Estratégia de Projeto de VPNs MPLS com Qualidade de Serviço

Adão Boava

Dissertação de Mestrado

Instituto de Computação

Universidade Estadual de Campinas

Estratégia de Projeto de VPN MPLS com Qualidade de Serviço (QoS)

Adão Boava

Junho de 2004

Banca Examinadora:

- **Prof. Dr. Maurício Ferreira de Magalhães (Orientador)**
  Faculdade de Engenharia Elétrica, Unicamp.
- **Prof. Dr. Edmundo Roberto Mauro Madeira**
  Instituto de Computação, Unicamp.
- **Prof. Dr. Leonardo de Souza Mendes**
  Instituto de Computação, Unicamp.

Estratégia de Projeto de VPN MPLS com Qualidade de Serviço (QoS)

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Adão Boava e aprovada pela banca examinadora

Campinas, Junho de 2004

Maurício Ferreira de Magalhães
Faculdade de Engenharia Elétrica, Unicamp
Orientador

Dissertação apresentada ao Instituto de Computação, Unicamp, como requisito parcial para obtenção do título de mestre em Ciência da Computação.

Dedicatória

"*in memoriam do meu pai*"

Agradecimentos

À Deus, por eu existir e possibilitar realizar esse trabalho.

Aos meus pais, Lidia e José Boava, à minha esposa Suzana, ao Murillo, a Bárbara e demais familiares pelo incentivo e apoio durante todo o trabalho.

Ao Professor Maurício Ferreira Magalhães pela sua orientação e amizade.

Aos membros da banca, pela sua presença na banca examinadora.

Aos funcionários do instituto de computação da Unicamp.

Conteúdo

Lista de Figuras

Lista de tabelas

Lista de Siglas

ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
AS	Autonomous system
ATM	Asynchronous transfer mode
ASBR	Autonomous System Boundary/Border Router
BA	Behavior Aggregate
BGP	Border Gateway Protocol
CE	Customer Edge
CPE	Customer Premise Equipament
CU	Currently Unused
DiffServ	Differentiated Service
DLCI	Data-Link Connection Identifier
DoS	Denial – of – Service
DSCP	DiffServ Codepoint
EBGP	External BGP
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
FEC	Forwarding Equivalence Class
GRE	Generic Routing Encapsulation
IBGP	Internal BGP
IGP	Interior Gateway Protocol
IntServ	Integrated Services
IP	Internet Protocol
ISP	Internet Service Provider
IPSec	IP Security Protocol
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocol
LSP	Label Switched Path
L2TP	Layer 2 Tunneling Protocol
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
P	Provider
PDU	Protocol Data Unit

PE	Provider Edge
PHB	Per-Hop Behavior
PIR	Packet Inserted Rate
POP	Point Of Presence
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality Of Service
RD	Route Distinguisher
RED	Random Early Detection
RFC	Request For Comments
RR	Route Reflector
RT	Rotas Targets
RTT	Round-trip time
RSVP	Resource Reservation Protocol
SLA	Service-level agreement
SP	Service Provider
ToS	Type Of Service
UDP	User Datagram Protocol
VCI	Virtual Channel Identifier
VoIP	Voice over IP
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding

Resumo

A garantia de níveis de serviço das Redes Privadas Virtuais (VPNs) depende fundamentalmente da presença de um modelo de projeto que seja função, não somente dos recursos da rede, como também dos serviços de comunicação (fim a fim) das estações e das aplicações. Esse modelo deve ser de fácil atualização e flexível o suficiente para a implantação rápida e eficiente de novas funcionalidades. As tecnologias VPN/MPLS e DiffServ têm sido propostas para o provimento de qualidade de serviço para a próxima geração das VPNs. Esta dissertação apresenta uma estratégia para o projeto de redes VPNs baseada nestas tecnologias. O trabalho proposto utiliza um ambiente de teste desenvolvido para esta dissertação com o objetivo de validar a implementação de VPNs MPLS com DiffServ. Foram realizados três tipos de testes voltados para a geração de dados referentes à conectividade, isolamento e qualidade de serviço. Esses dados permitiram a realização de análises do desempenho das VPNs MPLS.

O trabalho apresenta também o desenvolvimento, o uso e implementação do modelo de projeto de VPNs MPLS para várias classes de serviços. O modelo descreve uma estratégia simplificada para dimensionamento das classes de serviços por VPN. De forma geral, é capaz de representar o desenvolvimento de VPNs MPLS para várias classes com qualidade de serviço fim a fim, as quais transportam tráfegos de diversas aplicações: tráfego melhor esforço (best effort), tráfego com prioridades (AF1, AF2, AF3, AF4) e tráfego de voz (EF).

Os conceitos relacionados à conectividade e ao isolamento dos roteadores virtuais utilizados nas VPNs MPLS também são abordados neste trabalho. A tendência do mercado

de VPNs IP é também apresentada, sendo estas comparadas às VPNs de nível 2 predominantes no mercado e, normalmente, baseadas na tecnologia Frame Relay.

Abstract

The guarantee of degrees of VPN service depends largely on the existence of a project model that is a function of network resources, as well as of communication services (end-to-end), stations and applications. This model must be easily updated and flexible enough so that new functions may be added to it when necessary. VPN MPLS and DiffServ are being analyzed for the provision of service quality necessary to the next VPN generation. This work proposes a strategy for the project based on VPNs in these technologies. This work is based on an environment of tests, which was developed to this work and had as its objective to investigate the viability of implementing a VPN/MPLS with DiffServ. Three tests were performed in such environment and provided data referring to the connectivity, isolation and quality of service. This data permitted to analyze some VPN MPLS performance.

This work also shows the development, application and implementation of the VPN IP MPLS model in several degrees of services. Such model offers a simplified methodology of VPN IP MPLS projects. Besides that, it permits to measure the type of services by VPN. In general, this model is able to represent the VPN IP MPLS development to several degrees of services with the quality of end-to-end services, which transport traffic of diverse applications: Data (Best Effort), Data with priority (AF1, AF2, AF3, AF4) and Voice (EF).

The ideias about connectivity and isolation of Router Virtuals of VPN IP MPLS are analyzed in this work. The VPN IP market's tendency is also presented, comparing VPN IP to those of level 2, which prevail on market.

Ficha Catalográfica elaborada pela biblioteca do IMECC da Unicamp

Boava, Adão

B63e Estratégia de Projeto de VPN MPLS com QoS/ Adão Boava – Campinas,[S.P.:s.n],2004.

Orientador: Maurício Ferreira de Magalhães

Dissertação (Mestrado) – Universidade Estadual de Campinas, Instituto de Computação.

1.MPLS (Sistema). 2. Redes de Computação. 3. Estratégia
I – Magalhães, Maurício Ferreira. II – Universidade Estadual de Campinas

Capítulo 1

Introdução

1.1– Proposta do Trabalho

Observa-se nos últimos anos um aumento das exigências por serviços de comunicação de dados capazes de integrar várias mídias como dados, voz e imagem, com qualidade de serviço e segurança.

Constata-se um crescente interesse pelas aplicações multimídia distribuídas (vídeo-conferência, telemedicina, telefonia IP, etc.) na utilização das redes IP na forma de redes privadas. Essas aplicações caracterizam-se, principalmente, pelo emprego de diversos tipos de mídia que impõem requisitos distintos de QoS ao sistema de comunicação. Como exemplos de atributos de QoS podemos destacar: retardo máximo, variação máxima do atraso, taxa de transmissão, taxa de perda, disponibilidade, etc. Entretanto, as VPNs IP tradicionais, com seu modelo de serviços do tipo melhor esforço, começam a dar sinais de estrangulamento. Uma das conseqüências da adoção desse modelo é que todo o tráfego é tratado de maneira uniforme, sem nenhum tipo de diferenciação ou priorização. Contudo, nem todos os tipos de tráfego e transações são equivalentes ou têm a mesma importância para os usuários. É desejável que algumas aplicações recebam tratamento diferenciado segundo suas demandas específicas, o que não é possível no modelo atual. Por essa razão, pesquisas têm sido conduzidas nesse sentido, dando origem a várias arquiteturas de

serviços que buscam integrar as tecnologias VPN MPLS e DiffServ. Constata-se, também , que para garantir uma qualidade de serviço diferenciada na rede é importante que os elementos finais dessa cadeia, os servidores SAP, Web, VoIP, etc, sejam também capazes de oferecer um tratamento diferenciado às solicitações dos vários clientes.

São muitos os desafios relacionados ao projeto de redes VPN baseadas na tecnologia MPLS com qualidade de serviço (QoS). O principal desafio deste trabalho é determinar, de maneira clara e objetiva, um modelo de projeto que contemple qualidade de serviço de acordo com os requisitos da aplicação do usuário através do emprego de várias tecnologias de acesso.

1.2– Contribuições e Trabalhos Relacionados

VPNs MPLS são tratadas na RFC 2547 e Qualidade de Serviço por meio de DiffServ é proposta nos seguintes documentos: RFC 2475 (Uma arquitetura de Serviços diferenciados), RFC 2983 (Serviços Diferenciados e Túneis) e RFC 3270 (MPLS suportando DiffServ).

