UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA DE REDES DE COMPUTADORES

LUÍS GUSTAVO JUNQUEIRA DE MACEDO

Soluções de Balanceamento e Contingência em Circuitos WAN

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. João César Netto
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

AGRADECIMENTOS

Gostaria de agradecer a minha esposa Michele Gorga Azambuja e jovem filha Rafaela Azambuja Macedo, pelo tempo dos finais de semanas despendidos aos estudos neste curso de Especialização em Tecnologia, Gerência e Segurança de Redes realizado no Instituto de Informática da Universidade Federal do Rio Grande do Sul. Foi importante que minha família acreditasse no projeto e na necessidade desta formação no encaminhamento do meu desenvolvimento profissional para me apoiar nos momentos mais difíceis e cansativos.

E também gostaria de fazer referência aos meus pais, Antônio Luís de Almeida e Macedo e Ana Fátima Junqueira Macedo. A influência dos mesmos em minha infância me ensinou a acreditar na busca contínua e interminável pelo desenvolvimento e conhecimento na área de interesse, e na formação do meu caráter sério e profissional em minhas tarefas. Por eles, tenho ciência que não existem limites ao saber. Um abraço especial as minhas duas irmãs Andréa e Flávia.

Dedico este trabalho aos profissionais da Consultoria de Soluções da Embratel localizados em Porto Alegre, mais precisamente ao Mastella, Osvaldo e Peccolo que desapertaram em um jovem ainda não formado na Engenharia Elétrica o interesse pela área de redes de dados e telecomunicações.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

A	Availability
BGP	Border Gateway Protocol
CE	Customer Equipament
CPE	Customer Premises Equipment
EIGRP	Enhanced Interior Gateway Routing Protocol
FR	Frame Relay
GEEDS	Gerência, Escalabilidade, Disponibilidade, Desempenho e Segurança
GLBP	Gateway Load Balancing Protocol
HSRP	Hot Standby Redundancy Protocol
IGRP	Interior Gateway Routing Protocol
IOS	Internetwork Operational System
IP	Internet Protocol
LAN	Local Network Area
MAC	Media Access Control
MLPPP	Multi-Link PPP
MPLS	Multi-Protocol Label Switching
MRTG	Multi Router Traffic Grapher
MTTR	Mean Time to Repair
MTBF	Mean Time Between Failure
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PBR	Policu Based Routing
PE	Provider Edge
PNC	Plano de Continuidade de Negócios
PPP	Point-to-point Protocol
PPS	Pacote por Segundo
QoS	Quality of Service

RIP	Routing Information Protocol
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Este trabalho tem como objetivo apresentar técnicas e análises para dimensionamento de soluções de redes chamadas de longa distância. Serão abordadas propostas de topologia de balanceamento e/ou contingência através de protocolos contidos na camada dois (enlace) e três (redes) do Modelo de Referência OSI (Open Systems Interconnection), estruturado em sete níveis.

Não serão criados novos protocolos ou algoritmos de redes, mas será estudado uma série de protocolos e facilidades, que trabalhando em conjunto, são capazes de formar soluções estáveis e robustas para circuitos WAN (Wide Area Network).

Também avaliará a dependência tecnológica das empresas, e como conseqüência a crescente importância dos circuitos de longa distância nas pequenas, médias e grandes corporações, demandando projetos de alta disponibilidade e planos de continuidade de negócio. Farei um paralelo bastante interessante entre os negócios das grandes instituições e os conceitos extremamente técnicos que estudamos na área de redes e telecomunicações.

.

Palavras-Chave: WAN, redes, disponibilidade, contingência e balanceamento.

Balanced and **C**ontingency **S**olutions to **WAN C**ircuits

ABSTRACT

This paper presents techniques and analysis for the right dimension solutions for long distance networks. We present balancing topology and/or contingency propositions through protocols embedded on the second layer (link) and third layer (networks) of the OSI (Open Systems Interconnection), Reference Model, which is structured in seven levels.

Neither new protocols nor network algorithms will be created, but a series of protocols will be studied. Protocols that working at the same time, are capable of forming stable and strong solutions for WAN (Wide Area Network) circuits.

The study also assesses the technological dependence of companies, and, as a consequence, the growing importance of long distance circuits in small, medium and big corporations, demanding high disponibility projects and business continuity plans. I will draw a very interesting parallel between business in big companies and the extremely technical concepts studied in telecommunications and networks.

Keywords: WAN, nets, availability, contingency and balance.

1 INTRODUÇÃO

Este trabalho de conclusão do curso de Especialização em Tecnologia, Gerência e Segurança de Redes foi desenvolvido para abordar um tema que foi pouco explorado nas aulas do curso. A crescente importância da área de TI e redes de computadores nas empresas, até certa dependência das mesmas, e as tecnologias e soluções utilizadas nos dias atuais para desenvolver projetos que garantam maior confiabilidade e disponibilidade nas conexões de redes entre matriz e filiais e também no circuito que provém internet ao site central.

A verdade é que não existem fórmulas prontas para um projeto de contingência e/ou balanceamento e sim técnicas a serem utilizadas, e o funcionamento da solução será responsabilidade direta do funcionário que fez seu desenvolvimento.

Através deste, abordaremos uma evolução destas necessidades, faremos uma revisão teórica nos conceitos e protocolos que nos ajudarão a formatar um projeto, e concluiremos com alguns estudos de caso.

Mesmo com todo avanço tecnológico, a verdade é que os projetos e falhas passam por mãos humanas. Isso ocorre por ser um ambiente extremamente variável, onde existe abertura para diversas topologias físicas e lógicas, e cada profissional em sua empresa desenvolve sua rede de acordo com idéias e conhecimentos próprios.

E ainda existe a questão dos recursos disponibilizados a área de TI, que não são vistos como investimentos e sim como gastos de necessidade questionável. A verdade é que os diretores de determinadas instituições só analisam o tamanho do prejuízo de uma queda de circuito em um fábrica quando a mesma acontece, e gera perdas reais de produção.

1.1 Importâncias de Redes de Dados nas Corporações

A evolução das redes de dados nas corporações acompanhou a este mesmo crescimento dos computadores e m nossas casas. Não faz muito tempo, ter um computador era um luxo. O alto custo de aquisição, a reserva de mercado e o próprio sistema operacional criavam obstáculos que impediam o desenvolvimento da competitividade de empresas brasileiras no mercado internacional, ao contrário de suas concorrentes estrangeiras.

Com o advento do Windows, com a queda da reserva de mercado e com a redução de custos de aquisição, qualquer empresa -por menor que seja- só funciona atualmente se possuir um microcomputador. Pelo menos, para emissão de cupons fiscais.

Esse diferencial que agregou velocidade, escalabilidade e, principalmente, economia de recursos, gerou uma característica inesperada: a dependência.

Hoje em dia, raríssimas empresas possuem máquinas de escrever manuais. Pouquíssimas mantêm um arquivo em papel. Quase nenhuma deixa de acessar seu extrato bancário pelo computador. E isso, independente do tamanho da companhia. É claro que, quanto maior a empresa ou a sofisticação de seus produtos ou serviços, mais dependente de TI ela deverá ser, demonstrando o meio de sua manutenção no mercado. Entretanto, para o gestor de TI, surge uma equação de difícil solução: como definir os investimentos para o setor frente à necessidade de prestar suporte aos processos de negócio da sua empresa? Pode-se investir na melhoria de desempenho ou em proteção dos atuais recursos, ou ainda um back-up site pode ser proteção suficiente para impedir eventuais paradas dos componentes de TI.

A resposta à esta pergunta é extremamente pessoal face às características de cada empresa. Cada processo possui um tempo de resposta próprio e cada segmento de mercado possui uma determinada velocidade de realização do seu ciclo de negócio, inviabilizando um padrão único de avaliação.

Podemos pensar em perguntas como qual a velocidade do negócio de uma empresa de “call center”, ou de uma indústria? E se esta indústria for de algum equipamento de tecnologia ou comunicação, o seu ciclo será maior, provavelmente.

Na verdade, os investimentos em serviços de conectividade parecem ser custos não "visíveis", ao contrário da aquisição de um novo servidor ou de um aplicativo mais dinâmico. São custos que só se fazem perceber em situações de ameaça de parada, justificando seus gastos pela redução do tempo de parada da empresa ou pela manutenção dos negócios da empresa, frente a eventos.

O real valor do investimento em segurança de dados e sistemas é uma questão que nunca será respondida, a não ser em situações de exceção como quando o nosso servidor trava, quando nosso link é interrompido ou quando nossa rede é invadida por vírus. É correto imaginar que estas situações não são regras. Mas quando prevemos o custo de recuperação (direto e indireto) para os processos que dependem de TI, começamos a nos preocupar.

Pior, começamos a pensar se devemos "gerenciar" o risco de sofrer estes tipos de eventos ou se devemos realmente gastar um percentual de nossos limitados recursos, não para sua prevenção (que é nossa obrigação, como gestores do setor), mas para a mitigação de suas conseqüências, quando ocorrerem.

Em empresas multinacionais ou instituições financeiras, esta é uma realidade diária. No primeiro caso, por imposição cultural de países que sofrem ou sofreram de ameaças naturais e humanas que historicamente justificam o investimento em Planos de Contingência e de Continuidade de Negócios.

No segundo, devido a fortes imposições normativas que regulam o seu funcionamento. A maioria dos profissionais de TI acaba escolhendo o investimento em back-up sites como forma de proteger suas atividades, esquecendo que o negócio ou aplicativos não são diretamente relacionados aos processos deles dependentes.

1.1.1 Plano de Continuidade de Negócios

O conceito PCN vem a agregar no meu estudo de projetos de contingência e balanceamento de circuitos WAN. É um termo relativamente novo, resultante dos

Planos de Contingência e dos Planos de Recuperação de Desastres. Genericamente falando, o PCN é uma metodologia desenvolvida para garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e dos danos nos componentes (softwares, hardware, infra-estrutura, etc.) por ele utilizados.

Na verdade, as atividades de qualquer empresa dependem muito mais do fluxo de atividades que dependem de TI, do que dos próprios dados nele contidos. Em última instância, para efeito de simplificação, qualquer novo negócio fechado pode ser finalizado independente de outros já em andamento. É uma questão de normatização.

Por outro lado, a criação de Planos de Contingência Operacional e de Continuidade de Negócios sem uma validação externa poderá levantar o questionamento a respeito de sua validade frente às situações de crise reais.

No caso de ocorrer um evento real, quem pagará a conta no caso de falha? Os estagiários que atenderam às ordens superiores ou os gestores ligados aos processos afetados?

Como o custo de operação é elevado, as instituições estão atualmente investindo em meios de proteger as operações, por força normativa. Mas limitações existem, de várias origens e formas.

No caso de instituições bancárias, não é apenas um "back-up site" que vai garantir a continuidade das operações. É imprescindível que seus processos sejam mapeados e planificados para que, caso se concretize qualquer ameaça ao processo, possa responder dentro do limite de tempo exigido.

Assim ocorre com outras situações de negócio, como o "call center", que não pode deixar de atender ao cliente frente à ameaça de perda da venda ou do próprio cliente, insatisfeito com a ausência de atendimento.

A gerência de TI, nos dias de hoje, está muito mais voltada para resultados mensuráveis de seu desempenho do que a simples gestão de hardware ou software. A área de informática da maioria das grandes empresas é vista como um setor de negócios, cuja principal missão é a de oferecer suporte ao principal processo de negócio da empresa, seja ela do segmento que for. Penso que se não pensarmos desta forma, estaremos fadados à inércia de uma fase que já passou, quando a informática era vista como um luxo ou uma necessidade de poucos abastados.

O brasileiro é um povo assumidamente tranqüilo, quando o assunto é segurança. Geralmente, só consertam a fechadura da casa, depois que os ladrões ficam sabendo que ela tem um defeito.

Um histórico de sucessos e finais sem dificuldades não devem ser considerados como situações predominantes em ambientes de negócios. As variáveis que compõe uma equação empresarial são muito heterogêneas, cada vez mais dependentes de terceiros, por vezes situados fora da mesma localidade para a qual presta serviço.

Quando falamos em PCN, não estamos nos preocupando com o tipo de desastre que ameaça a Empresa. Estamos preocupados, com a sua continuidade, frente aos riscos que podem se concretizar.

Diferentemente de um seguro, que está voltado para a redução na perda, o PCN está voltado para a redução do impacto nos negócios da empresa, haja vista a quantidade de conseqüências negativas que podem acompanhar uma ocorrência.

Conseqüências que vão desde a perda financeira (que geralmente é o ponto fundamental para sensibilizar o principal executivo da empresa, na compra de um seguro ou na contratação de um especialista em PCN), até a própria perda de mercado, devido à parada da empresa por um período crítico.

A realidade no Brasil, lugar onde trabalhamos, onde as ameaças são ocasionais, os executivos continuam se deixar levando pela tranqüilidade de quem prefere não pagar por uma possibilidade, do que assinar um pedido de despesas para algo que poderá nunca ser utilizado.

1.2 A Busca por Soluções sem Falhas

Desde o início de soluções de redes, vem aumentando a demanda por projetos e/ou topologias que buscam a perfeição em termos de alta disponibilidade. Ao fornecer circuitos de contingência, deve-se aprender o máximo sobre as características e necessidades do cliente.

