RADIAL FACULDADES E CENTRO DE EDUCAÇÃO TECNOLÓGICA
CURSO SUPORTE Á MICROINFOMÁTICA

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

Projeto Integrado

São Paulo
2005

RADIAL FACULDADES E CENTRO DE EDUCAÇÃO TECNOLÓGICA
CURSO SUPORTE Á MICROINFOMÁTICA

Projeto Integrado
4º Semestre

Gustavo Sester
Henrique M. Chaves
Hugo de Oliveira
Leandro S. Melo
Renato P. Laguna

Professor Responsável:
Lisandro

São Paulo
29/11/2005

ÍNDICE / SUMÁRIO

1. Introdução 5
2. Resumo 5
3. Cenário Atual 5
3.1. Problemática 5
3.2. Levantamento 5
3.3. Planejamento 6
4. Solução 6
4.1. Equipamentos e Estações. 6
4.2. Servidores 7
4.2.1 Backup's 7
4.2.2 Servidor de Banco de Dados, Arquivos e Antivírus 8
4.2.3 Servidor de Aplicação e Impressão 8
4.2.4 Servidor de AD, DHCP, DNS, WINS e Monitoramento 9
4.2.5 Servidor de Web, E-mail e Intranet 9
4.2.6 Servidor IDS 9
4.2.7 Servidor FireWall 9
4.3. Implementação do VoIP. 9
4.4. Segurança 11
4.4.1 Controle de Diretórios 11
4.4.2. Firewall HardWare 12
4.4.3. Firewall Iptables 13
4.4.4. Serviço Ipsec 15
4.4.5. Bastion Host 15
4.4.6. Antivírus Centralizado 16
4.4.7. Distribuição dos IP´s. 17
4.4.8. Redundância de link 17
5. Protocolos Principais 17
5.1 OSPF – Open Shortest Path First 17
5.2 VRRP – Virtual Router Redundancy Protocol 19
6. Topologias 19

6.1. Geral 20
6.2. Matriz 22
6.3. Filiais 23
7. Plantas 24
7.1. Planta do 1° andar - Matriz 24
8. Orçamento 26
9. Cronograma 27
10. Conclusão 28
11. Referencias Bibliográficas 29

1. Introdução

No projeto a seguir temos a solução de infra-estrutura de redes em sua parte física e lógica gerada a partir da proposta da empresa “É poco pra nois” que atua no ramo alimentício e possui ao todo 4 filiais conectadas a sua matriz. Foi pedido pelo gerente da empresas o Sr. Rogério Pereira um sistema de prevenção na matriz que funcione no sistema 24 horas 7, dias por semana, já nas filiais não requer toda a mesma estrutura porem deve ser boa suficiente á ponto de corresponder ás necessidades de redundância básica e não ficando mais do que um dia fora.

2. Resumo

Foi elaborado um projeto de solução buscando segurança performance e praticidade onde buscamos manter na matriz uma centralização de todos os dados contidos em 4 filiais e também do acesso a Web uma vez que hoje temos link´s individuais e não proporcional aos serviços atendidos, por tanto temos na matriz um investimento maior pois seu sistema de segurança requer mais cuidado e preparação. Nas filiais foram elaborados sistemas mais simples porem com capacidade de funcionamento equivalente ao apedido pelo cliente.

3. Cenário Atual

3.1. Problemática

- Falta de conexão entre matriz e filiais;
- Alto custo em telefonia;
- Link’s individuais e de baixa qualidade;
- Equipamentos mal distribuídos e com configurações inadequadas;
- Falta de segurança e política da mesma;
- Armazenamento de informações inadequadas e desorganizadas.

3.2. Levantamento

- Fazer levantamento local dos equipamentos;
- Verificar todos os equipamentos que devem ser adquiridos;
- Analisar quais equipamentos podem ser aproveitados;

- Analisar estrutura atual do cabeamento e da topologia existente;

3.3. Planejamento

- Interligar a Matriz as Filiais “4” ao todo;
- Fazer entrevistas com responsáveis para que se possam montar políticas de segurança;
- Distribuir funções, determinando objetivos e tempo disponível para cada tarefa, sendo que a distribuição de tempo para cada tarefa consta no cronograma.
- Elaborar um cronograma geral;
- Apresentar orçamento geral porem com previsões de alterações;
- Apresentar aos responsáveis o cronograma para realização do projeto. Onde poderá ser discutida alteração do mesmo buscando um bom senso geral;

Para que seja cumprido todos os pontos a cima será firmado um acordo com o as duas empresas prevendo uma multa de 50% baseada no valor de mão de obra no caso do não cumprimento de ambas.

4. Solução

4.1. Equipamentos e Estações.

O cliente possui na Matriz apenas 1 Servidor (Pentium 3 de 1GHz, 512MB de RAM, Hard Disk de 80GB e Windows 2000 Server), 49 Estações sendo que estas estão padronizadas com a mesma configuração (Pentium 2 500GHz, 128MB de RAM, Hard Disk de 10GB e Windows 98 SE). Nas duas filiais que já estão em funcionamento a configuração das estações são a mesma porem as filiais não possuem servidor. Para as filiais que serão abertas as configurações das estações deverão manter o mesmo padrão. O cliente também possui 1 Switch de 8 portas ligando 8 HUB´s de 12 portas para distribuir o sinal da Rede, o cabeamento é feito por cabos UTP em canaletas separada da rede elétrica. A topologia atual se baseia em desenhos feito pela pessoa que foi contratada para fazer a rede tanto da matriz como das filiais. De acordo com os dados acima citados solicitamos:

- 28 Servidores para Matriz e Filiais sendo que serão 5, para suportar os serviços de AD (Active Director), DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), WINS (Windows Internet Name Services) e

Monitoramento, 5 para Banco de Dados, Arquivos e Antivírus, 5 para Impressão e Aplicação, 5 para Backup Local, 5 para configuração de Firewall Ipsec e Iptables, 1 para IDS, 1 para Bastion Host e 1 para Backup Central.

- 6 Roteadores sendo que 2 ficaram na Matriz para dar suporte a uma rede 24h por 7 solicitado pelo cliente e os outros 4 serão para as respectivas filiais.
- As estações podem ser mantidas no padrão atual incluindo as duas novas filiais e o servidor existente será utilizado para espelhamento da configuração dos Roteadores que ficaram na Matriz. Alem das Estações que será adquiridas para as novas filiais de acordo com o cliente o total de 50 para cada uma será necessário a compra de uma a mais para cada filial, ou seja, mais 4 que servirão para o espelhamento de seus respectivos roteadores.
- Será necessária a compra de 750 conectores RJ 45, o cabeamento atual tanto da Matriz como das Filiais será aproveitado para fazer os Jack Box, e para o novo cabeamento pedimos um total de 12.500 metros de cabos UTP e 250 metros de Fibra Óptica Multimodo.
- O Switch e os HUB´s existentes não serão aproveitados por tanto pedimos a aquisição de 6 Switches de 8 Portas, 5 Switches de 12 Portas e 14 Switches de 24 Portas.
- A rede Elétrica devera ser revisada por uma terceira companhia onde deve ser verificado se a mesma se encontra nos padrões adequados para suportar o serviço. Na Matriz deverá existir um sistema que suporte quedas de energia para que a rede não possa parar pois não trabalhamos com sistemas de redundância de rede elétrica.

4.2. Servidores

A seguir teremos as definições básicas dos servidores que serão utilizados para a realização do projeto.

