ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM REDES DE COMPUTADORES

DIANA MOURA VASCONCELOS

VPN: INTERCONEXÃO ENTRE AS UNIDADES DE ENSINO

VILA VELHA – ES
2011

DIANA MOURA VASCONCELOS

VPN: INTERCONEXÃO ENTRE AS UNIDADES DE ENSINO

Monografia apresentada ao Curso de Redes de Computadores da Escola Superior Aberta do Brasil como requisito para o título de Especialista em Redes de Computadores, sob orientação da Profª. Beatriz Christo Gobbi.

VILA VELHA – ES
2011

DIANA MOURA VASCONCELOS

VPN: INTERCONEXÃO ENTRE AS UNIDADES DE ENSINO

Monografia aprovada em de de 2011.

Banca Examinadora

_____

_____

_____

VILA VELHA – ES
2011

Agradecimentos

Agradeço a Deus, pela força e saúde para poder enfrentar as dificuldades e lutar pelos meus objetivos. Aos meus familiares e amigos, pelo apoio fornecido em todo momento.

Finalmente, agradeço ao orientador e a todos os tutores, cujos conhecimentos transmitidos, através das disciplinas cursadas, embasaram este trabalho e contribuíram para o meu desenvolvimento intelectual e, conseqüentemente, possibilidade de uma boa capacitação profissional.

RESUMO

O trabalho que segue descreve o projeto de uma interconexão de computadores, baseada na arquitetura cliente-servidor, entre máquinas clientes, localizadas nas Unidades Municipais de Ensino, e uma máquina servidores, fixada nas Secretarias Municipais de Educação, tomando por base o estudo realizado na situação atual do município de Aracaju, que reflete a realidade da estrutura de trabalho na estrutura educacional de todo o País. Inicialmente, o trabalho contempla um estudo sobre redes de computadores, hardware e software de redes de computadores, interconexão de redes, segurança em redes, tunelamento, criptografia e seus algoritmos e redes privadas virtuais (VPNs) e suas características. Em seguida, traz uma explanação da situação atual da administração escolar no município, evidenciando a demanda e os benefícios da interconexão projetada, e a apresentação da solução a ser adotada, bem como descrição de sua implementação em um cenário experimental. Evidenciando, por fim, as razões que indicaram a escolha da VPN como solução ideal e demais resultados obtidos com o trabalho.

Palavras-Chave: Redes Privadas Virtuais, Redes de Computadores, Segurança, Tunelamento e Criptografia.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O uso de soluções informatizadas vem se propagando nas mais diversas atividades humanas, justificado pela facilidade e agilidade na manipulação de grandes quantidades de informações, bem como pela capacidade de compartilhamento e mobilidade dos dados, introduzidas pelo advento das redes de computadores e, em particular, da Internet.

De maneira geral, com o avanço da informática, é comum uma empresa que possua uma ou várias filiais e necessitar de uma comunicação entre elas. Entretanto, na maior parte dos casos, estas ligações são dificultadas, principalmente pelo fator financeiro e, em alguns casos, devido à grande distância existente entre elas.

No caso particular das unidades de educação, em que são usados sistemas manuais para execução das tarefas administrativas, recaindo em processos lentos e extremamente burocráticos. Considera-se importante viabilizar o desenvolvimento de sistemas informatizados, a fim de automatizar parte destas tarefas administrativas, melhorando o processo de execução das mesmas. Para tanto a principal demanda é o estabelecimento de alguma forma de conexão entre as unidades escolares e a unidade administrativa á qual se reportam, que em geral é designada de secretaria de educação, seja no âmbito municipal ou estadual.

Atualmente, a *Virtual Private Network* (VPN) ou Rede Privada Virtual é uma das formas mais usada para se unir diferentes redes de uma organização, utilizando para isso um meio público, quase sempre a Internet, para transferir os dados. Sua principal característica é a criação de “túneis virtuais” entre essas redes, estabelecendo um canal de comunicação seguro.

1.1 O PROBLEMA

O presente trabalho busca responder à questão: Como interligar as unidades de ensino de uma mesma região, provendo uma comunicação eficaz, segura e capaz de suportar a heterogeneidade das possibilidades de conexão a serem encontradas em cada unidade?

1.2 OBJETIVO GERAL

O objetivo principal desse trabalho é estudar a interligação das unidades de ensino de uma mesma região, provendo uma comunicação eficaz, segura e capaz de suportar a heterogeneidade das possibilidades de conexão a serem encontradas em cada unidade.

1.3 OBJETIVOS ESPECÍFICOS

- Discutir sobre redes de computadores, segurança em redes e implementação de VPN em Linux Ubuntu 10.10 e Windows 2003 Server;
- Identificar uma solução que atendam à implantação da interconexão, considerando os requisitos levantados;
- Definir como implementar uma VPN entre as unidades envolvidas, utilizando a Secretaria de Educação como estação servidora e as demais unidades como clientes, considerando a utilização tanto do sistema operacional Windows e Linux.

1.4 JUSTIFICATIVA

Utilizar uma VPN permite o compartilhamento de arquivos e a utilização de aplicativos de produtividade e gerenciamento, fornecendo o acesso à rede interna da organização de qualquer local em que haja uma conexão com a internet. Tal

conexão é demandada pela implantação de sistemas informatizados de apoio às atividades escolares e administrativas da secretarias e de suas unidades de ensino.

1.5 METODOLOGIA

A realização do trabalho será iniciada por um estudo sobre os conceitos que envolvem a redes de computadores, interconexão de redes, segurança em redes, tunelamento, criptografia e algoritmos de criptografia.

A seguir será feita uma contextualização com a descrição da situação atual, tomando como base o município de Aracaju/SE, através da observação pessoal e de entrevista com o responsável pela Coordenação de Tecnologia da Informação da Secretaria Municipal de Educação, deste município, durante o mês de novembro de 2010. Em seqüência, apresentar-se-á a solução proposta, qual seja aquela que, com base nos estudos realizados anteriormente, melhor atenda aos requisitos levantados.

A terceira etapa será a descrição e o estudo da montagem de um cenário experimental, que valide a solução escolhida, utilizando-se de máquinas virtuais, para documentar os passos necessários à implementação da solução recomendada.

2 REDES DE COMPUTADORES E SEGURANÇA

Nesta seção serão expostos os principais conceitos que fundamentam a aplicação das técnicas e ferramentas utilizadas neste projeto, tais como: redes de computadores, arquitetura e equipamentos de redes, Internet, segurança em redes, tunelamento e criptografia.

2.1 REDES DE COMPUTADORES

As redes de computadores foram iniciadas na década de 60, inicialmente para suprir uma necessidade, militar durante a chamada Guerra Fria (1945-1991), entre os Estados Unidos da América e a União Soviética. Neste período os americanos iniciaram grandes pesquisas, em busca de uma forma de interconectar os vários centros de comando do país, de modo que o seu sistema de informações fosse robusto, ou seja, que continuasse funcionando mesmo que houvesse um conflito nuclear (MIRANDA, 2008).

A expansão do uso de redes computadores foi iniciada em 1970 nos Estados Unidos onde, foram escolhidas de quatro Universidades para serem conectadas na rede computacional ARPANET[1]. Além da comunidade acadêmica, a rede original atendia também à comunidade militar americana. A rede se expandiu rapidamente, incluindo com sucesso computadores de variadas plataformas e, assim, demonstrando que a comunicação entre sistemas de concepções diferentes, era possível. E assim, muitas empresas começaram a ver nessa rede uma saída para a limitação ao uso de computadores que era, até o momento, a falta de comunicação elas (FAVARETO, 2008).

[1] ARPANET - Primeira rede nacional de computadores criada em 1969 pelo Departamento de Defesa (DoD) dos Estados Unidos de Norte América para garantir a segurança em caso de acidente nas comunicações.

Usuários individuais de sistemas de computação não trabalham isolados e necessitam de alguns dos benefícios oferecidos por um sistema centralizado. Assim, o desenvolvimento de ambientes de trabalho cooperativos tornou-se uma realidade tanto nas empresas como nas universidades, incrementando o uso de soluções informatizadas, em que a demanda por troca de informações entre os computadores, exigia a interconexão dos equipamentos nessas organizações.

Para tanto os pesquisadores criaram novas arquiteturas, que propunham a distribuição e o paralelismo como forma de melhorar desempenho, confiabilidade e modularidade dos sistemas computacionais. A idéia de redes de computadores começava a se formar.

De forma simplificada, uma rede é um sistema que permite a comunicação entre unidades computacionais instaladas em pontos distintos, ou seja, um sistema que permite a troca de informações entre computadores. Neste sentido, os componentes básicos de uma rede são um emissor (origem da informação), o meio através da qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem ou a informação que se deseja transmitir.

Rede de computadores é um conjunto de computadores autônomos interconectados, trocando informações entre si, através de algum meio como, por exemplo, um fio de cobre, fibras ópticas, rádio, microondas ou satélites de comunicação (TANENBAUM, 1997). Assim, o conceito de redes de computadores inclui todos os equipamentos e aplicativos necessários à interconexão de dispositivos. Esses dispositivos que se comunicam entre si podem ser chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede.

Os usos mais tradicionais de redes de computadores estão nas atividades empresariais, comerciais, acadêmicas e até pessoais. Em empresas com uma quantidade significativa de microcomputadores, o advento das redes de computadores surge como uma excelente estratégia para o compartilhamento de recursos e para fornecer mobilidade da informação. Particularmente no caso da

informação, vale ressaltar que atualmente, com a popularização dos microcomputadores, qualquer empresa de médio a grande porte utiliza informações computadorizadas (TANENBAUM, 2003).

Neste sentido, o uso das redes de computadores vem facilitar o acesso e o armazenamento das informações, de forma que várias máquinas podem acessar e manipular uma mesma base de dados localizada em um dos computadores desta rede, garantindo a integridade e eliminando a redundância que existiria no caso de cada máquina possuir a sua base de dados individual, como ocorria antes das redes existirem.

Embora não haja um critério bem definido para se classificar as redes, elas podem ser qualificadas quanto a sua natureza, em dois tipos: cliente-servidor (*client-server*) e ponto-a-ponto (*peer-to-peer*). As redes cliente-servidor possuem dois módulos básicos: o Servidor e o Cliente. O módulo servidor é composto por uma ou mais máquinas, responsáveis por servir aos Clientes da rede com aquilo que é solicitado. O módulo cliente, por máquinas que solicitaram informações ou recursos que estarão contidas no Servidor. Exemplos de serviços oferecidos aos clientes são: controle de usuários, aplicativos, filas de impressão, armazenamento de arquivos, que sendo gerenciados como uso de sistemas operacionais específicos para esta atividade. As máquinas que requerem esses serviços são chamadas de clientes ou *hosts*, e as máquinas que os fornecem são chamadas de servidores (MIRANDA, 2008).

Já na rede ponto-a-ponto não existem servidores, todas as estações compartilham seus recursos mutuamente, sendo clientes e servidores ao mesmo tempo. Dessa forma, possuem as vantagens de uma implementação simples e de os computadores funcionarem normalmente independente da rede. No entanto, apresentam deficiências de segurança, em relação ao controle de acesso aos recursos, e de tolerância a falhas, levando à indisponibilidade de recursos em caso de falhas no computador que o hospeda. Há também uma limitação quanto ao crescimento, pois não é possível estendê-las muito (MORIMOTO, 2004).

Assim, o modelo mais comumente adotado por empresas são as redes cliente-servidor, tendo as redes ponto-a-ponto pouca utilização.

2.2 ARQUITETURA DE REDES

Os projetos iniciais de redes de computadores eram focalizados na estruturação do hardware, deixando o software de lado. Na atualidade isto já não acontece, nas últimas décadas cresceu a preocupação com o software de rede, que se apresenta altamente estruturado (TANENBAUM, 2003).

Para reduzir a complexidade dos projetos, na maioria das redes adota-se uma organização em camadas para o software de rede. Assim, ao conjunto de camadas e protocolos que estruturam o software de uma rede dá-se o nome de arquitetura de rede. Os modelos que influenciam as arquiteturas de redes praticadas atualmente apresentam uma estrutura montada em camadas, como pilhas de protocolos. São eles: o modelo OSI (*Open Systems Interconection* – Interconexão de Sistemas Abertos), desenvolvido pela ISO (*International Standards Organization* – Organização Internacional de Padrões), que possui sete camadas e o modelo TCP/IP, assim chamado graças a seus dois principais protocolos e que, por usa vez, possui apenas quatro camadas (TANENBAUM, 2003).

No modelo OSI, as camadas são distribuídas uma acima da outra, hierarquicamente, de acordo com a função que desempenham. Uma entidade é um elemento ativo em uma camada. Duas entidades em uma mesma camada são denominadas entidades pares. As entidades de uma camada prestam serviços às entidades da camada imediatamente acima e, por sua vez, recebem serviços da camada situada imediatamente abaixo. Nessa dinâmica, as camadas adjacentes, se comunicam através de interfaces, que definem quais informações deverão passadas de uma pra outra e como elas estarão estruturadas Por exemplo, considerando a ilustração 1, as entidades da camada de apresentação prestam

serviços à camada de aplicação e recebem serviços da camada de sessão (MIRANDA, 2008).

A idéia básica do modelo de referência OSI é que cada camada seja responsável por algum tipo de processamento. Assim no momento da transmissão de dados para a rede, os dados partem da camada mais alta (aplicação) e vai sendo repassado cada por camada. Cada camada recebe dados da camada superior, acrescenta suas informações de controle e passa os dados para a camada imediatamente inferior. Já na recepção acontece o processo inverso, os dados iniciam na camada mais baixa (física), e cada camada recebe dados da camada inferior, processa os dados recebidos removendo informações de controle pelas quais ela seja responsável e passa os dados para a camada imediatamente superior. Em resumo, cada camada adiciona (quando o computador estiver transmitindo dados) ou remove (quando o computador estiver recebendo dados) informações de controle de sua responsabilidade (TORRES, 2007).

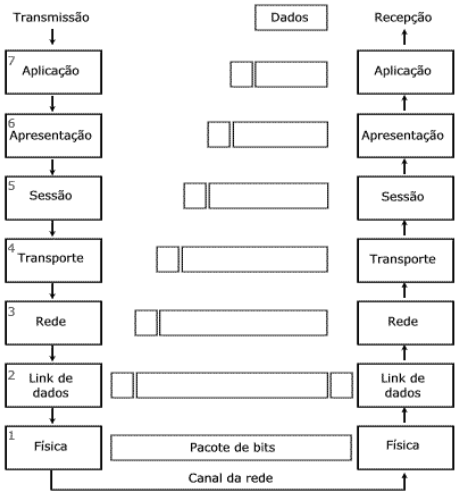

Ilustração 1 - Comunicação Host a Host na arquitetura em camadas
Fonte: MIRANDA (2008)

Pode-se dizer que o modelo OSI é apenas uma referência, não possuindo implementação concreta, seu objetivo é fornecer uma base comum para o desenvolvimento de padrões para a interconexão de sistemas. Nesse contexto, tem-se o modelo TCP/IP, um padrão fisicamente implementado, baseado na

arquitetura OSI e que é a base da internet e demais redes em funcionamento atualmente, sendo, por isso, detalhado na subseção seguinte (MIRANDA, 2008).