Este é o momento de fazer batimentos para saber quais são os objetivos do projeto ou ainda, porque o solicitante está demandando tal tarefa. Deve-se pensar se teremos contingência, balanceamento, os dois, ou o chamado *disaster recovery*. E entender quais são os níveis de contingência devem ser contingenciados.

Diferentes operadores às vezes usam as mesmas instalações, significando que o seu caminho de backup é suscetível às mesmas falhas do caminho principal. Neste ponto, entra a estrutura básica de estudo em três pontos: roteadores backcbone (PE - *Provider Edge*) acesso de última milha e roteador do cliente (CPE - *Customer Premises Equipment*). Deve-se realizar um trabalho investigativo para assegurar que o caminho chamado secundário realmente é um backup. Utilizamos também o termo diversidade de circuitos para se referir à situação ótima de circuitos que usam caminhos diferentes.

Como as operadoras alugam capacidade umas às outras e usam empresas independentes que fornecem capacidade a várias operadoras, fica mais difícil garantir a diversidade de circuitos. À medida que as operadoras usam cada vez mais técnicas automatizadas para repetição de roteamento de circuitos físicos, torna-se ainda mais complicado planejar a diversidade, pois a repetição de roteamento é dinâmica.

1.2.1 Estudo do Risco

A análise de gestão do risco faz parte do trabalho para desenvolver topologias de alta disponibilidade. Define-se por risco um evento (acontecimento) ou condição (situação) incerta que, se ocorrer, provocará um efeito, neste caso negativo, nos objetivos do projeto. Ainda inclui-se neste estudo a identificação, avaliação de impactos e probabilidades, planejamento de respostas e monitoração/controle dos riscos.

Quando direcionamos a área de redes, enxergamos algumas causas de problemas recorrentes como falhas de hardware ou software, erros humanos de projetos, desastres naturais, entre outros.

Na verdade, como o principal foco de um trabalho de soluções de alta disponibilidade é a continuidade de processos frente ocorrência de eventos, aproveitamos suas conseqüências para elaborar um índice que indica a importância de cada um. Os riscos, sempre inerentes a processos, lugares e pessoas, são particulares.

Não podem ser generalizados, tampouco avaliados sem uma vistoria pessoal. É uma variável extremamente subjetiva: dependendo do objetivo que perseguimos, podemos considerar itens agravantes ou não.

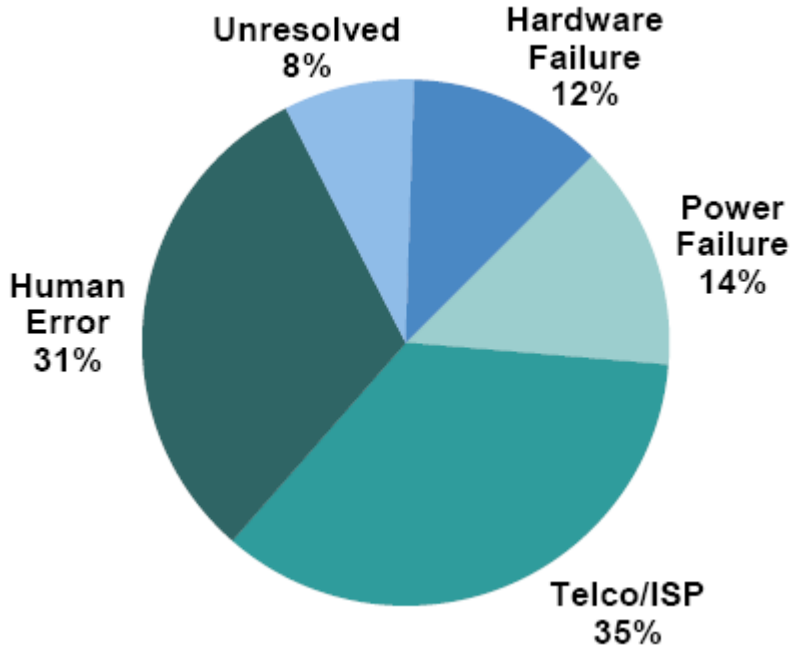

Figura 1.1: Distribuição de problemas de redes

1.2.2 Definições de Redundância, Contingência e Balanceamento

É bastante comum utilizarmos as palavras redundância e contingência. Por isso resolvi neste item fazer breve explanação destes conceitos e ainda inseri-los no contexto deste trabalho.

O projeto bem sucedido de uma rede de computadores pode ser representado pela capacidade desta em oferecer os serviços essenciais requeridos por seus usuários e por preservar os seus principais componentes na eventual ocorrência de falhas.

A fim de prevenir eventuais falhas e oferecer alternativas que evitem que estas acarretem maiores prejuízos, se faz necessário que os projetos contemplem planos de redundância e contingência constituídos por uma série de ações e procedimentos que visam soluções e dispositivos de recuperação relacionados com essas falhas.

No ambiente das redes de computadores podemos destacar vários aspectos críticos que podem ser considerados pontos de falhas potenciais para o sistema: cabeamento, servidores, subsistemas de disco, entre outros. Nesse contexto, as falhas são consideradas como eventos danosos, provocados por deficiências no sistema ou em um dos elementos internos dos quais o sistema dependa.

As falhas podem ser derivadas de erros no projeto do software, degradação do hardware, erros humanos ou dados corrompidos. Entretanto, só existem duas variáveis

para a paralisação temporária de uma rede em função de condições de falha que não se podem definir ou prever redundância.

O termo redundância descreve a capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes, ou seja, um sistema redundante possui um segundo dispositivo que está imediatamente disponível para uso quando da falha do dispositivo primário do sistema.

Uma rede de computadores redundante caracteriza-se, pois, por possuir componentes como sistemas de ventilação e ar condicionado, sistemas operacionais, unidades de disco rígido, servidores de rede, links de comunicação e outros, instalados para atuarem como backups das fontes primárias no caso delas falharem.

Essa redundância significa que se um sistema falhar (primário), deve ser o outro sistema tão eficiente e operacional como o primeiro, pronto para entrar em operação, testado, treinado e suficiente.

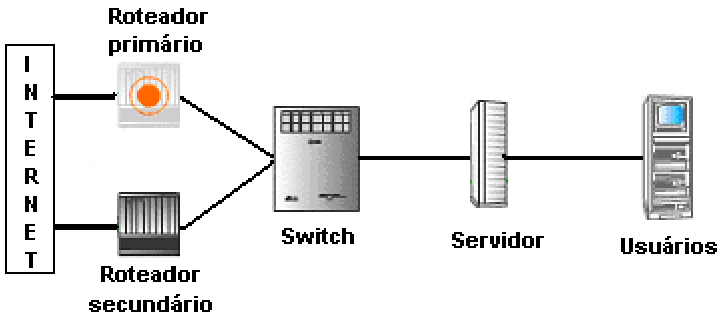

Figura 1.2: Estrutura básica de redundância

No exemplo da figura acima, com a falha do roteador primário, imediatamente o secundário entrará em atividade de forma a manter o funcionamento ininterrupto da comunicação da rede local com o ambiente externo (Internet).

Outro exemplo de redundância está em múltiplas estações de trabalho usadas para monitorar uma rede. A perda de uma estação não prejudica a visualização ou a operação do sistema. Nesse caso, um servidor de banco de dados (igualmente redundante) garante que nenhuma informação seja perdida, na hipótese de falha do servidor primário.

Podemos ter também a redundância física de um subsistema de alimentação de energia, projetado para prover chaveamento automático no caso de falha pelo acréscimo de uma segunda fonte. Nesse subsistema redundante, as fontes possuem a mesma capacidade e, no caso de falha de uma delas, a outra assume instantaneamente toda a carga da rede.

Outro aspecto que deve ser considerado é a contingência operacional proporcionada pela redundância de equipamentos. Quanto maior a vulnerabilidade de um sistema dentro de uma rede, maior a redundância necessária para garantir a integridade dessa rede. Em alguns casos, porém, a simples contingência representada pela redundância dos equipamentos e do processo de backup não são suficientes para tornar o *downtime* compatível com a necessidade operacional da empresa.

Quanto à contingência define-se como a possibilidade de um fato acontecer ou não. É uma situação de risco existente, mas que envolve um grau de incerteza quanto à sua efetiva ocorrência. As ações de contingenciamento são encadeadas, e por vezes sobrepostas, de acordo com procedimentos previamente acordados no projeto da rede. O seqüenciamento das ações depende dos acontecimentos que precederam o evento (contingência) bem como das condições contextuais que vão sendo construídas no próprio processo, ou seja, o processo de contingenciamento é construído e negociado à medida que a interação se processa.

Sucintamente, as condições necessárias para a existência de uma contingência são: possibilidade de um acontecimento futuro resultante de uma condição existente, incerteza sobre as condições operacionais envolvidas e a resolução destas condições dependerem de eventos futuros.

O projeto do contingenciamento da rede deve estar baseado em políticas que visem alta disponibilidade de informações e sistemas, através de suporte técnico, sistemas de segurança, esquemas de backup, planos de contingência, redundância de equipamentos e canais de comunicação e gerenciamento pró-ativo. O objetivo é implantar, conectado à estrutura de rede de computadores, um plano de acesso seguro, eficiente e gerenciado, capaz de restabelecer as funções críticas numa situação excepcional.

Inicialmente, utilizávamos uma redundância estática. Ou seja, após a percepção de queda do circuito primário, existia um chaveamento manual para o circuito secundário, dependendo de intervenção humana.

Depois, o processo de contingência passou a ser automático, porém o acesso secundário não tinha a mesma capacidade de carga do circuito original. Tínhamos como exemplo, uma linha dedicado como principal e uma segunda tecnologia, como acesso discado, para pelo menos manter o site no ar, mesmo que não atendendo efetivamente todas as aplicações necessárias.

Por último, passamos a utilizar duas linhas idênticas, com chaveamento automático e com o chamado balanceamento de carga. O balanceamento faz com que as duas linhas fiquem disponíveis com desempenho muito superior, e em caso de queda em uma delas, a restante suportaria o site e suas aplicações a contento.

Pelo fato de links de WANs poderem ser peças críticas de uma rede corporativa, links de WANs redundantes (de backup) são incluídos freqüentemente em uma topologia. Uma rede WAN pode ser projetada com uma malha total ou parcial.

Uma topologia de malha total oferece redundância completa. Ela também proporciona bom desempenho, porque há apenas um retardo de um link entre dois locais quaisquer. Porém esta proposta é mais dispendiosa para implementar, manter, atualizar e solucionar problemas. É, com freqüência, caro demais projetar uma WAN em malha completa.

Não obstante, pode-se utilizar uma malha parcial que forneça vários caminhos de custo idêntico entre sites. A definição de caminhos de custo idêntico depende do protocolo de roteamento a ser escolhido. Idealmente, dois sites devem ser diretamente conectados por caminhos diferentes, para minimizar o retardo.

1.2.3 Disponibilidade

A disponibilidade se refere ao tempo durante o qual uma rede está disponível para os usuários, logo é uma meta crítica para os clientes de projeto de rede. A

disponibilidade pode ser expressa como uma porcentagem de tempo de atividade por ano, mês, semana, dia ou hora, em comparação com o tempo total referente a esse período. Em números, a disponibilidade da rede é a relação entre o tempo médio de falhas (MTBF - *Mean Time Between Failure*) e o tempo médio de reparação (MTTR - *Mean Time to Repair*).

Disponibilidade = MTBF / (MTBF + MTTR) x 100%

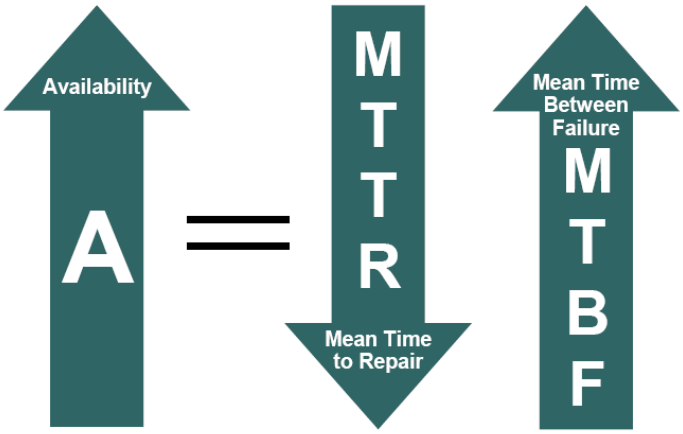

Figura 1.3: Relação de parâmetros de disponibilidade

Em geral, a disponibilidade significa a proporção do tempo em que a rede está operacional. A disponibilidade está vinculada à redundância, mas nem sempre este item é uma meta de rede. A redundância é uma solução para a meta de disponibilidade, ou seja, significa a adição de vínculos ou dispositivos duplicados a uma rede para evitar o tempo de inatividade.

A disponibilidade também está vinculada à confiabilidade, mas tem um significado mais específico (percentual de atividade) que a confiabilidade. A confiabilidade se refere a uma grande variedade de assuntos, inclusive precisão, taxas de erros e estabilidade.