4.2.1 Backup’s

O backup dos dados da empresa será feito em duas etapas:

- Backup local e diário. Será feito o backup dos dados (a critério da empresa) diariamente, tanto na matriz quanto nas filiais. Será utilizada a ferramenta de

backup do próprio sistema operacional - Windows Server 2003. Os Backup's locais serão feitos manualmente por pessoa(s) específica(s) – (a critério da empresa). Os dados serão gravados não só nos HD's como também mídias e armazenados em locais específicos

- Backup Diário Centralizado. No final do dia, após o expediente, o backup que foi feito na matriz e nas filiais, serão enviados para um servidor de backup central, localizado na matriz. O software de backup utilizado no servidor de backup central será o S.O.S Backup Database da fabricante Virtos. O backup central será feito automaticamente, em horário agendado no próprio software. Os dados serão gravados e espelhados em HD's específicos.

Tanto os Backup`s locais quanto o central serão do tipo incremental, onde serão gravados apenas os arquivos que foram alterados depois do último backup. Os horários dos backup`s serão determinados de acordo com o melhor momento para que este não interfira no desempenho da Rede.

Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB no local e de 500 GB no Central.

4.2.2 Servidor de Banco de Dados, Arquivos e Antivírus

No servidor de banco de dados será instalado o SQL Server 2000 da Microsoft. Este servidor será acessado pelos principais aplicativos utilizados na empresa. Para ser acessado, o usuário precisará de uma conta com permissão, o mesmo servidor terá configurados os serviços de arquivos e antivírus. Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB.

4.2.3 Servidor de Aplicação e Impressão

O servidor de aplicação conterá todos os principais programas utilizados pela empresa. O serviço utilizado para gerenciamento dos aplicativos será o do próprio sistema operacional, Windows Server 2003 (GPO – Group Policy Object) de acordo com as permissões de acesso de cada usuário. O próprio Windows Server 2003 ira controlar também as impressões, através de seu serviço de impressão de acordo com as permissões nele configurado. Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB.

4.2.4 Servidor de AD, DHCP, DNS, WINS e Monitoramento

Para todos esses serviços será utilizado o Windows 2003 Server devidamente configurado. O monitoramento dos micros será feito pelo programa DameWare, onde este será instalado no mesmo e tendo acesso apenas pelas pessoas autorizadas. Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB.

4.2.5 Servidor de Web, E-mail e Intranet

Windows 2003 Server onde esta será configurada adequadamente para servir todos os serviços onde para e-mail será utilizado o Web Access 2003. Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB.

4.2.6 Servidor IDS

Windows 2003 Server devidamente configurado com Processador Pentium 4 HT de 3.0 Gb, 1 GB RAM, HD de 80 GB.

4.2.7 Servidor Firewall

Para os Firewall's Ipsec, Iptables será utilizado uma única estação Linux e para o Bastion Host uma outra estação também em Linux.

Processador Celeron D315 de 1.8, 512 MB RAM de Memória e HD com capacidade para 40 GB.

4.3. Implementação do VoIP.

O Voip será implantado com 12 pontos na matriz e 8 pontos em cada filial sendo todos no sistema FXS, desta forma poderá ser mantida uma conversação entre matriz e filiais disponibilizando ate 28 ramais para comunicação entre elas. Será utilizado para isso o *Gateway Phoneway 2500* com a implementação do Codec G723 utilizando uma banda de 18 kbps para cada ponto estabelecendo assim uma qualidade estável e segura da ligação.

O gateway irá trabalhar sobre um link de 2 Mb dividido para voz e dados, onde para voz estará sendo reservado 512 Kbps. A reserva de 512 Kbps permite o funcionamento simultâneo dos 28 canais com uma sobra de 8 Kbps o que pode evitar possíveis falhas de transmissão caso for utilizado mais do que 28 canais simultâneos

em caso de crescimento sem o aumento de link poderá ser feita a substituição dos Codec´s por um de menor consumo consecutivamente com menor qualidade. Exemplos de Codec´s que podem ser utilizados e que também são suportados pelo Gateway utilizado são os G729 de 7,3 a 36 kbps e G711, 70,2 a 82,7 kbps.

Descrições do equipamento *VoIP GW Mod. 4 slots mais Controle de Banda mais Gatekeeper.*

Os gateway VOIP Phoneway agregam a mais avançada tecnologia para conectar suas ligações telefônicas via Internet.

Com os equipamentos Phoneway, você terá a melhor qualidade de voz, devido a função QoS (Quality of Service) e ToS (Type of Service), além de possuir um algoritmo que garante a recuperação de pacotes, mesmo em redes com 20% de perda de pacotes.

Os Gateways phoneway possuem um recurso patenteado de aprendizado do tom de desconexão do PABX, garantindo que o equipamento se adequará a qualquer marca e modelo de PABX e não haverá o problema de travamento da porta do Gateway.

O equipamento phoneway já vem com software de bilhetagem gratuito. Os gateway Phoneway inter operam com Microsoft NetMeeting, CISCO, Lucent, OK1, RadVision, NetSpeak, equipamentos compatíveis com H.323 v2/v3 & H.323 Open Gatekeeper, entre outros.

O PHWS-2500GK conta com 4 slots, que aceitam módulos de 04 portas, 1 porta WAN e 1 porta LAN. Este equipamento possui o recurso de IP sharing, podendo estar na frente do Firewall/NAT, compartilhando o mesmo IP. O equipamento PHWS-2500GK, é empalhável até 10 peças permitindo a implementação de 160 portas em um único IP. Outra vantagem deste equipamento é o recurso de controle de banda que permite configurar quanto cada estação da rede vai usar para web e-mail ou para qualquer outro aplicativo, além de permitir a priorização de alguma aplicação (VoIP, ERP, etc.), e este recurso funciona em qualquer link de dados (Internet, ADSL, Wireless, Frame Relay, etc). Além de ser um gateway de Voz sobre IP (VoIP), este equipamento poderá atuar como o Gatekeeper de sua rede de VoIP.

4.4. Segurança

A segurança será tratada de uma geral, ou seja, espaço físico e lógico. Desta forma pedimos a empresa contratante uma colaboração e união dos representantes de cada setor para que seja feita as regras e que conseqüentemente cumpridas, pois a segurança de uma rede começa na ação do próprio funcionário da empresa.

4.4.1 Controle de Diretórios

Para os controles de diretório serão criados grupos distintos na configuração do Active Director, definindo permissões através de autenticação, cada usuário terá seu login e senha que deverá ser trocada conforme as regras estabelecidas e cada login fará parte de um grupo de usuários onde terá vinculado todas as permissões e bloqueios para este estabelecido, ou seja, através deste login script que estará vinculado a um determinado grupo ou usuário, será possível à configuração automática da estação local do usuário, bloqueando ou Liberando funções do computador como o acesso ao painel de controle ou a sites externos.

Para que isso seja possível será implementado também os serviços de Firewall e Proxy que podem ter configurados controles de pacotes na rede que será permitido ou não, dependendo do grupo o qual um usuário está vinculado. Para isso será instalado como proteção um servidor de Firewall, Proxy com o serviço (software) Squid e o Firewall Iptables.

Squid é um ProxyCache de alta performance para clientes Web, suportando protocolos FTP e HTTP. O Squid mantém meta dados e especialmente objetos armazenados em sua memória RAM, cacheia buscas de DNS e implementa cache negativo de Requests falhos, suporta SSL, listas de acesso complexas e loging completo. Por utilizar o Internet Cache Protocol, o Squid pode ser configurado para trabalhar de forma hierárquica ou mista para melhor aproveitamento da banda.