2.2.1 Modelo TCP/IP

Este modelo é um conjunto de protocolos desenvolvidos para permitir que computadores compartilhem recursos dentro de uma rede. A arquitetura TCP/IP surgiu da necessidade de expansão da ARPANET, que se formava como uma rede que permaneceria intacta caso um dos servidores perdesse a conexão, e para isso, necessitava de protocolos (robustos) que assegurassem tais funcionalidades trazendo confiabilidade, flexibilidade e que fosse fácil de implementar. Em uma definição mais básica, o nome correto para este conjunto de protocolos é “Conjunto de Protocolos para a Internet". Os protocolos TCP e IP são dois dos protocolos deste conjunto. Como os protocolos TCP e IP são os mais conhecidos, é comum se referir a TCP/IP para referenciar toda a família de protocolos. (MIRANDA, 2008).

Por essa razão, de acordo com FAVARETO (2003), o projeto do modelo TCP/IP, foi concebido com priorização das seguintes características:

- **Boa recuperação de falhas -** a rede deveria funcionar mesmo que alguns componentes ficassem indisponíveis;
- **Novas Sub-Redes podem ser conectadas rapidamente** - a conexão de novas redes deveria ser feita sem parar o serviço em execução;
- **Manipulação de Taxas de Erros Altas -** O serviço deve ser capaz de tolerar taxas de erro altas ou imprevisíveis, e ainda nessas condições, fornecer um serviço extremamente confiável.
- **Independência de Host -** o serviço de conexão deveria funcionar independente do fornecedor ou marca dos equipamentos;

Além da robustez, era necessária uma arquitetura flexível e capaz de oferecer vários serviços, como transmissão de arquivos e voz (TANENBAUM, 2003). Assim, foram definidas, conforme ilustração 2, as seguintes camadas:

- **Física/ Enlace –** esta camada trata da transmissão dos pacotes IP entre as unidades da rede ou entre redes, embora o modelo não defina qual o protocolo utilizado para isso, podendo ele variar entre *hosts* e entre redes;
- **Rede –** deve permitir que os *hosts* enviem pacotes pela rede que irão trafegar, ou seja, o roteamento, independentemente e chegar ao seu destino, mesmo que de forma desordenada, neste caso as camadas superiores são responsáveis pela ordenação, se for exigido. Para tal esta camada define um formato de pacote e de endereçamento universais e um protocolo para cumprir a função a ela empregada, o IP, que será apresentado na subseção seguinte;
- **Transporte –** a função básica desta camada é permitir a conversação entre a origem e o destino das mensagens transmitidas. Para isto define dois protocolos: o TCP e o UDP (*User Datagram Protocol* – Protocolo de Datagrama do Usuário). O TCP é confiável e orientado a conexão, assim, garante a entrega sem erros de um fluxo de bytes entre máquinas da rede e também controla o fluxo, para tratar a diferença de velocidade entre emissor e receptor. Já o UDP não é orientado e não oferece controle de fluxo nem da seqüência dos pacotes transmitidos;
- **Aplicação –** esta camada contém os protocolos de mais alto nível, responsáveis pelos serviços oferecidos aos usuários, dentre os quais encontram-se: o FTP para transferências de arquivos, o SMTP para correio eletrônico, o TELNET para acesso remoto, o http para navegação de hipertextos na Internet e alguns outros;

A idéia por trás do TCP/IP é exatamente a mesma que a do modelo de referência OSI: a comunicação fim-a-fim de cada camada com a sua correspondente, do transmissor ao receptor (TORRES, 2007). A principal diferença entre eles está na pilha de camada, pois o TCP/IP tem duas camadas que se formam a partir da

fusão de algumas camadas do OSI, elas são: as camadas de Aplicação, que engloba as funções das camadas: Aplicação, Apresentação e Sessão (OSI); e Rede, que encarrega-se das atividades relativas às camadas Link de dados e Física (OSI), conforme apresentado na ilustração 2 (MIRANDA, 2008).

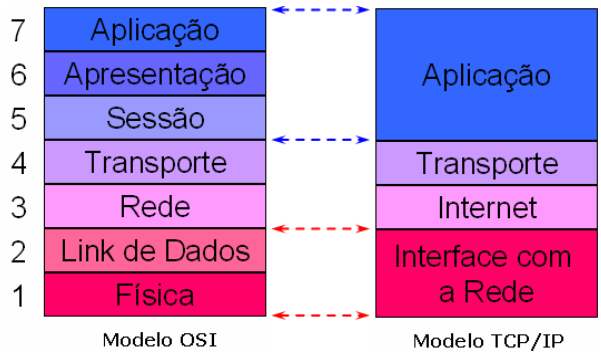

Ilustração 2 - Arquitetura TCP/IP em quatro camadas
Fonte: MIRANDA (2008)

2.2.1.1 O Protocolo IP

Sendo o protocolo da camada de rede do modelo TCP/IP, pode-se definir a tarefa do IP como fornecer a melhor forma de transportar pacotes da origem para o destino, independente de essas máquinas estarem na mesma rede ou em outras redes intermediárias (TANENBAUM, 2003). É importante expor algumas das principais características do protocolo IP:

- Não é orientado a conexão;
- O checksum, mecanismo de controle de integridade, confirma apenas a integridade do cabeçalho do pacote;
- A responsabilidade dos dados contidos no pacote do IP é tarefa de protocolos de mais alto-nível;
- Esconde a arquitetura física da rede;
- Cria identificadores universais - Endereços IP;

- Define unidade de transferência do protocolo - Datagramas IP;
- Faz encaminhamento da informação, mas fornece um serviço não confiável, de comunicação entre máquinas

Todo protocolo da camada de rede define um tipo de endereçamento para identificar o computador e a rede. O IP tem um endereço formado 32 bits, em que traz o ID (identificador) da Rede e o ID do computador dentro da rede específicada. Os 32 *bits* endereço IP são divididos em 4 octetos, ou 4 *bytes*, que, em formato binário (sistema numérico de base 2) são de difícil manipulação pelos seres humanos é bastante difícil, por isso é comum a conversão para o base decimal, tornando-se mais legível e facilitando o seu mapeamento (MIRANDA, 2008). Dessa forma, por exemplo, o endereço IP de 32 bits, que na base binária seria indicado pela seqüência 11111111.11111111.11111111.00000001, pode ser representado por quatro números na base decimal: 255.255.255.0.

2.2.1.2 O Protocolo TCP

Sendo protocolo da camada de transporte, o TCP tem a função de oferecer um fluxo de bytes fim a fim, confiável, por meio de uma inter-rede não confiável (TANENBAUM, 1997). Para tanto este protocolo tem como principais características:

- Estabelece canais virtuais com ligação máquina a máquina;
- Fornece um serviço confiável;
- Fornece comunicação nos dois sentidos em simultâneo (full-duplex);
- Realiza controle de fluxo através do uso de buffer para armazenamento dos dados enviados e recebidos.
- Implementa o conceito de portas dando capacidade de distinguir mensagens de múltiplos destinos para uma mesma máquina;

- Garante a entrega dos pacotes e assegura o seqüenciamento correto dos mesmos;
- Seu checksum valida o cabeçalho e os dados;
- É o responsável pela retransmissão de um pacote faltoso, perdido ou estragado;
- Requer que o destinatário informe o recebimento do pacote;

É importante frisar que seus serviços de confirmação geram tráfego adicional na rede, diminuindo a taxa de transferência de dados em favor da confiabilidade. Por isso, o modelo TCP/IP, tem como alternativa o protocolo UDP, que pode ser usado em ocasiões em que, não são necessários todos os recursos do protocolo TCP. O UDP foi designado para aplicações em que não é necessário enviar seqüências longas de datagramas. Ele trabalha como o protocolo TCP, porém ele não divide os dados em múltiplos datagramas, e o cabeçalho inserido por ele é muito menor do que aquele inserido pelo TCP. Além disso, o protocolo UDP opera no modo sem conexão e fornece um serviço de datagrama não confiável, só mantém controle sobre os dados enviados, sendo, portanto, uma simples extensão do protocolo IP (MIRANDA, 2008).

2.3 PRINCIPAIS TIPOS DE REDE

Pode-se distinguir os diversos tipos de rede de acordo com a topologia e a tecnologia de transmissão utilizada. A topologia refere-se à forma estrutural como os computadores são interligados entre si ou com o meio de transmissão, de forma a se comunicarem. De acordo com MIRANDA (2008), existem três topologias básicas:

- **Barramento** – ilustração 3-a, em que os computadores são ligados seqüencialmente como uma fila ao longo de um único meio de transmissão, disposto de forma linear;

- **Estrela** – ilustração 3-b, onde todos os computadores são conectados por cabos separados e um ponto central único, como um concentrador;
- **Anel –** ilustração 3-c, em que os computadores são conectados a um único cabo, disposto de forma circular.

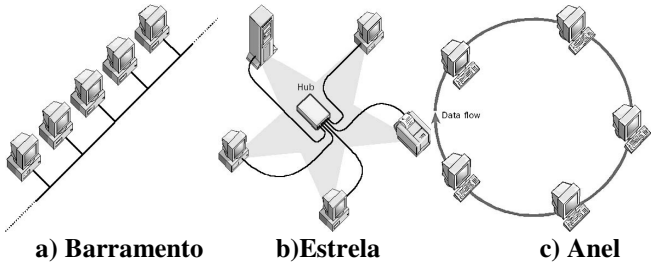

Ilustração 3 - Topologias de Rede
Fonte: Elaboração própria (2010)

Já a tecnologia de transmissão, refere-se à forma como as máquinas se comunicam, existindo, conforme TANEMBAUM (1997), duas maneiras básicas:

- **Redes de difusão** - consistem no compartilhamento de um único canal de comunicação por todas as máquinas;
- **Redes ponto a ponto** – consistem em muitas conexões entre pares de máquinas individuais;

Em redes de difusão, as máquinas são identificadas por um endereço, que referencia cada máquina unicamente. Nesta tecnologia, as mensagens trocadas entre máquinas são geralmente chamadas de pacotes. Quando uma máquina deseja enviar uma mensagem a alguma outra, ela deve adicionar ao pacote o endereço da máquina destino. Considerando que o meio de transmissão é compartilhado, o pacote será recebido por todas as máquinas e elas olharão o endereço do destinatário nele contido. Dessa forma, somente a máquina à qual se destina o pacote irá processá-lo e receberá a mensagem.

Já nas redes ponto a ponto, para ir de sua origem ao destinatário, um pacote pode precisar passar por algumas máquinas intermediárias, que receberão o pacote e o repassarão, desde que elas sejam seu destino. É importante frisar a possibilidade de existir vários caminhos para se chegar se uma máquina a outra. Assim, os algoritmos de roteamento são extremamente importantes neste tipo de tecnologia.

Outro critério que pode ser usado para diferenciar os diversos tipos de rede é a escala, ou seja, o nível de abrangência da conexão. De acordo com este critério, segundo FAVARETO (2003), pode-se obter quatro tipos de redes de computadores, conforme caracterização a seguir.

2.3.1 Redes Locais - LANs

As redes locais, conhecidas como LANs (*Local Área Network*), são redes privadas contidas em pequenas áreas geográficas, com até alguns quilômetros de extensão, como um campus universitário, um edifício ou um escritório. As LANs têm três características que as distingui de outros tipos de rede: o tamanho, pois elas têm o tamanho restrito; a tecnologia de transmissão, pois se baseiam na tecnologia de difusão; e a topologia, uma vez que admitem diversas topologias, através da qual se pode determinar a distribuição das unidades de rede e do cabeamento utilizado, e definir o modo como os computadores se comunicam (FAVARETO, 2003).

2.3.2 Redes Metropolitanas - MANs

Conhecidas como MANs (*Metropolitan Area Network*), as redes metropolitanas são uma versão ampliada das LANs. Têm em geral as mesmas características das LANs, porém podem utilizar dois cabos de transmissão e não possuem elementos de comutação. Por isso, são padronizadas por uma especificação especial a 802.6, que consiste em dois barramentos aos quais os computadores

são conectados. Há uma outra padronização que se refere a MANs, a 802.16, do IEEE, que trata se acesso à internet sem fio a alta velocidade (FAVARETO, 2003).

2.3.3 Redes Geograficamente Distribuídas - WANs

As WANs (*Wide Area Network*), como são também chamadas as redes geograficamente distribuídas, atuam em amplas áreas geográficas, chegando a abranger um país ou mesmo um continente. Estas redes são compostas por conjuntos de máquinas cliente, chamadas de *host*, cuja finalidade, em geral, é executar alguma aplicação, conectadas por uma sub-rede. Esta sub-rede consiste em dois componentes distintos: linhas de transmissão, que transportam as informações entre as máquinas e são, em geral, linhas administradas por uma operadora telefônica que atua em toda a região, e os elementos de comutação, que são computadores que interligam duas ou mais linhas de transmissão, fazendo o trabalho de roteadores (FAVARETO, 2003).

2.3.4 Inter-Redes

Chama-se inter-rede o conjunto de redes interconectadas. Um caso particular e mais comum de inter-rede é a rede mundial de computadores ou Internet. Em geral, uma inter-rede pode ser vista como várias LANs interconectadas por uma WAN, o que permite que máquinas em LANs distintas possam se comunicar. No entanto, para isso, é preciso, como foi visto nas WANs, que algumas máquinas sirvam de comutadoras, para permitir a comunicação de toda LAN a que pertence com a WAN que as interliga.

Não há, ainda um consenso quanto estas terminologias utilizadas para definir as redes e, por isso, os conceitos de sub-rede e inter-redes se confundem. Um ponto de vista é aplicar a denominação sub-rede, quando se trata de redes fisicamente distribuídas, formando um conjunto de máquinas, roteadores e canais de

comunicação, sendo as inter-redes conexão entre diferentes redes – uma de difusão e outra ponto a ponto, por exemplo – estão conectadas (TANENBAUM, 1997).

2.4 CABEAMENTO ESTRUTURADO

A grande maioria das redes corporativas utiliza-se de cabos como meio de transmissão, transportando sinais entre as unidades de rede, computadores e ativos. Existem diversos tipos de cabo com características distintas para atender às necessidades de cada estrutura ou topologia de rede.

A padronização 802.3 do IEEE sobre cabeamento, o padrão 802.3, descreve os tipos de cabeamento adequados para projetos de rede *ethernet*, padrão mais difundido, com especificações de distancia máxima e tipo de topologia ao qual se adaptam, conforme a tabela 1[2].

Estas estruturas de cabeamento que operacionalizam fisicamente a norma 802.3, são normativamente identificadas segundo a convenção TT base D, para sinais digitais, ou TT broad D, para sinais analógicos. Nesta convenção, TT representa a transmissão nominal da estrutura, em Mbit/s, e D, o comprimento máximo de cada segmento de rede, em centenas de metros. Os segmentos podem ser interligados por repetidores, sendo que há um limite para o comprimento máximo de toda a rede, designado pelo parâmetro domínio de colisão, que é especificado para cada tipo estrutura.