A disponibilidade também está associada com a resiliência, uma palavra mais popular na área. O termo significa a quantidade de tensão que uma rede pode controlar e a rapidez com que a mesma pode se recuperar de problemas. Um projeto com boa resiliência normalmente tem razoável disponibilidade.

Outro aspecto de disponibilidade é a recuperação de desastres. Algumas das grandes instituições têm um plano para recuperação de desastres naturais, como inundações, incêndios, furacões e terremotos. Um plano de recuperação de desastres incluiu um processo de comutação para tecnologia de reserva, de forma automática ou manual, com intervenção humana, caso as tecnologias principais sejam afetadas por determinado incidente.

É bastante importante fazer estimativas de disponibilidade da rede e especificar com precisão seus requisitos. Existe a diferença entre um tempo de atividade de 99,70% e um tempo de atividade de 99,95%. Considerando uma semana, o primeiro significa um tempo de 30 minutos de parada, enquanto o segundo representa apenas 5 minutos, que se pode considerar um tempo bastante razoável.

Availability	Downtime per Year (24x7x365)		
99.000%	3 Days	15 Hours	36 Minutes
99.500%	1 Day	19 Hours	48 Minutes
99.900%		8 Hours	46 Minutes
99.950%		4 Hours	23 Minutes
99.990%			53 Minutes
99.999%			5 Minutes
99.9999%			30 Seconds

Figura 1.4: Tempo de queda com relação a disponibilidade

Como forma de garantir determinada disponibilidade é realizado um acordo de SLA. Trata-se na realidade de um contrato entre um fornecedor de serviços de TI e um cliente especificando, em geral em termos mensuráveis, quais serviços o fornecedor vai prestar.

Níveis de serviço são definidos no início de qualquer relação de outsourcing e usados para mensurar e monitorar o desempenho de um fornecedor. Muitas vezes, um cliente pode cobrar multa de um prestador de serviços se determinados SLAs não forem atingidos.

Empregado criteriosamente, SLA é eficaz para que o fornecedor trabalhe de maneira correta e apropriada. Mas o cliente final não quer se encarregar de aplicar e recolher multas. Serviço ruim de um fornecedor, mesmo com grande desconto, continua sendo serviço ruim e pode acarretar problemas maiores. É melhor despender a energia para descobrir quais SLAs estão sendo descumpridos e se empenhar em resolver a situação.

1.3 A Estrutura em Análise

No projeto da maioria das implementações de WAN (Wide Area Network), a confiabilidade é a meta mais importante, porque a WAN é, com freqüência, parte do backbone de interconexão de redes. Todavia, os recursos WAN são caros. Projetar uma rede totalmente redundante para maximizar a disponibilidade é um compromisso para se projetar uma rede eficaz em termos de custo. É necessário fatorar o custo de tempo de interrupção (downtime) sempre que for tomar decisões de negócio ou técnicas. Outos aspectos importantes sobre WAN que precisam ser consideradas incluem:

- Aspectos sobre a latência;
- Custos dos recursos de WAN;
- Quantidade de tráfego que irá atravessar a WAN;

- Quais protocolos serão permitos na WAN;
- Compatibilidade com padrões de sistemas legados;
- Simplicidade e facilidade de configuração da solução proposta;
- Suporte total as filiais e telecomputadores;

Em suma, se a WAN não for funcional, quantas pessoas não poderão trabalhar e quanta receita será perdida nesse ínterim?

Dois tipos de opção estão disponíveis para redes remotas – linhas dedicadas ou conexões comutadas. As conexões comutadas podem ser por circuito (circuit-switched) ou por pacotes (packet-switched)/células(cell-switched).

As metas de projeto do núcleo de WAN em nível micro devem focalizar os três componentes a seguir: maximização de troughput, minimização do retardo (delay) e overhead de tráfego em circuitos WAN.

Muitas decisões contribuem para um uso eficaz da WAN. Essas decisões dizem respeito a aplicações e protocolos nos hosts, e os recursos das versões de sistema operacional nos roteadores. Pode ser possível, ou talvez não, alterar ou sintonizar as aplicações e os protocolos host para torná-los mais amigáveis com a interconexão de redes. Podemos verificar alguns desses itens que devem ser verificados para otimizar sua WAN:

- Programe aplicações menos intensivas na rede, como cliente/servidor;
- Ajuste os tamanhos das janelas de protocolo para transporte ótimo;
- Implemente protocolos de roteamento mais silenciosos que utilizem somente quando ocorrem alterações;
- Use largura de banda sob demanda para que os enlaces sejam utilizados mais eficientemente;
- Use métodos de priorização de protocolo para que as aplicações de missão crítica tenham largura de banda garantida;
- Use filtros para manter o tráfego desnecessário longe da WAN;
- Utilize compressão para maximizar a eficiência da linha

Agentes que proporcionam utilização otimizada de largura de banda abrangem compactação, filtros, largura de banda sob demanda, ajuste do tamanho de janelas e priorização de tráfego.

Podemos assim pensar alguns fatores relacionados a protocolos de aplicação que devem ser considerados. Protocolos de transporte, no caso TCP, devem ajustar o tamanho da janela de forma dinâmica em resposta a congestionamentos. Pacotes de tamanhos maiores podem ser mais eficazes, pois aumentam a relação tráfego útil x cabeçalho de cada pacote. Enviar broadcast repetidamente pode gerar excesso de tráfego.

1.3.1 Modelo de Camada OSI

Conforme descrito, o cenário a ser trabalhado neste trabalhado faz referências as camadas inferiores do modelo de referência OSI. Essas camadas fornecem os serviços de rede. Os protocolos implementados nessas camadas devem aparecer em todos os nós da rede. As quatro camadas superiores fornecem os serviços para os usuários finais e não para a rede (isto é, não são implementados nos nós de rede e sim nos equipamentos dos usuários finais).

Mas o Modelo de Referência OSI é composto por 7 camadas (ou níveis) e por isso vamos fazer rápida revisão sobre as funções de cada camada:

• (1) Camada Física: Ela define a interface elétrica e o tipo de mídia, por exemplo, com fio, sem fio, fibra, satélite, etc. Define, também, a eletrônica (por exemplo a modulação) para os bits 1 e 0. A camada física garante que um bit entrante numa extremidade do acesso chegue íntegro na outra extremidade.

• (2) Camada de Acesso: Usando a camada inferior de "serviço transporte de bit", o propósito do protocolo de enlace (na camada de enlace) é garantir que os blocos de dados sejam transferidos de forma confiável através do enlace. Assim, essa camada presta o serviço para a camada superior (camada de rede) de transformar um enlace físico numa "linha livre de erros de transmissão". Ela realiza isso quebrando os dados de entrada em blocos de dados, chamados "frames".

• (3) Camada de Rede: A função da camada de rede é rotear os dados, através da rede, do nó de origem até o nó de destino. Essa camada também fornece controle de fluxo ou congestionamento. Para realizar esse serviço, a camada de rede usa os serviços da camada de acesso (camada inferior).

• (4) Camada de Transporte: Essa camada permite, às redes, diferenciarem os tipos de aplicações. Por exemplo, transmissões de vídeo e voz, através de redes de dados, talvez recebam uma prioridade ou qualidade de serviço superior à do correio eletrônico. Os dispositivos da camada 4 também são responsáveis pela segurança em roteadores conectados à Internet ou redes virtuais privadas – VPN. Os filtros em roteadores autorizam ou negam o acesso às redes, com base no endereço IP do remetente.

• (5) Camada de Sessão: Essa camada gerencia o diálogo das sessões numa rede. Por exemplo, as pontas podem enviar ao mesmo tempo? Ou devem ser half duplex (uma de cada vez)? Ou só um lado pode enviar (simplex)?

• (6) Camada de Apresentação: Essa camada controla o formato ou aparência das informações na tela do usuário.

• (7) Camada de Aplicação: Essa camada inclui a aplicação, em si, e serviços especializados, como a transferência de arquivos ou serviços de impressão.

2 REVISÃO TEÓRICA

Na revisão, trabalharemos a evolução das soluções de alta disponibilidade e utilização de tecnologias já existentes para aumentar a disponibilidade de determinado circuito. Sempre com ênfase na estrutura de PE que é o roteador no backbone da operadora, acesso de última milha, podendo ser par metálico, fibra ótica, radio ou satélite, e o CE, sendo esse o equipamento de menos porte instalado nas dependências do cliente.

2.1 Evolução de Soluções de Alta Disponibilidade

As redes desenvolvidas com propósito de diminuir a quantidade de quedas e aumdantar o tempo em funcionamento já são pensadas desde que trabalhamos com circuitos dedicados ou E1s. E a demanda veio junto com a evolução dos protocolos de WAN, como as redes de tecnologia Frame-Relay ou ISDN.

As redes com circuitos dedicados davam maior abertura para se trabalhar os requisitos de protocolo de roteamento, já que não existiam roteadores de borda no backbone e sim o chamado “tubo” dedicado entre os equipamentos.

O Frame-relay, por ser uma tecnologia de nível 2, também deu bastante abertura para soluções de contingência. Tivemos caso de projetos utilizando OSPF em redes Frame-Relay para projetos diferenciados.

Para Internet, os projetos iniciais utilizavam o chamado multihoming, ou seja, fornecer mais de uma conexão para um sistema ter acesso e oferecer srviços de rede.

2.2 Conceitos Técnicos Importantes

Neste item vamos estudar uma série de conceitos importantes na área de redes de computadores e configurações de roteadores.

Em algumas interconexões de redes, pode haver um requisito de que somente o IP nativo possa ser utilizado no backbone de WAN. Esse requisito de somente IP pode ocorrer porque um departamento separado é responsável pela manutenção do backbone, ou os recursos WAN talvez tenham sido alugados de um provedor de serviços IP ou, ainda, porque o projeto esteja considerando empregar QoS com base em IP. Seja qual for o caso, é altamente recomendável que todos os outros protocolos deevem ser encapsulados em datagrama IP.

A WAN é mais fácil de ser gerenciada quando o IP é o único protocolo utilizado no núcleo. Problemas de endereçamento e configuração relacionados a outros protocolos

são evitados. Um custo dessa simplicidade é a largura de banda da WAN necessária para acomodar o overhead de largura de banda adicional dos datagramas encapsulados.

2.2.1 Protocolos de Roteamento

O roteamento é a principal forma utilizada na área de redes IP para a entrega de pacotes de dados entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores etc.). O modelo de roteamento utilizado é o do salto por salto (hop-by-hop), onde cada roteador que recebe um pacote de dados, abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este processo se repete e assim segue ate' a entrega do pacote ao seu destinatário. No entanto, para que este funcione, são necessários dois elementos: tabelas de roteamento e protocolos de roteamento.

Tabelas de roteamento são registros de endereços de destino associados ao numero de saltos até ele, podendo conter varias outras informações.

Protocolos de roteamento determinam o conteúdo das tabelas de roteamento, ou seja, são eles que ditam a forma como a tabela e' montada e de quais informacoes ela e' composta. Existem dois tipos de algoritmo atualmente em uso pelos protocolos de roteamento: o algoritmo baseado em Vetor de Distancia (Distance-Vector Routing Protocols) e o algoritmo baseado no Estado de Enlace (Link State Routing Protocols).

Os roteadores utilizados para trocar informações dentro de Sistemas Autônomos são chamados roteadores internos (interior routers) e podem utilizar uma variedade de protocolos de roteamento interno (Interior Gateway Protocols - IGPs). Dentre eles estao: RIP, IGRP, EIGRP, OSPF.

Roteadores que trocam dados entre Sistemas Autônomos são chamados de roteadores externos (exterior routers), e estes utilizam o Exterior Gateway Protocol (EGP) ou o BGP (Border Gateway Protocol). Para este tipo de roteamento sao considerados basicamente coleções de prefixos CIDR (Classless Inter Domain Routing) identificados pelo numero de um Sistema Autônomo.

2.2.1.1 RIP (Routing Information Protocol)

O RIP foi desenvolvido pela Xerox Corporation no inicio dos anos 80 para ser utilizado nas redes Xerox Network Systems (XNS), e, hoje em dia, e' o protocolo intradominio mais comum, sendo suportado por praticamente todos os fabricantes de roteadores e disponível na grande maioria das versões mais atuais do sistema operacional UNIX.

Um de seus benefícios é a facilidade de configuração. Além disso, seu algoritmo nao necessita grande poder de computação e capacidade de memória em roteadores ou computadores.

O protocolo RIP funciona bem em pequenos ambientes, porem apresenta serias limitações quando utilizado em redes grandes. Ele limita o numero de saltos (hops) entre hosts a 15 (16 e' considerado infinito). Outra deficiência do RIP e' a lenta convergência, ou seja, leva relativamente muito tempo para que alteracoes na rede

fiquem sendo conhecidas por todos os roteadores. Esta lentidao pode causar loops de roteamento, por causa da falta de sincronia nas informacoes dos roteadores.

O protocolo RIP é também um grande consumidor de largura de banda, pois, a cada 30 segundos, ele faz um broadcast de sua tabela de roteamento, com informações sobre as redes e sub-redes que alcança.