Atualmente, os grandes provedores de serviços possuem uma enorme quantidade e disponibilidade de tecnologias de acesso como, por exemplo, Frame Relay, ATM, Linhas dedicadas e ADSL. As VPNs MPLS podem permitir a integração de todas essas tecnologias viabilizando a otimização da planta instalada.

Uma contribuição das VPNs MPLS é o nível de segurança equivalente às VPNs de nível 2 como Frame Relay e ATM. Uma das grandes barreiras para a migração de usuários de VPNs nível 2 para VPNs nível 3 IP sempre foi a segurança que as VPNs de nível 2 oferecem para seus usuários, pois as mesmas são orientadas à conexão por meio de circuitos virtuais privados (CVP). Com o surgimento das VPNs MPLS criou-se o conceito de LSP, que é equivalente ao CVP do nível 2 do Frame Relay , oferecendo os mesmos níveis de segurança.

Outra contribuição das VPNs MPLS para as operadoras é o fato de usar o conceito de Roteador Virtual que reduz significativamente a necessidade de equipamento para cada enlace do usuário dentro da operadora.

O mercado de VPNs é formado basicamente pelos segmentos governo, corporativo, pequenas e médias empresas, sendo o governo e o segmento corporativo atendidos quase totalmente por VPNs de nível 2, e as pequenas e médias empresas por VPN de nível 3 sem QoS e segurança. A proposta deste trabalho sugere o desenvolvimento das VPNs MPLS com várias classes de serviço. Este trabalho contribui com a classe de dados melhor esforço para o mercado de pequenas e médias empresas e as classes AF (AF1, AF2, AF3, AF4) e EF para o mercado governo e corporativo.

A principal contribuição deste trabalho é oferecer uma estratégia de projeto de VPNs MPLS que contemple QoS por meio de várias classes de serviços. Para isso foi necessário a união das principais características das VPNs MPLS com DiffServ de acordo com suas respectivas RFCs.

1.3 – Tendências mercadológica das VPNs MPLS

As VPNs IP aliadas ao MPLS oferecem grandes benefícios às empresas. Juntos, elas fazem com que a rede seja mais segura e tenha maior agilidade no tráfego. Permitem, também, a integração de qualquer tipo de rede, planos de endereçamento e roteamento, fato que os protocolos convencionais não conseguem fazer. O IP é, hoje, o centro das atenções da maioria dos projetos de redes virtuais. O protocolo da internet, ainda segundo a IDC[1], deve responder por 40% do tráfego de longa distância em 2005 no Brasil e movimentar mais de US$ 800 milhões. As VPNs baseadas em MPLS são, hoje, uma das principais estratégias de operadoras, fabricantes e integradores.

A AT&T é uma das empresas que fornece o serviço VPN e já possui cerca de 1.200 clientes no Brasil que usam a rede VPN IP. As boas perspectivas de demanda foram um dos aspectos que também levaram a Intelig a apostar na VPN IP como plataforma de transmissão. O crescimento dos projetos de VPNs também vem estimulando os fabricantes de dispositivos de rede a investirem alto no desenvolvimento da tecnologia.

O mercado brasileiro de telecomunicações está passando pelo segundo momento mais importante de toda a sua existência. O primeiro momento ocorreu em 1997 e 1998, com a privatização do setor e, agora, com desregulamentação e ampliação da

[1] IDC –International Data Corporation do Brasil realiza estudo de mercado no Brasil

concorrência no mesmo. A tecnologia IP vem se desenvolvendo nos últimos anos e hoje é considerada uma das principais ferramentas que vai fortalecer a concorrência nos próximos anos. Novos serviços, como *Unified Messaging*, Voz sobre IP (VoIP) e acessos privativos virtuais (VPNs) são alguns dos serviços que serão alavancados com a evolução da tecnologia IP e estarão cada vez mais acessíveis aos usuários, com a ampliação da concorrência.

A tecnologia IP está sendo e deve continuar a ser a principal ferramenta adotada por operadoras para oferecer serviços em outras regiões (Telefônica oferecer serviço na área da Telemar e Vice Versa), pois apresenta diversas características favoráveis para atuar em novas áreas e ampliar a competição. Entretanto, ainda não será a principal tecnologia adotada para oferecer serviços na área atual de operação, uma vez que ainda existem muitas incertezas, tais como o comportamento da tecnologia IP, para o tráfego de voz em grandes volumes (como o tráfego gerado na cidade de São Paulo).

O tráfego telefônico tradicional está sofrendo um impacto com a entrada da telefonia IP uma vez que haverá queda no preço do minuto utilizado e novos serviços que agregarão valor aos serviços de voz. O tráfego existente tradicional migrará para as redes de comunicação de dados, alterando todo o serviço existente atualmente e principalmente a forma de tarifação. Porém, isso ocorrerá gradativamente, à medida que IP comece a trabalhar conjuntamente com MPLS com o objetivo de oferecer qualidade de serviço para as aplicações de voz.

A ampliação e evolução da oferta dos serviços também será o foco das operadoras e a tecnologia IP, aliada ao MPLS e a possibilidade de unificar as redes de voz e dados, alavanca benefícios econômicos e tecnológicos para as operadoras, tais como redução nos custos de manutenção das redes, unificação da tarifação, entre outros.

As operadoras tradicionais de telecomunicações no Brasil já estão em fase de implementação de seus serviços baseados na tecnologia IP/MPLS; porém, essa oferta de serviços deverá estar concentrada na expansão geográfica dos serviços e não nas redes atuais, pois a intenção destes fornecedores é otimizar a utilização das redes existentes e disponibilizar serviços sobre as mesmas.

Acredita-se que o mercado de VPN/MPLS IP começará a surgir no segundo semestre de 2004, principalmente com ofertas para o setor corporativo de médias e grandes empresas. Muitas destas empresas já possuem redes de comunicação de dados

implementadas, usando como acesso tecnologias tradicionais como Frame Relay, ATM e DSL. Portanto, essas empresas deverão ser as primeiras beneficiárias das soluções de VPN/MPLS em suas redes e principais usuárias dos novos serviços que estarão agregando valor à tecnologia.

O segmento de pequenas e médias empresas deverá ser o segundo grande mercado a receber os benefícios deste novo cenário de telecomunicações no Brasil. Com a ampliação da concorrência e a redução nos custos de implantação de uma rede de comunicação de dados, este mercado deve migrar gradativamente para os novos serviços baseados em comunicação de dados e serviços de valor agregado. Contudo, essa nova tecnologia requer novos investimentos, o que ocorrerá ao longo dos próximos anos.

O segmento residencial será o último setor a utilizar esses novos serviços e usufruir os benefícios da Tecnologia IP. É muito provável que com a evolução das tecnologias de acesso banda larga (xDSl, cable modem,etc.) as classes de maior poder aquisitivo (A e B) começarão a utilizar os novos serviços e, principalmente, voz sobre IP e videoconferência.

Serviços X.25 continuam em declínio no mercado, embora ainda respondam por 6% do mercado total; porém, nos próximos anos irão perder ainda mais participação devido à migração dos seus clientes para outras tecnologias. Essas redes são uma herança do antigo Sistema Telebrás, o qual utilizava esta tecnologia para interligar o Brasil em uma grande rede de pacotes, principalmente as operadoras de cartões de crédito. Essas redes devem sobreviver por mais alguns anos, pois, como toda a atual tecnologia, já está passando por um processo de congelamento e transição a outras formas de atendimento, principalmente o frame relay.

O frame relay, por sua vez, é uma tecnologia em expansão no mercado brasileiro. Está sendo muito utilizado para fornecer serviços ao segmento de pequenas e médias empresas, em virtude do seu menor preço mensal, se comparado às linhas dedicadas. O frame relay obteve uma participação no mercado de aproximadamente 14% do total. Um dos principais aceleradores deste mercado é a migração dos clientes X.25 e linhas dedicadas para as redes frame relay.

Os serviços IP são responsáveis por aproximadamente 14% do mercado. As redes ATM para acesso do usuário final ainda são incipientes no Brasil, respondendo por apenas 3% do faturamento total das empresas. As principais operadoras do mercado têm

investido na comunicação por pacotes e na procura por novos clientes corporativos, ao passo que os clientes procuram formas de atendimento que satisfaçam suas necessidades de comunicação de forma rápida, com qualidade e menor custo. Por esses motivos, os serviços de transmissão por pacotes vêm crescendo no mercado. A queda nos preços mensais é outro importante fator para o crescimento do mercado de comunicação de dados por pacotes.

