BRV204

Firewall:

- NAT Firewall e SPI Firewall

Segurança:

- Filtro de URLs, controle de acesso, proteção de passwords, e-mails de alerta e logs.

VPN(IPsec):

- MD5-HMAC/SHA1-HMAC, Autenticação, DES-CBC, 3DES-CBC, criptografia, Internet Key Exchange.

VPN Túneis:

- 10 túneis IPsec
- 10 túneis PPTP

VPN Pass-through:

- IPSec, PPTP, L2TP (100 sessões)

6.4 Pesquisa e Análise de Serviços de Conexão de Internet

A partir da escolha do roteador TW100-BRV204, passamos para a fase de escolha do tipo de conexão com a internet que seria utilizada. Foram analisadas as características técnicas de 4 tipos tecnologias de conexão de internet, são eles: ADSL, Wireless, a cabo e link dedicado. Foram analisadas também as vantagens e desvantagens de cada uma das tecnologias.

A primeira decisão a ser tomada nesta faze foi a de que as duas pontas da VPN iriam usar o mesmo tipo de tecnologia e de um mesmo fornecedor do serviço, dessa forma temos a vantagem de se utilizar a mesma malha de transmissão, diminuindo, assim, a latência na comunicação entre as duas redes e ocasionando melhor eficiência na transmissão de dados.

Uma característica importante para a implantação de uma VPN, é a necessidade da conexão de Internet escolhida possuir um IP válido na internet, pois para estabelecer a comunicação de dois roteadores na internet, é preciso que exista um IP válido para cada um dos roteadores.

Depois das pesquisas e análises realizadas, percebeu-se que a tecnologia ADSL tinha as características citadas anteriormente, combinada com uma latência consideravelmente baixa e com custos de mensalidades baixos. Portanto esta tecnologia foi adotada no projeto em questão.

A ADSL (*Asymmetric Digital Subscriber Line*), utiliza uma tecnologia de transporte de dados digitais através de linhas telefônicas convencionais. Como o nome diz, ela é assimétrica, ou seja, nessa tecnologia existe a necessidade da taxa de download ser diferente da de upload. No caso deste projeto foi utilizados um link de 512 Kbps e outro de 256 Kbps. O ADSL funciona numa freqüência elevada, acima da utilizada nas comunicações via voz. Isto permite que, com o uso de filtros, o telefone comum possa ser utilizado simultaneamente com a rede ADSL.

6.5 Análise de Custos de Implantação e de Manutenção

A solução proposta no projeto em questão, tinha como uma das principais finalidades a diminuição de custos de implantação e mensalidades de uma VPN, então essa fase tornou-se uma das mais importantes.

De acordo com o cenário do projeto, mostrado na Figura 6.1, foram utilizados dois modems ADSL e dois roteadores TW100-BRV204, que custam em torno de R$ 300,00 (trezentos reais) e R$ 600,00 (seiscentos reais) repectivamente. Totalizando um valor de R$ 1.800,00 (um mil e oitocentos reais) em equipamentos.

A definição dos custos de mão de obra de configuração da VPN também está dentro do escopo deste projeto. O valor desta mão de obra, considerando o cenário do projeto em questão, está em torno de R$ 2.200,00 (Dois mil e duzentos reais). Ou seja, se algum tipo de empresa ou instituição necessitar de um projeto de interligação através de VPN, pode-se considerar uma previsão de custos em torno de R$ 3970,00 (Três mil novecentos e setenta reais), considerando todos os equipamentos e mão de obra para a implantação de uma VPN com duas pontas.

6.6 Implantação do Projeto

A implantação de um projeto de uma VPN com pontas de IP dinâmicos, é constituída de 4 fases: Instalação do Sistema Cliente de DNS Dinâmico, Configuração do Sistema Cliente de DNS Dinâmico, Configuração dos Roteadores e Testes de Conexão, de Roteadores e de Desempenho da VPN.

6.6.1 Instalação do Sistema Cliente de DNS Dinâmico

O DNS Dinâmico é simplesmente um modo de prender um *hostname* estático em um endereço de IP dinâmico. Na Internet, existe um número limitado de endereços de IP. Quando você conecta ao seu provedor de acesso (ISP), é atribuído um endereço de IP temporário para você utilizar enquanto estiver conectado. Uma vez que você desconectar, este endereço IP será utilizado por outra pessoa, e assim por diante. Se você estiver tentando operar um servidor de jogos, ou um servidor de *web* pessoal, ou qualquer outro

serviço que exige que outros computadores achem o seu na internet, é necessário saber qual o endereço IP atual de sua conexão ADSL.

Quando se utiliza uma conexão de internet que utiliza o endereçamento dinâmico de IP, torna-se mais difícil a tarefa de conseguirmos mostrar para todo mundo qual o seu endereço de IP atual. Pode-se comparar essa situação a mudar o número de telefone de sua residência todos os dias, isso geraria o problema de ninguém conseguir saber qual o seu número em um determinado momento.

O Sistema Cliente de DNS Dinâmico foi instalado com o intuito de solucionar o problema de endereçamento dinâmico de IP da conexão ADSL. São estes sistemas que são responsáveis pela sincronização entre o hostname e o endereço de IP, toda vez que o endereço IP da conexão mudar.

Dentre os vários sistemas pesquisados e analisados, o sistema cliente escolhido foi o DYNDNS UPDATER 3.0.0, por ter demonstrado um maior número de recursos e um melhor desempenho. Abaixo será exemplificado todos os procedimentos de instalação do sistema.

Inicialmente é necessário criar uma conta em algum serviço de DNS dinâmico. No caso do projeto em questão foi escolhido o DYNDNS.org (www.dyndns.org). Em seguida, pode-se criar gratuitamente até 5 *hostnames* diferentes para essa conta. Como este trabalho utiliza uma VPN de duas pontas, foram criadas apenas 2 *hostnames* (gammon-vpn.dvr.org e gammon-vpn.dvr.org), ou seja, um para cada uma das 2 conexões ADSL.

Depois de configurarmos os *hostnames*, pode-se instalar o softtware cliente de DNS dinâmico, que pode ser baixado do próprio site de DYNDNS.org. Após o arquivo de instalação do sistema ser baixado, é necessário apenas executa-lo e seguir as instruções de acordo com as ilustrações abaixo.