Por fim, o RIP determina o melhor caminho entre dois pontos, levando em conta somente o numero de saltos (hops) entre eles. Esta técnica ignora outros fatores que fazem diferença nas linhas entre os dois pontos, como: velocidade, utilização das mesmas (trafego) e toda as outras métricas que podem fazer diferença na hora de se determinar o melhor caminho entre dois pontos.[RFC 1058]

2.2.1.2 IGRP (Interior Gateway Protocol)

O IGRP também foi criado no inicio dos anos 80 pela Cisco Systems Inc., detentora de sua patente. O IGRP resolveu grande parte dos problemas associados ao uso do RIP para roteamento interno.

O algoritmo utilizado pelo IGRP determina o melhor caminho entre dois pontos dentro de uma rede examinando a largura de banda e o atraso das redes entre roteadores. O IGRP converge mais rapidamente que o RIP, evitando loops de roteamento, e não tem a limitacao de saltos entre roteadores.

Com estas características, o IGRP viabilizou a implementação de redes grandes, complexas e com diversas topologias.

2.2.1.3 EIGRP (Enhanced IGRP)

A Cisco aprimorou ainda mais o protocolo IGRP para suportar redes grandes, complexas e criticas, e criou o Enhanced IGRP.

O EIGRP combina protocolos de roteamento baseados em Vetor de Distancia (Distance-Vector Routing Protocols) com os mais recentes protocolos baseados no algoritmo de Estado de Enlace (Link-State). Ele também proporciona economia de trafego por limitar a troca de informações de roteamento àquelas que foram alteradas.

Uma desvantagem do EIGRP, assim como do IGRP, e' que ambos são de propriedade da Cisco Systems, não sendo amplamente disponíveis fora dos equipamentos deste fabricante.

2.2.1.4 OSPF (Open Shortest Path First)

Foi desenvolvido pelo IETF (Internet Engineering Task Force) como substituto para o protocolo RIP. Caracteriza-se por ser um protocolo intra-dominio, hierárquico, baseado no algoritmo de Estado de Enlace (Link-State) e foi especificamente projetado para operar com redes grandes. Outras características do protocolo OSPF são:

- A inclusão de roteamento por tipo de serviço (TOS - type of service routing). Por exemplo, um acesso FTP poderia ser feito por um link de satélite, enquanto que um acesso a terminal poderia evitar este link, que tem grande tempo de retardo, e ser feito atraves de um outro enlace;

- O fornecimento de balanceamento de carga, que permite ao administrador especificar multiplas rotas com o mesmo custo para um mesmo destino. O OSPF distribui o trafego igualmente por todas as rotas;

- O suporte à 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 (ver abaixo) 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 e' 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 areas, os pacotes são primeiramente roteados para a Área 0 (o backbone). Isto pode não ser bom, uma vez que não há roteamento interarias enquanto os pacotes não alcançam o backbone. Chegando à Área 0, os pacotes são rateados para a Área de Destino, que e' 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 OSPF.[RFC 1583]

2.2.1.5 BGP (Border Gateway Protocol)

O BGP [RFCs 1771,1772,1773,1774,1657] assim como o EGP, e' um protocolo de roteamento interdominios, criado para uso nos roteadores principais da Internet.

O BGP foi projetado para evitar loops de roteamento em topologias arbitrarias, o mais serio problema de seu antecessor, o EGP (Exterior Gateway Protocol). Outro problema que o EGP nao resolve - e e' abordado pelo BGP - e' o do Roteamento Baseado em Politica (policy-based routing), um roteamento com base em um conjunto de regras não técnicas, definidas pelos Sistemas Autônomos.

A ultima versão do BGP, o BGP4, foi projetado para suportar os problemas causados pelo grande crescimento da Internet.

Maiores detalhes sobre este importante protocolo de roteamento serao vistos nas próximas edições deste boletim.

2.2.2 Balanceamento por Pacote

Ao dividir o tráfego por dois caminhos, como o próprio nome se refere, um pacote IP é enviado por um e o próximo pacote por outro.

Essa divisão pode ser considerada precisa, ou seja, os tráfegos nos dois circuitos serão exatamente iguais, a percepção do usuário. Ocupa mais CPU do roteador e é considerado mais vulnerável a ataques de DoS.

A solução é imprópria para redes corporativas MPLS, ou seja, redes com tráfego multimídia. O balanceamento por pacote não faz distinção dos tipos de pacote, podendo encaminhar pacotes de tamanhos e protocolos distintos, pode ocorrer atraso, perdas, jitter e outras ocorrência que interferem na qualidade da voz, por exemplo.

Já para projetos de acesso a internet, é mais indicada, já que temos uma banda agregada, formando 4 Mbps com 2 x Mbps (duas interfaces seriais), e aumentam as "velocidades" de downloads e outras necessidades dos usuários finais.

2.2.3 Balanceamento por Destino

Quando os protocolos de roteamento encontram caminhos de mesmos custos, é natural que ocorra o chamado balanceamento de carga entre os dois enlaces disponíveis. É uma divisão de tráfego de dados que pode ser realizada em diferentes formas.

Essa solução é configuração default realizada pelos equipamentos, sem necessidade de configurações complementares. O dois caminhos são iguais para diversos destinos e o roteador divide o tráfego enviando tudo que for para um destino por um caminho e tudo que for para um segundo destino por outro caminho. O equipamento faz essa divisão por controle de fluxos TCP.

Os pontos positivos são a menor ocupação de CPU do roteador e baixa vulnerabilidade a ataques de DoS. Ao fazer uma análise de tráfego entre circuitos balanceados por destino, podemos verificar os tráfegos não são idênticos, pois varia de acordo com a divisão de fluxos realizados.

É uma solução pronta para implementação de QoS, incluindo o tráfego chamado de multimídia, com dados, voz e vídeo. Sua solução não interrompe ou atrapalha essas aplicações.

Porém é desaconselhável para empresas provedoras de serviços de internet. Isso porque fica a impressão ao cliente que os circuitos não estão com balanceamento, já que um fluxo pode ocupar 95% da banda disponível em um dos meios, porém um segundo fluxo ocupando somente 30% do segundo circuito. Assim, o primeiro usuário "sentirá" lentidão, enquanto existe disponibilidade no segundo circuito. Em resumo, ao usar esse modelo de balanceamento, não estamos somando a banda disponível dos circuitos agregados. Em uma estrutura de 2 x 2 Mbps, não teremos banda disponível de 4 Mbps.

2.2.4 Configuração Multilink PPP

O protocolo Multilink PPP pertence a camada 2 do modelo OSI. Tem alguns diferencias quanto a configuração de fragmentação e "interliving", mas tem como

possibilidade a agregação de diversos circuitos WAN, formatando uma solução de N x 2 Mbps.

O Multilink PPP (MLPPP) oferece suporte para agregação de canais PPP. A agregação de canais pode ser usada para balanceamento de carga e para proporcionar largura de banda extra. Com a agregação de canais, um dispositivo pode abrir automaticamente canais adicionais à medida que aumentam os requisitos por largura de banda.

O MLPPP assegura que os pacotes chegarão em ordem ao dispositivo receptor. Para conseguir isso, a configuração faz o encapsulamento de dados no PPP e atribui um número de seqüência aos datagramas no equipamento originador. No dispositivo receptor, o PPP usa o número de seqüência para recriar o fluxo de dados original. Vários canais aparecem como um único link lógico para os protocolos da camada superior.

As interfaces básicas e primárias de RDIS oferecem a possibilidade de abrir múltiplos canais simultâneos entre equipamentos terminais, dando aos utilizadores largura de banda a pedido, obviamente com custos adicionais.

Há várias propostas que proporcionam sincronização entre múltiplos fluxos ao nível de bit, de que se destaca a proposta BONDING, mas que têm o inconveniente de requererem hardware adicional.

A solução definida na RFC 1990, "The PPP Multilink Protocol (MP)", pode ser implementada inteiramente em software, sendo baseada num cabeçalho de 4 octetos e em regras simples de resincronização.

Na figura 2.1 apresenta-se um diagrama esquemático do funcionamento do PPP Multilink.

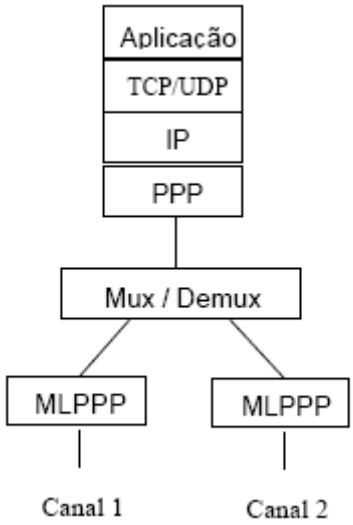

Figura 2.1: Diagrama de funcionamento do PPP Multilink

São definidos dois formatos de tramas que diferem no tamanho do número de seqüência. Na figura 2.2 apresenta-se a estrutura dos pacotes MP com Número de Seqüência Longo.

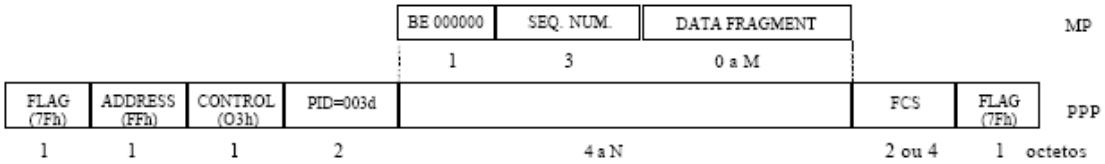

Figura 2.2: Formato PPP Multilink com Número de Seqüência Longo

Na figura 2.3 apresenta-se a estrutura dos pacotes MP com Número de Seqüência Curto.

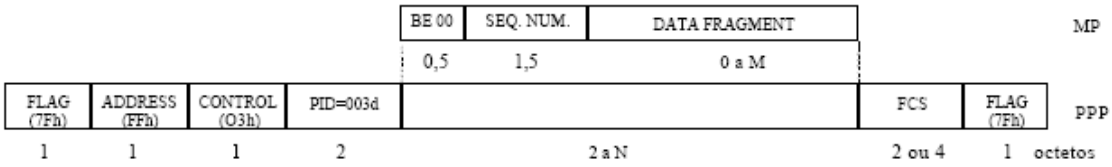

Figura 2.3: Formato PPP Multilink com Número de Sequência Curto

O bit B (Beginning) é posto a 1 no primeiro fragmento derivado do pacote PPP e posto a 0 para todos os outros fragmentos do pacote PPP. O bit E (Ending) é posto a 1 no último fragmento derivado do pacote PPP e posto a 0 para todos os outros fragmentos do pacote PPP.

Na figura 2.4 exemplifica-se a segmentação de um pacote PPP em dois fragmentos MP, em que se constata que o primeiro fragmento de MP contém dois cabeçalhos, o primeiro de MP e o segundo de PPP. Como se vê na figura, o identificador do protocolo PPP-ML é 003d.

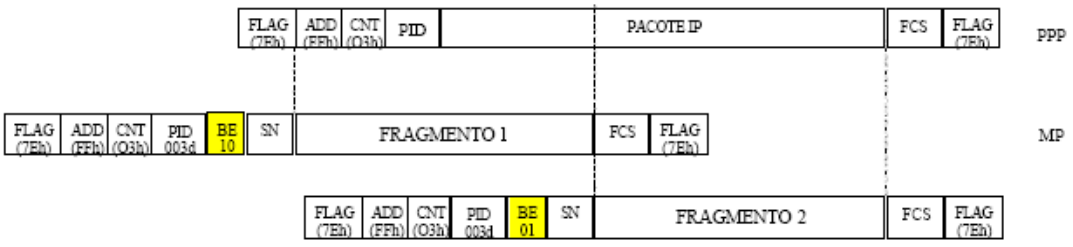

Figura 2.4: Exemplo de segmentação de pacote PPP em dois fragmentos MP

2.2.5 Configuração VRRP – (Cisco HSRP)

Na maioria das redes, apenas um equipamento é apontado como gateway padrão e os hosts internos deste segmento encaminham suas solicitações externas para este endereço. Mesmo com links e equipamentos duplicados, a falha no dispositivo ou link principal causa uma interrupção nas comunicações, até que a ativação do roteador ou link secundário seja realizada. Neste sentido, o protocolo da Cisco HSRP (Hot Standby Router Protocol) foi desenvolvido para promover a alta disponibilidade em roteadores,

de forma que, mesmo durante falhas, a rede sempre tenha um equipamento em funcionamento atuando como gateway padrão.

A alta disponibilidade é obtida através de um endereço virtual que é compartilhado entre dois ou mais equipamentos. Este endereço é definido como gateway padrão da rede para os hosts internos. Na ocasião de uma falha no equipamento principal, outro componente do grupo de alta disponibilidade assume o seu papel, utilizando o endereço virtual. Desta forma, a falha fica imperceptível aos clientes locais, já que a comunicação permanece ininterrupta.

Tecnicamente falando, quando o HSRP é configurado em um segmento de rede, ele fornece tanto um endereço MAC quanto um endereço IP virtual, que são compartilhados entre o grupo de roteadores que executam este protocolo. Um destes equipamentos é selecionado para se tornar o ativo, ou seja, o dispositivo principal que receberá os quadros destinados ao MAC virtual do grupo.