1.3.1 - Tendências de VPNs baseadas em Rede e CPE

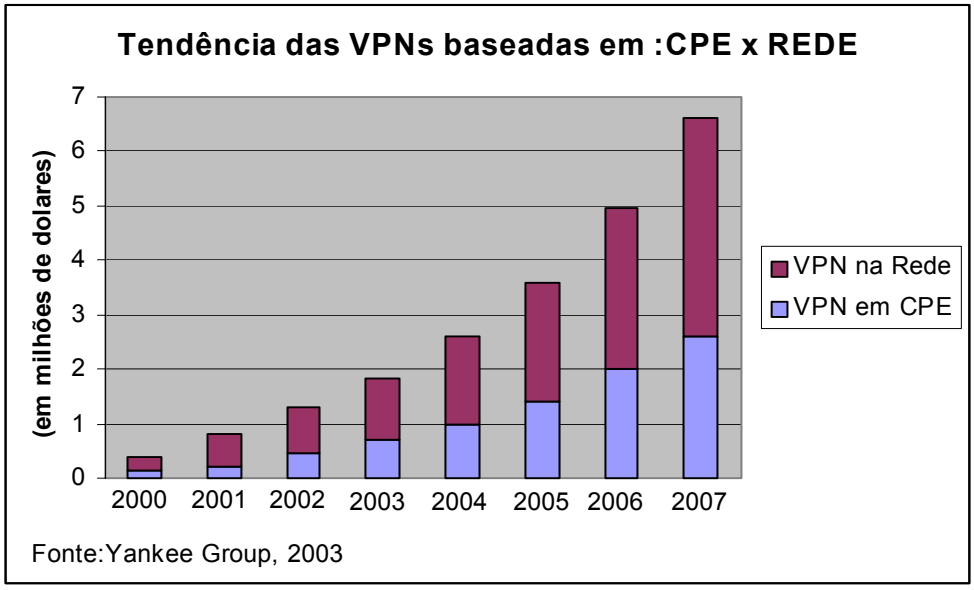

Figura 1.1 – Tendências das VPNs baseadas em CPE e Rede

Análise

É visível o grande crescimento a partir de 2004 no mercado mundial das VPNs IP baseada em CPE[2] (configuração da VPN é realizada de CPE a CPE) e principalmente aquelas baseadas em Rede (configuração da VPN é realizada na rede do provedor). Estudos têm mostrado que o Brasil seguirá a mesma tendência mundial de crescimento das VPNs IP.

As demandas por serviço legado estão em queda e novos serviços estão sendo desenvolvidos pelas operadoras; um desses são as VPNs MPLS. Oferecer VPNs MPLS para o mercado significa maior gerenciamento, melhor relação benefício/custo, maior

[2] CPE: *Customer Premise Equipment – D*esigna o equipamento que é instalado no ambiente do usuário utilizado para conectar com a rede do provedor.

flexibilidade de rede e principalmente maior fidelização do cliente. Os serviços de VPN desenvolvidos devem ser adequados para os diversos segmentos, inclusive o residencial. Apesar de ser uma tecnologia nova no Brasil, já é percebido que as VPN MPLS começam a dominar as soluções de comunicação. Podemos citar os casos do SPB (Sitema Brasileiro de Pagamento) e, recentemente, o Banco do Brasil (Aproximadamente 8000 acessos ligando todas às agências). O crescimento do serviço tem a tendência de seguir o modelo mundial, ou seja, um crescimento exponencial.

1.4 – Estrutura do Trabalho

Esta dissertação encontra-se organizada da seguinte forma: o capítulo 2 apresenta um resumo dos principais conceitos e protocolos utilizados neste trabalho; o capítulo 3 apresenta o método para o desenvolvimento de VPNs MPLS para várias classes de serviços formado por 7 passos; o capítulo 4 mostra um estudo de caso elaborado para validar o passo 5 apresentado no capítulo 3, que trata da configuração da VPN MPLS; no capítulo 5 são realizados testes de conectividade, isolamento e QoS das VPNs MPLS e, por último, o capítulo 6 apresenta as conclusões do trabalho.

Capítulo 2

Fundamentos

Neste capítulo será apresentada inicialmente uma descrição das características mais importantes das tecnologias VPN, MPLS, BGP e Diffserv para a modelagem de construção de VPNs MPLS com QoS. Na sequência são apresentados os principais conceitos e características dos Modelos *Overlay e Peer*. Em seguida são mostrados os métodos tradicionais de construção das VPNs MPLS. É apresentado, ainda, o conceito de serviços diferenciados com o objetivo de fornecer qualidade de serviço no modelo das VPNs MPLS. Por fim, apresenta-se um resumo das principais implementações de VPN MPLS baseadas na RFC 2547bis e suas vantagens.

Cada empresa tem diferentes necessidades de qualidade de serviço (QoS), segurança, número de pontos de acesso, número de usuários, complexidade de roteamento, aplicações de missão crítica e volumes de tráfego. Para satisfazer essas necessidades, os provedores de serviços oferecem um portfólio em que constam diferentes modelos de soluções de VPN:

- VPNs Tradicionais
    - Frame Relay (Nível 2)
    - ATM (Nível 2)
- VPNs baseadas em CPE
    - PPTP e L2TP(Nível 2)
    - IPSec (Nível 3)
- VPNs aprovisionada pelo provedor

- VPNs de nível 2 baseadas em MPLS
- VPNs BGP/MPLS de nível 3 ou RFC2547bis

Este capítulo estará focado no entendimento do Modelo das VPNs MPLS baseadas no BGP[8] e DiffServ[1] que atualmente é de grande interesse dos provedores de serviços.

2.1 – O que é uma VPN

Considere uma empresa que tem um conjunto de pontos[3] geograficamente dispersos. Para interconectar esses pontos a empresa precisa de uma rede. A rede é privada, pois é usada somente por esta empresa. Também é privada, porque os planos de endereçamento e roteamento através da rede são totalmente independentes dos planos de todas as outras redes. A rede é virtual, pois as facilidades usadas não necessariamente precisam ser dedicadas para um único usuário.

Pode-se dizer, informalmente, que VPN é um conjunto de pontos de acesso do usuário que podem comunicar entre si. Mas, formalmente, uma VPN é definida como um conjunto de políticas que controlam a conectividade e qualidade de serviço da rede privada [18].

Muitas das contribuições concebidas para a arquitetura de Rede Virtual Privada (VPN) têm sido submetidas aos órgãos de padronização. Outro aspecto importante é que vários provedores têm implementado o serviço VPN sobre uma infra-estrutura MPLS (Multiprotocol Label Switching) [3].

2.1.1 - Definição de VPN Intranet e Extranet

Conforme mencionado no item anterior, uma VPN pode ser definida como um subconjunto de pontos de acesso do usuário baseado em um conjunto de políticas. No exemplo apresentado na figura 2.1, seis diferentes pontos são incorporados pela rede do backbone do provedor de serviço. Os pontos A, B e C pertencem a uma empresa e os pontos X,Y e Z pertencem a outra empresa. Os pontos A, B e C podem compartilhar

[3] Ponto e rede de cliente/usuário equivale a “site” em inglês nesse trabalho

conectividade IP entre si porque eles fazem parte do mesmo subconjunto de políticas, ou seja, eles estão na mesma VPN (VPN ABC). Os pontos X,Y e Z são partes de uma outra VPN, pois compartilham um conjunto de políticas diferente daquele associado à VPN ABC.

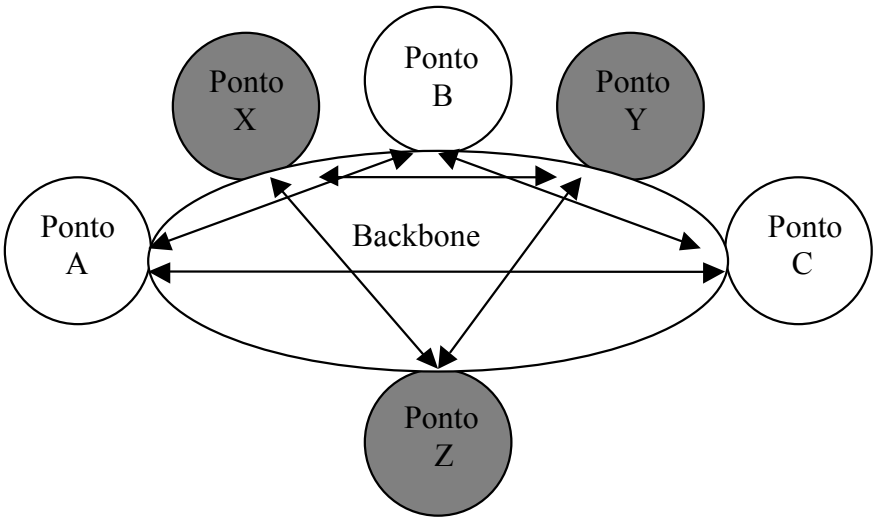

Figura 2.1 – BGP[4]/MPLS VPN: Sites e Backbone de rede

A figura 2.2 a seguir apresenta o cenário onde um novo conjunto de políticas é introduzido definindo que os pontos A e Z compartilham conectividade IP.