Figura 6.3 – Instalação do Sistema Cliente 1

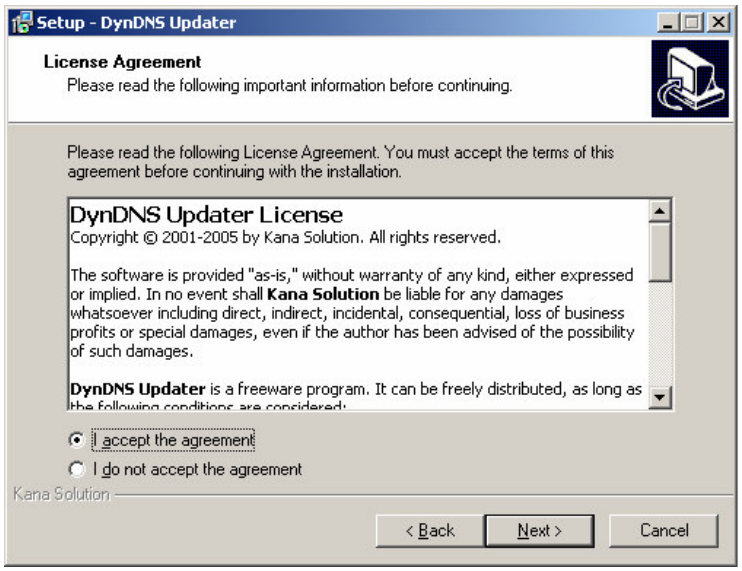

Figura 6.4 – Instalação do Sistema Cliente 2

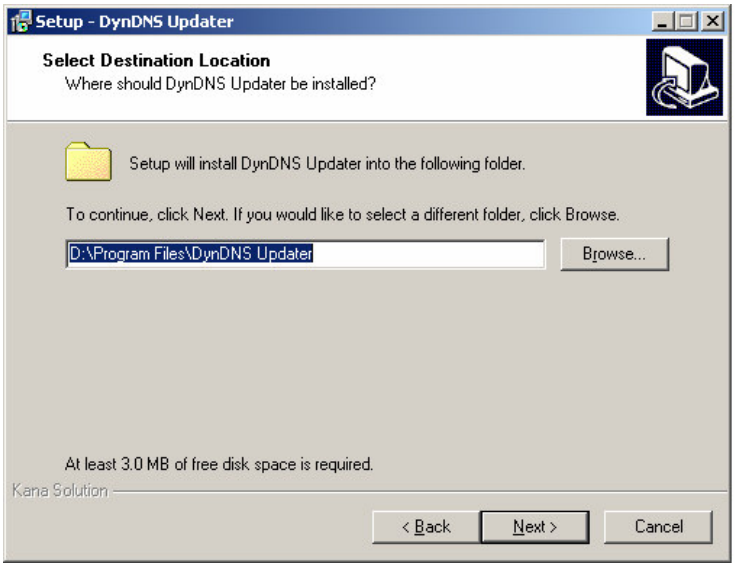

Figura 6.5 – Instalação do Sistema Cliente 3

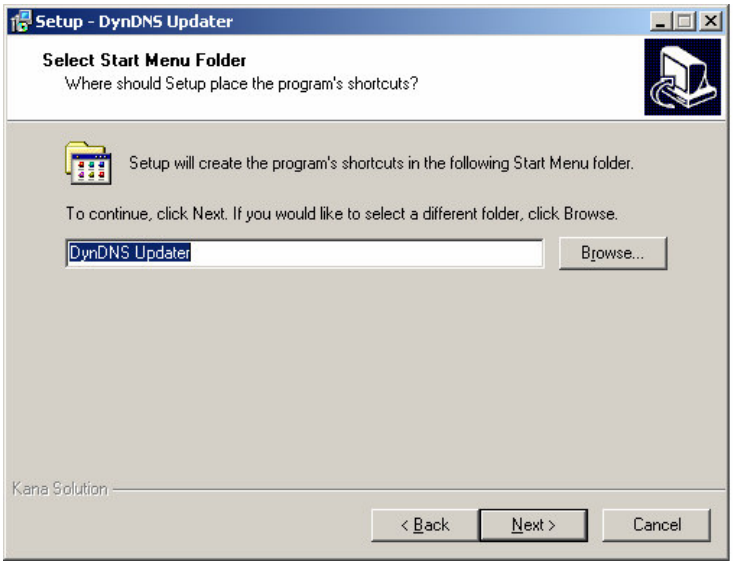

Figura 6.6 – Instalação do Sistema Cliente 4

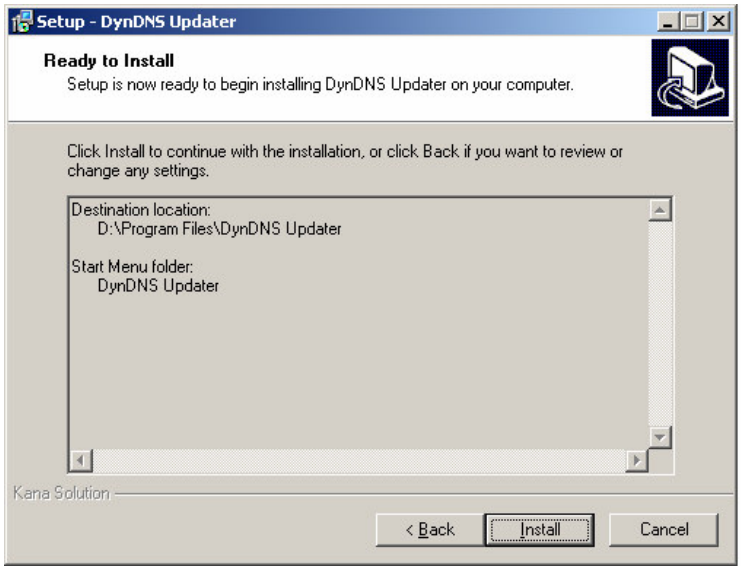

Figura 6.7 – Instalação do Sistema Cliente 5

O sistema foi instalado em dois computadores da REDE A e dois computadores da REDE B, que ficam 24 horas ligados, pois, como já foi mostrado, são eles os responsáveis pela sincronização entre o *hostname* e o IP válido da conexão.

6.6.2 Configuração dos Sistemas Clientes de DNS Dinâmico

Depois de instalado nos computadores da REDE A e REDE B, o sistema deve ser configurado de acordo com a necessidade de cada uma das redes. Neste tópico, mostraremos a configuração nas duas redes ao mesmo tempo, e quando ocorrer alguma configuração diferente será mostrado separadamente.

Ao executarmos pela primeira vez o sistema, tem-se a tela que é mostrada na Figura 6.8, e como se pode ver ela nos mostra que não existe nenhuma conta de DNS Dinâmico cadastrada nela. Como há a necessidade de configurar essa conta no sistema, basta clicar no botão *Add*. Após essa ação, será mostrada a tela ilustrada na Figura 6.9, onde se deve preencher o campo com o nome do grupo, que nada mais é que um nome que o instalador desejar. Para este trabalho foi adotado o nome de TesteVPN. Após preencher este campo, é necessário apenas clicar no botão de OK.