Podemos falar que o Squid consiste em um programa principal “squid” sistema de busca e resolução de nomes “dnsserver” e alguns programas adicionais para reescrever “requests”, fazer autenticação e gerenciar ferramentas de clientes. Visando aproveitar ao máximo a banda utilizaremos ProxyCache, segundo a Rede Nacional de Ensino e Pesquisa (RNP – http://www.rnp.br), com a utilização do ProxyCache

podemos ter uma economia que varia entre 3% e 50% nos momentos de maior consumo da rede, isso significa que para um link de 2 Mbps operando com toda sua banda, considerando uma redução de 30%, o mesmo produziria um ganho de aproximadamente 600 Kbps, ou seja, uma simples implementação de um ProxyCache gera uma economia que pode no final de um mês gerar grandes diferenças financeiras para a empresa.

4.4.2. Firewall Hardware

Será implementado o Firewall Hot Brick LB-2 VPN, é um firewall com 10 túneis de VPN e roteador com 2 portas WAN que combina soluções de compartilhamento da conexão banda-larga, segurança de rede, balanceamento de cargas e redundância feitas sob medida para proteger e dar performance às redes de pequenas e médias empresas. Estabelece conexões seguras entre localidades remotas suportando encriptações como DES, 3DES e AES, o LB-2 VPN também é um firewall com inspeção de pacotes, VPN IPSec, NAT avançado, detecção e proteção contra intrusos, filtro de conteúdo, bloqueio e controle à sites indesejáveis e controle de acesso com políticas distintas para diferentes grupos de usuários, o firewall LB-2 também é capaz de utilizar conexões redundantes, ou seja, no caso de uma conexão cair ele pode assumir outra automaticamente. Abaixo temos listados todas as suas especificações:

- Verdadeiro Firewall - NAT, SPI, anti DoS. Alertas de ataques via e-mail.
- 2 portas WAN de alto desempenho permitem duas conexões de banda larga redundantes, duplicando a largura de banda, além de determinar como o tráfego de internet é dividido entre elas.
- 10 Túneis de VPN simultâneos sem licenças.
- Suporta DSL e Cabo, IP fixo e/ou dinâmico, PPPoE e PPTP.
- Filtro de Acesso e Bloqueio de URL - permite política de acesso, divisão de usuários em até 5 grupos com políticas distintas. Bloqueio e controle à sites indesejáveis.
- Suporta múltiplos endereços IP, podendo mapear IP´s para cada PC
- Aplicações especiais - permite o uso de algumas aplicações não padrão, onde a porta usada para resposta é diferente da usada para a "pergunta".

- Servidor virtual - permite usuários acessarem servidores de internet na sua LAN.
- Limite de sessão - se o número total de novas sessões excederem o valor especificado, toda e qualquer nova sessão será ignorada.
- Exceção do Firewall - os pacotes podem não ser processados pelo firewall ou pelo modulo NAT, mas serão processados direto pelo sistema estático de protocolo.
- Suporta QoS - prioridade à pacotes específicos (phone, vídeo, etc.) configurável.
- Servidor DHCP - pode atuar como um servidor DHCP para até 253 usuários.
- Suporta multi-segmentos de rede, através de tabelas de roteamento estático.
- ARP Proxy - permite determinar um endereço de IP externo para uma porta LAN.
- Atualizações de Frameware por http (Web) e Backup sem licenças.
- Gerenciamento remoto (interface gráfica web).
- Switch 4 portas 10/100BaseT.
- Suporta DMZ / Múltiplos DMZ.
- Syslog.
- Suporta UPNP (Plug&Play Universal).

4.4.3. Firewall Iptables

Iptables é um Firewall que trabalha comparando endereço ou portas de origem e destino do pacote e etc, desta forma ele consegue saber quando um pacote tem ou não permissão para entrar ou sair da rede, com a utilização de configurações mais detalhadas, o pacote bloqueado pode ser registrado para que o administrador da rede tenha um maior controle do que está acontecendo em seu sistema. Aplicativos suportados pelo Iptables:

- Especificação de portas e endereço de origem e destino;
- Suporte a protocolos TCP / UDP / ICMP;
- Suporte a interfaces de origem e destino dos pacotes;
- Manipulação dos serviços de proxy na rede;

- Tratamento de tráfego dividido em chains (para um melhor controle do tráfego que entra e sai da estação e tráfego redirecionado) permitindo um número ilimitado de regras por chain;
- Rápido, estável e seguro;
- Mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados;
- Módulos externos para expansão das funcionalidades padrões, oferecidas pelo código de Firewall e também completo ao roteamento de pacotes, tratados em uma área diferente de tráfegos padrões;
- Especificação de tipo de serviço para priorizar o tráfego de determinados tipos de pacotes;
- Especificar exceções para as regras ou parte das mesmas e detecção de fragmentos;
- Envio de alertas personalizado ao syslog sobre o tráfego aceito ou bloqueado;
- Redirecionamento de portas e Masquerading;
- Suporte a SNAT (modificação do endereço de origem das estações para um único IP ou uma faixa de IP's e também DNAT modificação do endereço de destino das estações para um único IP ou faixa de IP's);
- Contagem de pacotes que atravessaram uma interface (regra);
- Limitação de passagem de pacotes ou conferência de regra (muito útil para criar proteções contra, syn flood, ping flood, DoS, etc).

Com a configuração do Firewall podemos prevenir aplicações como uma estação que esta tentando enviar seus pacotes para fora ou, por exemplo, no caso de uma estação Windows ser infectada por um Trojan, o firewall poderá bloquear qualquer tentativa de conexão vinda da Internet (cracker) para as estações de sua rede.

Os Chains são locais onde as regras do Firewall definidas pelo usuário são armazenadas para operação. Existem dois tipos de chains, os embutidos (como os Input, Output e Forward) e os criados pelo usuário. Os nomes dos chains embutidos devem ser especificados sempre em maiúsculas (note que os nomes dos chains são case-sensitive, ou seja, o chain input é completamente diferente de INPUT).

4.4.4. Serviço Ipsec

O IPSec é um protocolo que oferece serviços de criptografia, integridade e autenticação ao tráfego de rede com base em IP. Como o IPSec proporciona proteção entre servidores, ele pode ser usado para combater ameaças internas na rede, incluindo espionagem, violação, ataques por interceptação, spoofing de IP e outros ataques com base em senhas. O IPSec é completamente transparente para os aplicativos, pois os serviços de criptografia, integridade e autenticação são implementados no nível do transporte. Isto significa que os aplicativos continuam a se comunicar normalmente uns com os outros usando as portas TCP e UDP. Usar o IPSec a fim de restringir os protocolos e as portas que os clientes podem usar para se conectar a um servidor SQL.

4.4.5. Bastion Host

O que é: Bastion host é qualquer máquina configurada para atuar em uma rede sendo um ponto crítico de segurança, Marcus J. Ranum, um dos responsáveis pela popularidade deste termo na comunidade profissional de Firewall segundo ele "bastions são áreas críticas de defesa, em um castelo, por exemplo, são representadas por fortes muralhas, salas para tropas extras, e um ocasional e útil reservatório de óleo quente para desencorajar os atacantes". Um bastion host deve ser de estrutura simples e fácil, mais que possa garantir a segurança. É importante que se esteja preparado para o fato de que o bastion host seja comprometido, considerando que ele provavelmente será alvo de ataques. Existem mais de um tipo de bastion host, por exemplo, Dual homed host, Victim machines e Internal bastion hosts.