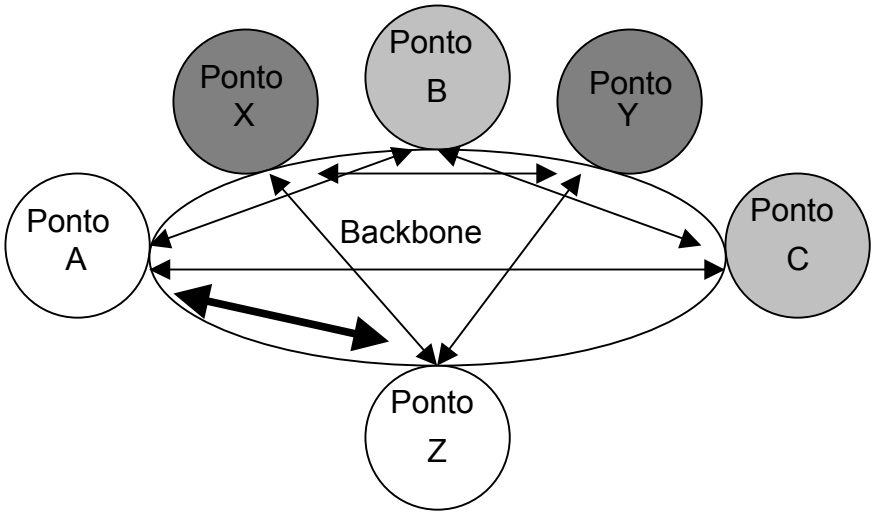

Figura 2.2 – Um novo subconjunto de políticas

[4] BGP/MPLS VPN usa os benefícios do BGP para troca de rotas entre os roteadores de borda no backbone do provedor

Dois pontos podem unicamente ter conectividade IP através do backbone da rede se há no mínimo uma VPN que contenha ambos os pontos. Pode haver a situação em que todos os pontos que estão em uma VPN pertençam a uma única empresa. Nesse caso, a VPN é chamada de Intranet[5]. As VPNs ABC e XYZ são exemplos desses tipos. Se os pontos em uma VPN pertencem a mais que uma companhia, por exemplo a VPN AZ, temos uma VPN extranet (figura 2.3).

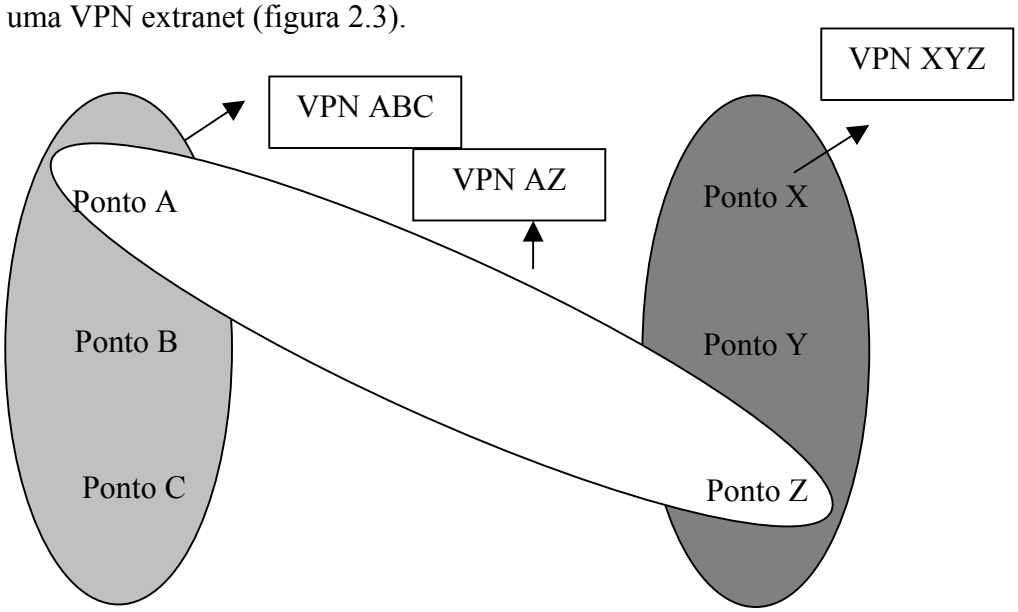

Figura 2.3 - Uma terceira VPN é criada

Ambas as topologias (Intranet e Extranet) apresentadas anteriormente são possíveis de ser implementadas com a tecnologia VPN MPLS (RFC 2574bis). Uma VPN MPLS consiste de duas redes: a rede do provedor e a rede do cliente. A rede do provedor é constituída de roteadores de borda (PE) que provêem serviços de VPN e conectividade para as redes dos clientes. As redes dos clientes são normalmente constituídas, fisicamente, por diferentes pontos de acessos. Os roteadores dos clientes que se conectam aos provedores dos serviços das VPNs são chamados de *Router Customer Edge* (CE) , como mostra a figura 2.4. Basicamente, uma VPN MPLS usa uma combinação dos benefícios das tecnologias não orientada a conexão(CE-PE) com a tecnologia orientada a conexão (PE-PE). Os protocolos de roteamento entre o CE e PE poderão ser: RIPv2, Rota estática, BGP4

[5] O termo Intranet refere-se ao fato de que a aplicação Internet (www, ftp, correio) está sendo executada completamente em uma rede privativa.

ou OSPF e entre os PEs é utilizado Multiprotocolo BGP (MP-BGP). As próximas sessões do capítulo irão abordar em detalhe a implementação de VPN MPLS.

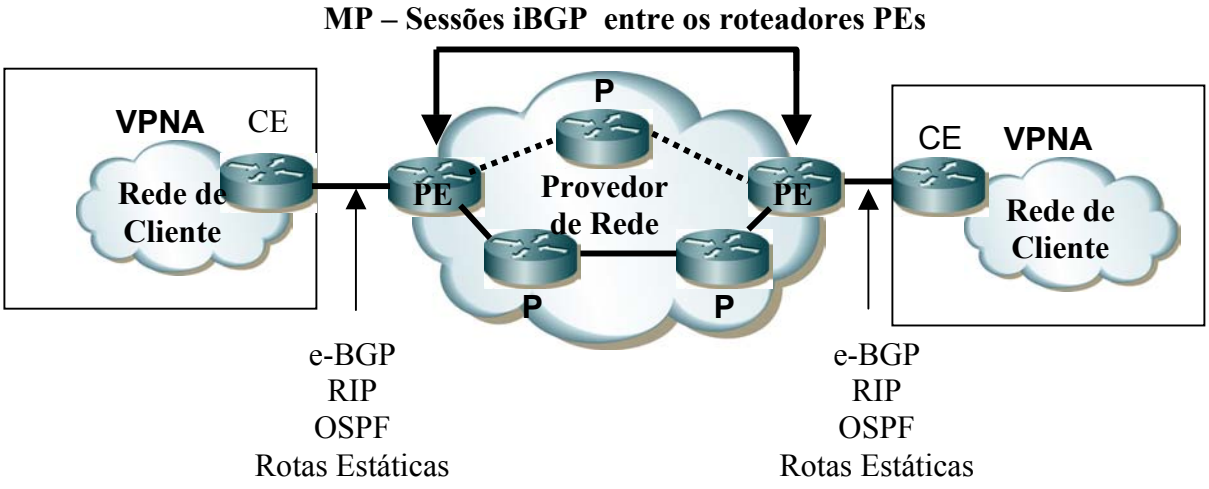

Figura 2.4 – Visão Geral de uma VPN MPLS

2.2 – Modelo Overlay

As técnicas mais comuns atualmente para prover serviços VPN são baseadas no modelo Overlay (predominantemente Frame Relay[6]). Neste modelo, cada ponto de acesso do ambiente do usuário tem um roteador que é conectado, através de enlaces ponto a ponto, até outro roteador remoto do usuário. O ambiente do usuário pode ter um ou mais roteadores que podem ser conectados a todos os outros pontos ou a um subconjunto destes. A tecnologia utilizada para oferecer enlaces ponto a ponto pode ser: linhas dedicadas, Frame Relay ou ATM. A rede formada por estes enlaces ponto a ponto e os roteadores instalados formam um "Backbone Virtual". É nesse backbone virtual que os provedores de serviços formam as VPNs para interligar os pontos das redes dos usuários (Figura 2.5).

[6] Frame Relay é tecnologia que domina o mercado para implementação de VPNs de nível 2. Esta tecnologia surgiu no fim da década de 80 como uma simplificação do X.25, para aumentar, principalmente, a vazão e reduzir o atraso.