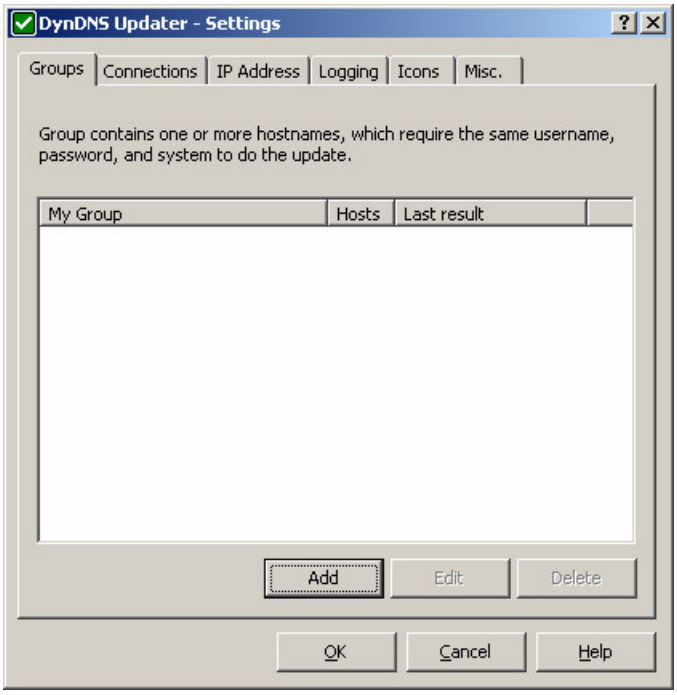

Figura 6.8 – Configuração do Sistema Cliente 1

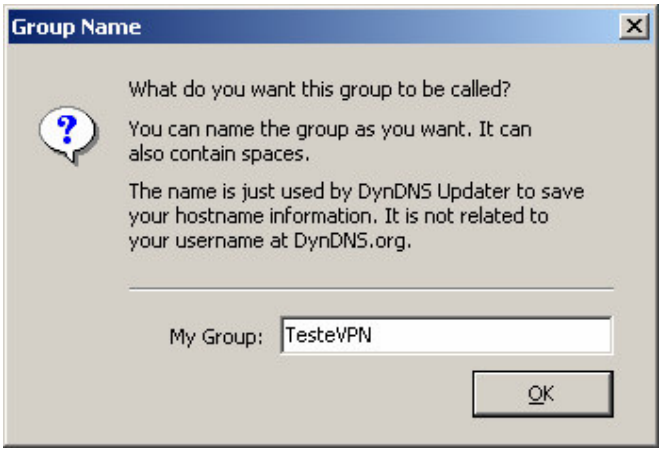

Figura 6.9 – Configuração do Sistema Cliente 2

As figuras 6.8 e a 6.9, inicialmente esta totalmente em branco, então entramos com o *Username* e o *Password* da conta de DNS Dinâmico criada anteriormente. E após preencher estes dados corretamente clicamos no botão de *Donwload*, com isso o sistema irá verificar todos os *hostnames* existentes na conta criada. Como se pode ver, a conta criada para este projeto possui dois *hostnames*, que são exatamente os que são mostrados nas Figuras citadas acima.

Por padrão, após clicarmos no botão de *Donwload*, verificamos que os dois *hostnames* estão marcados, porém a Figura 6.10 nos mostra como é a configuração do sistema para a REDE A, e como precisamos apenas de um *hostname* para cada uma das redes, então deixamos marcado apenas o *gammon-vpn-1.dvrdns.org*, ou seja, é este nome que será sincronizado com IP dinâmico da REDE A. Após esse procedimento clicamos no botão de OK.

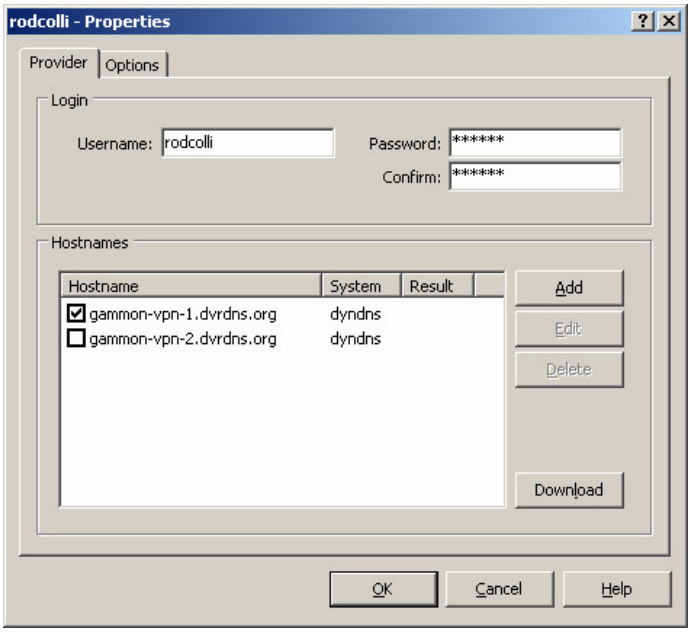

Figura 6.10 – Configuração do Sistema Cliente 3

A Figura 6.11 é o mesmo caso da anterior, a diferença é que ela mostra como é feita a configuração para a REDE B, quando clicamos no botão de *Download*, verifica-se que os dois *hostnames* estão marcados, porém agora deixamos marcado apenas o *gammon-vpn-2.dvrdns.org*, que será sincronizado com IP dinâmico da REDE B. Após esse procedimento clicamos no botão de OK.

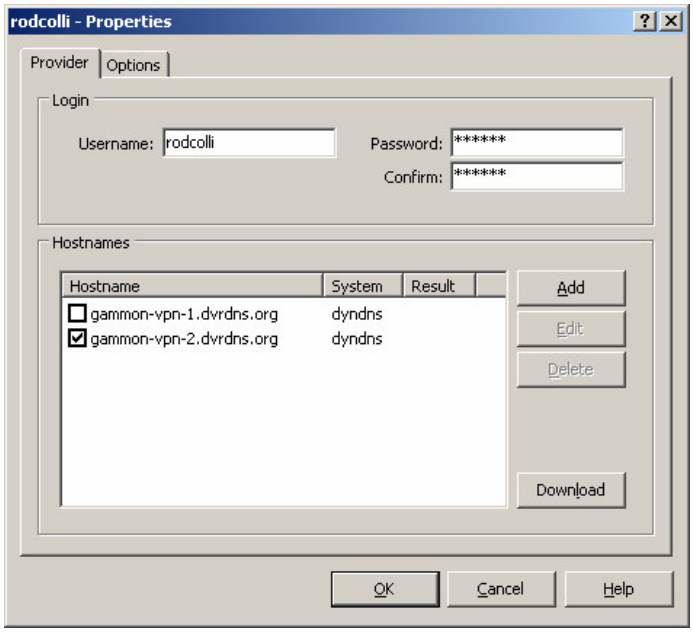

Figura 6.11 – Configuração do Sistema Cliente 4

Depois de configurarmos a conta de DNS Dinâmico ao qual o *hostname* será sincronizado com cada uma das redes, a tela representada pela figura 6.12 será mostrada. Como vemos o próprio sistema obtém o endereço de IP da conexão de internet e também possui algumas configurações padrão. Porém estas configurações não são as ideais, necessitando realizar algumas modificações na mesma.

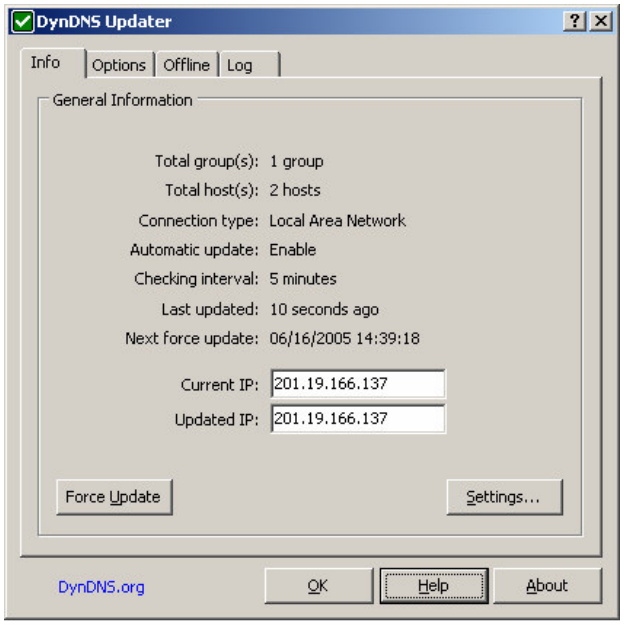

Figura 6.12 – Configuração do Sistema Cliente 5

Para alterarmos as configurações padrões, devemos clicar na aba *Options*, e deixarmos todas as configurações de acordo com a figura 6.13, onde devemos deixar as opções *Start with* Windows (o sistema irá inicializar quando o Windows inicializar), *Enable Automatic Update* (habilita a atualização automática) habilitadas. E preenchermos os campos *Checking Interval* (quanto menor o tempo de checagem melhor, porém o mínimo é de 5 em 5 minutos) e *Force Update within* (força sincronização do *hostname* e IP da conexão de internet se o tempo determinado for ultrapassado) com 5 minutos e 25 dias respectivamente. E clicamos no botão de OK.