O bastion host tem responsabilidades diferentes do packet filter, dependendo do seu tipo. Alguns autores enfatizam que enquanto o packet filter atua em um nível mais baixo o bastion host se encarrega de todos os níveis. Na realidade, um host pode acumular tanto as funções de filtragem de pacotes como também pode prover alguns serviços, neste caso ele seria um packet filter e bastion host simultaneamente (exemplo: dual homed host). Independentemente de qual seja a nomenclatura adotada, o que se deve ter em mente é o papel que estes dois componentes desempenham: filtrar e prover serviços. Traçando um paralelo destes dois componentes em relação ao

modelo OSI, o packet filter realiza um exame dos pacotes até o nível 4 (transporte) enquanto que o bastion host se encarrega basicamente dos níveis superiores (fundamentalmente o nível 7, aplicação), também pode ser definido como application gateway porque funciona como um gateway a nível de aplicação. Os servidores disponíveis nos bastion host são denominados de proxy servers, ou seja, servidores por procuração que atuam como intermediários entre o cliente e o servidor. Neste caso, os serviços só podem ser providos via bastion host, obrigando o cliente (por exemplo, via regras de filtragem nos roteadores) a acessar estas máquinas, portanto, este é um mecanismo que garante que o serviço será provido de forma segura para usuários internos e externos e impede que o bastion host seja desviado.

Para que é utilizado: O bastion host é utilizado para fortificar uma rede contra invasões e atua basicamente em uma DMZ (Zona Desmilitarizada), e pode também servir como uma espécie de isca para que esta invadindo. Para se construir um bastion host deve – se seguir alguns passos básicos:

- Tornar a máquina segura;
- Desabilitar todos os serviços não desejados;
- Instalar ou modificar os serviços que se deseja prover;
- Reconfigurar a máquina a partir de uma configuração conveniente para desenvolvimento em seu estado final de execução;
- Rodar uma auditoria de segurança para estabelecer uma linha base;
- Conectar a máquina na rede na qual ela será utilizada.

4.4.6. Antivírus Centralizado

A vantagem da implementação de antivírus centralizado (servidor de antivírus) é a possibilidade de mantermos portas fechadas de acesso a Wan das estações locais sem que para isso o antivírus da estação deixe de ser atualizado. Desta forma todo o trabalho de atualização, escaneamento e remoção do vírus ficam pendurados em um único servidor dedicado. Este tipo de serviço é oferecido por todas as grandes fabricantes de antivírus existentes no mercado. Serão instalados softwares de antivírus clientes nas estações locais que executarão os comandos conforme as especificações do servidor de antivírus.

4.4.7. Distribuição dos IP´s.

A distribuição dos IP´s será feita através de servidores DHCP que irão distribuir os mesmos automaticamente para as estações trocando – os a cada 30 dias, no entanto, sera reservado uma faixa exclusiva para os servidores que terão seus IP fixos. Para isso sera usado a seguinte faixa privada “192.168.10.0/25 (255.255.255.128)”, sendo os IP´s “192.168.10.0” e “192.168.10.129 Rede e os IP´s “192.168.10.128” e 192.168.10.255” Broad Cast, desta forma termos um total de 126 IP´s disponíveis para cada Sub – Rede, porem utilizaremos somente a primeira Sub – Rede pois esta já supri o numero das estações o que nos da uma tranqüila porcentagem de crescimento, quase 150%.

4.4.8. Redundância de link

A redundância dos Link´s de conexão entre Matriz e Filiais já estão previstos nas próprias companhias de telefones, pois os mesmos serão feitos via VPN, como todas as filiais irão acessar a internet através da matriz a redundância desta parte sera feito na Matriz a inclusão de dois Link´s Wan de 2 Mbps cada um, porem sera feito com os mesmos um sistema de balanceamento, no caso da queda de um dos links a rede tem autonomia para operar com apenas um porem pode haver um pouco de lentidão. Na Matriz terá dois Roteadores sendo que cada um recebera um link desta forma se houver também a queda de um Roteador a conexão da rede não para. Para que isso seja possível sera utilizado o protocolo VRRP. Serão feitos também redundâncias internas nos empilhamentos de Switchs, neste caso utilizaremos a técnica de Spaning Tree para evitar infinitos Loop´s.

5. Protocolos Principais

A escolha dos protocolos VRRP e OSPF foram baseados no conceito de os mesmos serem protocolos de uso aberto (não proprietários), portanto podem ser utilizados em qualquer roteador disponível no mercado e que suporte os serviços neles aplicado.

5.1 OSPF – Open Shortest Path First

Desenvolvido pelo IETF – *Internet Engineering Task Force* [RFC 1583] como substituto para o protocolo RIP. Caracteriza-se por ser um protocolo intradomínio,

hierárquico, baseado no algoritmo de Estado de Enlace *Link-State* e foi especificamente projetado para operar com redes de grandes escalas. Outras características do protocolo OSPF são:

- A inclusão de roteamento por tipo de serviço TOS – *type of service routing*. Por exemplo, um acesso FTP – *File Transfer Protocol* poderia ser feito por um link de satélite, enquanto que um acesso ao terminal poderia evitar este link, que tem grande tempo de retardo, e ser feito através de um outro enlace;
- O fornecimento de balanceamento de carga, que permite ao administrador especificar múltiplas rotas com o mesmo custo para um mesmo destino. O OSPF distribui o trafego igualmente por todas as rotas suportando também o suporte a rotas para hosts, sub – redes e redes especificas;
- A possibilidade de configuração de uma topologia virtual de rede, independente da topologia das conexões físicas. Por exemplo, um administrador pode configurar um link virtual entre dois roteadores mesmo que a conexão física entre eles passe através de uma outra rede;
- A utilização de pequenos *hello packets* para verificar a operação dos links sem ter que transferir grandes tabelas. Em redes estáveis, as maiores atualizações ocorrem uma vez a cada 30 minutos.

O protocolo ainda especifica que todas os anúncios entre roteadores sejam autenticados (isto não quer dizer que necessariamente reflita a realidade das implementações). Permite mais de uma variedade de esquema de autenticação e que diferentes áreas de roteamento utilizem esquemas diferentes de autenticação;

Duas desvantagens deste protocolo são a sua complexidade, e maior necessidade por memória e poder computacional, característica inerente aos protocolos que usam o algoritmo de Estado de Enlace (Link-State).

O OSPF suporta, ainda, roteamento hierárquico de dois níveis dentro de um Sistema Autônomo, possibilitando a divisão do mesmo em áreas de roteamento. Uma área de roteamento é tipicamente uma coleção de uma ou mais sub – redes intimamente relacionadas. Todas as áreas de roteamento precisam estar conectadas ao *Backbone* do Sistema Autônomo, no caso, a Área 0. Se o trafego precisar viajar entre duas áreas, os pacotes são primeiramente rateados para a Área 0, o *Backbone*.

Isto pode não ser bom, uma vez que não há roteamento inter – áreas enquanto os pacotes não alcançam o *Backbone*. Chegando a Área 0, os pacotes são rateados para a Área de destino, que é responsável pela entrega final. Esta hierarquia permite a consolidação dos endereços por área, reduzindo o tamanho das tabelas de roteamento. Redes pequenas, no entanto, podem operar utilizando uma única área.