Inicialmente trabalhou-se com as estruturas de 10Mbit/s, em seguida surgiram as estruturas 100baseT, 2ª geração do padrão *Ethernet*, conhecidas popularmente como *Fast Ethernet*, que utilizam taxas de transmissão de 100 Mbit/s, introduziram modificações no nível físico, mas mantiveram a compatibilidade com os níveis superiores das versões a 10 Mbit/s. Existem duas implementações distintas para o *fast ethernet*: a 100baseT4, que são suporta comunicação *full-*

[2] Adaptada da fonte: http://www.dei.isep.ipp.pt/~andre/documentos/ethernet.html

duplex[3], implementação atualmente em desuso, que fora substituída pelas 100baseTX e 100baseFX que utilizam apenas dois pares de cobre com blindagem ou duas fibras ópticas e suportam *full-duplex*. Com o advento da fibra ótica, o padrão *Ethernet* já chegou em sua terceira geração, a *Gigabit Ethernet*, com velocidades de até 1 Gbit/s e comunicação *full-duplex* (SOARES NETO, 1999).

Tabela 1 - Principais Estruturas de Cabeamento do Padrão 802.3

Identificação	Taxa Transm.	Comp. Max. Segmento	Meio Físico	Conector e Cablagem	Topologia Física
10base5	10 Mbit/s	500 m	coaxial 50 Ω grosso	não existe	Barramento
10base2	10 Mbit/s	185 m	coaxial 50 Ω fino	BNC	Barramento
10broad36	10 Mbit/s	1800 m	Coaxial CATV 75 Ω	-	Barramento
10baseT	10 Mbit/s	100 m	Par trançado não blindado (UTP)	RJ-45	Estrela
10baseFL	10 Mbit/s	1000 m	1 par de fibras óticas	ST	Estrela
100baseT4	100 Mbit/s	100 m	4 pares trançados UTP	RJ-45	Estrela
100baseTX	100 Mbit/s	100 m	2 pares trançados blindados (STP)	RJ-45	Estrela
100baseFX	100 Mbit/s	100 m	1 par de fibras óticas	ST	Estrela
1000baseT	1 Gbit/s	100m	4 pares trançados UTP	RJ-45	Estrela
1000baseSX	1 Gbit/s	550 m	Fibra multimodo	ST	Estrela
1000baseLX	1 Gbit/s	3 Km	Fibra monomodo	ST	Estrela
1000baseCX	1 Gbit/s	25 m	Bi-axial	-	Estrela

Fonte: Adaptada de http://www.dei.isep.ipp.pt/~andre/documentos/ethernet.html

De acordo com a tabela 1, os tipos de cabeamento mais utilizados são os cabos coaxiais, par trançado e a fibra óptica, bem como suas principais características como limite máximo de seguimento, taxa de transmissão, e topologia a que é

[3] Transmissão e recepção simultâneas - Mais eficiente em enlaces entre s*witches* e entre um s*witch* e um servidor, nos quais o tráfego é continuamente pesado em ambas as direções.

aplicável. A apresentação dessas informações valida as limitações físicas de uma rede cabeada, de acordo com tipo de cabeamento utilizado.

2.5 INTERNET

Apesar da atual popularização da Internet, ela teve início com o já citado surgimento das redes de computadores no final da década de 50, no auge da Guerra Fria, com o objetivo de proteger e transferir informações vitais na eventualidade de um ataque nuclear por parte da antiga União Soviética (FAVARETO, 2003).

Em 1957, o Departamento de Defesa dos Estados Unidos criou a ARPA (*Advanced Research Project Agency*), que, no início da década de 60, criou a ARPANET, conectando vários centros de pesquisa norte-americanos (MIRANDA, 2008).

Em virtude da rápida expansão da ARPANET, o protocolo de comunicação utilizado já não estava mais suprindo as necessidades desta rede. Foi então que, após intensa atividade de pesquisa na década de 70, surgiu o conjunto de protocolos que até hoje é a base da Internet, conhecido como TCP/IP (FAVARETO, 2003).

Em 1985, a NSF (*National Science Foundation*) interligou os seus supercomputadores, formando a NSFNET (NSF *Network*), que, no ano seguinte, interligou-se à ARPANET. A união dessas redes passou a ser conhecida oficialmente como Internet (MIRANDA, 2008).

No Brasil, a Internet chegou em 1988, através das comunidades acadêmicas de São Paulo e do Rio de Janeiro. No ano de 1989, foi criada a RNP (Rede Nacional de Pesquisa), instituição com o objetivo de coordenar os serviços de acesso à Internet no Brasil (MIRANDA, 2008).

Daí até os dias de hoje o uso da Internet cresceu extremamente, assim como a quantidade de serviços que são oferecidos através dela, tais como correio eletrônico, grupos de notícias e discussões, ambientes de conversação em tempo real (*chats*), troca de arquivos, divulgação de textos e documentos, entre outros. Desta forma a Internet começou a atuar nas mais diversas áreas da atividade humana como comércio, educação, pesquisa e entretenimento, por exemplo.

2.6 SEGURANÇA EM REDES

Atualmente, as grandes corporações enfrentam a necessidade de acessar e distribuir informações com outras empresas, fornecedores, filiais, clientes ou até mesmo com funcionários geograficamente distantes do seu local de trabalho.

A grande questão é que cada vez mais as empresas possuem informações sigilosas disponíveis em seus computadores, fazendo com que certos cuidados sejam necessários, a fim de protegê-las, como limitar o acesso físico e lógico aos computadores, através de mecanismos de segurança.

O desenvolvimento de técnicas destinadas a comprometer os serviços ou fornecer acesso não autorizado a dados que trafegam em redes que seguem a arquitetura TCP/IP vêm, acompanhado do crescimento exponencial da Internet e do uso constante desta arquitetura em redes coorporativas (MARQUES, 2001). Assim, a preocupação com a segurança vem tornando-se ainda maior, considerando-se o risco de informações confidenciais serem acessadas ou alteradas, caso elas não estejam bem protegidas.

Neste sentido, segurança em redes vêm sendo objeto de intensos estudos e trabalhos, nos últimos anos. Em Monteiro apud VASQUES (2005), encontra-se a seguinte definição das funções da segurança em redes de computadores:

- **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;
- **Integridade** – Assegura que os dados não serão alterados durante uma transmissão;
- **Controle de acesso –** Limita o acesso e a utilização de recursos apenas a pessoas autorizadas;
- **Disponibilidade –** Mantém os recursos disponíveis, mesmo em caso de ataques;
- **Não-repúdio –** Impede que uma entidade (computador, pessoa, etc.) envolvida em uma transação negue a sua participação no evento.

Dessa forma, nos últimos anos vêm surgindo várias técnicas e tecnologias, que operacionalizam estas funções, e que devem ser utilizadas quando se deseja proteger as informações que trafegam numa rede privada. Dentre as quais são relevantes a este trabalho aquelas expostas nas sub-sessões seguintes.

2.6.1 Firewall

O *Firewall* é uma combinação de hardware e software, cujo objetivo é controlar o trânsito de informações entre as redes privadas e a Internet, como se houvesse uma barreira entre ambas, de modo que os acessos não autorizados sejam impedidos (OLIVEIRA, 2009).

Os *Firewalls* podem ser de três tipos: filtros de pacotes, inspeção de pacotes com informações de estado e aplicativos de *Firewalls* e de *proxy*[4] . O filtro de pacotes é o tipo mais comum de *Firewall* e tem como objetivo permitir ou negar a entrada de um determinado pacote de informações em uma rede, levando em consideração o endereço IP ou a porta de origem e de destino. Possui como vantagens ser mais barato e rápido que os outros tipos de *Firewall*, uma vez que ele não se importa

[4] *Software* utilizado para permitir o acesso de uma rede à Internet, geralmente através de um `firewall`.

com o conteúdo dos pacotes. Entretanto, por fazer apenas uma filtragem superficial, sua principal desvantagem é ser mais inseguro que os demais (FAVARETO, 2003).

A inspeção de pacotes com informações de estado, além de desempenhar as funções do filtro de pacotes, inspecionam o estado da conexão, ou seja, apenas aquelas conexões previamente estabelecidas e válidas, que cumprem as condições configuradas pelo *Firewall*, têm acesso à rede. Uma de suas vantagens é não ter a necessidade de configurar cada computador dentro da rede, reduzindo os encargos administrativos. Todavia, suas configurações são complicadas e não fornecem autenticação de usuário (FAVARETO, 2003).

Os aplicativos de *Firewall* e de *proxy* são os mais complexos, pois varrem todos os dados que passam por eles, descartando os perigosos ou não autorizados e nunca deixando um computador de dentro da rede ficar exposto à redes externas. Possui como vantagens oferecer a maior segurança dos três tipos de *Firewalls*, além de autenticar as atividades dos usuários. Devido ser mais complexo, ele também é mais lento e mais caro que os demais.

2.6.2 Certificado digital

O certificado digital é um arquivo assinado eletronicamente por uma entidade confiável, chamada Autoridade Certificadora (AC). Um certificado tem o objetivo de associar a chave pública a uma pessoa ou entidade, servindo, assim, como um mecanismo para a divulgação da chave pública.

Qualquer entidade que conheça a chave pública da AC pode examinar o conteúdo e confirmar a autenticidade de um certificado emitido por esta autoridade, uma vez que a AC assina os certificados com a sua chave privada.

Dentre os dados de um certificado digital, as seguintes informações estão presentes: chave pública do usuário, número de série do certificado, nome da AC

que emitiu o certificado, a assinatura digital da AC, entre outras. A recomendação mais aceita e utilizada para a produção de certificados digitais é a X.509v3, formulada pela ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*).

2.6.3 Criptografia

A palavra 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. No contexto da segurança em redes de computadores ela garante confidencialidade, autenticidade, integridade e não-repúdio SCHNEIER apud MARQUES (2001).

O processo de criptografia em geral, baseia-se na idéia de tomar a mensagem original de um emissor, chamada texto plano e cifrá-la, utilizando uma chave e um algoritmo determinados e, desta forma, gerando um outro texto, chamado de texto cifrado. O texto cifrado é transmitido ao receptor, que uma vez recebendo-o efetuará o processo inverso e obterá o texto original, ou seja, o texto plano criado pelo emissor. É fácil notar que mesmo sendo interceptada por quem não tem autorização de lê-la a mensagem estará a principio incompreensível, exceto se o interceptador conhecer a forma de decifrá-la.

Neste sentido fica claro que deve haver uma grande preocupação quanto ao sigilo da chave utilizada. Em geral, a chave utilizada em processos de criptografia é uma combinação de bits e, dependendo da forma como a chave é utilizada, a criptografia classifica-se em:

2.6.3.1 Simétrica

Neste tipo, a mesma chave utilizada para criptografar será usada para descriptografar a mensagem. Essa chave, chamada de chave privada, deve ser previamente trocada entre o emissor e o receptor por um canal de comunicação seguro.

A principal desvantagem em se utilizar este tipo de chave deve-se ao fato de que, como apenas uma chave é utilizada para cada par emissor-receptor. Assim, é preciso uma segurança rígida sob o processo de troca de chaves e se o número de máquinas a se comunicar for muito grande, serão necessárias inúmeras chaves, o que dificultará ainda mais a gerência das mesmas (MARQUES, 2001).

No entanto, os algoritmos que utilizam este tipo de chave têm melhor desempenho que os que utilizam a chave assimétrica. Pode-se citar alguns desses algoritmos com seus respectivos tamanhos das chaves:

- ***Data Encryption Standard*** (DES) – chave composta de 56 bits.
- ***Triple Data Encryption Standard*** (3DES) – chave composta de 112 bits.
- ***Advanced Encryption Standard*** **(AES)** – chave composta de 128, 192 ou 256 bits.
- ***Blowfish*** – chave composta de até 448 bits.
- Carlisle Adams and Stafford Tavares (CAST) – chave composta de 128 ou 256 bits.
- ***Twofish*** – chave composta de 128, 192 ou 256 bits.
- ***Serpent –*** chave composta de 128, 192 ou 256 bits.

2.6.3.2 Assimétrica

A criptografia assimétrica, por sua vez, envolve o uso de duas chaves distintas. Pode-se utilizar qualquer uma das chaves para cifrar a mensagem. Entretanto, somente a chave inversa deve ser utilizada para decifrá-la. Em geral, fixa-se uma das chave para cifrar, chamada de chave pública, e a outra decifrar, chamada de chave privada. A chave púbica deve ser amplamente divulgada e será utilizada por quem desejar enviar uma mensagem cifrada ao seu proprietário.

Desta forma, se um emissor utiliza a chave pública de um determinado receptor para cifrar uma mensagem, esta só poderá ser decifrada pela chave privada que o receptor deve manter em sigilo absoluto. Assim, garante-se autenticidade e confidencialidade.

Além disso, se o emissor utilizar sua chave privada para cifrar parte da mensagem, qualquer pessoa poderá decifrá-la com sua chave pública. Este principio dá base ao que se chama se assinatura digital: o emissor assina a mensagem com sua chave privada e o receptor verifica sua assinatura com a sua chave pública, garantindo que a mensagem foi realmente emitida pelo assinante.

Como exemplo de algoritmo assimétrico, pode-se citar o RSA (*Rivest Shamir Adleman*), que utiliza chaves compostas de 512, 768, 1024 ou 2048 bits. Este algoritmo é a base da maioria das aplicações de criptografia assimétrica utilizadas atualmente, pois seus mecanismos dificultam a obtenção da chave utilizada (MARQUES, 2001).

2.6.4 *Virtual Private Network* (VPN– Rede Privada Virtual)

A tecnologia de VPNs surgiu por volta de 1997. As VPNs são redes de computadores que estão separadas fisicamente e, que através de um meio

público de comunicação – geralmente a Internet – comunicam-se de forma segura, através da utilização de criptografia.

As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em contrapartida, estas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

Neste caso, a rede privada é chamada de virtual, porque fisicamente utiliza-se de recursos públicos. O que torna sua rede privada são os protocolos de tunelamento porque não permitem que os dados que trafegam entre as extremidades do “túnel” sejam manipulados pelos demais usuários da rede pública.

Esse tipo de rede favoreceu às empresas que não tinham recursos para investir em projetos de interligação de seus escritórios, que, a fim de reduzir os custos, podem utilizar a infra-estrutura de uma rede pública, como a Internet, que já apresenta suporte completo para o tráfego dos dados e cujo acesso é simples e barato.

Porém, ao trafegar dados em uma rede pública, significa submetê-los a uma provável interceptação e até mesmo modificação dos mesmos, por parte de pessoas não autorizadas. As VPNs implementam um processo de comunicação usando criptografia e encapsulamento para tornar a transmissão de informações entre dois pontos segura.

Sua principal função é garantir uma comunicação segura entre as partes envolvidas, através de um “túnel” que simula uma comunicação ponto-a-ponto. Os protocolos de tunelamento possuem mecanismos como: autenticação, controle de acesso e criptografia que na verdade compõem as premissas básicas da VPN.