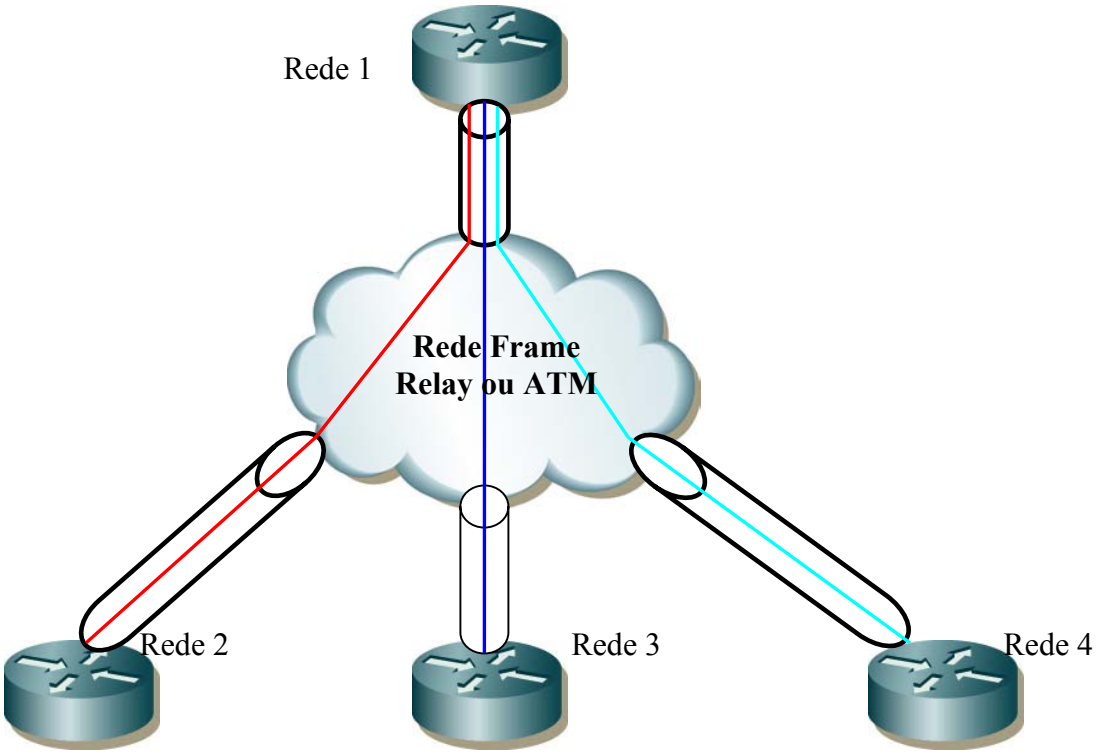

Figura 2.5 – Modelo Overlay

As soluções das VPNs baseadas no modelo overlay são as predominantes no mercado mundial. Este tipo de solução apresenta vários problemas que limitam o desenvolvimento em larga escala do serviço VPN. O primeiro problema vem da necessidade que o cliente tem em operar e projetar sua própria VPN no backbone virtual. Neste caso é necessário um conhecimento sobre roteamento IP, o que não é comum na maioria das organizações pois estas estão focadas em seus negócios e não em redes IP, principalmente nas pequenas e médias empresas. Como resultado, muitas empresas não utilizam o serviço VPN pois requerem projeto e operação nos seus backbones virtuais. Há necessidade também do conhecimento em QoS IP, QoS de camada 2 e mapeamento entre QoS da camada IP com a camada 2. Isso porque, enquanto ATM e Frame Relay podem prover QoS, essa QoS é expressa em termos dos parâmetros da camada dois e não em termos de QoS IP.

Com o objetivo de resolver este problema, provedores de serviços oferecem o que é conhecido como "*Roteador Gerenciável*" no qual o provedor projeta e opera o backbone virtual para cada VPN dos clientes. Portanto, enquanto se resolve um problema,

cria-se outro, pois requer que o provedor de serviço opere um backbone virtual para cada VPN de cliente. Essa necessidade faz com que o provedor encontre dificuldade em oferecer serviços para um grande número de clientes (imagine um provedor que tem 100.000 VPN de clientes e tendo que operar 100.000 backbone virtuais, um para cada cliente). Também como conseqüência desse problema, o custo do serviço torna-se alto. O serviço de gerenciamento de roteador, somente, não resolve o problema.

A dificuldade em suportar um grande número de clientes é justamente um dos problemas do modelo overlay. O segundo problema vem dos clientes que têm um grande número de pontos (100 ou mais) e precisam conectividade completa com todos os pontos (configuração *mesh*). Neste caso, para uma VPN com n pontos, cada roteador precisará de (n-1) pontos de troca de tráfego (*peering*). Este problema é o mesmo encontrado na interconexão baseada no modelo overlay de redes IP sobre ATM.

Outro problema com o modelo *overlay* é a quantidade de configuração necessária para inclusão de um novo ponto em uma VPN existente. Para uma VPN que requer conectividade completa (full *mesh*) entre todos os pontos, cada um destes pontos necessita de uma conexão e roteamento ponto a ponto com todos os outros pontos da VPN.

Uma variação do modelo *overlay* é o modelo em que o provedor de serviço desenvolve roteadores que são capazes de atuar como Roteadores Virtuais (VR). Nesse caso, um simples roteador atua como uma coleção de roteadores virtuais. Um "VR" é funcionalmente equivalente a um roteador convencional, exceto que compartilha CPU, largura de banda e recursos de memória com outros roteadores virtuais.

Um Roteador Virtual é conectado a outro, via enlaces ponto a ponto. Para reduzir o número de enlaces ponto a ponto requerido, é possível fazer a multiplexação de várias conexões em um único enlace por meio de Frame Relay ou ATM, através da introdução de alguma forma de multiplexação do cabeçalho do pacote. Cada ambiente do usuário possui um roteador conectado em um roteador virtual. Nesse caso, o backbone virtual é composto de tais roteadores virtuais e os enlaces que os interligam.

Uma das vantagens do uso do Roteador Virtual é que ele reduz a quantidade de equipamentos físicos que um provedor necessita disponibilizar. O uso do roteador virtual não altera o modelo; ele permite simplesmente que um único roteador seja fisicamente compartilhado por vários roteadores virtuais.

A garantia de QoS no modelo *overlay* é usualmente expressa em termos de largura de banda (CIR[7]) em um determinado Circuito Virtual (VC) e da taxa máxima de transmissão (PCR). A garantia de banda é usualmente provida por meio de serviços estatísticos da camada 2, mas depende da estratégia de "*overbooking*" do provedor de serviço.

Além dos circuitos Frame Relay e ATM, poderiam também ser utilizado mecanismo de túneis como GRE e IPSec para conectar os roteadores. Entretanto, túneis GRE e IPSec atuam unicamente para prover um mecanismo de conexão de roteador ponto a ponto mantendo as características do modelo Overlay e introduzem um novo problema conhecido como *spoofing de dados*.

Uma das principais deficiências dos protocolos e serviços TCP/IP é usar esquemas baseados em endereços IP para autenticar máquinas na rede. A autenticação é feita com base no endereço IP de origem de um pacote recebido, todavia, é impossível determinar com certeza a identidade da máquina que originou o pacote. Isso torna muito fácil para atacantes personificarem outras máquinas. Esta técnica de personificação é conhecida como *IP spoofing*.

Um dos caminhos para resolver o problema de *spoofing* de dados é a utilização de IPSec em vez de GRE. No caso do IPSec, o final do túnel poderá autenticar o transmissor permitindo que somente os pacotes iniciados originalmente pelo seu dono cheguem ao final do túnel. Todos os outros pacotes são rejeitados.

A vantagem oferecida pelos túneis GRE e IPSec sobre Frame Relay e ATM é a habilidade de oferecer serviços de VPNs para qualquer lugar onde exista conectividade com a Internet.

2.3 – O Modelo Peer

A principal contribuição desse modelo, relativamente ao modelo overlay, é a possibilidade de oferecer o serviço de VPN em grande escala.

O modelo *peer* provê um número de vantagens sobre o modelo *overlay*:

[7] CIR é a taxa que a rede concorda suportar para uma determinada conexão no modo frame.

- O roteamento, do ponto de vista do usuário, torna-se essencialmente simples, pois o roteador do cliente troca informações de roteamento com um (ou poucos) roteador(es) de borda do provedor, enquanto no modelo *overlay* este número de roteadores pode crescer significativamente.
- Considerando principalmente uma topologia *full mesh*, o aprovisionamento da largura de banda é simples porque é necessário especificar somente a largura de banda de entrada e saída para cada acesso da VPN entre CE e o PE. No caso do modelo overlay o aprovisionamento é mais complexo, pois será necessário uma análise fim a fim em cada CVPs, acessos e banda da VPN.
- A adição de um novo ponto/site é simples porque o aprovisionamento pelo provedor do serviço é unicamente adicionar um ponto/site com um roteador CE e configurar um dos protocolos de roteamento entre o CE e o roteador PE. No modelo overlay de VPN o provedor de serviço deverá aprovisionar um conjunto inteiro de VCs do ponto principal/origem para o outro ponto/destino do cliente da VPN.

A implementação de VPN baseada no modelo de pares (modelo peer) tem, no caso do MPLS, duas possibilidades de implementação:

- Método com roteador compartilhado [4] – Nesse método, os usuários compartilham o mesmo roteador PE;
- Método com roteador dedicado [4] – Nesse método, cada usuário tem um roteador PE dedicado.

2.3.1 – Método com roteador compartilhado

Neste caso, o roteador na borda da rede do provedor é compartilhado entre vários usuários. As listas de acessos têm que ser configuradas em todas as interfaces PE-CE nos roteadores PE para garantir isolação entre usuários das VPNs (ilustrado no teste de isolamento da VRF realizado no capítulo 5), prevenindo que um cliente de uma VPN possa

acessar outra VPN, ou até mesmo para evitar ataques do tipo Denial-of-Service (DoS)[8] em outra VPN.