O HSRP detecta quando o roteador designado ativo falha, e a partir deste ponto, um roteador *standby* assume o controle dos endereços do grupo. O controle sobre qual equipamento deve assumir o papel de ativo ou *standby* é realizado através de um valor denominado prioridade. Para se tornar ativo, a prioridade de um roteador deve ser maior que a dos outros do grupo.

Para detectar uma falha ou alterações de prioridade e designar os papéis, os equipamentos trocam mensagens do tipo *HELLO*. Estes pacotes são destinados ao endereço IP multicast 224.0.0.2 sob o protocolo de transporte UDP na porta 1985. O roteador ativo envia pacotes com o endereço IP da sua interface local e o MAC virtual; já o roteador *standby* envia pacotes também com o endereço IP da sua interface, mas com o seu próprio endereço MAC.

Existem três mensagens que são trocadas entre os roteadores do grupo HSRP:

HELLO – esta mensagem transmite aos demais roteadores o valor de prioridade e informações do estado HSRP do equipamento que a originou;

COUP – esta mensagem é enviada por um roteador *standby* quando este quer assumir a função de ativo;

RESIGN – esta mensagem é enviada pelo roteador ativo quando ele está prestes a desligar ou quando ele recebe uma mensagem *HELLO* ou *COUP* de um roteador com uma prioridade maior.

Em qualquer dado momento, um roteador num grupo HSRP estará em um dos seguintes estados do protocolo:

ACTIVE – o roteador neste estado está desempenhando o papel de ativo e transmite os pacotes recebidos pelo grupo HSRP;

STANDBY – o roteador neste estado está preparado para assumir a função do equipamento ativo no caso de falha;

SPEAK – o roteador neste estado está enviando e recebendo mensagens *HELLO*;

LISTEN – o roteador neste estado está recebendo mensagens *HELLO.*

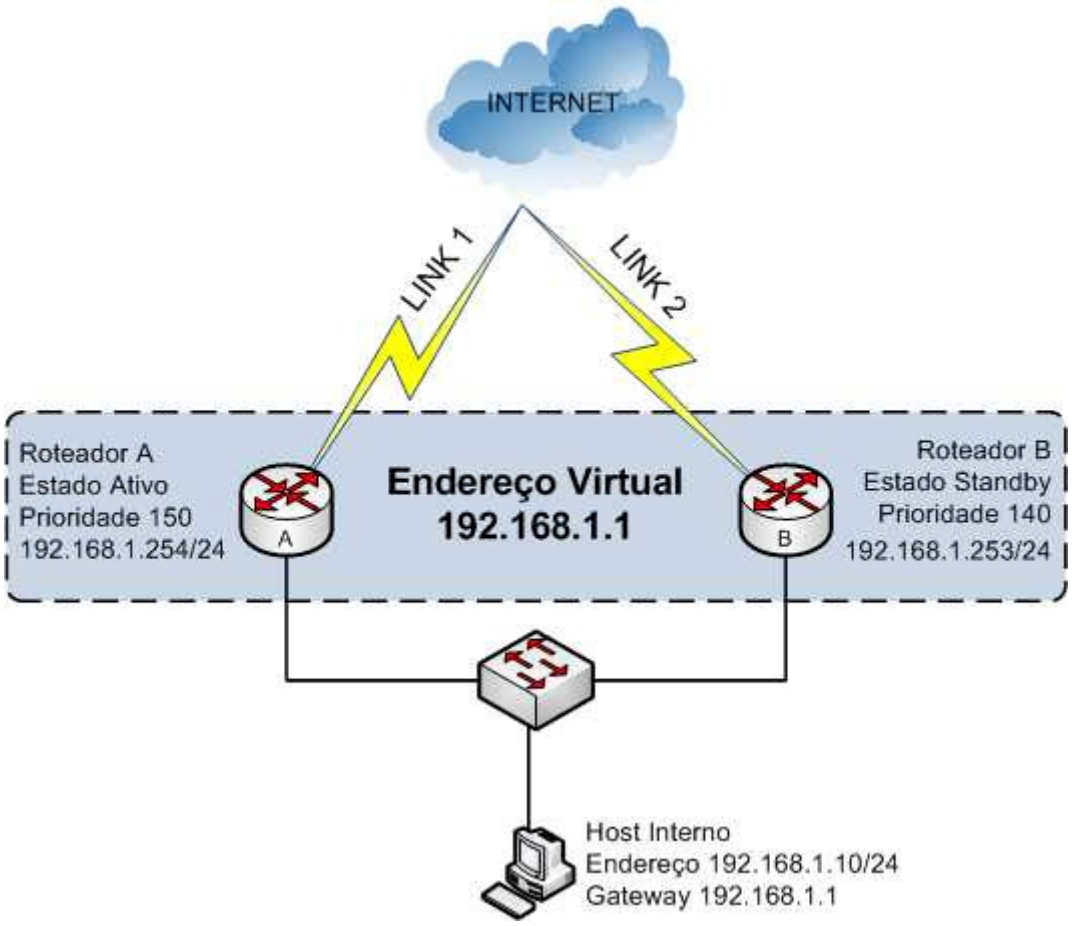

Figura 2.5: Projeto base com tecnologia HSRP

2.2.6 Configuração GLBP

O advento do protocolo HSRP trouxe vários benefícios, principalmente no suprimento da necessidade de alta disponibilidade. Muitos administradores de rede também sentem grande necessidade de fazer o Balanceamento de Carga entre seus roteadores de Internet. Com o protocolo GLBP (*Gateway Load Balancing Protocol*), é possível criar um ambiente que atenda seus requisitos de disponibilidade e balanceamento de maneira bastante prática.

De maneira bastante similar ao HSRP, o protocolo GLBP também se utiliza de um endereço virtual que é compartilhado entre dois ou mais equipamentos. A grande vantagem do GLBP com relação a outros protocolos chamados *first-hop* é justamente pelo fato de promover o balanceamento de carga entre os dispositivos, enquanto outros protocolos mantêm um equipamento ativo transmitindo o tráfego e outro redundante apenas aguardando alguma falha. Na realidade, o HSRP também pode realizar o balanceamento de carga, mas seria necessário configurar múltiplos grupos, cada qual com um endereço virtual e apesar desta funcionalidade, os hosts internos deverão ser configurados com endereços diferentes de gateway padrão, o que aumenta bastante o trabalho de administração.

Tecnicamente, o funcionamento do protocolo GLBP é muito similar ao HSRP, pois os conceitos de roteador ativo e standby também são utilizados. Os equipamentos

pertencentes ao grupo elegem o gateway virtual ativo, que determina um endereço MAC virtual para cada roteador participante. Para cada requisição ARP recebida para o endereço virtual, o gateway virtual ativo responde com um dos endereços MAC virtual, transferindo a responsabilidade do encaminhamento dos pacotes ao dono daquele MAC e conseguindo desta forma o balanceamento. Por padrão, o método de escalonamento dos endereços MAC é round-robin.

No GLBP também trabalhamos com a variável prioridade, que determina qual papel cada roteador deve desempenhar. Este valor varia de 1 a 255, onde o maior valor dentro do grupo define quem será o gateway virtual ativo, ficando os outros dispositivos como gateways virtuais redundantes. Como no HSRP, os equipamentos na função de standby trocam mensagens do tipo HELLO com o equipamento ativo, a fim de detectar qualquer problema. Essas mensagens são destinadas ao endereço IP multicast 224.0.0.102 sob o protocolo de transporte UDP na porta 3222.

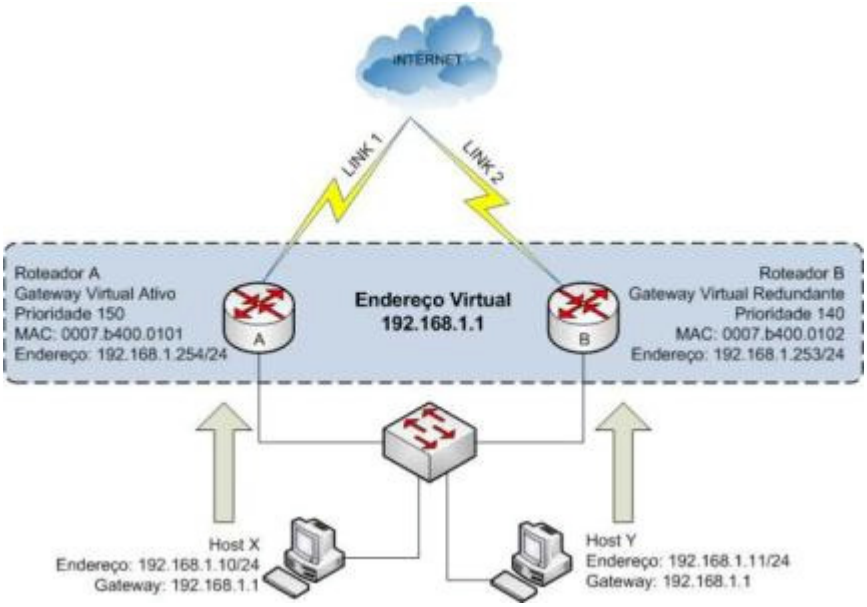

Figura 2.6: Projeto base com tecnologia GLBP

2.2.7 Policy Based Routing

O PBR é uma técnica usada para fundamentar decisões de roteamento com base em políticas definidas pelo administrador da rede. Quando um roteador recebe um pacote, ele normalmente decide onde encaminha-lo baseado no endereço de destino do pacote, usado para consultar a tabela de roteamento.

Entretanto, em alguns casos, é necessário usar ou critério, como endereço de origem, o tamanho do pacote, a sua aplicação, ou ainda uma combinação de características para definir a origem deste pacote.

Através do PBR, pode-se forçar um determinado fluxo de pacotes por um caminho diferente daquele que o fluxo normalmente seguiria se estivesse sendo roteado pela tabela de roteamento padrão de um roteador. Por exemplo, assim que um fluxo chega

até uma das interfaces de um roteador, este roteador deve consultar a tabela de roteamento para determinar para qual interface os pacotes deverão ser comutados e isso é o comportamento padrão de um roteador IP.

3 PLANO DE SOLUÇÃO

O desenvolvimento da solução dependerá da necessidade do cliente e investimento. Numa rede IP com vários sites, havendo exigência de alta disponibilidade em um site é necessária a utilização de dois links de acesso a rede, esse dois podem ser por meios físicos diferentes, por porta (roteador de borda) diferente ou até mesmo chegando em equipamentos diferentes.

Links redundantes são utilizados em caso de alta disponibilidade ou quando é impossível atender a demanda com um único circuito. Um exemplo disso é quando entregamos um link de 4 Mbps através de duas interfaces V.35 de 2 Mbps. Nesta secção, analisaremos várias possibilidades de redes com enlaces redundatnes de alta disponibilidade

3.1 Apenas Balanceamento de Carga

Nesta solução, utilizamos apenas tecnologia já preparadas, como balanceamento por destino, por pacote, ou a configuração Multilink PPP. Seu utilizarmos acesso iguais, a disponibilidade poderá ser considerada igual a de um circuito único, pois um possível interrupção em um dos circuitos de acesso, como a queda de um poste, representará a queda total do serviço ao cliente.

É importante neste caso apenas verificar as características de aplicativos do cliente para se adequar ao tipo de balanceamento. Por pacotes é indicado para serviços de internet básica, enquanto por destino é para solução de rede corporativa com QoS. O Multilink PPP pode ser utilizado nos dois casos, pois atende ambas as demandas. Ele se diferencia por trabalhar na camada 2, enquanto as duas primeiras configurações já atuam em nível de Redes, camada 3.

Abaixo o cenário de análise. O projeto só passa a ser de alta disponibilidade quando os acessos são distintos, e isso na prática, nem sempre é possível.

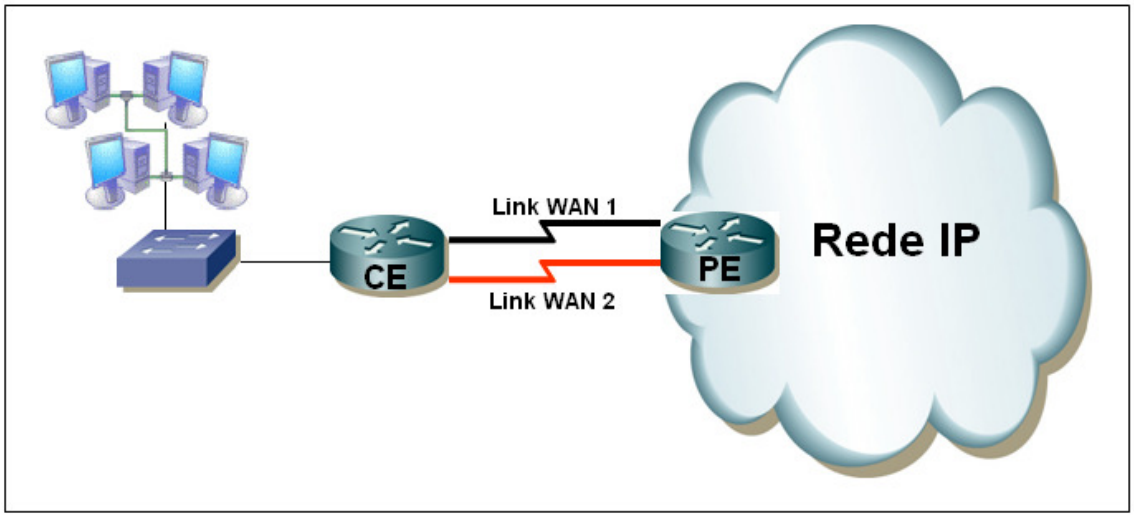

Figura 3.1: Exemplo com balanceamento de carga

Em seqüência, tenho uma série de gráficos com base em MRTG (Multi Router Traffic Grapher) onde verificamos o comportamento dos três tipos de balanceamento de carga. O primeiro caso visualizamos um MLPPP de 6 Mbps e os três circuitos de 2 Mbps que compõe o grupo multilink.