2.6.4.1 Tunelamento

A tecnologia de tunelamento surgiu antes das VPNs. O tunelamento pode ser definido como um processo de encapsular um protocolo dentro de outro, adicionando ao pacote o cabeçalho do protocolo encapsulador, conforme ilustração 4.

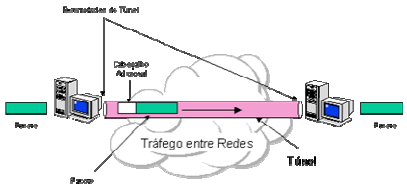

Ilustração 4 - Conceito do Tunelamento
Fonte: CHIN (1998)

Já nas redes privadas virtuais, o tunelamento adiciona um novo componente: a criptografia. O pacote além de ser encapsulado é também criptografado e enviado através da Internet ao seu destino, onde o mesmo é desencapsulado e descriptografado. Esta criptografia é realizada para que se o pacote for interceptado durante o percurso, ele não seja legível. Uma das características mais importantes em um tunelamento VPN é que pacotes de certos protocolos podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX poderão ser encapsulados e enviados por pacotes TCP/IP.

No cabeçalho adicionado no ato do encapsulamento, estarão as informações de roteamento necessárias para a transmissão dos mesmos pela rede intermediária. A rede intermediária pode ser uma rede pública ou privada. As extremidades do túnel da rede intermediária é que farão o roteamento desses pacotes. O túnel pode ser entendido como o caminho percorrido pelos pacotes ao longo da rede intermediária. Ao chegar em seu destino, os pacotes são desencapsulados e

encaminhados ao seu destino final. De acordo com Favareto (2003), existem duas estratégias de tunelamento a serem utilizadas:

- **Tunelamento Voluntário**: quando uma estação ou servidor de roteamento utiliza um software para “cliente” de tunelamento com a finalidade de criar uma conexão virtual até o servidor VPN. Este tipo de tunelamento pode requerer conexões IP através de LAN, mas geralmente é utilizado por clientes com acesso discado, que primeiro estabelecem uma conexão à Internet, para depois utilizar o software para criar o túnel. Neste caso, o computador do usuário funciona como “cliente” do túnel e como uma das extremidades do túnel, ou seja, o “cliente” passa a ser o fim do túnel, conforme a ilustração 5;

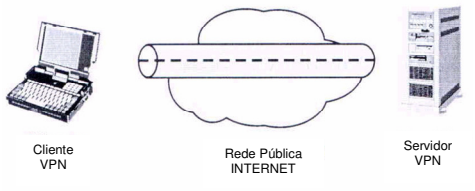

Ilustração 5 - Modelo do Tunelamento Voluntário
Fonte: CHIN (1998)

- **Tunelamento Compulsório**: quando existe um servidor NAS (Servidor de Autenticação de Rede) na rede. A configuração de autenticação é de responsabilidade deste servidor. Assim, o fim do túnel não será o computador do cliente e sim o servidor NAS, que estará localizado entre o computador do cliente e o servidor do túnel. Será através deste servidor de autenticação de rede que as informações da outra rede serão acessadas pelos clientes, conforme ilustração 6.

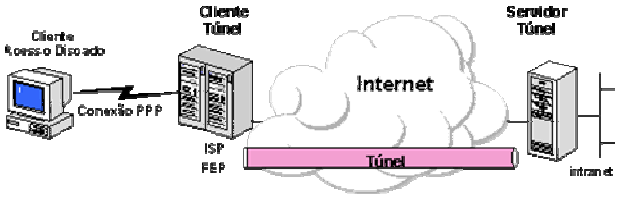

Ilustração 6 - Modelo de Tunelamento Compulsório
Fonte: CHIN (1998)

2.6.4.2 Topologias VPN

Segundo Favareto (2003), são três as topologias básicas, utilizadas para estabelecer VPNs:

- ***Host* a *host***: cada *host* é um computador que possui acesso à Internet, através desta topologia dois *hosts* separados fisicamente comunicam-se, fornecendo a segurança necessária para a troca de informações via Internet;
- ***Host* a rede:** esta topologia permite a conexão de um *host* móvel a uma determinada rede através da Internet;
- **Rede a rede:** este tipo de configuração possui um *gateway* VPN nas extremidades de duas ou mais redes fazendo a conexão segura entre elas. Esta topologia é ideal para redes de uma mesma empresa geograficamente distantes entre si.

2.6.4.3 Protocolos de Tunelamento

Conforme visto acima, o tunelamento é peça importantíssima para se estabelecer conexões VPNs. As VPNs possuem seus próprios protocolos de comunicação que atuam em conjunto com o TCP/IP, fazendo com que o túnel virtual seja estabelecido e os dados trafeguem criptografados. Os protocolos de tunelamento são os responsáveis pela abertura e gerenciamento de sessões dos túneis em VPNs. Podem ser realizados na camada 2 (enlace) ou na camada 3 (rede), considerando a arquitetura do modelo de referência OSI.

Nos túneis orientados à camada 2, um túnel é similar a uma sessão, onde as duas extremidades do túnel negociam a configuração dos parâmetros para o estabelecimento do túnel (endereçamento, criptografia, parâmetros de compressão, etc.). A gerência do túnel é realizada através de protocolos de

manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias da camada 3 não existe a fase de manutenção do túnel.

O tunelamento na camada 2, como atua em um nível inferior do modelo ISO/OSI, possui algumas vantagens em relação ao tunelamento do nível 3, como a simplicidade de configuração, a compressão e codificação completa e a inicialização bidirecional do túnel. Suas desvantagens são referentes às questões como escalabilidade, confiabilidade e segurança porque atua num nível mais próximo ao hardware.

Já o tunelamento na camada 3 tem como vantagens: escalabilidade, confiabilidade e segurança. Suas principais desvantagens são a limitação do número de fabricantes e uma maior complexidade em seu desenvolvimento. Dentre os principais protocolos de tunelamento VPN, pode-se destacar o PPTP (*Point-to-Point Tunneling Protocol*), o L2TP(*Layer Two Tunneling Protocol*) e o IPSec (*Internet Protocol Security*), os quais abordados a seguir.

2.6.4.4 PPTP

Este protocolo foi desenvolvido pelo Fórum PPTP, um consórcio que inclui *US Robotics, Microsoft, 3Com, Ascend e ECI Telematics*, porém a sua implementação mais conhecida é a da *Microsoft*, que é amplamente utilizada em sistemas *Windows*.

Ele atua na camada 2 e utiliza o PPP (*Point-to-point Protocol*) para fazer as conexões e, em seguida, encapsula os dados através do GRE (*Generic Routing Encapsulation*) e os envia à outra extremidade da VPN.

Para autenticação, o protocolo PPTP utiliza o MS-CHAP (*Microsoft-Challenge Handshake Authentication Protocol*) e para criptografia, o MPPE (*Microsoft Point-to-point Encryption*).

Existem algumas vantagens em se implementar uma VPN utilizando o protocolo PPTP, como, por exemplo, o suporte a outros protocolos diferentes do IP, como o NetBEUI e o IPX. Contudo, uma de suas principais desvantagens é relativa à sua segurança, pois este protocolo fornece suas chaves de encriptação utilizando a senha do usuário como base, ou seja, se esta senha for fraca, como palavras encontradas em dicionários ou números de telefones, a chave também o será.

2.6.4.5 L2TP

Projetado pela *Cisco Systems* e, posteriormente, homologado pela IETF (*Internet Engineering Task Force*) como protocolo padrão, baseia-se no L2F (*Layer Two Forwarding*) para solucionar os problemas do PPTP, sendo considerado o seu herdeiro. Algumas características, como a camada de atuação, a utilização do PPP para fornecer o acesso remoto e a operação em ambientes como o NetBEUI e o IPX, são mantidas do PPTP.

No entanto, uma diferença visível em relação a seu predecessor é quanto à forma de autenticação, pois ela é feita em dois níveis, No primeiro, o usuário é autenticado pelo provedor de acesso antes do túnel ser instalado e, no segundo, quando a conexão é estabelecida entre os *gateways.*

Sendo um protocolo padrão, qualquer fabricante pode criar produtos que utilizem o L2TP, de forma que provedores de acesso e consumidores em geral não dependam de produtos fornecidos por uma única empresa.

Apesar de ser atual, o L2TP apresenta como desvantagem não possuir um mecanismo eficiente de encapsulamento, ou seja, para executar esta tarefa, ele

necessita do protocolo IPSec, que será explicado e que faz a criptografia e gerenciamento de chaves em ambiente IP posteriormente, para que juntos possam garantir a segurança da VPN.

2.6.4.6 IPSEC

O IPSec foi desenvolvido pelo Grupo de Trabalho de Segurança do IP da IETF com o intuito de ser o protocolo padrão de endereçamento para a nova versão do IP, chamada IPv6. O IPSec atua na camada 3 e é composto por três principais funcionalidades:

- **Cabeçalho de autenticação (AH – *Authentication Header*):** que fornece a integridade dos pacotes e a garantia de sua origem.
- Cabeçalho de encapsulamento do payload (ESP – ***Encapsulation Security Payload***): que fornece a confidencialidade dos dados que trafegam pela rede pública.
- **Protocolo de negociação e troca de chaves (IKE – *Internet Key Exchange*)**: que permite a negociação das chaves de comunicação entre as organizações de modo seguro.

O IPSec permite ao usuário, ou ao `gateway` seguro que está agindo em seu favor, autenticar ou criptografar cada pacote IP, ou ainda, fazer os dois processos simultaneamente. Dessa forma, o IPSec pode atuar de dois modos:

- **Modo Transporte**: neste modo os pacotes criados são adicionados cabeçalhos IPSec entre o cabeçalho IP original e os dados. Este modo é muito utilizado para computadores em diferentes redes, comunicando-se diretamente entre si, e que desejam proteger o seu tráfego IP por encapsulamento, autenticação ou ambos.
- **Modo Túnel**: Neste modo, um cabeçalho IPSec também é adicionado, porém a diferença para o modo transporte é que será adicionado um novo cabeçalho IP e o pacote original será tratado como se fosse um dado só,

sendo todo ele criptografado pelo cabeçalho IPSec na parte referente ao dado do novo cabeçalho.

O modo túnel é comumente utilizado na comunicação entre *gateways*, pois fornece maior segurança aos dados originais criptografados dentro do novo pacote. Um dos processos mais importantes do IPSec é o gerenciamento de chaves e grande parte da segurança da comunicação reside nele, principalmente nas trocas inicias de chaves. Um esquema bem definido de trocas deve ser adotado para se evitar ataques em que o *hacker* pode capturar as trocas de informação dos dois lados da comunicação, alterando-as de acordo com seus interesses.

3 CONTEXTUALIZAÇÃO

3.1 A SITUAÇÃO ATUAL

Segundo a Secretaria Municipal de Educação de Aracaju (SEMED) o sistema manual de controle das atividades executadas nas escolas, bem como das informações cadastrais dos docentes e discentes e do rendimento escolar dos docentes recai em um processo complexo e lento. Pois, no panorama atual todo acompanhamento e controle técnico-pedagógico sobre as Unidades de Ensino é feito por meio de preenchimento e envio periódico de formulários para informar a situação de freqüência e rendimento escolar dos discentes.

Neste sentido, a Coordenação de Informática e Tecnologia (CODINTEC/SEMED), num esforço para automatizar estes processos, a SEMED vem desenvolvendo aplicações cliente-servidor, que visam propiciar maior agilidade e praticidade a essas tarefas. No entanto, para tornar o uso desses sistemas viável, é necessário que os computadores das unidades de ensino (clientes das aplicações) estejam conectados de alguma forma ao servidor da aplicação, que deve localizar-se na SEMED. Além disso, dada a importância dos dados a serem manipulados por essas aplicações, é imprescindível que a comunicação entre as unidades utilize um canal seguro de conexão, o que inviabiliza a idéia de expô-las na internet, devidos à falta de segurança da rede pública de computadores.

Atualmente a rede municipal de ensino é composta por 78[5] unidades escolares, distribuídas nas mais distintas localidades do município de Aracaju, que ocupa uma área de 181,8 Km[26]. Também foi levantado que em cada unidade existe pelo menos um microcomputador com acesso à internet, muitas delas possuindo suas próprias redes locais. No entanto, esse acesso é feito de formas distintas,

[5] Fonte: Sítio Oficial do Município na internet, disponível em http://www.aracaju.se.gov.br/educacao/?act=fixo&materia=unidades_de_ensino.
[6] Fonte: Sítio Oficial do Município na internet, disponível em http://www.aracaju.se.gov.br/aracaju/?act=fixo&materia=aspectos_geograficos.

podendo ser: através de conexões banda larga via telefonia fixa (ADSL – Velox OI), banga larga 3G (de diversas operadoras) ou Internet via rádio. Havendo ainda, em raros casos, acesso via linha discada. Assim, um requisito básico é que a solução construída possa, além de ter custos reduzidos, aproveitar toda estrutura já existente, uma vez que o processo de compra de equipamentos em órgãos públicos geralmente é burocrático e extenso.

Dessa forma, constitui-se a demanda de manter uma conexão inter-redes entre a rede da SEMED e as redes localizadas nas unidades a ela subordinadas, desenvolvendo-se este projeto como uma proposta para conexão desejada.

3.2 SOLUÇÃO PROPOSTA

Em vista da grande dispersão geografia, em que se encontram as unidades a serem interligadas, compreendendo toda extensão territorial do município, a princípio adotar-se-ia como solução a instauração de uma WAN ou MAN. No entanto, conforme já visto em seções anteriores, estes tipos de rede demandam altos investimentos, devido aos requisitos para sua implantação – como, por exemplo, a contratação de linhas telefônicas de acesso dedicado em todas as unidades – tornando-se, assim, pouco viável.

Dessa forma, para viabilizar uma solução a custos mais baixos optou-se por instituir uma rede privada virtual (VPN) que, conforme já citado, equivale-se, conceitualmente, a uma WAN ou MAN, com as vantagens de implementar um nível mais alto de segurança e reduzir os custos da interconexão, uma vez que se utiliza de um simples acesso à Internet – seja ele discado, banda larga, ou a rádio – para prover a conexão máquinas geograficamente separadas.

Assim sendo, a VPN seria um serviço oferecido pela máquina servidora da aplicação, na SEMED, sendo que as estações clientes acessariam ao servidor, que através da Internet, e após se autenticarem na VPN, teriam acesso à aplicação servida.

Neste sentido, a VPN pode ser considerada uma solução integrada, por fornecer a estrutura desejada, imprimindo a ela um nível aceitável de segurança, para que se mantenha um canal de comunicação confiável entre a unidades. Além disso, por ter requisitos mais simples, como um simples acesso à Internet, conforme já visto na revisão teórica, a VPN permite que se aproveite toda estrutura já existente, tanto na Secretaria, quanto nas demais unidades, requerendo que apenas se acrescentem alguns recursos, conforme descrito na seção seguinte.

É relevante considerar ainda, como vantagem, que tal serviço possui uma compatibilidade com as plataformas Windows e Unix de sistemas operacionais, podendo ser utilizado com qualquer versão do sistema operacional Windows, superior ao Windows 95, que já suporta o protocolo de tunelamento PPTP, visto anteriormente, como também versões do sistema operacional Linux. Dessa maneira, permite-se a compatibilidade com os equipamentos que já estiverem em uso.