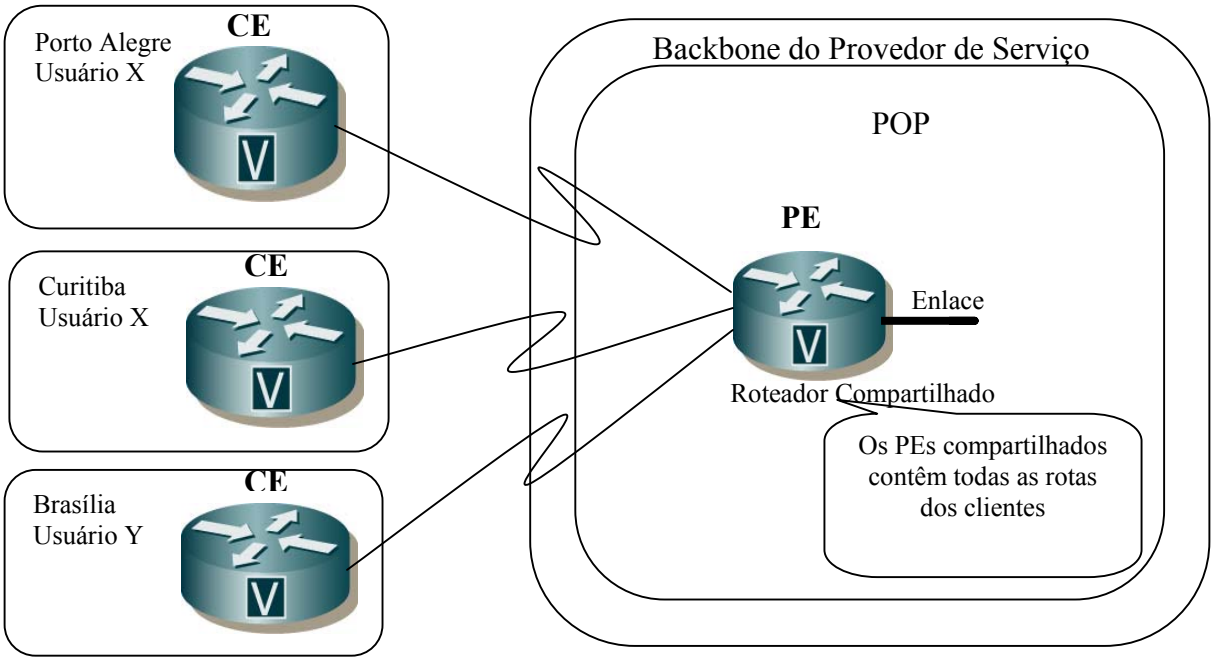

Figura 2.6 – Modelo de Roteador compartilhado

2.3.2 – Método com roteador dedicado

Nesse método, todas as VPNs dos usuários têm seu próprio roteador PE dedicado (como mostra a figura 2.7 abaixo) e possuem seus acessos somente para os roteadores incluídos na tabela de roteamento do roteador PE.

[8]A essência dos ataques se baseia no princípio de saturar a capacidade de processamento dos serviços

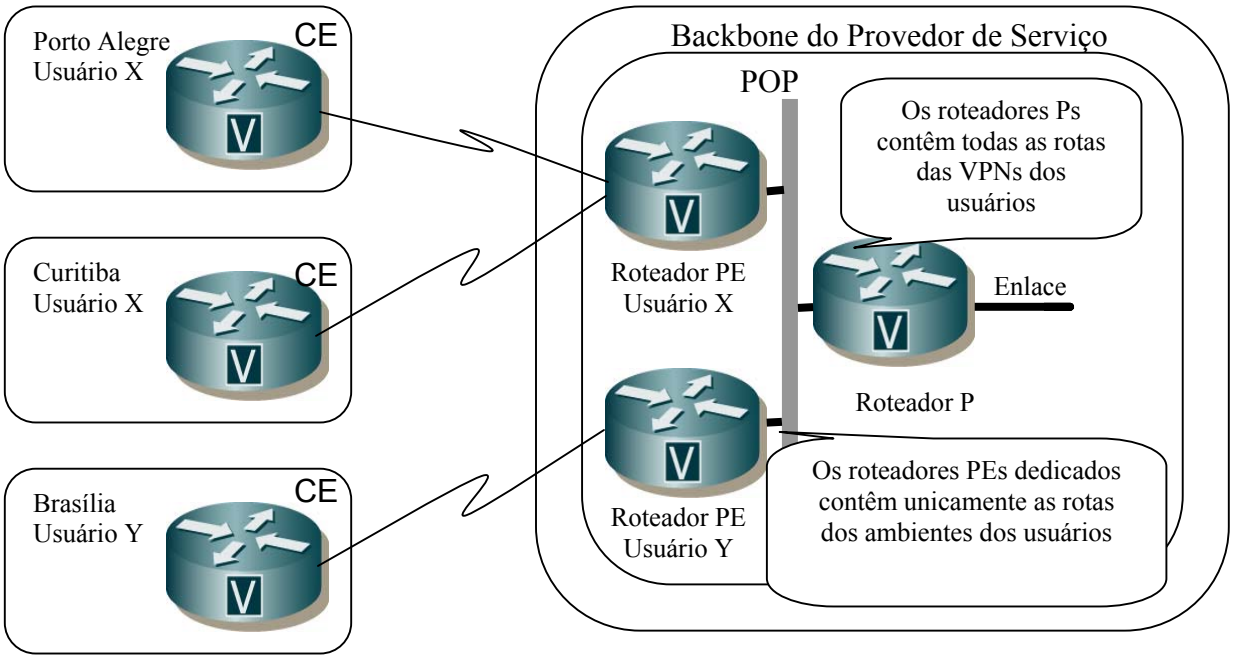

Figura 2.7 – Modelo VPN "Peer-to-Peer" com roteador dedicado

O modelo de roteador dedicado usa protocolos de roteamento para criar tabelas de roteamento para cada VPN nos roteadores PEs. Estas tabelas contêm somente as rotas anunciadas pela VPN conectada, resultando em uma perfeita isolação entre as mesmas. O roteamento no roteador dedicado pode ser implementado da seguinte forma:

- O protocolo de roteamento é executado entre os roteadores PE e o CE;
- O BGP é executado entre os roteadores PE e P;
- Os roteadores PEs redistribuem as rotas recebidas do CE através do BGP;
- Os roteadores Ps propagam as rotas unicamente com o BGP community (observar o anexo A, item A.5) para os roteadores PEs.

Esse modelo com roteador dedicado, no entanto, não tem sido implementado na prática em função da alta quantidade de roteador necessário.

2.3.3 - A implementação do modelo Peer

A implementação do modelo peer pode ser realizada através da utilização de um novo tipo de endereçamento (VPN-IP) e através da tecnologia MPLS.

2.3.3.1 – Endereços VPN-IP

Até esse momento foram apresentados mecanismos que permitem especificar como é feito o controle da conectividade entre os pontos dos usuários de uma VPN básica. Mas esses mecanismos usam BGP que assume determinadas condições sobre o endereçamento IP. Especificamente, o BGP assume que os endereçamentos IP sejam únicos. Esta associação não é adequada no ambiente de VPN pois um mesmo bloco de endereçamento IP poderá ser simultaneamente utilizado por múltiplas VPNs dos usuários. Também, para o uso do BGP, é necessário entender como usar o BGP em um ambiente onde endereços IP não são únicos [49]. Uma solução natural para esse problema seria estender o endereço IP através da agregação de um novo campo de modo a permitir a identificação das VPNs. Este novo tipo de endereço denomina-se de endereço de VPN e deve ser único.

Pela definição, um endereçamento VPN-IP é construído pela concatenação de um campo de comprimento fixo denominado *Route Distinguisher com o endereço IPv4*. Um *Route Distinguisher* é estruturado de forma a permitir que cada provedor de serviço VPN crie rotas próprias, sem o risco da mesma ser utilizada por outro provedor de serviço (veja capítulo 4 – Identificador de Rotas -RD). Com o objetivo de facilitar o entendimento do protocolo BGP o anexo A contém uma breve descrição dos conceitos fundamentais do protocolo.

2.3.3.2 – MPLS

MPLS - Multiprotocol Label Switching [43] é uma tecnologia desenvolvida no âmbito do IETF-Internet Engineering Task Force, inicialmente com o objetivo de tornar o encaminhamento e a comutação eficientes de fluxos de tráfegos através da rede. O MPLS é uma tecnologia utilizada em backbones[9] e tem o objetivo de solucionar problemas atuais de

[9] Backbone é uma conexão de alta velocidade que funciona como espinha dorsal de uma rede de comunicação

redes de computadores como velocidade, escalabilidade, gerenciamento de qualidade de serviço (QoS) e a necessidade de engenharia de tráfego-TE.