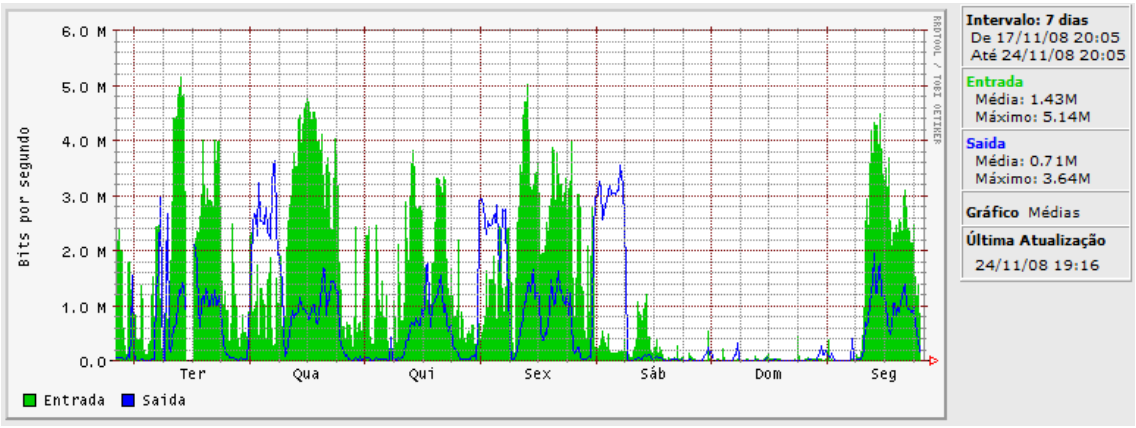

Figura 3.2: Tráfego de 6 Mbps do MLPPP

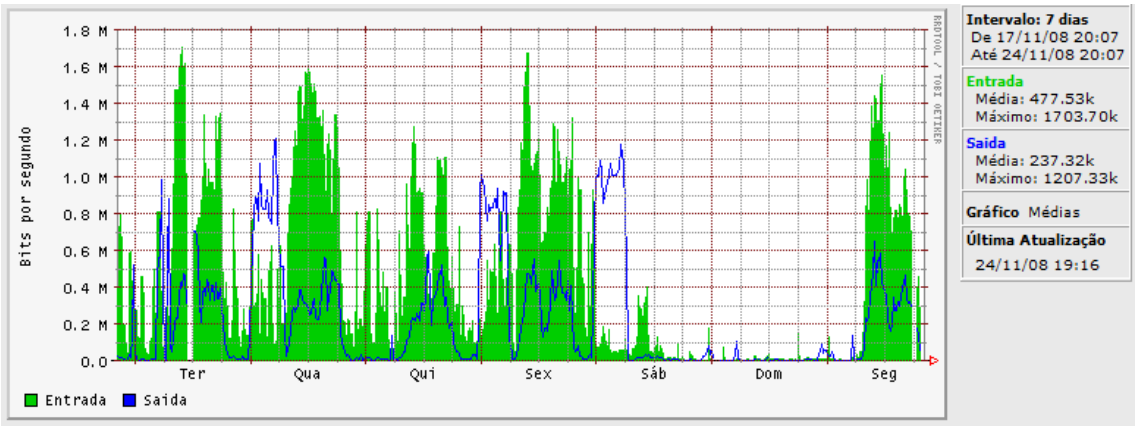

Figura 3.3: Tráfego do primeiro componente do Multilink

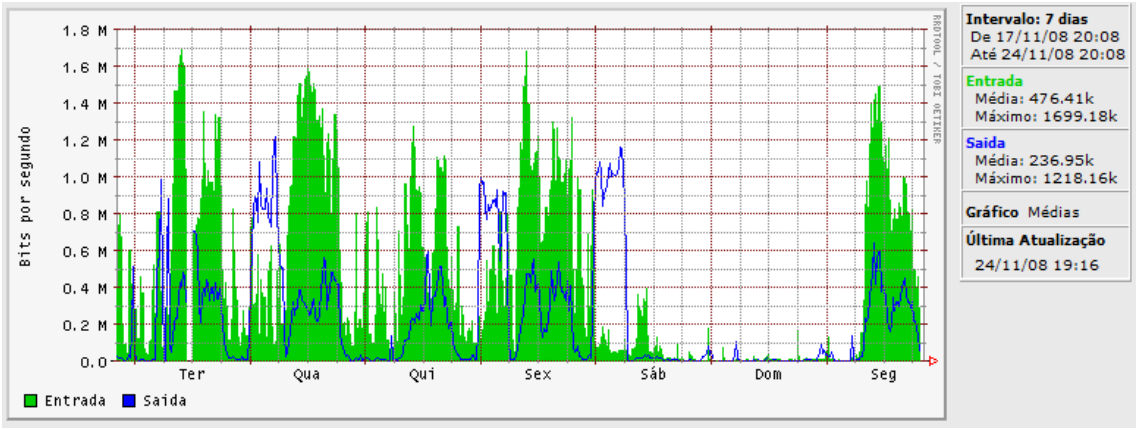

Figura 3.4: Tráfego do segundo componente do Multilink

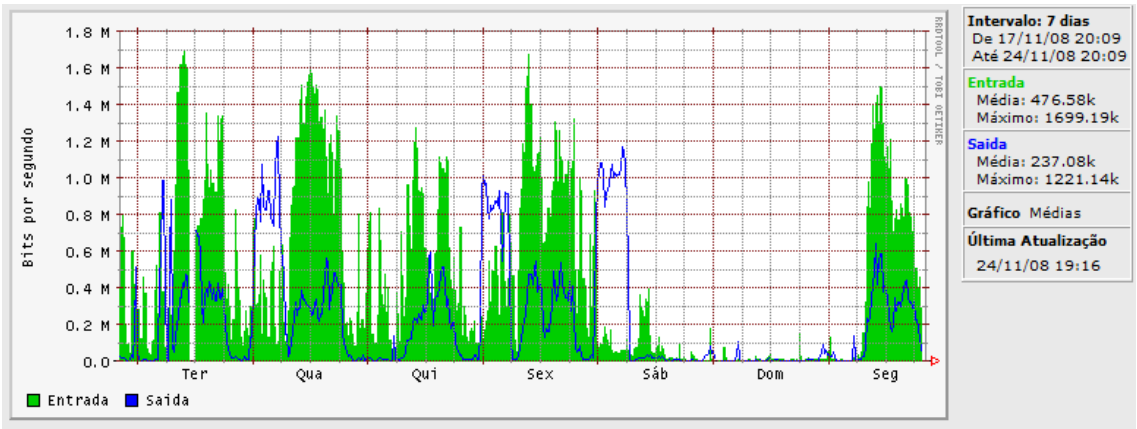

Figura 3.5: Tráfego do terceiro componente do Multilink

Podemos verificar que os gráficos dos componentes do multilink são exatamente iguais, e se somarmos os mesmos, chegaremos ao primeiro gráfico, com uma disponibilidade de banda máxima de 6 Mbps. Esta é uma rede corporativa IP, com utilização de QoS com diversos tipo de tráfego. A divisão por banda para prioridade é realizada sempre sobre um total do multilink, ou seja, 6 Mbps.

Nos próximos gráficos, temos um exemplos de balancemaneto por destino e balanceamento por pacote, considerando sempre dois circuitos.

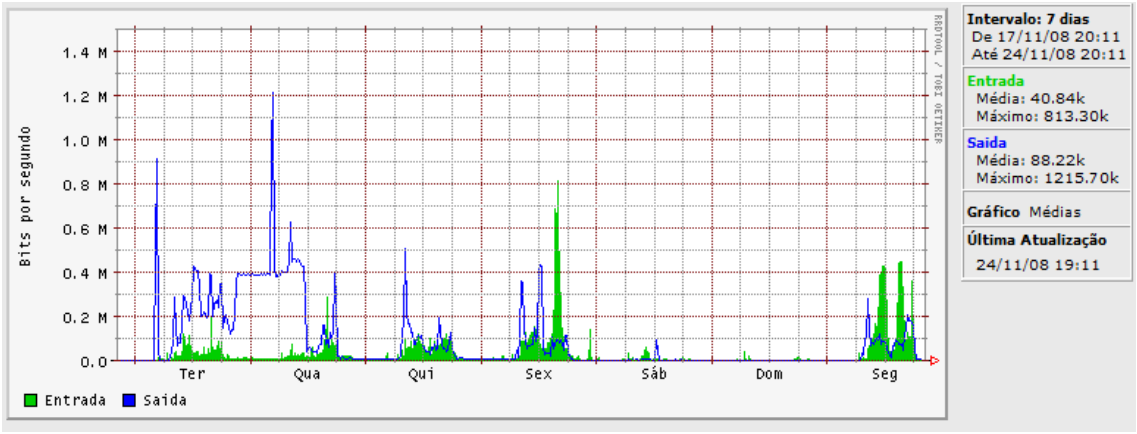

Figura 3.6: Tráfego do primeiro componente com balanceamento por destino

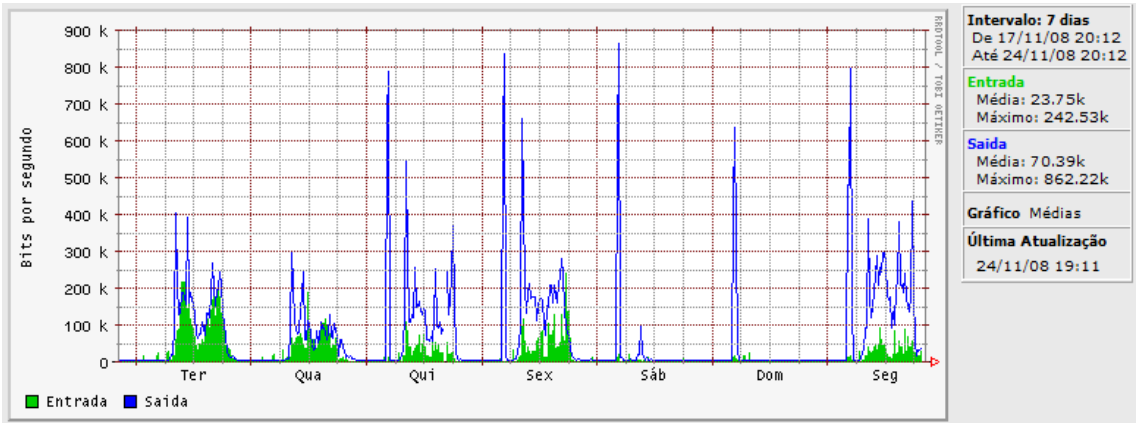

Figura 3.7: Tráfego do segundo componente com balanceamento por destino.

Podemos verificar que esse tipo de configuração gera gráficos de utilização totalmente assimétricos, nos dois sentidos. E estes sentidos têm tráfegos independentes um do outro, ou seja, os roteadores CE e PE fazem distribuição apenas com base em suas respectivas rotas. Os valores de download e upload jamais passarão os 2 Mbps disponíveis em cada circuito.