3.3 REQUISITOS DA SOLUÇÃO

Sendo a VPN um serviço que funciona na plataforma cliente-servidor, seu principal requisito é a disponibilização da máquina que o servirá. Para tanto, será necessário um servidor que deve possuir um endereço IP fixo e válido, ou seja, um endereço que possa ser único e reconhecido na Internet, seria necessário registrar um domínio em nome da Instituição para obter tal endereço, o que pode ser indicado como o recurso de maior custo, para esta implementação.

Visando a inclusão de todas as unidades escolares, faz-se necessária a disponibilização de pelo menos um microcomputador, provido, de alguma maneira, de acesso à Internet, preferencialmente acesso banda larga ou internet a rádio, que são de melhor performance.

3.4 O IMPACTO DA SOLUÇÃO PROPOSTA NAS ATIVIDADES DA INSTITUIÇÃO

Ao considerar o impacto que a implantação da estrutura proposta terá sobre a instituição, é preciso levar em conta não só a interconexão proposta em si, mas toda a idéia que está por traz da mesma, ou seja, a radical mudança que recairá sobre a rotina de trabalho dos profissionais envolvidos.

Neste sentido existem dois aspectos a serem analisados: o financeiro e o social. Ao primeiro refere-se à relação custo benefício da proposta e ao ultimo o reflexo desta sobre seus usuários.

Se por um lado a solução requer algum custo, mesmo diante de todos as escolhas e esforços visando a máxima redução dos custos a serem empregados, é importante levantar as economias que por outro lado serão geradas e os benefícios que o novo sistema de trabalho pode proporcionar.

Em contrapartida, pode-se facilmente visualizar economias quando se refere aos gastos com material burocrático como papeis, fitas, tonners e cartuchos para impressoras e máquinas xerográficas, cujo consumo deve diminuir significativamente com a tramitação eletrônica de documentos e informações, prevista no sistema informatizado. Além da redução no uso dos meios de transporte, atualmente utilizados para a tramitação desses documentos e, porque não citar a economia de tempo gerada pelo sistema proposto.

Tratando dos benefícios, conforme já citado anteriormente a facilidade, praticidade e agilidade atribuídas à manutenção dos dados cadastrais de docentes e discentes e acompanhamento da vida escolar dos alunos representa uma grande vantagem em face ao processo manual realizado atualmente. Os resultados poderão ser vistos a curto prazo, tais como agilidade em processos de transferências e a troca de informações entre as unidades e maior controle sobre a consistência destes dados.

É relevante considerar a portabilidade da estrutura proposta, através da qual poderão ser viabilizadas quaisquer outras aplicações que sejam necessárias ao controle das atividades da Instituição.

4 CENÁRIO EXPERIMENTAL

Considerando que a VPN é um serviço implantado na camada de rede, ela funciona independentemente da estrutura das camadas localizadas abaixo dela, no caso da arquitetura tcp/ip a camada física. De forma geral, esta última camada pode ser representada por uma ligação com a rede pública, Internet, ou por ligações ponto-a-ponto entre o servidor e o cliente VPN.

Para prover o acesso utilizando a Internet é necessário que o servidor utilizado esteja conectado a ela, com um endereço IP fixo e válido, para que seja acessível pelos clientes, conforme citado anteriormente.

Dessa forma, por questões de limitação de recursos para aquisição de um domínio na Internet, na montagem experimental desse estudo, optou-se por estabelecer a camada física através de uma ligação ponto-a-ponto, para isso, manter-se-á a camada física através do serviço de acesso remoto (RAS – Remote Access Service), pois sua conexão baseia-se na discagem por linha telefônica, permitindo a possibilidade de utilizar uma faixa de endereçamento IP não válido e assim, não demandando custos elevados.

Essa solução torna-se, inclusive, viável, caso seja necessário conectar alguma unidade sem uso da Internet Banda Larga, quer seja por limitação tecnológica de não haver este serviço na localidade ou por uma indisponibilidade temporária do serviço local. Já que requer apenas uma linha telefônica e que, por usá-la de forma dedicada, tem melhor performance que o acesso discado à Internet.

Uma vez configurado e testado o RAS, obtém-se uma estrutura sólida para se implantar o serviço VPN, na camada imediatamente acima.

Para a montagem do cenário experimental será utilizado como Servidor um computador com sistema operacional Windows 2003 Server R2 Standard Edition,

um cliente com sistema operacional Windows XP Professional e um cliente com Linux Ubuntu 10.10.

Neste sentido, esta seção será composta das seguintes etapas:

- Configuração do serviço RRAS no cliente e no servidor;
- Configuração do serviço VPN no cliente e no servidor;

4.1 CONFIGURANDO O SERVIÇO RAS

Nesta seção serão demonstradas as configurações necessárias para a configuração do servidor e cliente RAS, bem como apresentados os testes realizados para validar a configuração executada.

4.1.1 Servidor RAS

Para efeito de adequação com a estrutura aqui proposta, os passos para configuração do servidor, a seguir apresentados, baseiam-se no sistema operacional *Windows 2003 Server* da *Microsoft® Corporate*. Neste sistema o acesso remoto é disponibilizado pelo RRAS (*Routing and Remote Access Service* - Serviço de Roteamento e Acesso Remoto).

Neste sentido, a montagem do servidor consiste em configurar o serviço RRAS. Para tanto deve-se executar a seqüência de os passos a seguir:

1 – Inicialmente deve-se acessar o RRAS, através das opções de menu *Start>>Adminitrative Tools>>Routing and Remote Access*;

2 - No console apresentado a ilustração 7, deve-se clicar com botão direito do mouse e escolher a opção “*Add Server*” (Adicionar um Servidor);

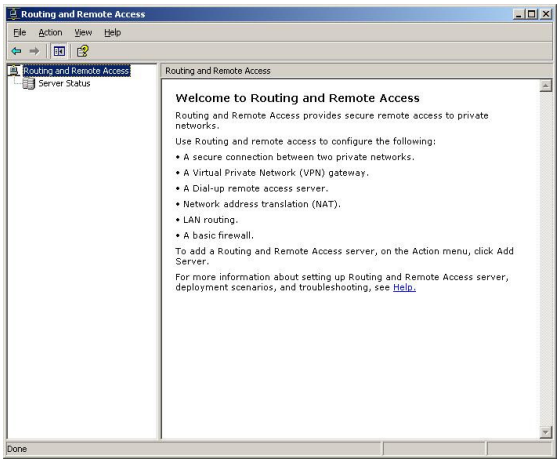

Ilustração 7 - Console para configuração do servidor RRAS

Fonte: Elaboração própria (2010)

3 - Na caixa de diálogo que será exibida, ilustração 8, é possível escolher qual equipamento será o servidor, se a própria máquina em que está sendo realizada a configuração ou em outro servidor, cujo nome deve ser informado. Para a configuração aqui proposta, deve-se selecionar a opção "*This Computer*" (Este Computador), para indicar que o servidor será este mesmo equipamento. Neste caso, será criado um servidor com nome do ao computador quando foi instalado o sistema operacional, de acordo coma ilustração 9, e para habilitá-lo basta clicar com o botão direito no servidor criado para poder configurá-lo, através da opção "*Configure and Enable Routing and Remote Access*";

Ilustração 8 - Escolha do equipamento servidor

Fonte: Elaboração própria (2010)

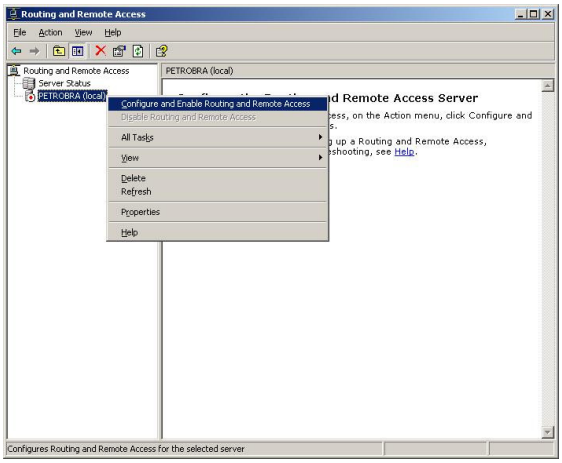

Ilustração 9 - Solicitando a configuração do servidor RRAS

Fonte: Elaboração própria (2010)

4 - Será exibida uma tela inicial, na qual deve-se clicar em "*Next*", para proceder de fato à configuração. Será necessário usar a tecla "*Next*" a cada passo da configuração;

5 – Na seqüência será exibida a ilustração 10, em que deve-se escolher a opção referente à configuração desejada, que no caso desta configuração é a opção "*Remote Access*" (*Dial-up* or VPN), ou seja, um servidor de acesso remoto para conexões *dial-up* ou vpn;

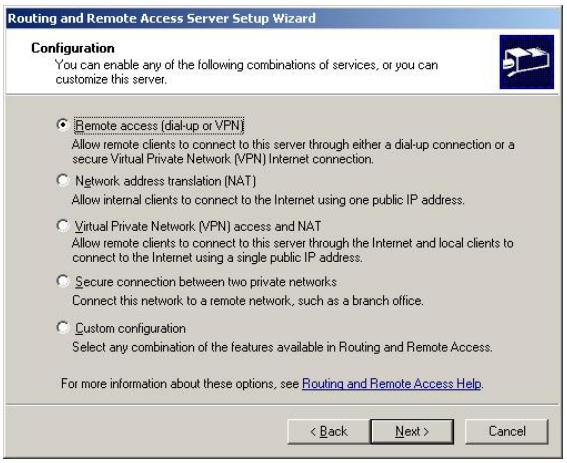

Ilustração 10 - Definindo tipo de RRAS

Fonte: Elaboração própria (2010)

6 – As próximas opções serão definir o tipo de endereçamento, em que deve se seguir a opção padrão, *Automatically*, e, em seguida, deverá ser informado se haverá utilização da autenticação RADIUS[7], o que não será necessário para este momento inicial, logo, será acionada a opção "*No, use Routing and Remote Access to authenticate connection request*", conforme ilustração 19; No passo seguinte basta clicar em "*Finish*" para finalizar a configuração do servidor;

7 – O próximo passo é cadastrar os usuários para que possam ser configurados os clientes RAS, o que deve ser feito através da opção de menu *Start>>Adminitrative Tools>> Active Directory Users and Computers*. Os usuários devem ter a permissão de acesso remoto habilitada em suas propriedades, conforme ilustração 11. Na aba "*Dial-in*", é preciso habilitar a permissão para recebimento de chamadas remoto, escolhendo a opção "*Allow access*";

8 - O passo seguinte, para configurar o servidor RRAS é definir as políticas de acesso que serão utilizadas. Elas são usadas, entre outras coisas, para definir quais usuários ou grupos de usuários terão permissão para utilizar o serviço. Para isso, basta clicar com o botão direito do mouse na opção "*Remote Access Policies*" e escolher "*New Remote Access Policies*", conforme ilustração 12;

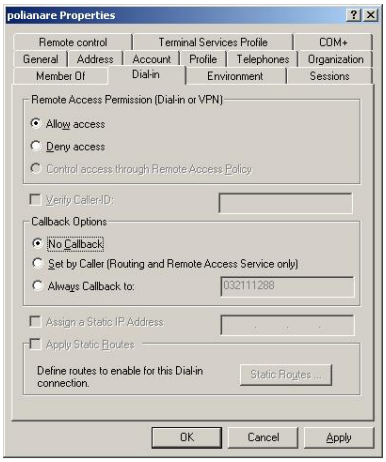

Ilustração 11 - Habilitando permissão ao acesso remoto para usuário

Fonte: Elaboração própria (2010)

[7] Serviço de autenticação cliente/servidor. O Radius autentica através de uma série de comunicações entre o cliente e o servidor. Uma vez que o usuário é autenticado, o cliente proporciona a ele, o acesso aos serviços apropriados.

8.1 - Será iniciado o processo de definição da política, em que a cada passo será necessário clicar em *Next.* O primeiro passo é atribuir um nome à política criada. Em seguida, é preciso definir a que tipo de acesso esta política se refere, conforme ilustração 13. Neste caso, deve-se selecionar a opção *Dial-up*;

8.2 - O próximo ponto, será adicionar os grupos de usuários que terão acesso ao serviço, conforme ilustração 14. E em seqüência será preciso definir o tipo de autenticação que será utilizado, de acordo com a ilustração 15. Visando compatibilidade com possíveis clientes Linux, é recomendável utilizar o EAP (*Extensible Authentication Protocol*) com criptografia através do método MD5, já que as demais opções são métodos proprietários da Microsoft. Em seguida é preciso definir os tipo de criptografia que serão suportados, de acordo com o tamanho da chave (40, 56 ou 128bits), onde podem ser selecionadas todas as opções, ou, até mesmo, não utilizar criptografia através da opção "*No Encryption*". Neste caso recomenda-se habilitar os três tipos de chave. Assim, definida toda política de acesso, basta clicar em "*Finish*", para concluir;

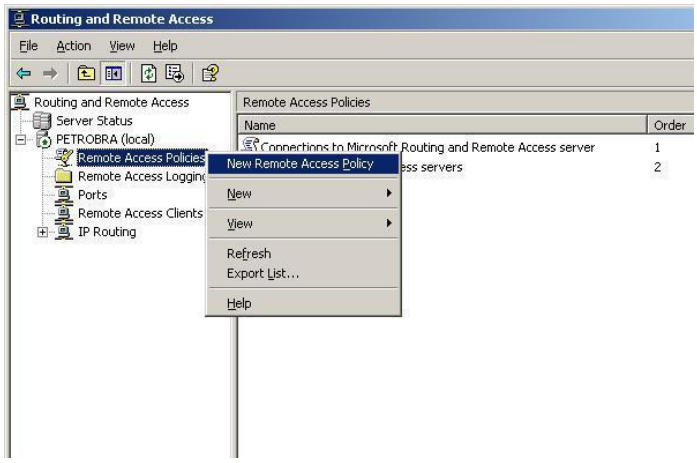

Ilustração 12 - Adicionando Política de Acesso Remoto
Fonte: Elaboração própria (2010)

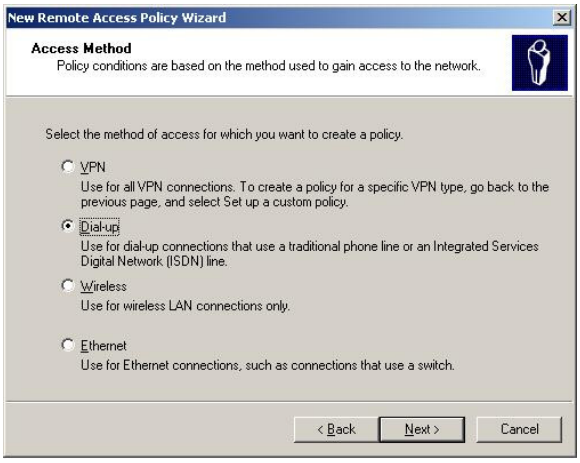

Ilustração 13 - Definindo tipo de acesso controlado pela política criada

Fonte: Elaboração própria (2010)