No roteamento tradicional em redes IP os pacotes seguem o menor caminho até o destino. Alguns roteadores podem então ficar sobrecarregados enquanto outros são subutilizados. Outro problema é que as buscas nas tabelas de rotas são demoradas pois as entradas não têm tamanho fixo: procura-se o maior prefixo de endereço que coincida com o endereço de destino do pacote (este método é conhecido como *Longest Match*). Além disso, o processo de roteamento, incluindo as buscas nas tabelas de rotas, é realizado em cada roteador para cada pacote recebido. Quando se utiliza MPLS nas redes IP convencionais, há drástica redução do tempo de busca nas tabelas de rótulos em comparação com as buscas nas tabelas de roteamento.

Uma das vantagens do MPLS é a sua utilização sobre ATM. Neste caso há a eliminação do problema conhecido como problema N^2 (o capítulo 3 detalha melhor esse problema) que surgiu com IP sobre ATM, em que são necessárias N-1 conexões para cada um dos N comutadores ATM. O MPLS contribui, basicamente, com a separação dos componentes dos planos de controle e encaminhamento. A figura 2.8 mostra abaixo a separação dos planos.

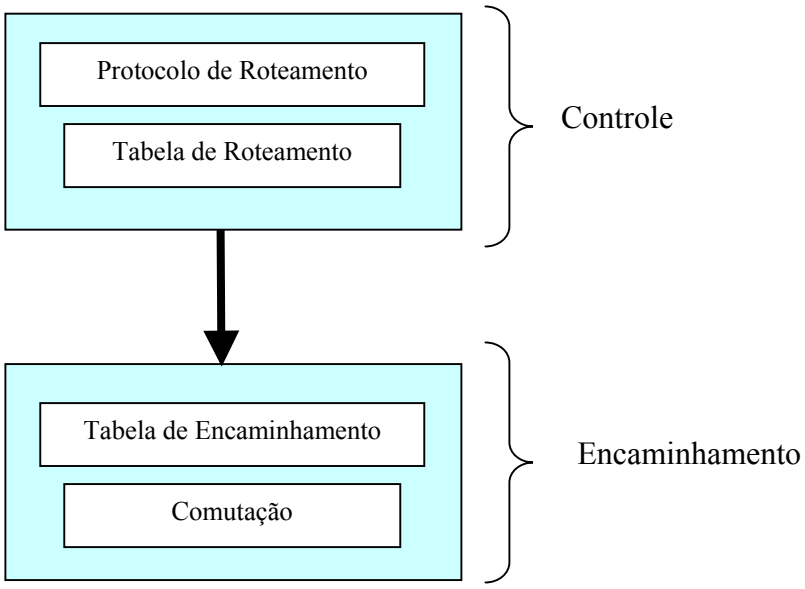

Figura 2.8 – Controle e Encaminhamento no MPLS

O plano de controle possui duas principais funções: determinar o caminho que envolve a criação das tabelas de roteamento e a função de sinalização. O protocolo de roteamento troca informações com outros roteadores para construir e manter as tabelas de roteamento, usando alguns protocolos de nível três (OSPF ou BGP-4). Os rótulos que compõem as tabelas de encaminhamento são distribuídos na rede por meio de um dos protocolos de sinalização (LDP ou RSVP).

O cabeçalho MPLS é formado de 32 bits e possui os seguintes campos.

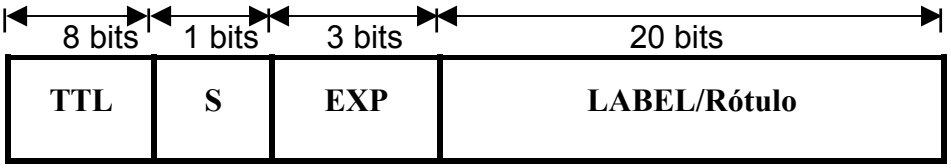

Figura 2.9 - Cabeçalho MPLS

LABEL – É formado de 20 bits e transporta o valor atual do cabeçalho MPLS.
EXP – Campo EXPerimental para prover QoS
S – O campo Stack suporta uma hierarquia de pilha de label.
TTL – Campo do tempo de vida.

2.4 - RFC 2547bis

Nessa seção será feito um resumo da implementação da RFC 2547 realizada pelos principais fornecedores de soluções VPN BGP/MPLS.

2.4.1 – Visão Geral

Redes Virtuais Privadas MPLS na RFC-2547bis [8] definem um mecanismo pelo qual os provedores de serviço podem usar seu backbone para prover serviço de VPN para seus clientes. Uma VPN é um conjunto de pontos que compartilham informações de roteamento e cuja conectividade é controlada por um conjunto de regras. A RFC-2547bis é também conhecida como VPN BGP-MPLS porque o BGP é o protocolo utilizado para

distribuição da informação de roteamento das VPNs e pela utilização do MPLS no estabelecimento dos circuitos virtuais e encaminhamento do tráfego.

Um provedor pode gerenciar múltiplas VPNs desde que as regras estejam habilitadas para manter separadas as rotas das diferentes VPNs (O capítulo 5 avalia o isolamento da VPN).

A conexão entre os roteadores CE e PE pode ser uma conexão remota através de Frame Relay ou ATM ou, ainda, um enlace Ethernet. As redes dos clientes trocam rotas com provedores de serviços (CE para PE), usando rotas estáticas ou via RIP, OSPF ou E-BGP (Ver capítulo 4 – seção 6).

Quando o roteador PE recebe a rota atualizada é criada uma tabela de roteamento e as informações de alcançabilidade são encaminhadas para cada ponto da VPN conectada no roteador.

Os roteadores PEs estabelecem sessões MP-iBGP[10] para trocar rotas de clientes. O tráfego da rede do provedor passa através do LSP (Label Switched Path) pré-estabelecido através dos protocolos de sinalização LDP ou RSVP-TE. O roteador PE adiciona dois rótulos como prefixos para cada pacote do tráfego IP do cliente. O "rótulo mais externo" identifica o próximo "salto" ao longo do LSP do provedor de rede, enquanto o "rótulo mais interno" identifica a VPN particular do cliente, conectada no roteador de destino. A informação do rótulo é trocada durante a sessão de configuração MP-iBGP.

Os principais objetivos da RFC 2547bis são**:**

- Oferecer serviços simples para os usuários com todo o potencial do roteamento IP;
- Oferecer serviço com grande escalabilidade e flexibilidade;
- Permitir regras que são usadas para criar uma VPN que será implementada pelo provedor do serviço, de forma independente ou trabalhando junto com o cliente;
- Permitir ao provedor de serviço a entrega de um serviço de valor adicionado que possa fidelizar seus clientes.

[10] MP-iBGP são sessões BGP PE a PE por meio do backbone VPN/MPLS

2.4.2 – Implementação da RFC 2547

Na arquitetura tradicional de roteamento IP há uma clara distinção entre rotas externas e internas. Na visão de um provedor de serviço, rotas internas incluem todos os enlaces internos do provedor e interfaces de loopback[11]. Essas rotas internas são trocadas com outras rotas na rede, por meio do protocolo IGP, tais como OSPF ou IS-IS. Todas as rotas aprendidas na Internet por meio de pontos de troca de tráfego (peering) ou de pontos de clientes são classificadas como rotas externas e são distribuídas por meio do protocolo externo (EGP), tais como BGP. Na arquitetura IP tradicional, o número de rotas internas é bem menor que o número de rotas externas [38].

2.4.2.1 – Componentes da Rede

No contexto da RFC 2547bis, uma VPN é uma coleção de regras para controle da conectividade entre um conjunto de redes. Uma rede de cliente é conectado pelo provedor do serviço por uma ou mais portas, sendo que o provedor de serviço associa cada porta com uma tabela de roteamento VPN. Na RFC 2574bis, a tabela de roteamento VPN é chamada VPN Routing and Forwarding (VRF). A figura 2.10 ilustra os blocos fundamentais para a VPN BGP/MPLS:

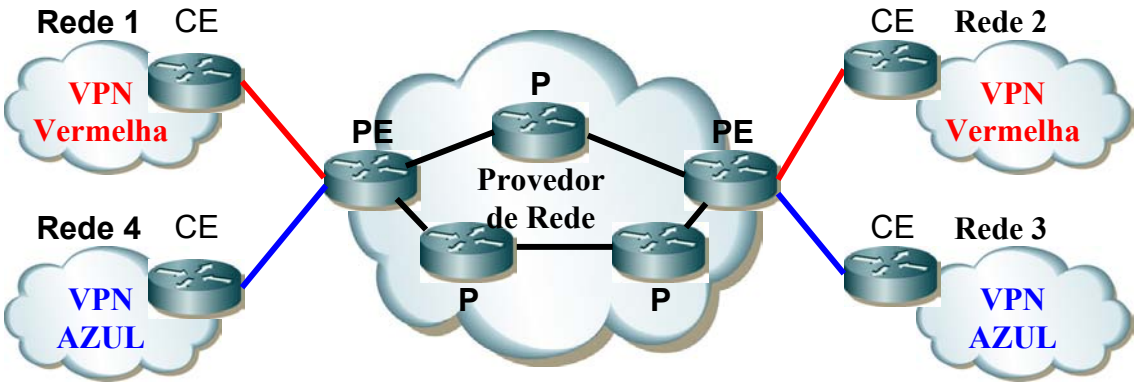

Figura 2.10 – Componentes da VPN/MPLS

- Customer Edge Devices (CE) – Equipamento de borda do cliente

[11] Loopback – Cada roteador PE necessita de um endereço único (Usualmente chamado de loopback) que é utilizado para alocar um rótulo e habilitar o encaminhamento dos pacotes da VPN através do backbone.