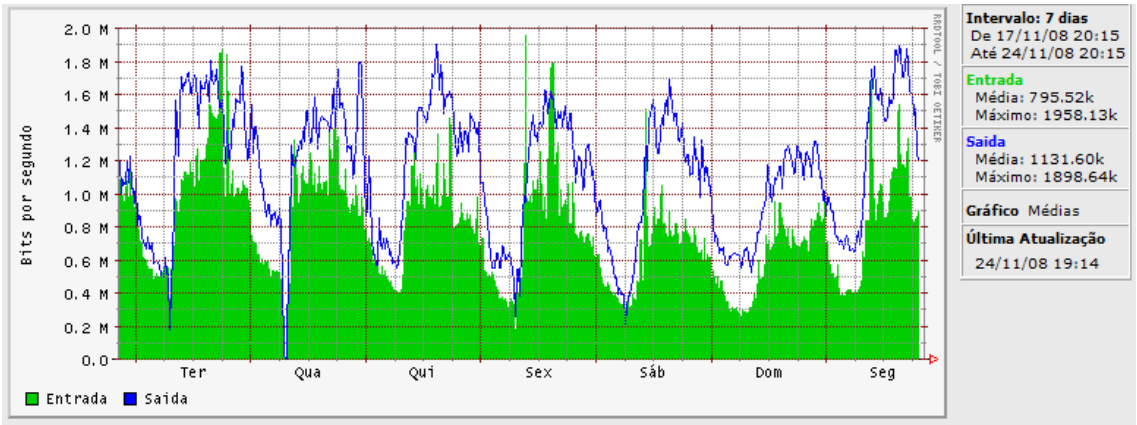

Figura 3.8: Tráfego do primeiro componente com balanceamento por pacote

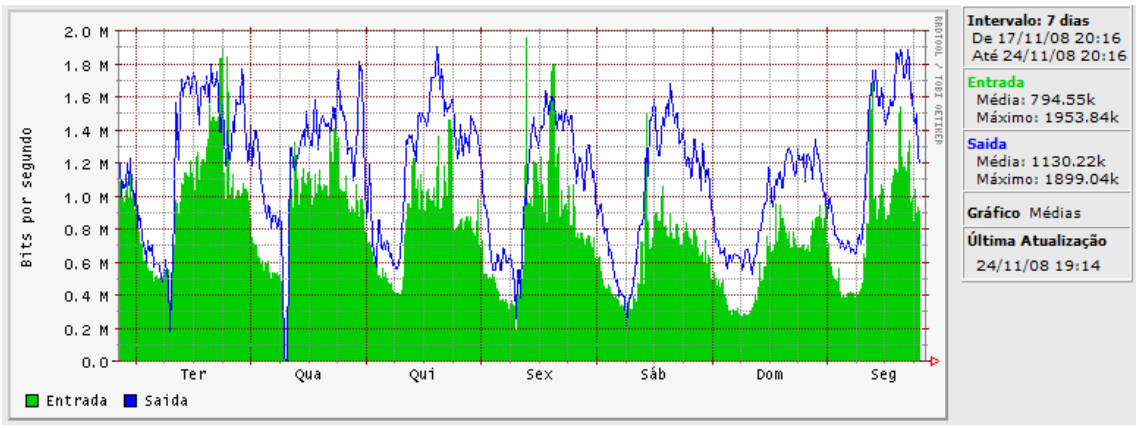

Figura 3.9: Tráfego do segundo componente com balanceamento por pacote

O último caso apresenta característica simétrica nos dois sentidos e as disponibilidades de banda se "somam" na percepção do cliente.

3.2 Apenas Contingência de Circuito

Neste cenário, também utilizaremos tecnologia já desenvolvidas para isso com as configurações de VRRP e HSRP, mas surge algumas possibilidades ainda não relatadas neste trabalho, com o conhecido dial backup (contingência com acesso discado) ou a solução de espelho do roteador.

A solução de contingência por acesso discado pode servir para sites remotos, ou filiais de menor porte. Trata-se de uma conexão discada efetuada em caso de falha de um circuito principal utilizando ISDN ou Dial-Up com rede de telefonia publica comutada. Caso o link principal restabeleça, a conexão backup é desligada.

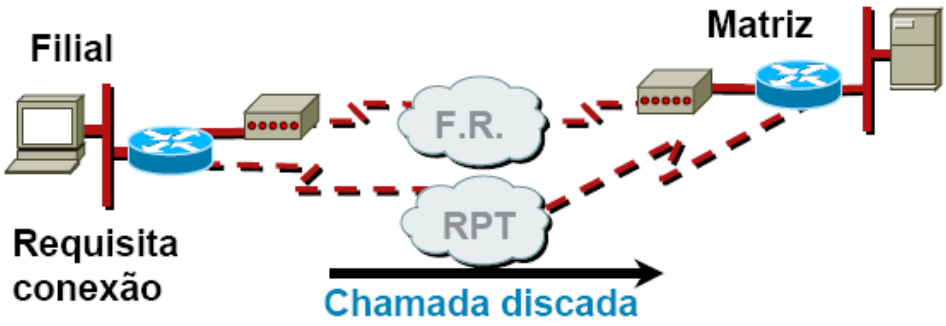

Figura 3.10: Solução com contingência Dial-Up

A solução chamada de espelho é uma contingência ao roteador. Significa ter um roteador desligado sempre com a configração espelho ao roteador em utilização, para uma possível falha deste. É uma ação manual, com intervenção humana, mas pode servir para trocar o roteador em mais de uma localidade, e também para um possível queima de placa do equipamento, que não é incomum.

3.3 Balanceamento e Contingência

A verdade é que ao longo do tempo, na área de desenvolvimento de projetos, soluções com apenas balanceamento ou ainda somente a contingência, acabaram não satisfazendo o cliente final. É inconcebível, aos olhos de quem patrocina a solução, existir um circuito secundário de dados com custos mensais apenas para ser contingência e atuar apenas na queda de um primário. Por esse motivo, surge a demanda por projetos com balanceamento e contingência.

O cálculo de Disponibilidade é realizado a partir dos Índices de Disponibilidade de cada componente da solução. Sabemos que o maior ofensor é o acesso. Porém os roteadores CE (CPE), PE também apresentam risco de queda.

Para exemplificar o Cálculo de Disponibilidade, suponhamos que, para cada componente, elas sejam as seguintes:

- Roteador CE: 99,9% - Probabilidade de Queda de 0,1%
- Enlace de Acesso: 99,8% - Probabilidade de Queda de 0,2%
- Roteador PE no Backbone: 99,99% - Probabilidade de Queda de 0,01%

3.3.1 Acesso

A solução de contingência de acesso se assemelha a alguns itens que já vimos como configurações de balanceamento. Mas neste caso, cada circuito deve percorrer acessos distintos.

O acesso chamado de última milha é considerado o ponto mais crítico para a disponibilidade de um circuito de dados. Hoje, a situação é mais complicada pela série de furtos de fios para revenda do cobre e um crescimento em desastres naturais que afetam acessos de fibra ótica.

É indicado utilizar acessos totalmente diferentes, como par de cobres e radio, sendo que os mesmos devem chegar a locais diferentes na estrutura da operadora. Caso contrário, não teremos sucesso no objetivo final do projeto.

Neste caso, podemos utilizar solução de PBR para controlar quais aplicações serão encaminhadas por qual tipo de acesso. Isso se faz necessário quando fazemos uma contingência de acesso com secundário sobre satélite, que por suas características físicas, tem grande latência dificultando aplicações de tempo real.

No caso de um circuito simples, temos os seguintes cálculos:

- 0,1 + 0,2 + 0,01 = 0,31, portando, a disponibilidade da solução é 99,69%

No caso da duplicação de acesso, os cálculos seriam os abaixo, com ganho razoável de disponibilidade no projeto:

- Probabilidade de queda do acesso: 0,2 x 0,2 = 0,04%, logo a probabilidade de queda seria de 0,1104% (0,1+0,0004+0,01), ficando assim a disponibilidade em 99,89%.

3.3.2 Acesso e Roteador (CE)

Para este escopo de projeto, utilizamos conceitos de roteamento dinâmico, estático, solução de HSRP caracterizando um projeto diferenciado. O roteador CE ou CPE, geralmente de pequeno ou médio porte, apresenta maior probabilidade de queda que que o roteador PE.

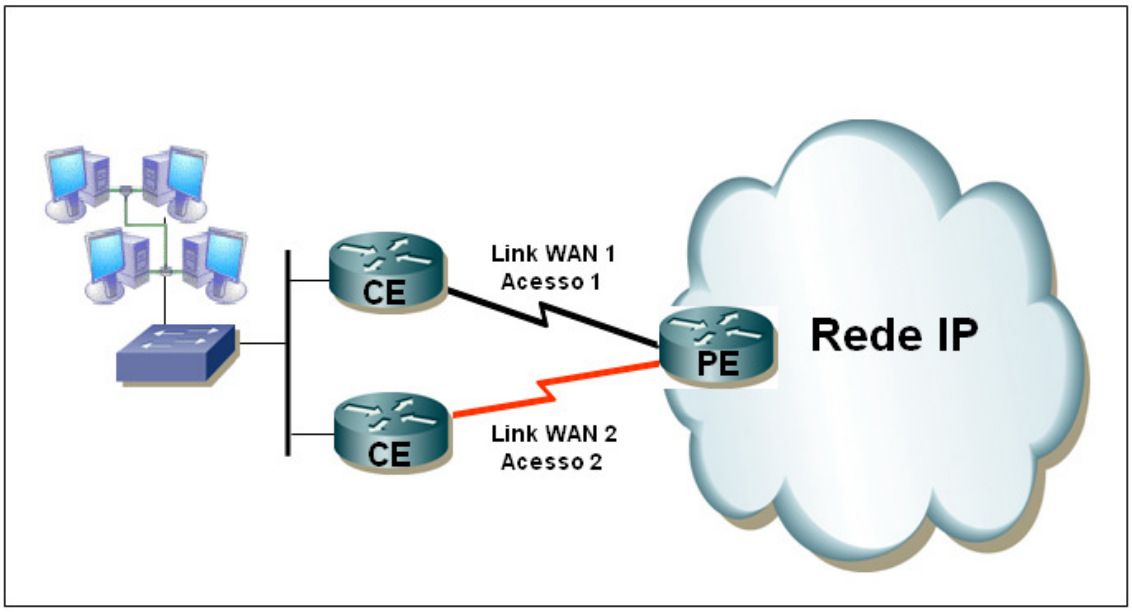

Figura 3.11: Solução com contingência de acesso e roteador Ces

Em uma rede com 2 CEs o rotemento fica um pouco mais complexo que o roteamento com único CE. Assim, julga-se necessário análise nos dois sentidos de tráfego, o sainte e o entrante.

Para o sainte, sentido cliente-backbone, o primeiro problema a se resolver a configuração de default gateway a seer configurada nas estações daquela localidade. E em caso de queda, as estações devrão saber que existe um default gateway backup. Como já verificamos, utilizamos o VRRP para resolver a questão. Teremos um IP virtual com primário em um roteador e o secundário no segundo, e este primário faz o balanceamento de carga utilizando, por exemplo o protocolo OSPF.

No sentido contrário, tráfego backbone-cliente, utilizamos apenas rotas estáticas de mesma métrica apontando para dus interfaces serias distintas, uma por cada acesso.

O cálculo de disponibilidade neste caso ficaria:

- Probabilidade de queda igual a 0,0105% (0,0001+0,0004+0,01) com disponibilidade de 99,9895

3.3.3 Acesso, Roteador (CE) e Backbone (PE)

Esta terceira solução pode ser considerada, com ênfase na questão de disponibilidade, com a mais completa. Além dos acessos separados e distintos, e ainda com dois CEs, utilizamos agora dois PEs diferentes, formando uma solução completa de contingência com balanceamento.

Ao se utilizar links de acessos redundantes, podem-se utilizar dois roteadores PE no backbone, sendo um para cada link. Este tipo de cenário só se justifica em casos de altíssima exigência de disponibilidade.

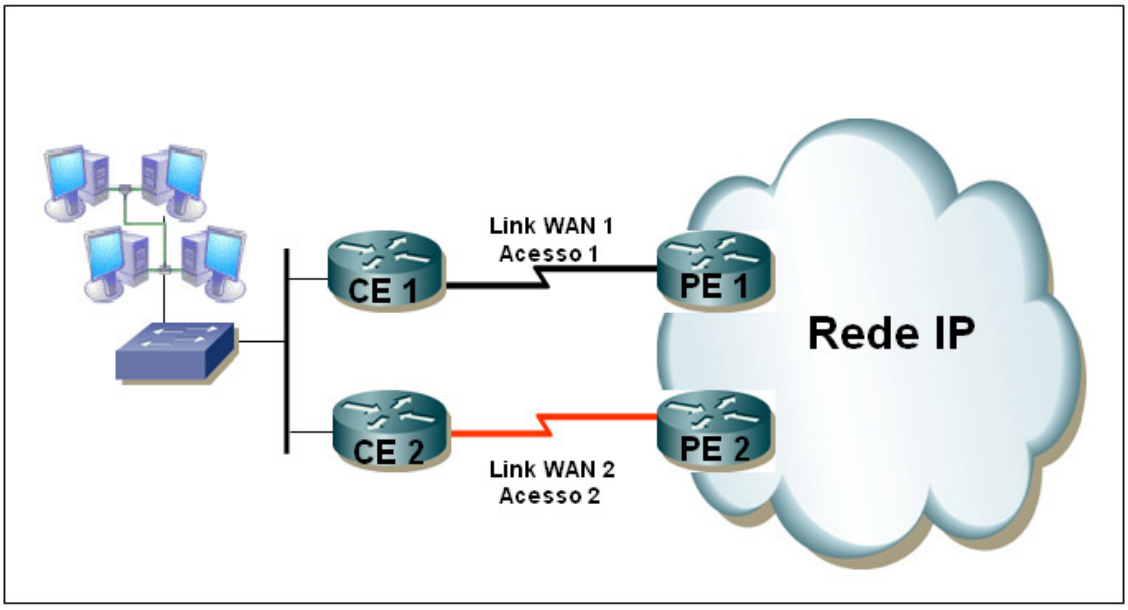

Figura 3.12: Solução com contingência de acesso, roteador CEs e PEs

Como vimos anteriormente, a duplicação de PE não acrescenta muito em termos de Disponibilidade, mas minimiza certo risco. É ideal para o cliente que deseja disponibilidade acima de cinco noves (99, 999%).