5.2 VRRP – Virtual Router Redundancy Protocol

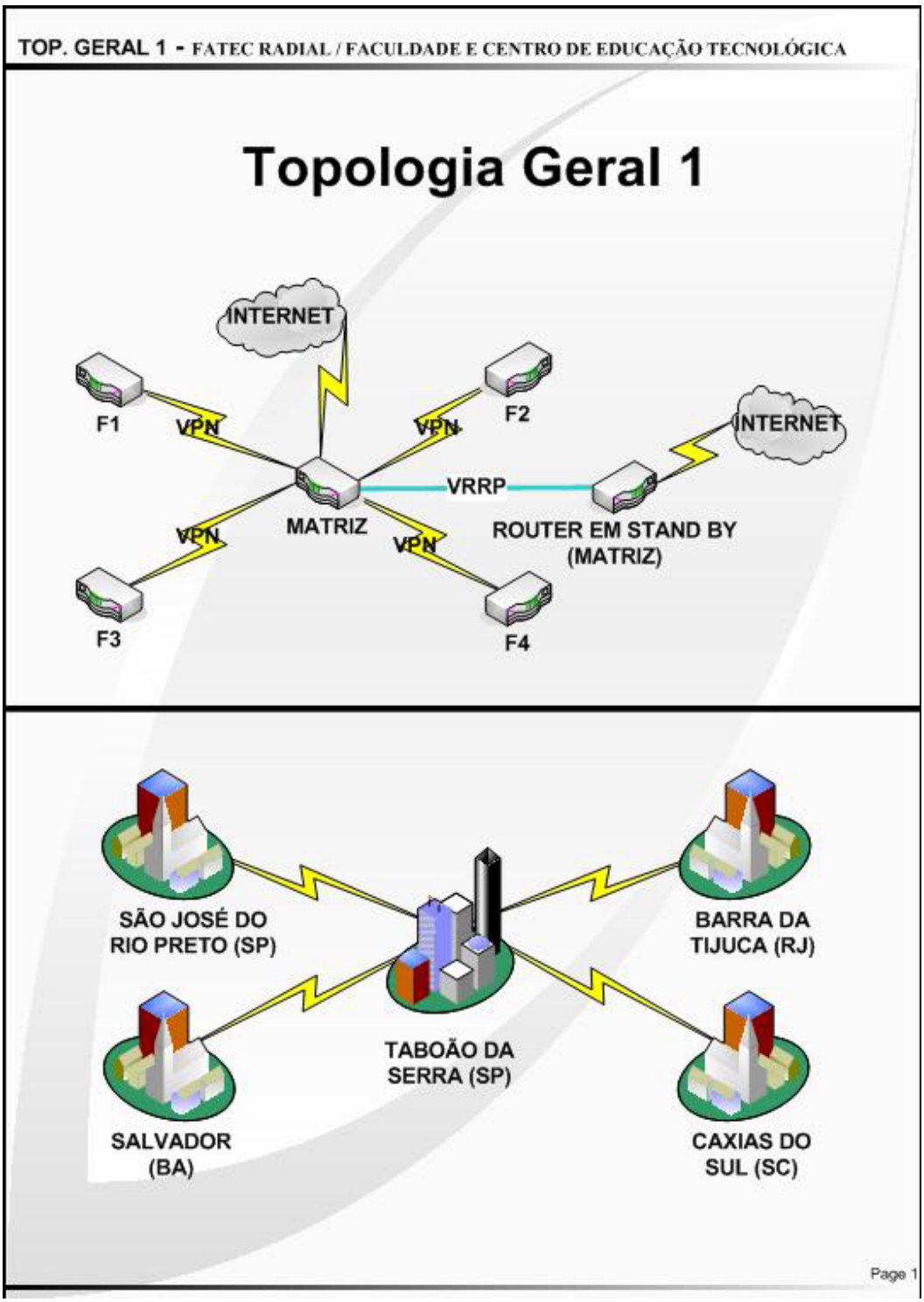
VRRP – é um protocolo executado na conexão entre os roteadores deixando um em espera e o outro ativo, fazendo com que o roteador que esta em espera sabe identificar quando o outro está em operação e se caso este venha a falhar possa assumir imediatamente sem que a rede tenha alguma paralisação. Este esquema se aplica as redes que necessitam de mais de um roteador criando no caso de saída da rede um único *Gateway* para eles, este pode ser especificado manualmente ou com protocolo dinâmico da configuração de um anfitrião DHCP. O Router que assumi a operação da rede é chamado de Router Mestre e o outros de Routers de apoio. Caso o mestre venha a falhar, como já foi dito antes um dos Routers de Apoio assume imediatamente e passa a ser o Router Mestre,

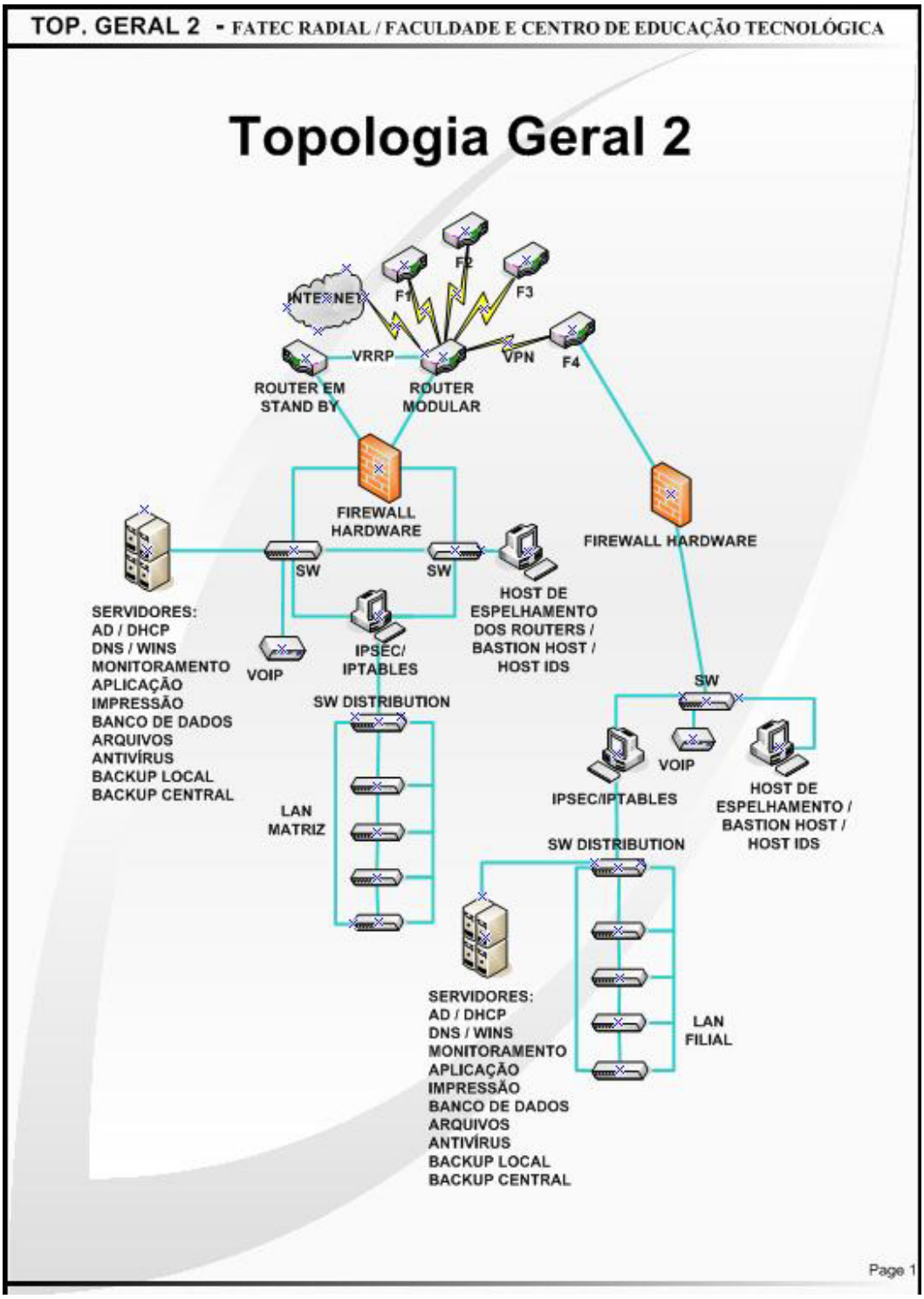
O VRRP pode também ser usado para balancear a carga e pode ser aplicado, tanto para Ipv4 como para o IPv6. Podemos usar também para este tipo de serviço o protocolo HSRP – *Hot Standby Router Protocol*, porem este seria proprietário CISCO podendo ser usados somente em roteadores da própria CISCO e foi desenvolvido tendo como base de estudos no VRRP.