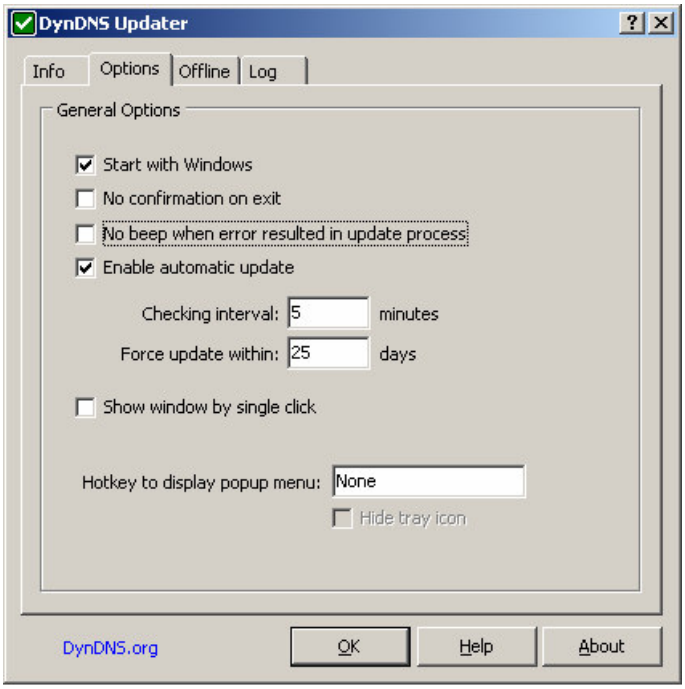

Figura 6.13 – Configuração do Sistema Cliente 6

Após todas as configurações concluídas, será apresentada a tela da Figura 6.14, que mostra o status da sincronização. Nela temos as informações de nome do grupo, que representa a conta, a quantidade de *hostnames* existentes nessa conta e o resultado da última sincronização.

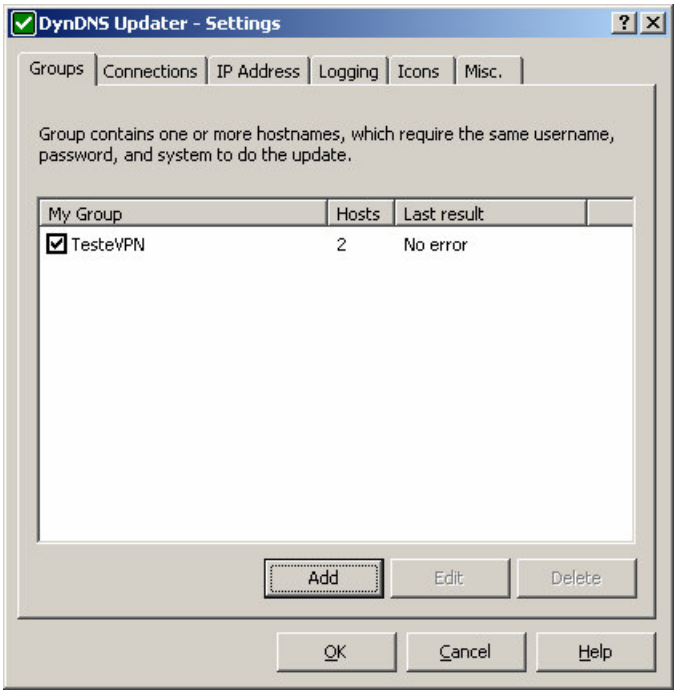

Figura 6.14 – Configuração do Sistema Cliente 7

6.6.3 Configuração dos Roteadores

Depois de instalado e configurado os sistemas cliente de DNS dinâmico, podemos seguir para o próximo passo que é a configuração dos roteadores. Neste tópico, será descrita toda a configuração dos roteadores VPN na REDE A e na REDE B, respectivamente. Pressupõe nesse projeto que os roteadores já estão configurados com relação à conexão ADSL.

A Figura 6.15, nos mostra a tela de configuração de políticas de VPN da REDE A. Inicialmente, deve abrir algum *browser* de internet e digitar o IP correspondente ao roteador, que neste caso é 192.168.1.254. Após digitarmos e teclar ENTER, aparecerá a tela geral de configuração do roteador. Então, na coluna esquerda, clicar na opção VPN, escolher VPN *Policies* e logo após a opção *ADD New Policy*. Com isso chegando a tela mostrada na Figura 6.15 onde poderemos configurar a VPN propriamente dita.

A primeira tarefa de configuração a ser realizada é escolher um nome da política de VPN. Não existe uma regra para este nome, porém, normalmente a política do roteador da REDE B tem o mesmo nome da política da REDE A, pois podemos ter várias políticas em

cada roteador e com isso facilitaria a administração de várias políticas. O nome adotado foi VPNPOLICY e a opção *Enable Policy* foi marcada para habilitar a política após ela ser salva.

Logo após, é solicitado o *Remote* VPN *Endpoint*, que nada mais é que a identificação da rede remota, neste caso é a identificação da REDE B, e como a identificação da REDE B é feita através de um nome devido ao IP dinâmico da conexão ADSL, a opção marcada foi a *Domain Name*, e o seu campo preenchido com *vpn-gammon-2.dvrdns.org*, que é o nome que identifica a rede remota.

Concluída esta fase, deve-se agora entrar com a faixa de IP interno da rede local (REDE A), então escolhemos a opção *Subnet Address*, pois com isso podemos usar apenas identificação da rede (192.168.1.0), para mostrar que as estações da REDE A estão da faixa de IP dessa rede. E logo após entramos com a máscara de sub-rede desta rede (255.255.255.0), e com isso pode afirmar que esta rede faz parte da classe C.

O próximo campo a ser preenchido é muito parecido com o exemplificado no parágrafo anterior, porém é a faixa de IP interno da rede remota (REDE B), então escolhe a opção *Subnet Address*, pois com isso podemos usar apenas identificação da rede (192.168.2.0) para mostrar que as estações da REDE B estão na faixa de IP dessa rede. Logo após entramos com a máscara de sub-rede desta rede (255.255.255.0), e a partir desse mascaramento, sabe-se que a rede também faz parte da classe C.

Após preencher os quatro primeiros campos, que são basicamente a identificação da rede local e da rede remota, pode-se iniciar a configuração dos tipos de autenticação e criptografia da VPN.

Podemos observar na Figura 6.15 que a opção AH *Authentication* não foi selecionada, pois ela é específica do protocolo IPv6, e como estamos utilizando IPv4, não é necessário utilizá-la. Foram marcadas apenas as opções ESP *Encription*, ESP *Authentication*, que têm por finalidade fornecer integridade e confidencialidade aos datagramas IP através da cifra dos dados contidos no datagrama. Os algoritmos de criptografia e de autenticação utilizados foram 3DES e MD5, respectivamente. Pois são os algoritmos que fornecem um maior nível de segurança.