9- Por fim, antes de utilizar o servidor RRAS é preciso verificar se as portas de serviço oferecidas estão de acordo com a utilidade e demanda de utilização. Para configurar as portas, é necessário escolher a opção "*Properties*", clicando com o botão direito na opção *Ports*, visualizada na ilustração 12, mostrada anteriormente. Será exibida uma janela, conforme ilustração 16, onde se deve marcar a opção "*WAN Miniport(PPTP)*", uma vez que o protocolo utilizado será o PPTP, conforme já foi citado e, em seguida, é necessário clicar na opção "*Configure*";

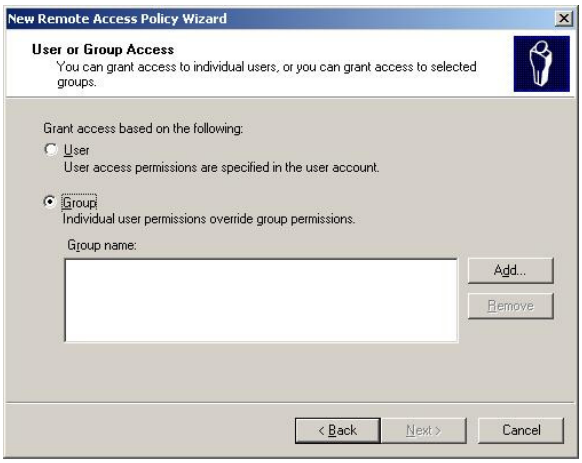

Ilustração 14 - Adicionando Grupos de Acesso

Fonte: Elaboração própria (2010)

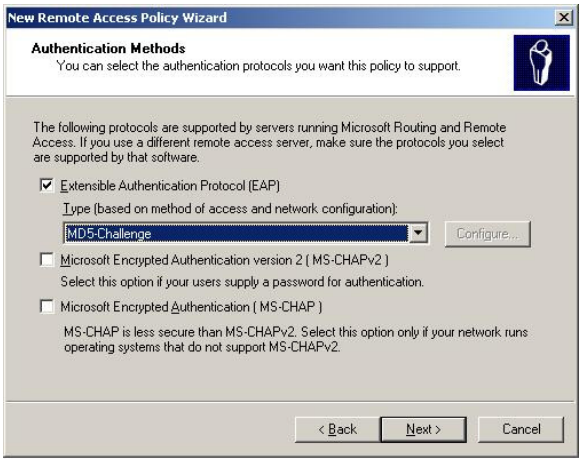

Ilustração 15 - Definindo método de autenticação

Fonte: Elaboração própria (2010)

10- Na configuração, de acordo com a ilustração 17, deverá ser marcada a opção "*Remote access connections(inbound only)*", uma vez que as portas serão utilizadas apenas para que o servidor receba conexões. Nesta oportunidade é possível, ainda, definir a quantidade máxima de portas suportadas, neste caso, para atender à demanda desta estrutura deve-se admitir 80 portas. E desta forma, o servidor RRAS está pronto para ser habilitado e utilizado.

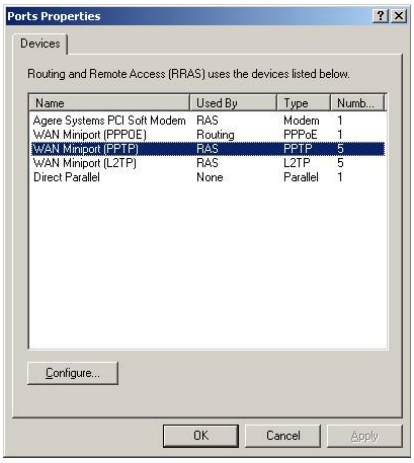

Ilustração 16 - Configuração de portas do RRAS

Fonte: Elaboração própria (2010)

Ilustração 17 - Definindo características das portas

Fonte: Elaboração própria (2010)

4.1.2 Configurando o cliente RRAS no Windows XP Professional

Na estrutura proposta serão admitidos clientes de diversas versões dos sistemas operacionais *Microsoft*®. Como a configuração do cliente RRAS é extremamente mais simples, se comparada à configuração do servidor, bastando apenas adicionar uma nova conexão de rede *dial-up*, em que o telefone indicado para discagem do provedor será o número da linha telefônica à qual está conectado o servidor RRAS.

Neste sentido, será ilustrada, a título de exemplo, apenas a configuração de um cliente com sistema operacional Windows XP Professional, quando utilizado em modo gráfico, o processo é feito de forma bastante semelhante, em que somente algumas alterações na interface gráfica poderão ser encontradas.

Existe mais de um caminho para executar a tarefa supra citada, será aqui adotado o caminho que combina maior praticidade e coincidência entre as versões abrangidas. Os seguintes passos são necessário para configuração do cliente:

1 – O primeiro passo é acessar o “Painel de Controle”, através da opção Inicar>>Configurações>>Painel de Controle, onde deverá ser aberto o item “Opções da Internet”;

2 – Será exibida uma nova janela em que deve ser escolhida a aba conexões, conforme ilustração 18. Nesta, selecionar-se-á a opção “Adicionar” para criar uma nova conexão;

3 – A seguir, iniciar-se-á o processo de configuração onde a cada passo deve-se clicar em “Avançar”. O primeiro requisito, conforme ilustração 19, será informar o número de telefone para o qual deverá ser discada a conexão, ou seja, o número da linha telefônica conectada ao servidor RRAS, anteriormente configurado, conforme exposto acima. O próximo passo será informar nomear a conexão e concluir a sua configuração.

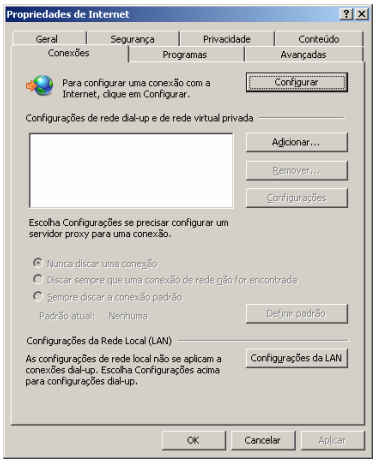

Ilustração 18 - Adicionar Conexão
Fonte: Elaboração própria (2010)

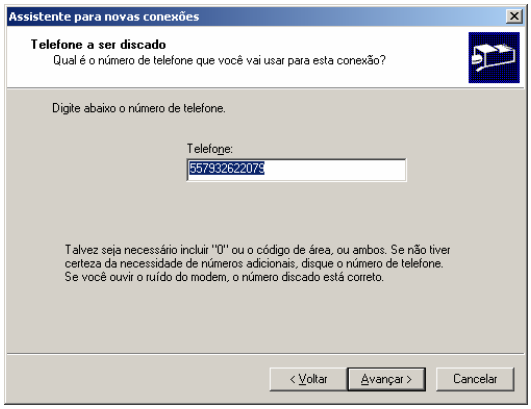

Ilustração 19 - Definindo número de discagem da conexão
Fonte: Elaboração própria (2010)

Adicionalmente, pode criar um atalho na área de trabalho (desktop), para facilitar e agilizar o acesso à conexão configurada. Caso contrário a conexão poderá ser iniciada a partir da opção de menu Iniciar>>Configurações>>Painel de Controle>>Conexões de rede.

Quando acionada a conexão, serão solicitados o nome do usuário e senha, para fazer a autenticação. Caso os dados informados estejam corretos e refiram-se a um servidor que possua permissão de conexão remota, o servidor permitirá o acesso e será estabelecida a conexão, caso contrário, o acesso será negado e a tentativa de conexão não terá sucesso.

No ambiente servidor, é possível verificar que a conexão foi corretamente efetuada, através do console do RRAS, uma vez que a opção *Remote Access Clients* exibe os usuários conectados no momento, como pode ser visto na ilustração 20.

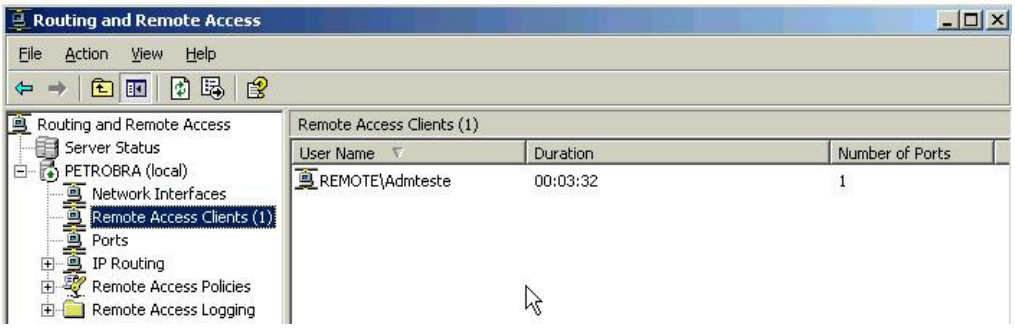

Ilustração 20 - Verificando usuários conectados ao servidor RRAS

Fonte: Elaboração própria (2010)

4.1.3 Configurando o cliente RRAS no Ubuntu 10.10

Para facilitar o entendimento, serão mostrados os passos necessários para a configuração do cliente no Ubuntu 10.10, com base em sua interface gráfica, considerando que se tenha iniciado o computador com um usuário com permissão de administrador (root). Assim devem ser seguidos os seguintes passos:

1 – Iniciar uma sessão do programa “Terminal”, através da opção de menu Aplicativos>>Acessórios>>Terminal. Na sessão do Terminal deve-se digitar o comando “sudo pppconfig”, para acessar as configurações do serviço PPP que permitirá criar uma conexão dial up no Ubuntu 10.10. Após o comando poderá ser solicitada a confirmação da senha do usuário;

3 – Ao ser iniciado o ambiente de Configuração PPP; deverão ser seguidos os passos conforme as ilustrações de 21 a 26, sempre efetuando a configuração de acordo com a tela mostrada e clicando em <OK>;

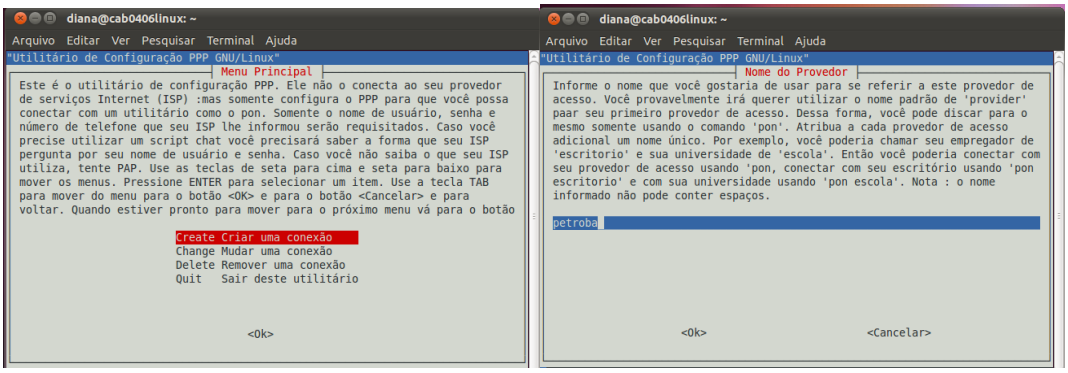

Ilustração 21 – Configurações PPP – Criando uma conexão e definindo o nome do provedor

Fonte: Elaboração própria (2010)

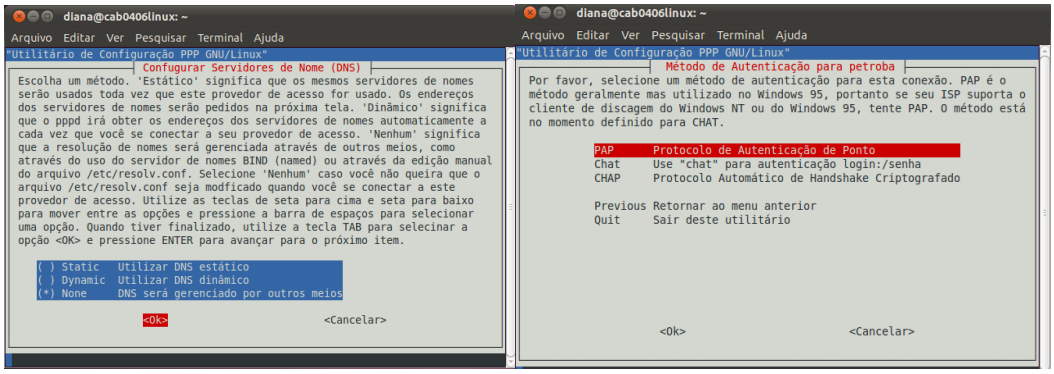

Ilustração 22 – Configurações PPP – Desabilitando resolução DSN na conexão e definindo método de autenticação

Fonte: Elaboração própria (2010)

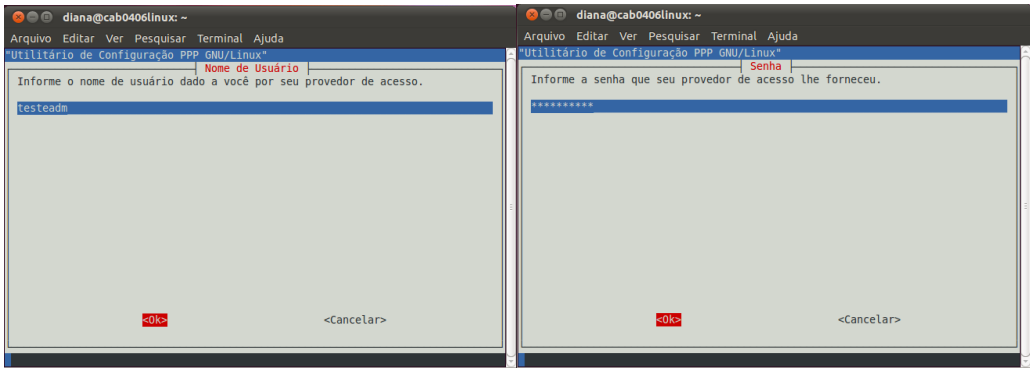

Ilustração 23 – Configurações PPP – Informando usuário e Informando senha de autenticação

Fonte: Elaboração própria (2010)

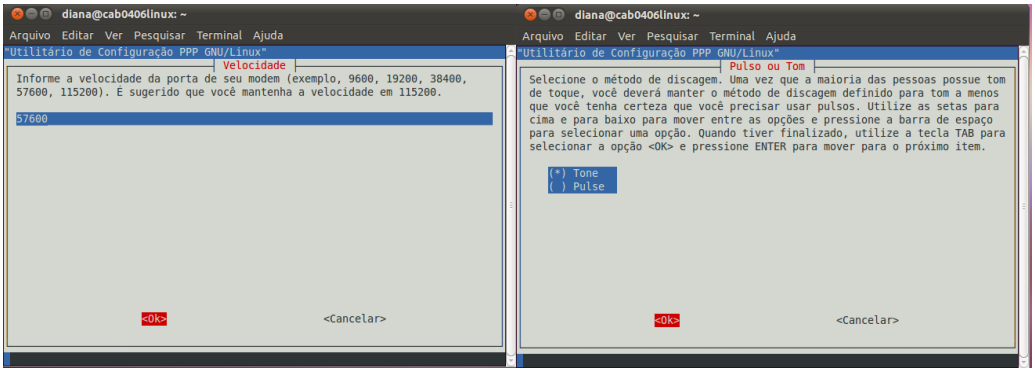

Ilustração 24 – Configurações PPP – Informando velocidade do modem e Definindo Método de discagem