6. Topologias

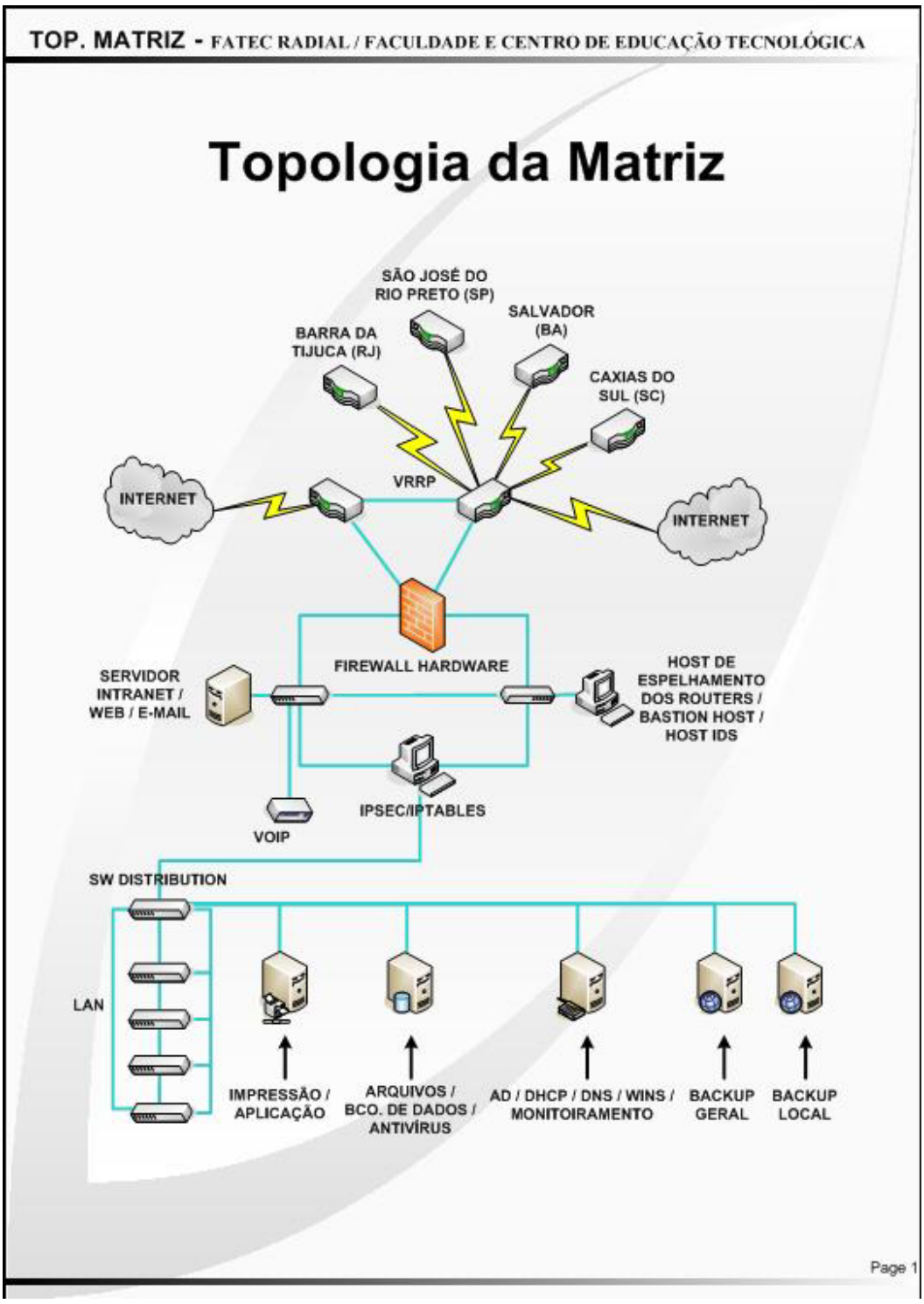
A seguir temos as imagens geradas através do software da Microsoft Visio, onde podemos esta vendo as topologias que serão implementadas no projeto. Estão disponíveis as topologias de conexão entre Matriz e filiais a qual chamamos de Geral, a topologia da Matriz e a das filiais a qual todas seguiram o mesmo padrão.