O próximo passo é configurar o IKE (*Internet Key Exchange*). Este mecanismo responsabiliza-se pela criação, eliminação e alteração das chaves para autenticação e validação de informações.

Inicialmente definimos que a solicitações de criação, eliminação e alteração de chaves, será feita por ambas as pontas da VPN, então escolhemos *Both Direction* para preencher a opção *Direction*.

Logo após deve-se entrar com a identidade da rede local (*gammon-vpn-1.dvrdns.org*) e da rede remota (*gammon-vpn-2.dvrdns.org*), definimos uma chave para ser pré-compartilhada para autenticação (VPNGAMMON), e que o algoritmo de autenticação e de criptografia para a troca de chaves será o MD5 e 3DES, respectivamente, pelos mesmos motivos citados anteriormente.

A partir do campo *Exchange Mode*, temos algumas opções que foram preenchidas de acordo com as recomendações do fabricante. E após todos os procedimentos concluídos podemos salvar a política VPN da REDE A.

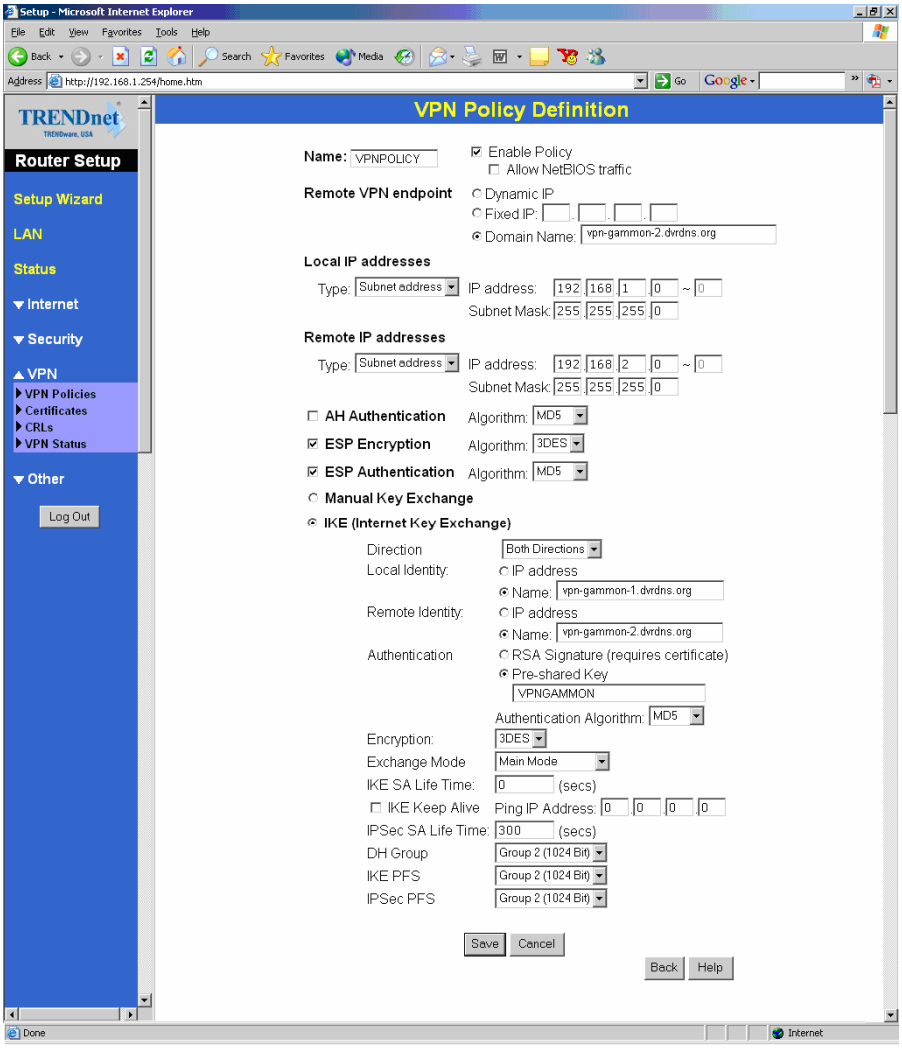

Figura 6.15 – Configuração do Roteador REDE A

A configuração do roteador da REDE B é bastante semelhante ao da REDE A, mudando apenas algumas informações que diz respeito a identificação das redes, que estão marcadas na Figura 6.16. As alterações feitas foram as seguintes:

- **Remote VPN endpoint** – a ponta remota agora é a REDE A, e o nome que identifica ela é *gammon-vpn-1.dvrdns.org*.
- **Local IP addresses** – como a rede local agora é a REDE B, o campo é preenchido com a faixa de IP interna de rede que é 192.168.2.0.

- **Remote IP addresses** – como a rede remota é a REDE A, o campo é preenchido com a faixa de IP interna de rede que é 192.168.1.0.
- **Local Identify** – este campo é identidade da rede local que é *gammon-vpn-2.dvrdns.org.*
- **Remote Identify** – este campo é identidade da rede local que é *gammon-vpn-1.dvrdns.org.*

Após realizarmos todas as configurações e salvamos a política VPN da REDE B, a conexão VPN é estabelecida automaticamente.

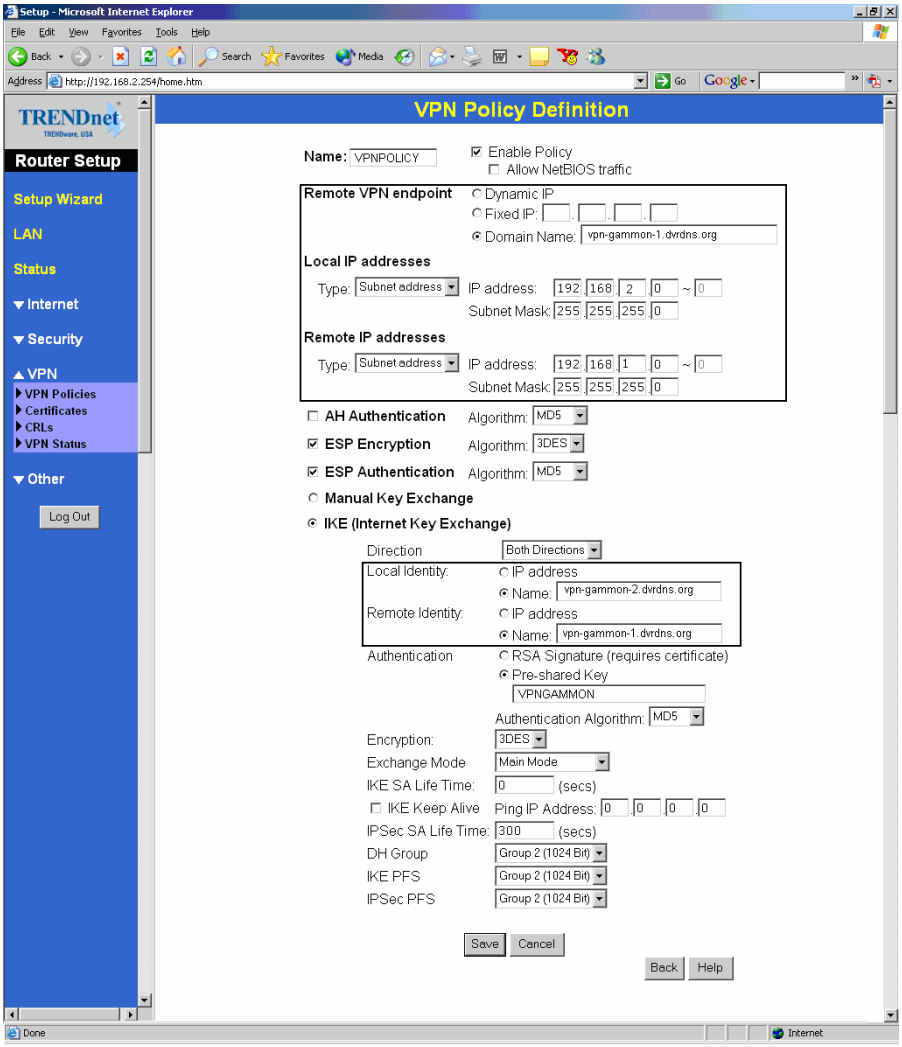

Figura 6.16 – Configuração do Roteador da REDE B.