Fonte: Elaboração própria (2010)

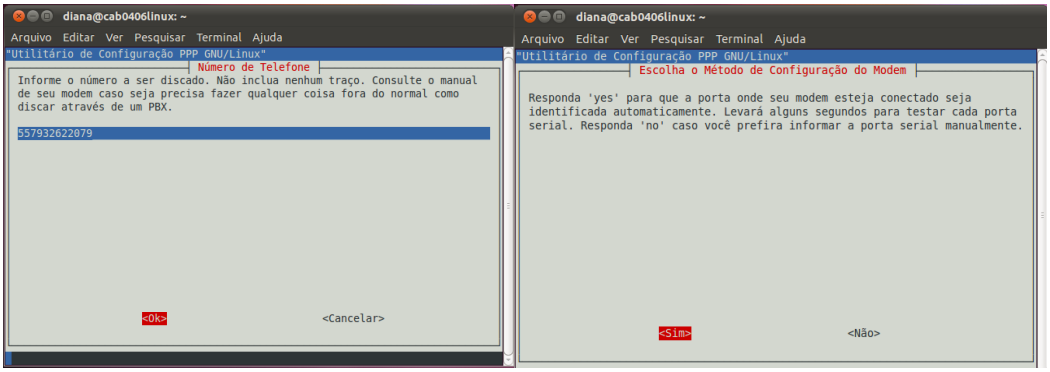

Ilustração 25 – Configurações PPP – Definindo número telefônico do servidor RRAS e Permitindo que o modem seja configurado automaticamente

Fonte: Elaboração própria (2010)

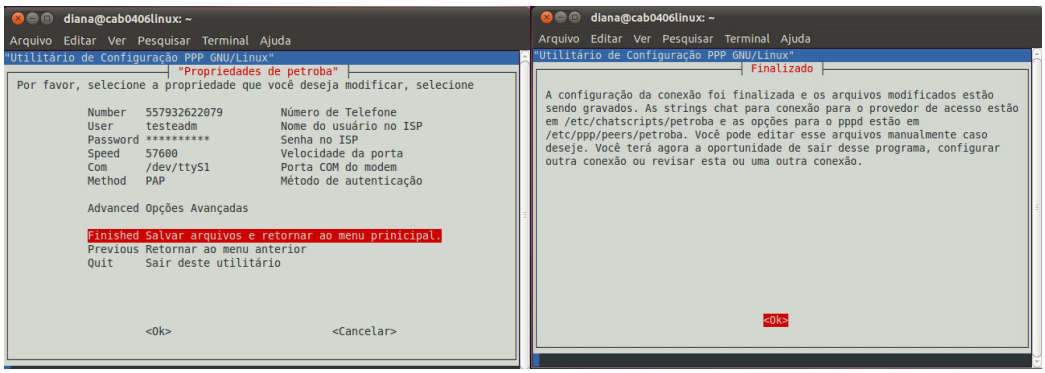

Ilustração 26 – Configurações PPP – Salvando a configuração e Finalizando a configuração

Fonte: Elaboração própria (2010)

Uma vez configurada a conexão, é possível executá-la através do comando “pon” e finalizá-la através do comando “poff”, numa sessão do aplicativo “Terminal”. Assim como no cliente Windows XP a conexão somente será estabelecida se os dados de usuário e senha informados forem de um usuário com permissão de acesso remoto, caso contrário a conexão será negada.

4.2 CONFIGURANDO SERVIÇO VPN

Agora que a camada física está configurada corretamente em ambas as partes, cliente e servidor, e que também foi testada, pode-se implementar o serviço lógico de VPN em cima da estrutura física estabelecida.

Para ativar o serviço de VPN serão igualmente necessárias algumas configurações tanto no servidor quanto no cliente, como segue.

4.2.1 Servidor VPN

Mantendo o ambiente inicializado no serviço anterior, serão necessárias algumas modificações nas características do servidor RRAS anteriormente montado, para que ele passe a suportar o serviço de VPN.

Assim sendo as alterações são constituídas pelos seguintes passos:

1 - Inicialmente é necessário configurar o servidor IAS (*Internet Authentication Service* – Servidor de Autenticação para Internet) este serviço está disponível na opção de menu *Start>>Adminitrative Tools>> Internet Authentication Service*;

1.1 – No console apresentado na ilustração 27, o primeiro passo é criar o cliente RADIUS[8] (*Remote Authentication Dial-in User Service* - Serviço de Autenticação a

[8] Padrão criado pela IETF, utilizado para autenticar, autorizar e identificar usuários remotos e conexões dial-in.

usuários Remotos Dial-in), através da opção *Action>>New RADIUS Client*. Seré iniciado o processo de configuração onde a cada passo deve-se clicar em "*Next*";

1.2 - Como resultado da ação anterior será exibida a janela apresentada na ilustração 28, onde deve ser informado o nome e o endereço do cliente RADIUS. Neste caso, será o próprio servidor, logo o nome será o nome atribuído à máquina e o endereço será "*localhost*";

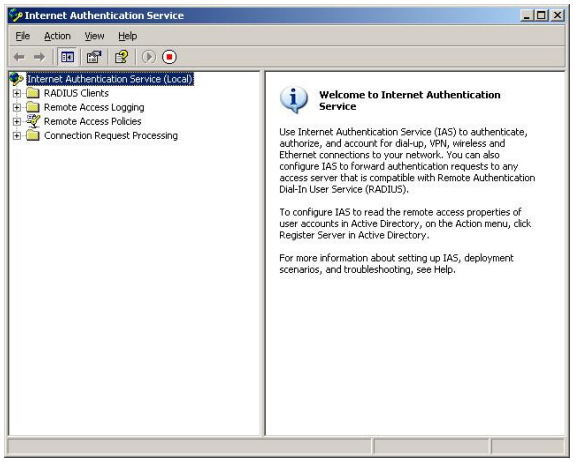

Ilustração 27 - Console de configuração do IAS
Fonte: Elaboração própria (2010)

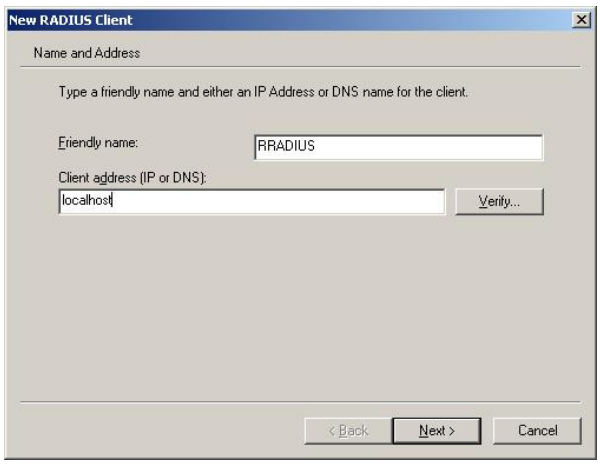

Ilustração 28 – Configuração do Cliente RADIUS - Nome e endereço do cliente
Fonte: Elaboração própria (2010)

1.3 - No passo seguinte, ilustração 29, deve-se escolher o tipo de RADIUS que será utilizado, uma vez que existem varias implementações distintas deste serviço. Recomenda-se a utilização da configuração padrão, representada pela opção "RADIUS *Standard*". A seguir define-se e confirma uma senha que será requerida para alterar as configurações do cliente e clica-se em "*Finish*" e está criado o cliente RADIUS;

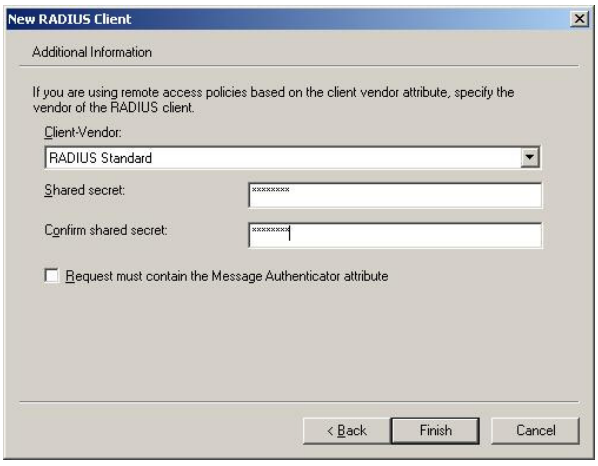

Ilustração 29 - Configuração do Cliente RADIUS - Tipo de implementação e senha
Fonte: Elaboração própria (2010)

1.4 - Agora é preciso definir as políticas de acesso do IAS. Para adicionar uma política seguem-se mesmos passos utilizados para executar esta tarefa na configuração do servidor RRAS, etapa 10 dessa configuração. É possível também alterar as propriedades das políticas-padrão já existentes;

1.5 - Em ambas as políticas, "*Connections to Microsoft Routing and Remote Access Server*" (conexão através do RRAS) e "*Connections to Other Access Servers*" (conexão através de outros servidores de acesso) é preciso adicionar permissão de acesso aos grupos de usuários criados quando o servidor RRAS foi configurado. Para isso, basta clicar com o botão direito do mouse e escolher a opção "*Properties*", conforme ilustração 30;

1.6 - Como resultado será exibida a janela apresentada na ilustração 31, onde deve ser escolhida a opção "*Add*", através da qual será mostrada a caixa de

dialogo da ilustração 32, onde deve ser escolhida a opção "*windows-groups*" e "*add*", escolher os grupos de usuários do Windows aos quais se deseja dar permissão de acesso;

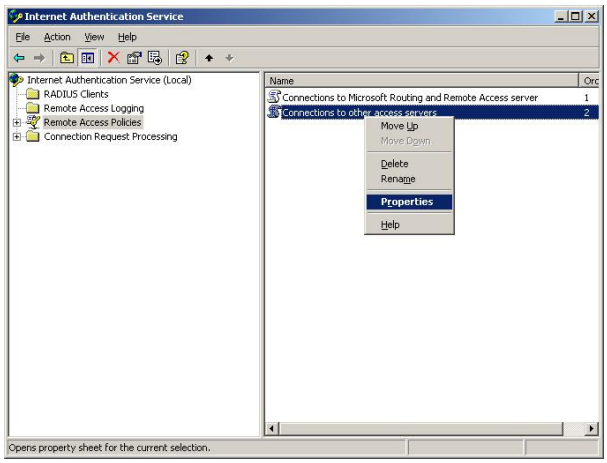

Ilustração 30 - Configurando políticas de acesso IAS

Fonte: Elaboração própria (2010)

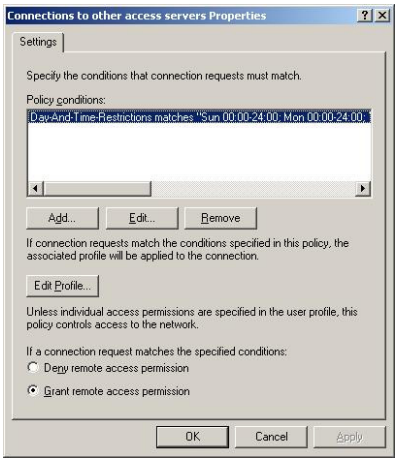

Ilustração 31 - Adicionando usuários à política de acesso IAS

Fonte: Elaboração própria (2010)

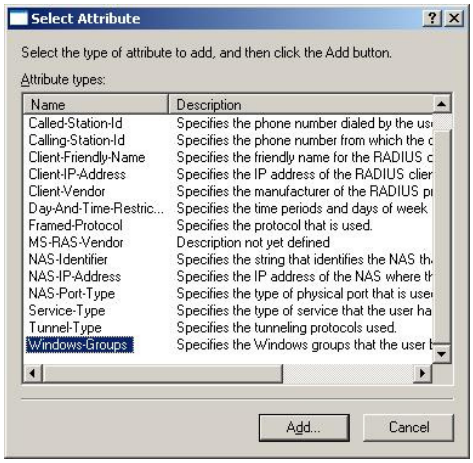

Ilustração 32 - Adicionando grupos de usuários do Windows

Fonte: Elaboração própria (2010)

1.7- De modo geral, algumas outras opções podem ser configuradas nas políticas de acesso para limitar o uso da conexão, tais como dias e horas em que o acesso será permitido, nível de criptografia utilizado, possibilidade de utilização de múltiplas conexões, entre outras opções, que fogem ao eixo central deste trabalho, uma vez que tratam do gerenciamento avançado da conexão.

2 – Agora que se tem um IAS funcionando, com o serviço RADIUS, é preciso reconfigurar o servidor RRAS, reiniciando no passo 3 da seção 4.1.1. No entanto, desta vez serão feitas duas pequenas alterações: no passo 7 será necessário incluir a opção VPN, uma vez que esse serviço estará sendo acrescentado, e no passo 8 deve-se informar que será utilizado o serviço RADIUS e, adicionalmente, será solicitado informar o nome do servidor RADIUS, que neste caso será a própria máquina. Assim, finalizada a configuração, ter-se-á o resultado apresentado na ilustração 59. Onde é possível observar que, neste caso, não será mais necessário definir as políticas de acesso, uma vez que serão usadas as políticas definidas no IAS;

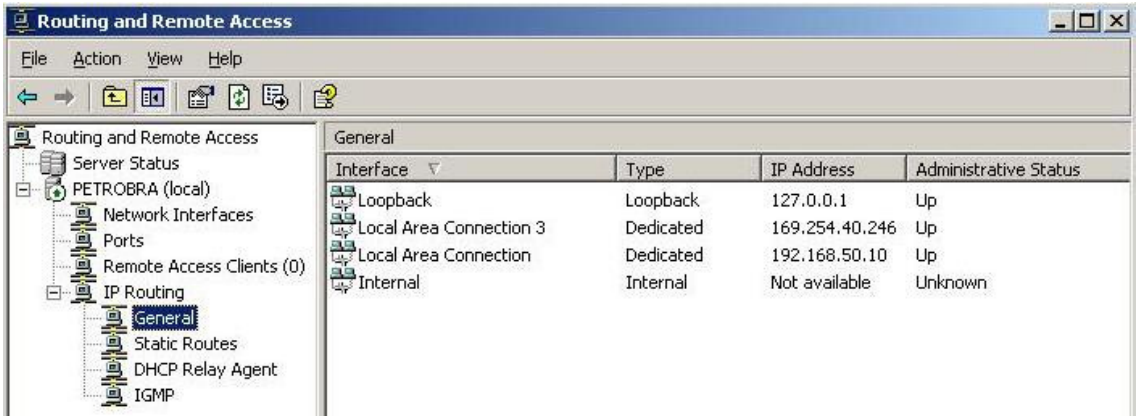

Ilustração 33 - Console do serviço RRAS no Windows 2003 Server
Fonte: Elaboração própria (2010)

4.2.2 Cliente VPN

De forma semelhante aos clientes RRAS existem diversas formas de configurar clientes VPN Windows, vamos demonstrar a forma mais prática, que compatível com todas as versões do Windows, uma vez que as configurações manuais são exclusivamente adaptadas às versões mais recentes como os Windows XP, 2000 e 2003, quando usados como clientes. Adicionalmente, como proposto será mostrada também a configuração necessária para conectar um cliente Linux ao serviço VPN.