Neste caso, o tráfego destinado é idêntico ao cenário com um PE e, portanto, não precisará ser verificado novamente. A diferença é nos pacotes com sentido cliente, onde entra a figura da configuração Multipath BGP. O Multipath BGP servirá para fazer com que as rotas para chegar até o site sejam anunciadas nos dois roteadores, e cda um deles, com sua respectiva interface serial para encontrar o destino.

Neste ponto chegamos em um projeto de alto grau de complexidade, utilizando dois protocolos de roteamento, e ainda configuração de VRRP, ou seja, uma composição de tecnologia que, trabalhando no mesmo cenários, nos trazem uma solução com imenso grau de disponibilidade. Com certeza, não é simples colocar a solução em prática.

Ainda teremos uma última solução, talvez mais completa e complexa ainda, que será apresentada no Estudo de Caso, onde teremos contingência de CEs, acessos e PEs, porém com operadores diferentes, utilizando números de AS também diferentes.

4 ESTUDO DE CASO

O estudo de caso vai abordar um projeto bastante complexo, onde inserimos ter o balanceamento de carga, e contingência de operadores, acessos diferentes, e por conseqüência PEs diferentes. Porém os roteadores CEs, instalados no cliente, serão um para cada localidade, com duas interfaces serias cada equipamento.

O caso dos acessos diferentes, a alteração é apenas na camada física, então não interfere na parte mais complexa que são as configurações de protocolo de roteamento. Utilizamos nessa solução sempre um acesso sobre o radio e um segundo com part trançado ou fibra ótica, conforme a abordagem no local.

Os equipamentos utilizados foram da marca Cisco, por isso as configurações previamente descritas serão para esta marca. Temos diversos modelos, e neste caso foi considerado o Cisco 2811, mas poderíamos utilizar um 2801 ou outro equipamento com IOS disponível para protocolo de roteamento dinâmico BGP.

A solução descrita difere do normal, pois protocolos de roteamento, especialmente o BGP, são utilizados para encontrar o melhor caminho, e não para fazer com que cargas sejam balanceadas. Assim a configuração normal do BGP com números AS diferentes faria com que todo o tráfego escorresse por um circuito só, anulando o segundo anúncio para o backbone da rede montada em paralelo.

Neste projeto, vamos avançar um pouco da estrutura até agora estudada, pois analisaremos um cenário com matriz e filiais de redes IP corporativas, nesse caso VPNs montadas através da tecnologia MPLS.

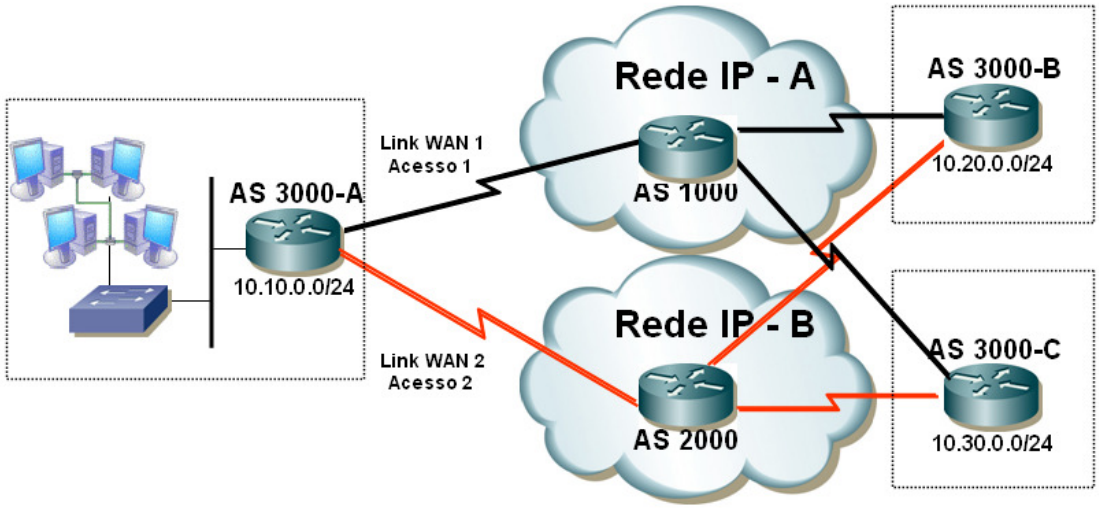

Figura 4.1: Solução com contingência de acesso, roteador CEs e PEs

Foram realizadas as seguintes configurações diferenciadas do normal para roteamento BGP:

```
#R3000A
router bgp 3000                          # definição número AS 3000
no synchonization
bgp log-neighbor-changes
redistribute connected                   # distribuição de redes diretamente conectadas
redistribute static                      # distribuição de rotas estáticas
neighbor 10.0.1.2 remote-as 1000         # anúncio pelo IP 10.0.1.2 do AS 1000
neighbor 10.0.1.2 allowas-in
neighbor 10.0.2.2 remote-as 2000
neighbor 10.0.2.2 allowas-in
neighbor 10.0.2.2 route-map ASPATH in    # representa a seqüência AS que
uma rota segue para atingir determinado destino.
maximum-paths 2                          # chegada de anúncio de 2 AS ( operadoras )
no auto-sumary
!
route-map ASPATH permit 10               #  atributo do AS PATH. Altera o anúncio
# as duas redes tenham mesmo peso
set as-path prepand 1000
```

E configuração no roteador de com AS 1000, localizado no backbone da Rede IP A

```
#R1000
router bgp 1000
no synchonization
bgp log-neighbor-changes
redistribute connected
redistribute static
neighbor 10.0.1.1 remote-as 3000          # anúncio para os sites – AS 3000
neighbor 10.0.1.1 route-map ASPATH out
neighbor 10.0.3.2 remote-as 3000
neighbor 10.0.3.2 route-map ASPATH out
neighbor 10.0.4.2 remote-as 3000
neighbor 10.0.4.2 route-map ASPATH out
maximum-paths 2
no auto-sumary
!
route-map ASPATH permit 10
set as-path prepand 2000
```

O AS_PATH é o atributo que representa a seqüência de ASs que uma rota segue para atingir determinado destino. Esses dados são incluídos na passagem ao anúncio em cada peer, que inclui seu número de AS juntamente ao anúncio da rota. Uma operação possível sobre este atributo é o chamado “prepend”, que se caracteriza por “piorar” o AS_PATH para determinada rota, forçando com que outros caminhos possam ser escolhidos. Um exemplo de prepend seria transformar o AS_PATH 1916 4230 para 1916 1916 4230. O menor AS_PATH é escolhido.

A partir dessas duas configurações diferenciadas, passamos a fazer diversos testes para análise da divulgação de rotas e conectividade. Para a solução estar correta, precisamos sempre a partir de um local, ter dois caminhos para chegar a um segundo ponto, indiferentes se matriz ou filiais.

Os testes realizados foram o seguinte:

```
R3000C#sh ip route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 14 subnets, 4 masks
```

```
B       10.10.0.0/24 [20/0] via 10.0.4.1, 00:13:18
        10.10.0.0/24 [20/0] via 10.0.6.1, 00:12:02
C       10.20.0.0/24 [20/0] via 10.0.4.1, 00:13:18
        10.20.0.0/24 [20/0] via 10.0.6.1, 00:12:02
```

```
R3000C#sh ip bgp
Network          Next Hop            Metric Path
*> 10.10.0.0/24  10.0.4.1            0  1000  2000  3000  ?
*                10.0.6.1            0  1000  2000  3000  ?
*> 10.20.0.0/24  10.0.4.1            0  1000  2000  3000  ?
*                10.0.6.1            0  1000  2000  3000  ?
```

De fato essa configuração foi testada em simulador chamado GNS3. A idéia inicial era utilizar o software Packt Tracer da Cisco, porém o mesmo não possui o protocolo de roteamento dinâmico BGP.

O GNS3 é um simulador de roteadores Cisco completo, com abertura para todos os comandos e protocolos, e com utilização de quaisquer versões ou *features* de IOS Cisco como no equipamento real, porém consome muita memória e processamento dos computadores onde foram simulados.

De qualquer a forma, após testes realizados com sucesso na ferramenta de piloto, a solução como descrita nesse trabalho foi implementada no cliente no site central e mais quatro filiais e resultou no esperado.

A princípio, o cliente iria fazer um tipo de engenharia de tráfego, já que cada filial tinhas duas redes não válidas, como por exemplo, 172.16.X.0 / 24 e 192.168.X.0/24 onde o X é igual e representa o número da filial de cada site. Em seu estudo, teríamos os pacotes com destino para a rede 172.16 saindo por uma operadora e o 192.168 saindo pela segunda, mas esse projeto não se caracterizava realmente como um balanceamento real de tráfego.

Ficamos com um balanceamento por destino em cada ponto da rede, utilizando o protocolo BGP, e o projeto é altamente escalavel, pois a inclusão de um site novo não resulta na reconfiguração dos demais elementos da rede. De forma dei finitiva, o projeto atendeu as expectativas do cliente final.

5 CONCLUSÃO

Como conclusão deste, é possível fazer uma análise GEEDS que avalia as variáveis de gerência, escalabilidade, desempenho, disponibilidade e segurança. E também poderemos fazer um comparativo direto entre as soluções compostas e o estudo de caso.

Considerando uma solução com apenas balanceamento de carga com acessos distintos, o fato de utilizar dois links de saída permite manejar com mais facilidade e expansão e manutenção da rede. À medida que a rede cresce, será necessária a ampliação do link de acesso.

Deve-se ficar bastante alerta ao parâmetro de desempenho, pois um enlace mal dimensionado pode acarretar em maiores retardos e perdas de pacotes. Quanto ao roteador, com diversas interfaces seriais, pode possuir limitações de memória, CPU ou ainda a capacidade de comutação de pacotes expressas em PPS.

A solução de disponibilidade é ampliada pelos dois links de acesso. Como este é o item com maiores riscos de queda, a solução atende bem um demanda para sites centrais ou filiais mais importantes.

Tabela 5.1: Planilha com comparativo de técnicas

Técnicas Básicas		
Tecnologias	Conceito	Cenário
Por Pacote	Balanceamento	Tráfego Dados
Por Destino	Balanceamento	Tráfego Multimídia
Multlink PPP	Agregar N x 2 Mbps	Tráfego Multimídia
VRRP	Contingência	2 Roteadores CEs
GLBP	Contingência e Balanceamento	2 Roteadores CEs

A inclusão de um segundo roteador facilita a lidar com recursos de segurança e escalabilidade, sendo que temos uma topologia redundante. No caso da escalabilidade, é mais simples incluir novos sites ou expandir link sem perda da conectividade padrão. O desempenho cresce, pois é inserido maior poder computacional na rede.

Tabela 5.2: Planilha com comparativo final de soluções

Sumarização de Soluções		
Topologias	Disponibilidade	Complexidade
Circuito Simples	99,6900%	Baixo
2 Acessos	99,8900%	Baixo
2 Acessos c/ 2 CEs	99,9895%	Médio
2 Acessos c/ 2 CEs e 2 PEs	99,9995%	Elevado
Estudo de Caso	99,8996%	Elevado

De modo geral, deve-se estudar bastante a demanda do projeto. Não é necessário inserir inteligência ou recursos diferenciados sem um objetivo claro. O estudo de caso, mesmo que utilize dois fornecedores de telecomunicações, não apresenta ganho de disponibilidade quando comparada a solução com contingência de roteadores e acessos.

A contribuição, do ponto de vista pessoal, foi que este projeto ajudou a desenvolver conceitos e definir algumas topologias. E serviu para obordar cenários cada vez mais comuns solicitados pelo mercado de soluções de redes de computadores e telecomunicações.

REFERÊNCIAS

BIRKNER, M. H. **Projetos de Interconexão de Redes:** Cisco Internetwork Design. São Paulo: Pearson Education do Brasil, 2003.

CHIOZZOTO, M.; SILVA, L. A. **TCP/IP Tecnologia e Implementação.** São Paulo: Érica, 1999.

CURSO de Gestão de Projetos : ensino a distância. Porto Alegre: Fundação Getúlio Vargas, 2008.

LAMMLE, T. **CCNA Cisco Certified Network Associate**: Study Guide. San Francisco: Sybex, 2000. (Exam 640-507).

OPPENHEIMER, P. **Projeto de Redes Top-Down:** um enfoque de análise de sistemas para o projeto de redes empresariais. Rio de Janeiro: Campus, 1999.

PROGRAMA de Capacitação em Tecnologia para Vendas: MPLS. Porto Alegre: Embratel, 2008.

PROGRAMA de Capacitação em Tecnologia para Vendas: roteamento e switching. Porto Alegre: Embratel, 2008.

PROGRAMA de Capacitação em Tecnologia para Vendas: internetworking & protocolos. Porto Alegre: Embratel, 2008.

PROGRAMA de Capacitação em Tecnologia para Vendas: voz e dados. Porto Alegre: Embratel, 2008.