7 RESULTADOS E DISCUSSÕES

Após configurarmos os roteadores, foi obtido primeiro resultado, que foi o fechamento da VPN, que nada mais é que o estabelecimento da comunicação entre a REDE A e a REDE B. Na Figura 7.1, é mostrado o status da VPN, onde temos algumas informações sobre o túnel. Caso a VPN não estivesse estabelecida, esta tabela estaria vazia.

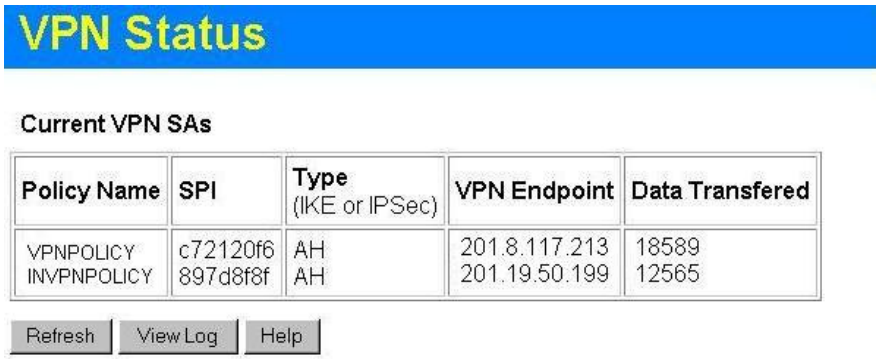

Figura 7.1 – Status VPN

O funcionamento da solução proposta pelo projeto é comprovado pelos fabricantes de roteadores apenas para países com o padrão de ADSL diferente do Brasil. E o principal desafio do presente projeto, foi testar a VPN baseada em conexões ADSL do padrão brasileiro. Podem-se, assim, termos resultados positivos, que seria o funcionamento da VPN de forma estável, ou negativo onde a conexão VPN não ficaria estabelecida de forma estável, e assim não se tornando um canal confiável para a utilização de recursos críticos entre duas redes.

7.1 Comportamento do Sistema Cliente de DNS Dinâmico

O sistema cliente de DNS dinâmico, o qual possui a finalidade de sincronização entre o hostname e o IP dinâmico da conexão ADSL, teve um desempenho muito bom, isso por que manteve o hostname sempre atualizado com o IP que a conexão estava no momento, e como a sua função era exatamente essa, pode-se afirmar que o sistema utilizado funciona, desempenha seu papel corretamente e que a instalação e a configuração dele foram feitas de forma correta.

7.2 Comportamento dos Roteadores VPN

Utilizando um computador da REDE A, foi executado o comando PING para testar se o roteador da REDE B respondia corretamente, como é mostrado na Figura 7.2. O mesmo procedimento foi repetido, porém utilizando um computador da REDE B para testar o roteador da REDE A com o mesmo comando, o PING, exemplificado na Figura 7.3.

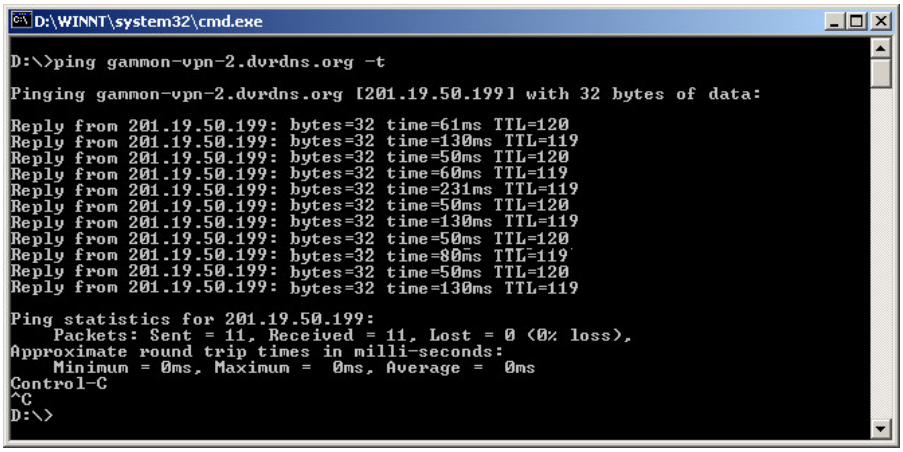

Figura 7.2 – Teste do Roteador da REDE B

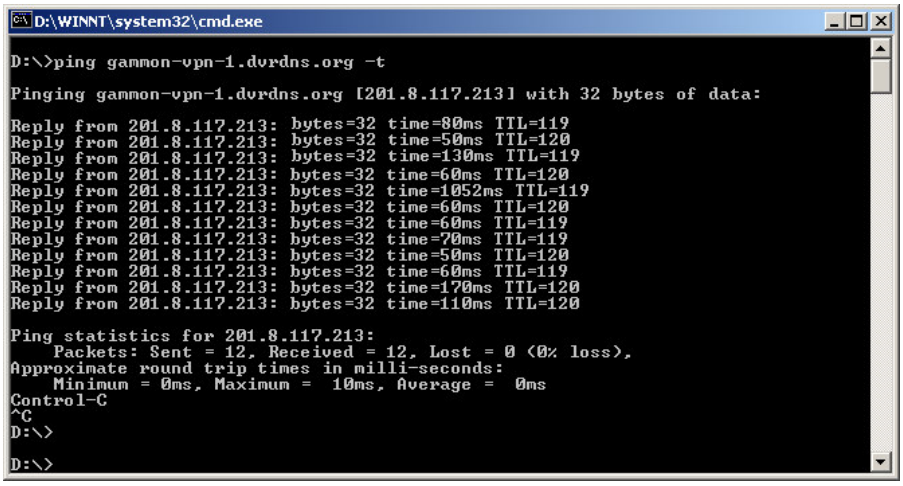

Figura 7.3 – Teste do Roteador da REDE A

Este teste serviu para analisar o desempenho dos roteadores VPN. Em termos de perda de pacotes, eles tiveram um desempenho excelente, tendo uma baixa porcentagem de pacotes perdidos.

Porém, com relação à estabilidade da VPN, não houve o mesmo desempenho, pois o suporte ao DNS Dinâmico não funcionou corretamente e, quando ocorria a troca do IP da conexão ADSL o roteador não fechava novamente a VPN. Um outro problema identificado foi que alguns roteadores travam após algum tempo de funcionamento, tendo assim que ser reinicializados.