4.2.2.1 Cliente Windows

Neste caso a primeira tarefa a ser executada é a criação do disco de instalação do serviço VPN, que deve ser feita no próprio servidor, de acordo com os seguintes passos:

1 - Inicialmente será necessário instalar o serviço de criação de discos no servidor, que geralmente não é incluído na instalação do Windows 2003 Server:

1.1 – Para isso, basta acionar a opção de menu *Start>>Control Panel>>Add and Remove Programs>> Add/Remove Windows Components.* Como resultado da ação anterior será exibida a janela apresentada na ilustração 34, em que deve-se selecionar a opção "*Management and Monotoring Tools*" (ferramentas de gerenciamento de monitoria) e clicar em "*Details*";

1.2 – Será então mostrada a janela correspondente à ilustração 35, onde deverão ser selecionadas todas as ferramentas e, em seguida, deve-se clicar em "*OK*", retornando assim à janela da ilustração 36, onde clica-se-á em "*Next*". Dessa forma as ferramentas selecionadas serão instaladas. É importante lembrar que é necessário utilizar o disco de instalação do Windows 2003 Server para que sejam instaladas as ferramentas

2 - Após instalar o serviço e possível iniciá-lo pela opção de menu *Start>>Administrative Tools>>Connection Manager Administration Kit*, o que dará inicio ao processo de criação do disco de instalação do serviço VPN. Este processo composto de uma seqüência de passo em que algumas configurações podem ser customizadas, mas como são de pouca relevância para o trabalho, optou-se por utilizar as opções padrão, clicando em na opção "*Next*" a cada passo.

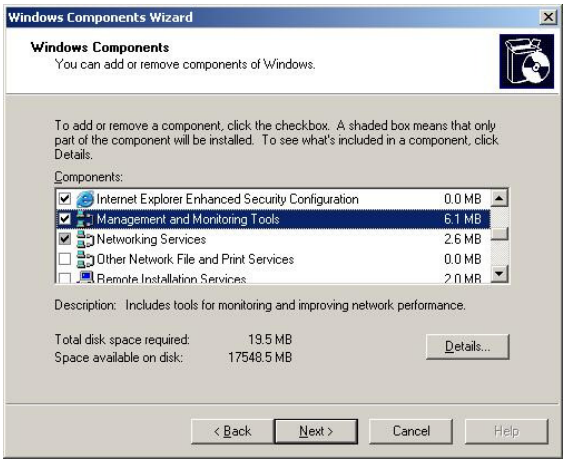

Ilustração 34 - Escolhendo componente a ser adicionado

Fonte: Elaboração própria (2010)

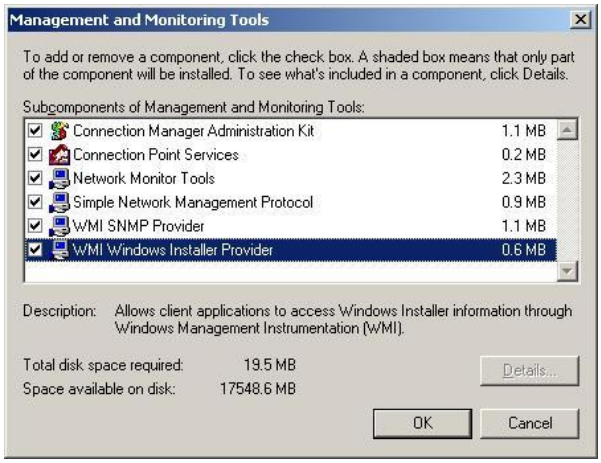

Ilustração 35 - Detalhamento das ferramentas a serem instaladas

Fonte: Elaboração própria (2010)

3 – Por fim será exibida uma última janela, em que deverá ser escolhida a opção "*Finish*". E assim um conjunto de arquivos de configuração será gravado no local indicado. Dentre estes arquivos encontrar-se-á um arquivo executável que deve ser utilizado para instalar o serviço nas estações clientes, o que o tornará acessível para ser conectado quando necessário.

Uma vez instalado o cliente VPN, para efetivar o tunelamento, basta conectar-se inicialmente ao servidor RRAS, através da conexão criada na configuração do cliente RRAS, que estabelecerá a conexão física, a princípio insegura. Em seguida, executar o cliente VPN, que apresentará a janela exibida na ilustração 36, em que devem ser informados o usuário e sua respectiva senha e escolhida a opção conectar. Estando o usuário devidamente cadastrado no servidor e sendo informada a senha correta, o usuário será autenticado pelo serviço RADIUS e está conectado logicamente ao serviço VPN que simulará o tunelamento na conexão física obtida anteriormente, tornando o canal de comunicação seguro.

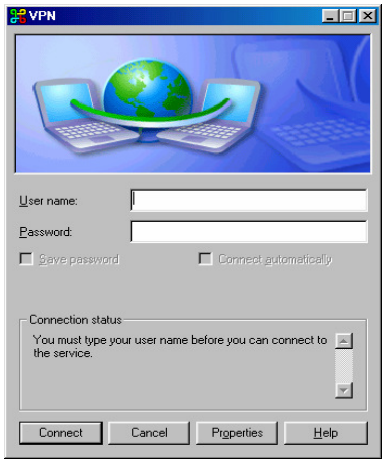

Ilustração 36 - Executando o cliente VPN

Fonte: Elaboração própria (2010)

4.2.2.2 Cliente Linux

Como o disco de configuração do cliente VPN, cuja criação foi ilustrada no item anterior, é compatível somente com sistemas operacionais Microsoft®, será demonstrado a seguir o procedimento manual para configuração de um cliente VPN no Ubuntu 10.10, em que a configuração basicamente consiste em informar o protocolo a ser utilizado, o endereço IP do servidor e os dados do usuário para autenticação. Para isso, basta efetuar os seguintes passos:

1 – Deve-se acessar as conexões de rede através da opção de menu Sistema>>Preferências>>Conexões de Rede. Na tela exibida como resultado, deve ser escolhida a aba VPN e a opção “Adicionar”. Em seguida, deve-se clicar no botão “Criar...”, de acordo coma ilustração 37;

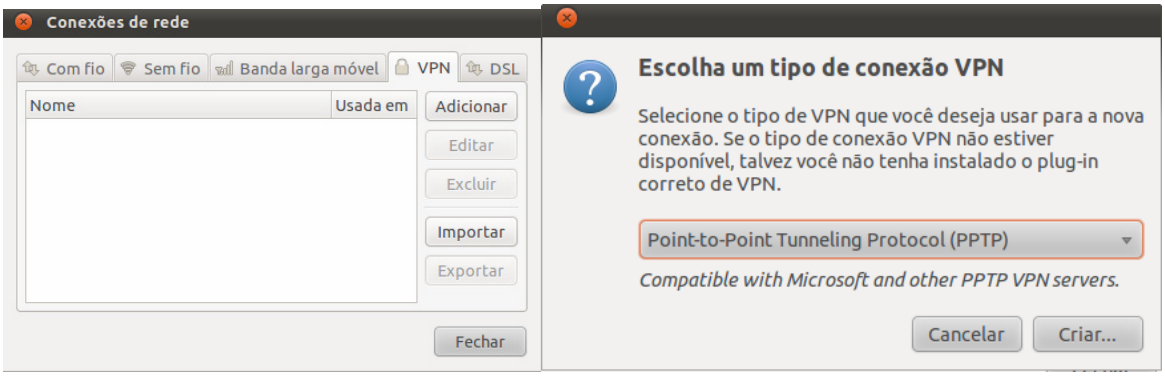

Ilustração 37 – Adicionando uma conexão VPN e Criando uma VPN PPTP

Fonte: Elaboração própria (2011)

3 – Agora basta preencher as informações da conexão, conforma ilustração 38, e clicar em aplicar. É possível ainda definir que a VPN seja conectada automaticamente, marcando a opção correspondente, caso contrário, a conexão pode ser iniciada através da barra de menu, como mostrado na ilustração 39;

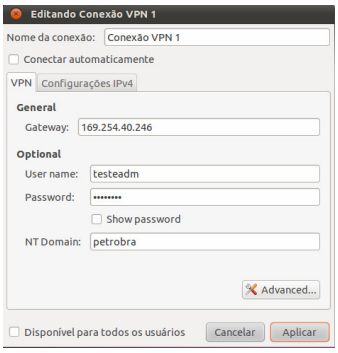

Ilustração 38 – Configurando dados da conexão VPN

Fonte: Elaboração própria (2011)

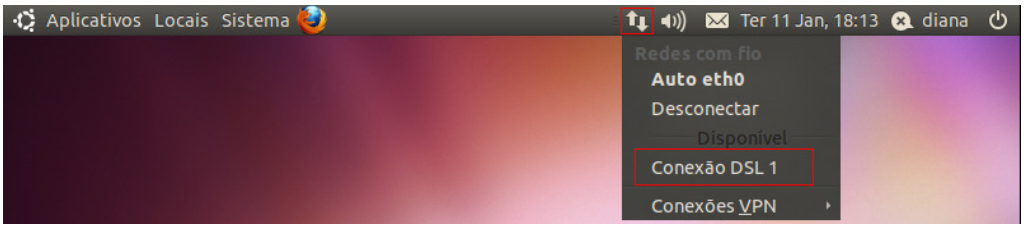

Ilustração 39 – Configurando dados da conexão VPN

Fonte: Elaboração própria (2011)

5 CONCLUSÕES

As VPNs podem se constituir numa alternativa segura para transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os *links* dedicados de longa distância, de alto custo, na conexão de WANs.

De acordo com o cenário utilizado durante a implementação e dos testes realizados, obtém-se a validação das configurações aqui propostas. No entanto, algumas dificuldades foram enfrentadas para a configuração do cliente Linux e alcance da comunicação deste com o servidor Windows, uma vez que as condições de compatibilidade entre tais plataformas ainda são um pouco restritas. Por utilizar recursos criptográficos, o desempenho da comunicação dos dados entre as redes é ligeiramente mais baixo, já que o tamanho dos pacotes que trafegam na rede aumentam. Em contrapartida a comunicação é segura e as informações sigilosas podem ser transmitidas.

Com base no cenário implementado, confirma-se também que a utilização do serviço lógico VPN independe do tipo de conexão que o cliente utiliza para se conectar ao servidor, seja ela uma conexão de rede *Ethernet*, um acesso remoto, ou por meio de um provedor de Internet. Esta facilidade aqui demonstrada pode ser bastante útil, quando de sua aplicação na SEMED, dada a diversidade formas de acesso à internet entre a s unidades de ensino.

É importante registrar que à medida em que se propôs neste trabalho mostrar como implementar uma VPN em heterogêneo, detalhando aspectos de suas configurações, foi possível se aprofundar em diversos conceitos que embasam a teoria das redes de computadores, o que pode ser notado diante do capítulo de conceitos teóricos. Particularmente sobre VPNs, pode se aprimorar os conhecimento não só sobre seu funcionamento, mas sobre sua implantação e,

ainda, perceber que a VPN é uma tecnologia em crescimento, que vem sendo comercializada, pelas principais empresas de telecomunicações no Brasil e no mundo. São inúmeros os serviços oferecidos por elas e por outras companhias que trabalham com interligação de redes.

No entanto, diante dos estudos realizados ficou claro que uma VPN sozinha não consegue garantir a segurança de uma rede. É essencial que um planejamento cuidadoso seja feito, envolvendo políticas rígidas de segurança, treinamento de usuários e permitindo que haja proteção física e lógica dos servidores e clientes utilizados.

Assim sendo, este trabalho demonstra-se de grande valia para a aluna que o desenvolveu. Além disso, tal proposta constitui uma opção que demonstra ser de grande utilidade para a administração da educação municipal, figurada pela SEMED, revertendo-se em benefício de comunidade do município de Aracaju por completo. E podendo ser expandida para conexões similares em quaisquer regiões do país.

Uma possível sugestão para trabalhos futuros e de forma a aprimorar os conhecimentos nesta tecnologia seria a utilização de VPN com suporte a certificados digitais X.509 e ao algoritmo simétrico AES, tendo o presente trabalho como subsídio básico para tal.

6 REFERÊNCIAS BIBLIOGRÁFICAS

CHIN, Liou Kuo. **Redes Privadas Virtuais**. Rede Nacional de Ensino e Pesquisa : Boletim Bimestral Sobre Tecnologia e Redes, vol 2, nº 08: 1998. Disponível em: <http://www.rnp.br/newsgen/9811/vpn>.html. Acesso: 10 jan. 2011.

FAVARETO, André Luiz. **Serviços de Redes**. 1ª ed. Vila Velha: ESAB, 2003.

MARQUES, Alexandre Fernandez. **Segurança em Redes IP**. Monografia Submetida à ASIT, 2001.

MINASI, Mark. **Dominando o Windows Server 2003 - A Bíblia.** Makron Books: 2003.

MIRANDA, Aníbal D. A.. **Protocolos de Redes**. 1ª ed. Vila Velha: ESAB, 2008.

_____. **Introdução a Redes de Computadores**. 1ª ed. Vila Velha: ESAB, 2008.

MORAES, Alexandre Fernandes de. **Redes de Computadores – Fundamentos.** 1ª ed. Érica: 2004.

MORIMOTO, Carlos. **Redes Guia Completo.** ed. 3. e-book. São Paulo: 2004.

OLIVEIRA, Gilberto. **Segurança de Redes**. 1ª ed. Vila Velha: ESAB, 2009.

ORTIZ, Eduardo Bellincanta. **Vpn - Virtual Private Network - Implementando Soluções com Windows 2000 Server.** 1ª ed. Érica, 2002.

TANENBAUM, Andrew S. **Redes de Computadores**. 3ª Edição. Rio de Janeiro: Campus, 1997.

_____. **Redes de Computadores**. 4ª Edição. Rio de Janeiro: Campus, 2003.

TORRES, Gabriel; LIMA, Cássio. **O Modelo de Referência OSI para Protocolos de Rede.** Clube do hardware, 2007. Disponível em: <http://www.clubedohardware.com.br/artigos/1349>. Acesso: 11 fev. 2011.

SOARES NETO, Vicente. Silva, Adelson de Paula. C. Júnior, Mário Boscato. **Telecomunicações –Redes de Alta Velocidade – Cabeamento Estruturado**. São Paulo: Érica, 1999.

VASQUES, Alan Tamer. SCHUBER, Rafael Priante. **Implementação de uma VPN em Linux utilizando o protocolo IPSEC**. Pará: Monografia submetida ao Centro Universitário do Estado do Pará, 2002.

WADLOW, Thomas. **Segurança de Redes**. 1ª ed. Rio de Janeiro: Campus, 2000.