6.1. Geral

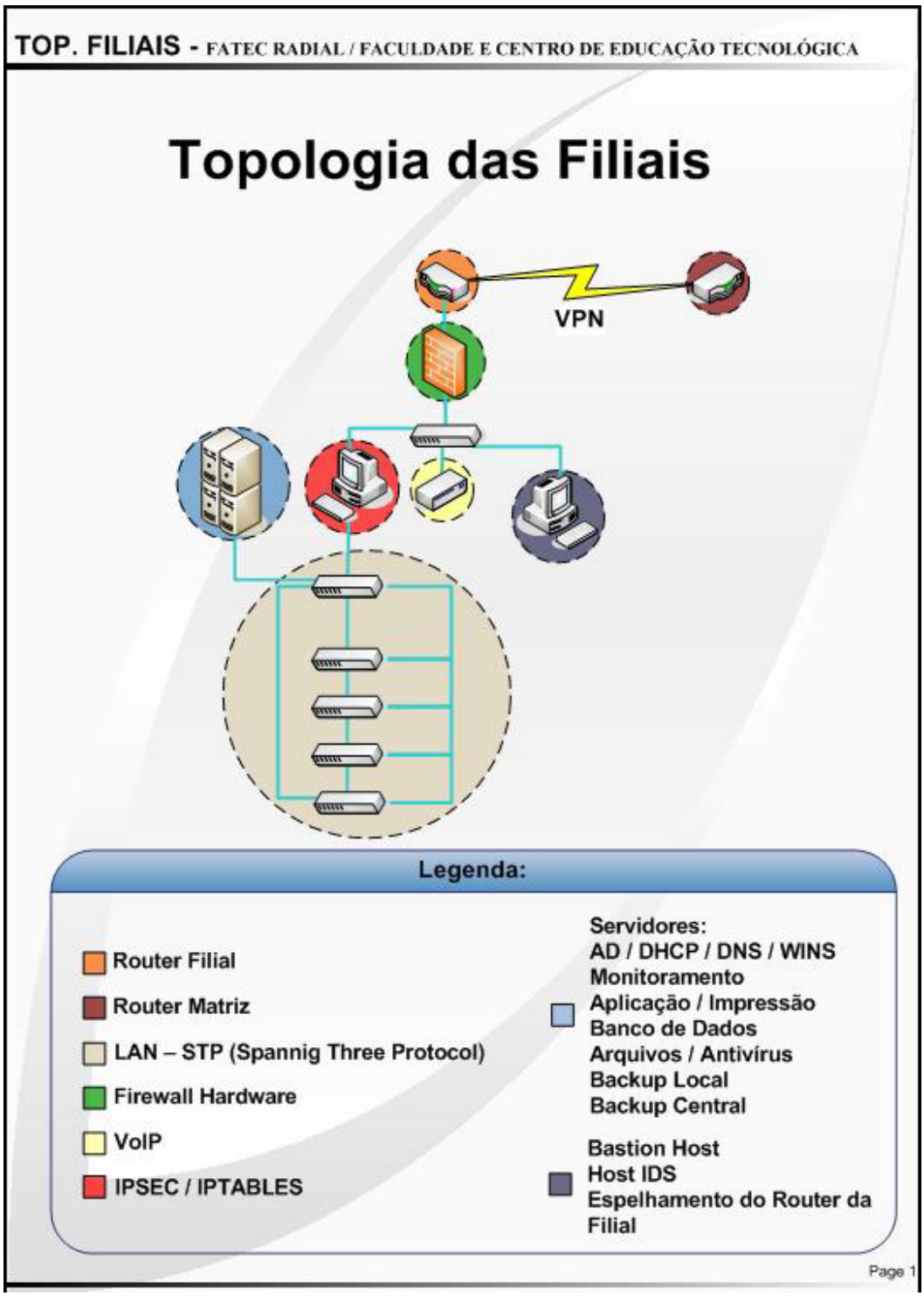

TOP. GERAL 1 - FATEC RADIAL / FACULDADE E CENTRO DE EDUCAÇÃO TECNOLÓGICA
Topologia Geral 1
INTERNET
F1
VPN
VPN
F2
INTERNET
VRRP
MATRIZ
ROUTER EM STAND BY
(MATRIZ)
VPN
VPN
F3
F4
SÃO JOSÉ DO
RIO PRETO (SP)
BARRA DA
TIJUCA (RJ)
TABOÃO DA
SERRA (SP)
SALVADOR
(BA)
CAXIAS DO
SUL (SC)
Page 1


TOP. GERAL 2 - FATEC RADIAL / FACULDADE E CENTRO DE EDUCAÇÃO TECNOLÓGICA
Topologia Geral 2
INTERNET
F1
F2
F3
F4
VRRP
VPN
ROUTER EM STAND BY
ROUTER MODULAR
FIREWALL HARDWARE
FIREWALL HARDWARE
SW
SW
SERVIDORES:
AD / DHCP
DNS / WINS
MONITORAMENTO
APLICAÇÃO
IMPRESSÃO
BANCO DE DADOS
ARQUIVOS
ANTIVÍRUS
BACKUP LOCAL
BACKUP CENTRAL
HOST DE ESPELHAMENTO DOS ROUTERS / BASTION HOST / HOST IDS
VOIP
IPSEC/ IPTABLES
SW DISTRIBUTION
LAN MATRIZ
SW
VOIP
IPSEC/IPTABLES
HOST DE ESPELHAMENTO / BASTION HOST / HOST IDS
SW DISTRIBUTION
SERVIDORES:
AD / DHCP
DNS / WINS
MONITORAMENTO
APLICAÇÃO
IMPRESSÃO
BANCO DE DADOS
ARQUIVOS
ANTIVÍRUS
BACKUP LOCAL
BACKUP CENTRAL
LAN FILIAL
Page 1

6.2. Matriz

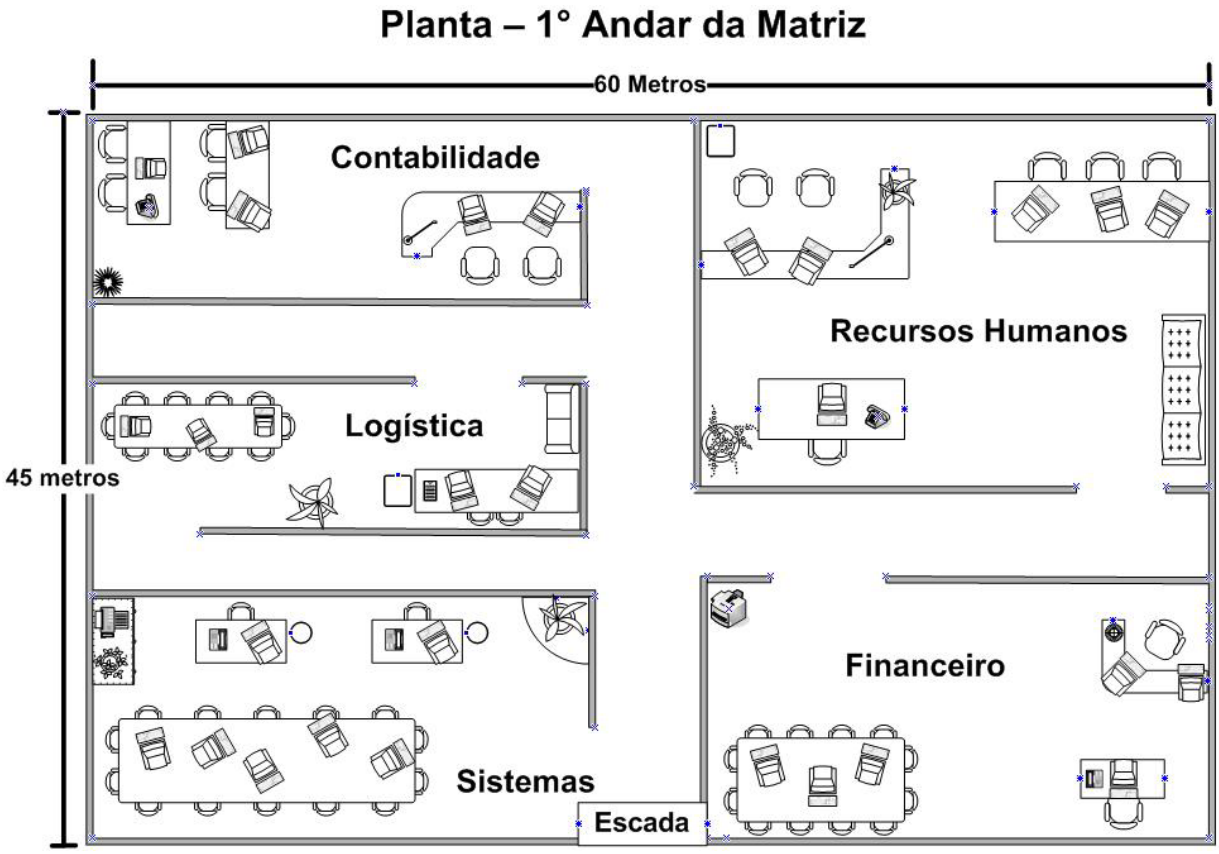

TOP. MATRIZ - FATEC RADIAL / FACULDADE E CENTRO DE EDUCAÇÃO TECNOLÓGICA
Topologia da Matriz
SÃO JOSÉ DO RIO PRETO (SP)
SALVADOR (BA)
BARRA DA TIJUCA (RJ)
CAXIAS DO SUL (SC)
INTERNET
VRRP
INTERNET
FIREWALL HARDWARE
SERVIDOR INTRANET / WEB / E-MAIL
HOST DE ESPELHAMENTO DOS ROUTERS / BASTION HOST / HOST IDS
IPSEC/IPTABLES
VOIP
SW DISTRIBUTION
LAN
IMPRESSÃO / APLICAÇÃO
ARQUIVOS / BCO. DE DADOS / ANTIVÍRUS
AD / DHCP / DNS / WINS / MONITOIRAMENTO
BACKUP GERAL
BACKUP LOCAL
Page 1