7.3 Desempenho da Conexão ADSL

Depois de ser testada através de transferências de arquivos de uma rede para outra e também através de teste com o comando PING, foi verificado que, mesmo utilizando as conexões de um mesmo fornecedor nas duas pontas da VPN para obter uma maior eficiência, ocorreu uma elevada latência de transmissão de dados e que os tempos de respostas tiveram uma variação elevada, como pode ser observado nas Figuras 7.2 e 7.3, mostradas anteriormente.

7.4 Comportamento da Conexão VPN

A conexão VPN, enquanto fechada, funcionou corretamente interligando as redes de computadores. O teste realizado e exemplificado na Figura 7.4, mostra um computador da REDE A com o endereço IP 192.168.1.123 fazendo um PING numa estação da REDE B com o endereço IP 192.168.2.123. E como se pode ver neste teste, os computadores estão em redes diferentes porém comunicando entre si através da VPN.

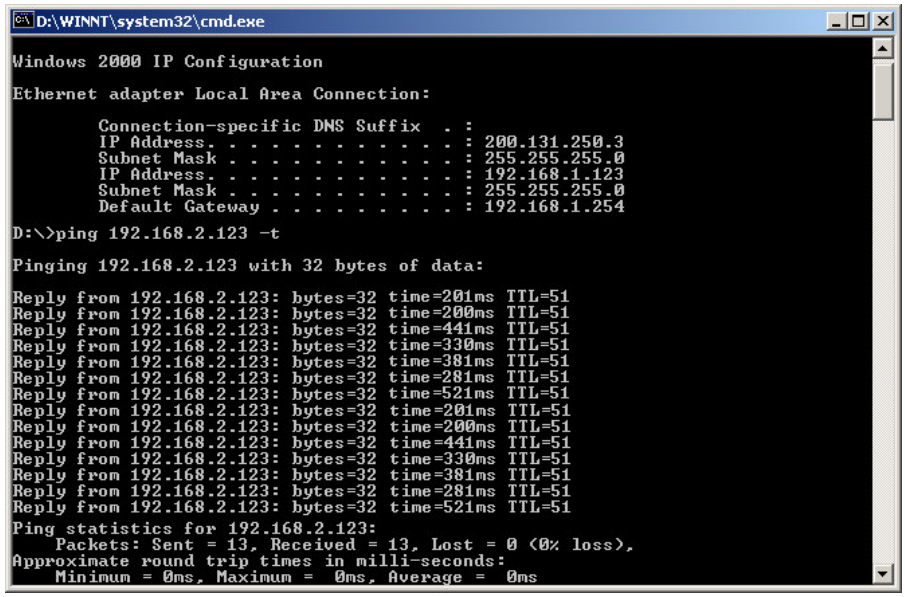

Figura 7.4 – Teste de Conexão VPN 1

Este mesmo procedimento foi repetido, porém utilizando um computador da REDE B pingando uma estação da REDE A como é mostrado na Figura 7.5.

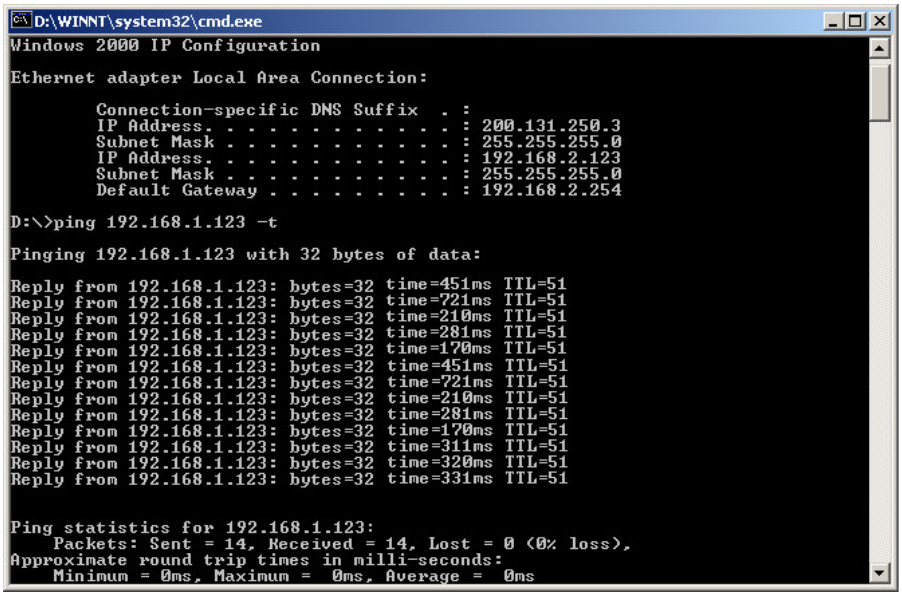

Figura 7.5 – Teste de Conexão VPN 2

7.5 Problemas com a VPN Proposta

Como explicado nos testes realizados, os roteadores e as conexões não tiveram um bom desempenho.

O problema relacionado à conexão ADSL foi a forma como é feita a autenticação dos usuários. Pois, além da conexão e autenticação PPPoE, é necessária uma autenticação adicional em um provedor de acesso (UOL, UAI, Terra, etc) para que a conexão seja liberada. Porém, o ideal para a solução proposta pelo projeto, seriam os próprios roteadores VPN ficarem responsáveis pelo estabelecimento da conexão e de qualquer tipo autenticação, não por softwares instalados em computadores da rede interna.

Os roteadores contribuíram para a instabilidade da conexão VPN, pois os mesmos não seguem o padrão brasileiro de autenticação, que foi descrito acima, mas sim de países cuja a conexão ADSL é estabelecida apenas pela conexão e autenticação PPPoE. E como o padrão brasileiro necessita de uma autenticação adicional, estes roteadores não são capazes de restabelecerem a conexão ADSL por si só, e isso prejudica seu funcionamento, fazendo com que algumas de suas funções como suporte ao DNS Dinâmico, onde poderíamos utilizar o serviço do roteador e não de um sistema cliente, não funcione corretamente.

Resumindo, devido ao padrão da conexão ADSL brasileira ou a falta de um roteador que suporte o padrão ADSL do país, a VPN baseada em conexões ADSL não tem a estabilidade para aplicações mais críticas, como autenticação de usuários e banco de dados centralizados. Pois todas as vezes que a conexão ADSL trocar seu IP, a conexão VPN será perdida, tendo assim que ser novamente conectada.

7.6 Solução Alternativa

Após ser verificado que a solução proposta não teve um bom desempenho para aplicações críticas, citaremos uma solução para estudos futuros que com garantia dos fabricantes dos roteadores, funciona adequadamente para qualquer tipo de aplicação.

Esta solução propõe que ao invés de termos todas as pontas da VPN com IP dinâmico e válido, termos na base central da VPN um conexão de internet com IP fixo e válido. A Figura 7.5, mostra um exemplo de uma matriz, onde é centralizada toda a base de dados, e duas filiais acessando a base de dados da matriz.