6.3. Filiais

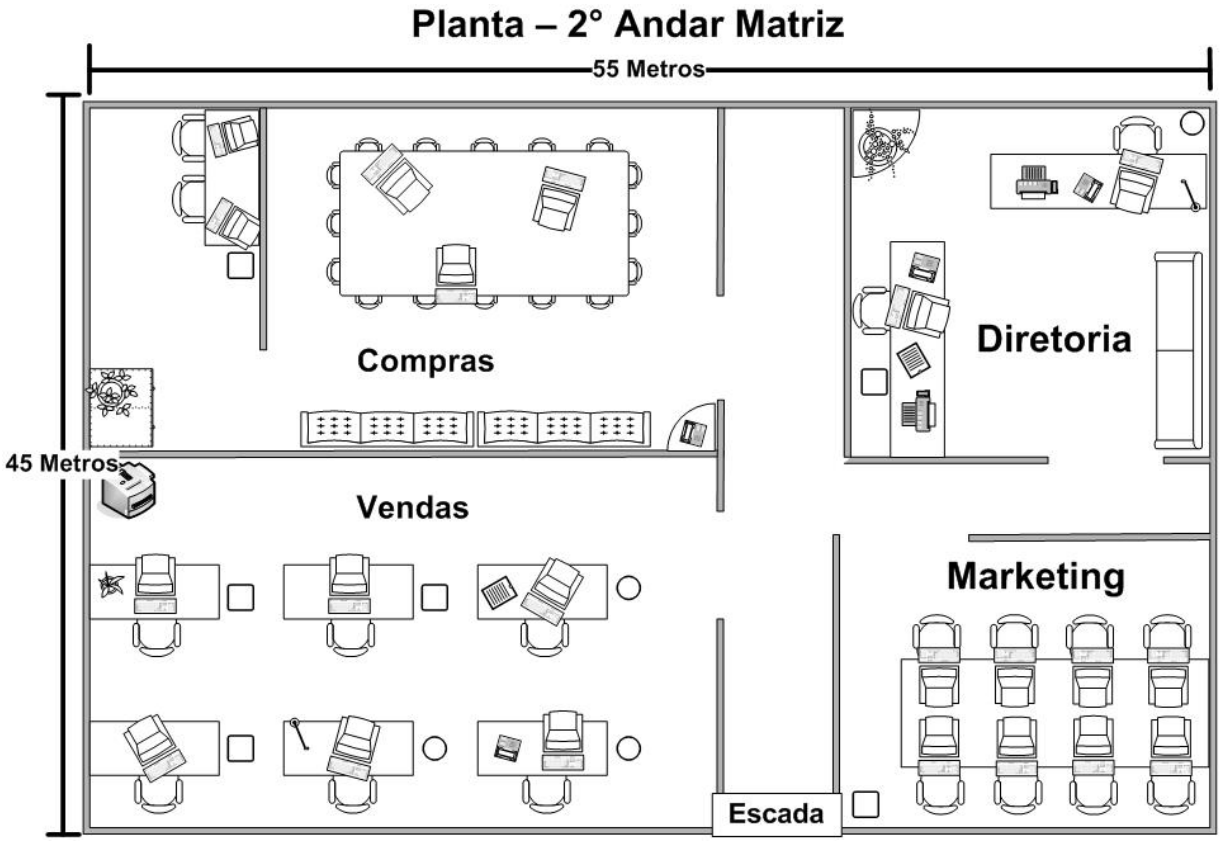

TOP. FILIAIS - FATEC RADIAL / FACULDADE E CENTRO DE EDUCAÇÃO TECNOLÓGICA
Topologia das Filiais
VPN
Legenda:
Router Filial
Router Matriz
LAN – STP (Spannig Three Protocol)
Firewall Hardware
VoIP
IPSEC / IPTABLES
Servidores:
AD / DHCP / DNS / WINS
Monitoramento
Aplicação / Impressão
Banco de Dados
Arquivos / Antivírus
Backup Local
Backup Central
Bastion Host
Host IDS
Espelhamento do Router da Filial
Page 1

7. Plantas

7.1. Planta do 1° andar – Matriz



7.2. Planta do 2º andar - Matriz



8. Orçamento

TABELA DE PREÇOS					
Equipamentos	**Fabricante**	**Modelo**	**Quant**	**R$ Unitário**	**R$ Total**
Conectores RJ 45	Furukawa	Padrão	750	R$ 0,30	R$ 225,00
Cabo UTP	Furukawa	24A	12500	R$ 3,00	R$ 37.500,00
Fibra Ótica	Furukawa	Mono e Multi Modo	250	R$ 4,50	R$ 1.125,00
Roteadores	CISCO	6500 Modular	6	R$ 8.200,00	R$ 49.200,00
SWITCH - 8 Portas	3COM	Office Conect	6	R$ 176,00	R$ 1.056,00
SWITCH - 12 Portas	3COM	2016	20	R$ 343,00	R$ 6.860,00
SWITCH - 24 Portas	3COM	2024	5	R$ 563,00	R$ 2.815,00
Canaletas	Banduith	Ban Poliuretano	100	R$ 12,00	R$ 1.200,00
Estações c/ montor	Montado p/ Equipe	Padrão da Empresa	4	R$ 1.250,00	R$ 5.000,00
Servidores AD, DHCP, WINS, DNS e Monitoramento	Montado p/ Equipe		5	R$ 2.500,00	R$ 12.500,00
Servidores de Aplicação e Impressão	Montado p/ Equipe		5	R$ 2.500,00	R$ 12.500,00
Servidores de Banco de Dados, Arquivos e Antivírus	Montado p/ Equipe		5	R$ 2.500,00	R$ 12.500,00
Servidores de Backup Local	Montado p/ Equipe		5	R$ 2.750,00	R$ 13.750,00
Servidor de Backup Central	Montado p/ Equipe		1	R$ 3.000,00	R$ 3.000,00
Servidor Bation Host	Montado p/ Equipe		1	R$ 1.750,00	R$ 1.750,00
Servidor IDS	Montado p/ Equipe		1	R$ 2.500,00	R$ 2.500,00
Servidores Fire Wall	Montado p/ Equipe		5	R$ 1.550,00	R$ 7.750,00
Fire Wall Hard Ware	Hot Brick	LB-2	5	R$ 2.499,00	R$ 12.495,00
VOIP Gatekeeper	Phoneway	GW 2500	11	R$ 500,00	R$ 5.500,00
Total de investimentos em Equipamentos					**R$ 183.726,00**
Valor cobrado pelo desenvolvimento do Projeto					**R$ 229.657,50**

Para visualizar o orçamento no Excel segure o CTRL e clique aqui.

9. Cronograma

Cronograma

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Agosto	10																											01			
Setembro	01		09		02				09			02				09			03					09			04				10
Outubro	09			05				09			06				09			06				09			07				09		08
Novembro		08																													

Legenda

01	Reuniao.
02	Visita.
03	Planejamento.
04	Desenvolvimento do Cronograma e Apresentacao.
05	Orçamemto Geral / Distribuição das Tarefas.
06	Inplementação.
07	dias disponiveis para Treinamento.
08	Dias reservados a esclarecimento da empresa contratante .
09	Finais de Samana não trabalhados.
10	Dias os quais nao fizeram parte do projeto.

10. Conclusão

Com a execução deste projeto teremos uma rede que trabalha com alta QOS – Qualidade de Serviço, otimizando o máximo todos os recursos necessários (dentro dos padrões da empresa), para suprir as necessidades desejadas pelo cliente, teremos também uma rede planejada para uma fácil ampliação prevendo já um futuro crescimento da empresa como um todo (Matriz e Filiais).

O projeto também foi elaborado para ter uma matriz que funcione baseado no sistema de Sete dias da semana, 24 horas por dia. Foram previstos para o projeto todo um sistema de segurança baseado no conceito de DMZ - Demilitarized Zone, com isso não só temos uma rede segura como também uma rede inteligente podendo detectar e resgatar dados do invasor.

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

11. Referencias Bibliográficas

Título: Construindo Redes Cisco para Windows 2000.
Autor: Craft, Melissa
Editora: Alta Books.

Título: Projeto de Interconexão de Redes - Cisco Internetwork Design.
Autor: Birkner, Matthew H.
Editora: Pearson Education.

Título: Redes de Computadores Curso Completo.
Autor: Torres, Gabriel
Editora: Axcel Books.

www.rnp.br
www.apostilando.com
www.projetoderedes.com.br