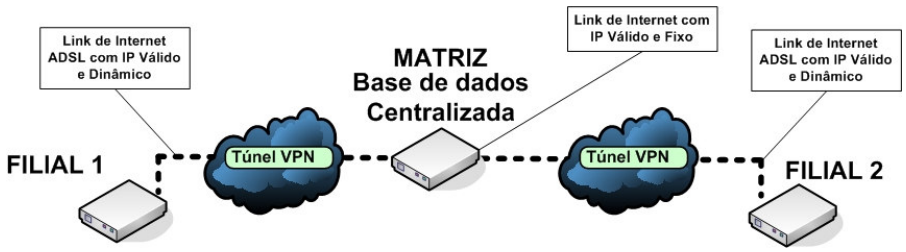

Figura 7.6 – Solução Alternativa VPN

Este tipo de solução não é baseada nas mesmas configurações dos roteadores mostrados nesse projeto, ou seja, existe uma configuração específica para este tipo de solução, e assim gerando um novo tema para estudos futuros.

8 CONCLUSÃO

O intuito de realização deste projeto foi a necessidade de se obter uma solução para interligação de redes de comunicação que estivesse ao alcance das pequenas e médias empresas e a possibilidade de testar um modelo que até então não foi implementado, podendo obter resultados positivos ou negativos.

Neste mesmo projeto foi realizado uma série de estudos para se obter parâmetros para dimensionar p projeto de uma VPN, e assim podendo definir de forma correta quais tipos de serviços e equipamentos adequados para cada situação. Além disso foi implementada uma solução de VPN com links ADSL, e isso gerou um desafio muito grande por ser uma tipo de solução não implementada no Brasil, contribuindo assim para a formação de uma literatura brasileira.

Outra aspecto mostrado neste projeto foi todo o procedimento de configuração dos softwares e dos roteadores, definindo quais as melhores configurações de criptografia e algoritmos de autenticação para serem utilizados na solução proposta.

Após a implantação e testes da interligação de redes de comunicação através de VPN baseadas em links ADSL, foi possível constatar na prática a instabilidade deste tipo de solução. Possivelmente devido a algumas limitações de recursos dos roteadores utilizados no projeto e principalmente devido a algumas deficiências do padrão de conexão ADSL brasileiro.

Apesar dos resultados mostrarem que a solução apresentada não obteve um bom desempenho, este projeto se mostrou de grande valia, pois foram definidos alguns parâmetros que servem como base para o dimensionamento de um projeto de interligação através de VPN. Outra grande contribuição deste projeto foi que até antes do mesmo não se tinha nenhuma possível justificativa para a instabilidade deste tipo de solução, e após o mesmo, obtivemos a possível causa desta instabilidade.

Uma proposta para futuros trabalhos é a análise, estudo e implantação de uma solução que proponha ao invés de termos todas as pontas da VPN com IP dinâmico e válido, na base central da VPN uma conexão de internet com IP fixo e válido e as todas as outras pontas com conexões ADSL.

REFERÊNCIAS BIBLIOGRÁFICAS

CHANDRA P.; MESSIER M.; VIEGA J. **Network Security with OpenSSL**, 1. ed. Estados Unidos da América: O'reilly, 2002, 384 p.

CHIN, L. K. **Rede Privada Virtual – VPN, Rede Nacional de Pesquisa, Rio de Janeiro** . Disponível em http://www.rnp.br/newsgen/9811/vpn.html . Acesso em 01 ago. 2004.

GAST, M. **802.11 Wireless Networks: The Definitive Guide**, 1. ed. Estados Unidos da América: O'reilly, 2002. 464p.

JACK, T. ; **CCNP: Building Cisco Multilayer Switched Networks** Copyright 2003 Sybex Inc.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma nova abordagem;** tradução de Arlete Simille Marques**.** São Paulo: Addison Wesley, 2003. 548 p. Título original: Computer networking; a top-approach featuring the internet.

MONTEIRO, E. **Segurança em redes**. Coimbra, Portugal, 1999, Capítulo 1. Disponível em: http://eden.dei.uc.pt/~sr/Teoricas/. Acesso em: 05 dez 2004.

PUTTINI, R. S. **Principais aspectos na Segurança de Redes de Computadores**. 2002. Disponível em: https://www.redes.unb.br/security/. Acesso em: 05 dez 2004.

SCHNEIER, B. **Applied Cryptography: Protocols, Algorthms, and Source code in C,** 2. ed. Estados Unidos da América: John Wiley & Sons, 1996, 1027 p.

SCOOT, C.; WOLFE, P.; ERWIN, M. **Virtual Private Networks,** 2. ed. Estados Unidos da América: O'reilly, 1999, 225 p.

SOARES, L. F. G.; LEMOS, G.; COLCHER S. **Redes de computadores : das LANs, MANs e WANs as Redes ATM.** 2. ed. Rio de Janeiro: Campus, 1995. 705 p. Edição revisada e ampliada.

STEVENS, W. R. **TCP/IP illustrated : the protocols.** Reading Mass: Addison-Wesley, 1998. v. 1. 576 p. (Addison-Wesley Professional Computing Series).

STRAUCH, S. B. **Aspectos de Segurança no Protocolo IP**. 1999. 122 p. Dissertação (Metrado em Ciência da Computação) – Universidade Federal do rio Grande do Sul, Porto Alegre. Disponível em: www.modulo.com . Acesso em: 01 dez. 2004

TANENBAUM, A. S. **Redes de computadores.** Tradução de Vandenberg Dantas de Souza; revisão técnica de Daniel Schwabe. Rio de Janeiro: Campus, 1994. 786 p. Título original: Computer networks.

TORRES, G. **Redes de Computadores: Curso Completo**, 1. ed. Rio de Janeiro: Axcel Books, 2001. 664p.

VASQUES, A. T.; SCHUBER R. P. **Implementação de uma VPN em Linux utilizando o protocolo IPSec**, 2002. Disponível em: http://www.alan.pro.br/publicacoes.htm. Acesso em 01 ago. 2004.

ZWICKY E. D.; Cooper S.; Chapman D. B. **Building Internet Firewalls,** 2. ed. Estados Unidos da América: O'reilly, 2000, 890 p.

RESUMO EXTENDIDO

Nos últimos anos, com a grande necessidade de compartilhamento de recursos (Internet, impressoras, sistemas), as Empresas e Instituições de todos os portes necessitam se conectar em rede local de computadores. Porém, na atualidade, ocorre uma grande necessidade de redes locais diferentes e distantes uma das outras, serem conectadas para que uma possa usufruir os recursos da outra e vice-versa.

Com o explosivo crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação, associado a um grande aumento nas velocidades de acesso, a Internet passou a ser vista como um meio conveniente para a interligação de redes diferentes.

No entanto, a passagem de dados pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio inseguro em um meio confiável. Com essa abordagem, o uso de VPNs (*Virtual Private Network*) sobre a Internet se torna viável e adequada.

A necessidade de se implantar um mecanismo de segurança eficiente em redes públicas é de extrema importância. Pois, para podermos trafegar dados numa rede pública, onde as informações estão desprotegidas, e estas podendo ser capturadas por pessoas não autorizadas, é extremamente importante a implementação de segurança através de um VPN. E como temos que transportar informações importantes e confidenciais sobre essa tecnologia, essa implementação se torna essencial.

As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou de outras redes públicas ou privadas para transferência de informações, de modo seguro, entre redes diferentes (que podem ser ou não geograficamente distantes) ou usuários remotos.

Este projeto consistirá na Interligação de duas redes remotas através de uma VPN baseada em conexões de internet ADSL com IP dinâmico e válido, tudo isso com o intuito de se obter uma solução de interligação de filiais para pequenas e médias empresas.