Um customer edge (CE) provê acesso do cliente até o provedor de serviço de rede. Tipicamente, o equipamento CE é um roteador IP que estabelece uma conexão diretamente com o roteador PE. Depois de estabelecida a conexão, o roteador CE anuncia as rotas dos pontos da VPN local para o roteador PE e aprende as rotas remotas da VPN.

- Provider Edge Routers (PE) – Equipamento de borda do provedor

Os roteadores PEs trocam informação de roteamento com os roteadores CEs através de roteamento estático, RIPv2, OSPF ou eBGP. Esse modelo de VPN realça a escalabilidade da RFC 2574bis porque elimina a necessidade dos roteadores PEs manterem rotas VPNs com todos os PEs do Provedor de Serviço.

Cada roteador PE mantém uma VRF para cada ponto conectado diretamente. Observa-se que múltiplas interfaces do roteador PE podem ser associadas com uma única VRF se todos os pontos de acesso participam da mesma VPN.

Após aprender as rotas das VPNs locais dos roteadores CEs, um roteador PE troca informação de roteamento com os outros PEs através do BGP (conhecida como iBGP, conforme figura 2.11). Roteadores PEs podem manter sessões IBGP para rotas refletidas (figura 2.11b) como uma alternativa para uma sessão "*full mesh*" (todos conversam com todos).

Quando foi concebido o BGP para as VPN MPLS, foi definido que todos os roteadores PEs de uma rede que utiliza BGP necessita de uma comunicação direta entre si (MP - iBGP), portanto uma combinação de todos os roteadores da rede, dois-a-dois, ou seja, um *full-mesh* de sessões. Para melhorar a escalabilidade e simplificar a configuração, foi criado o papel do *Route Reflector*, onde todos os roteadores estabelecem uma sessão BGP somente com estes elementos da rede. O segundo elemento existe para redundância.

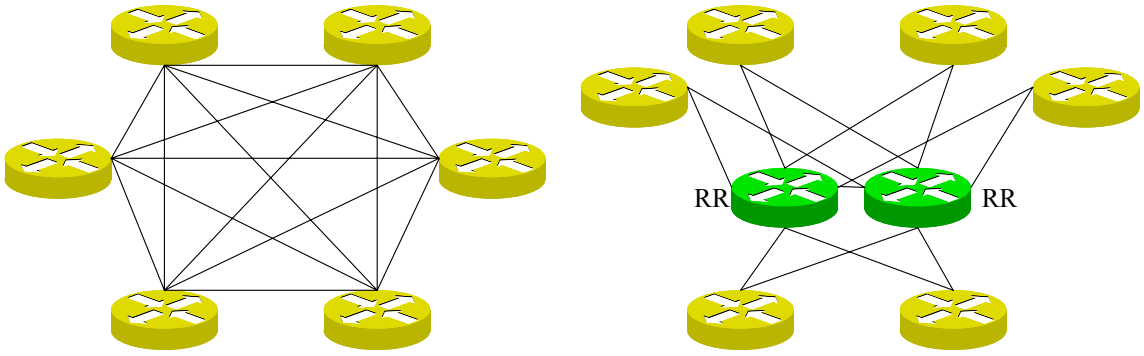

Figura 2.11 – (a) Combinação dos PEs dois a dois. (b) Configuração através de Route Reflector.

Finalmente, quando utiliza-se o MPLS para encaminhar o tráfego de dados das VPNs por meio do backbone do provedor, os roteadores PEs de ingresso e egresso funcionam como LSRs de ingresso e egresso respectivamente. A figura 2.12 apresenta o conjunto de protocolos normalmente disponível nos roteadores PEs para atender as necessidades dos provedores de serviços.

Na figura 2.12, múltiplos protocolos de acesso são suportados para permitir ao provedor do serviço flexibilidade em oferecer aos seus clientes vários métodos de tecnologia de acesso. O PE também suporta um número de protocolos que são específicos para aplicações de B-RAS (Servidor de acesso Banda Larga) que são: IP/PPP/ATM, IP/PPP/Ethernet/ATM, IP/PPP/FR, IP/PPP/Ethernet/FR.

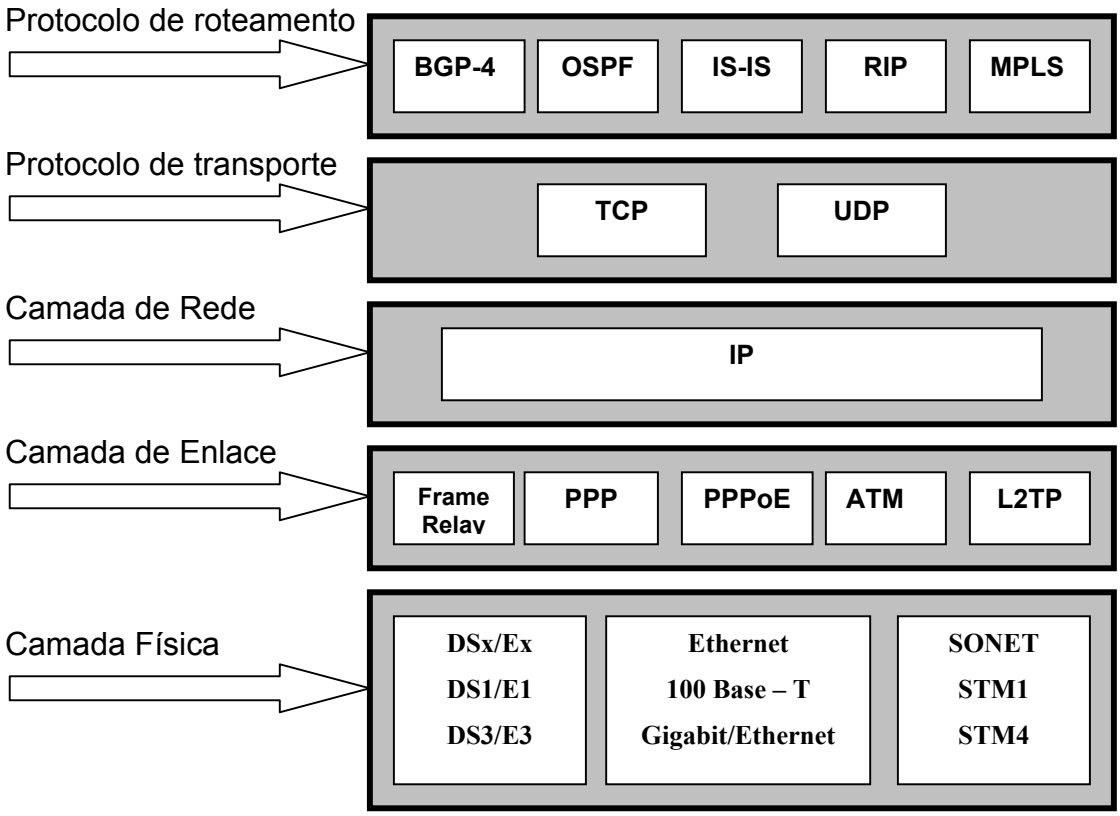

Figura 2.12 – Software normalmente suportado pelos PEs

- Provider Routers (P)

Um *Router Provider(P)* é um roteador na rede do provedor que não troca informação diretamente com o equipamento CE. A função dos roteadores Ps como

transporte MPLS é encaminhar tráfego de dados para os roteadores PEs, desde que o tráfego seja encaminhado por meio do backbone MPLS, usando duas camadas da pilha de rótulo (label stack) [3]. Os roteadores Ps são utilizados para manter rotas para os roteadores PEs; eles não são necessários para manter informação de roteamento específico para cada acesso do cliente.

- Tabela de Roteamento e Encaminhamento (VRF) da VPN

Um conceito chave na arquitetura VPN BGP/MPLS é o elemento chamado de tabela de Encaminhamento e Roteamento dos roteadores PE (figura 2.13). A VRF é uma tabela de encaminhamento e roteamento para cada VPN dentro dos roteadores PEs. Uma VRF privada é acessível unicamente pelas interfaces que fazem parte da VPN correspondente. Todos os pontos conectados no roteador PE devem fazer parte de uma VRF. Todas as informações das VPNs são refletidas na VRF e os pacotes que viajam através daquele ponto serão roteados e encaminhados com base unicamente na informação encontrada na VRF correspondente. O processo de como uma rota é incluída na VRF será explicada na sessão "Distribuição de Rotas".

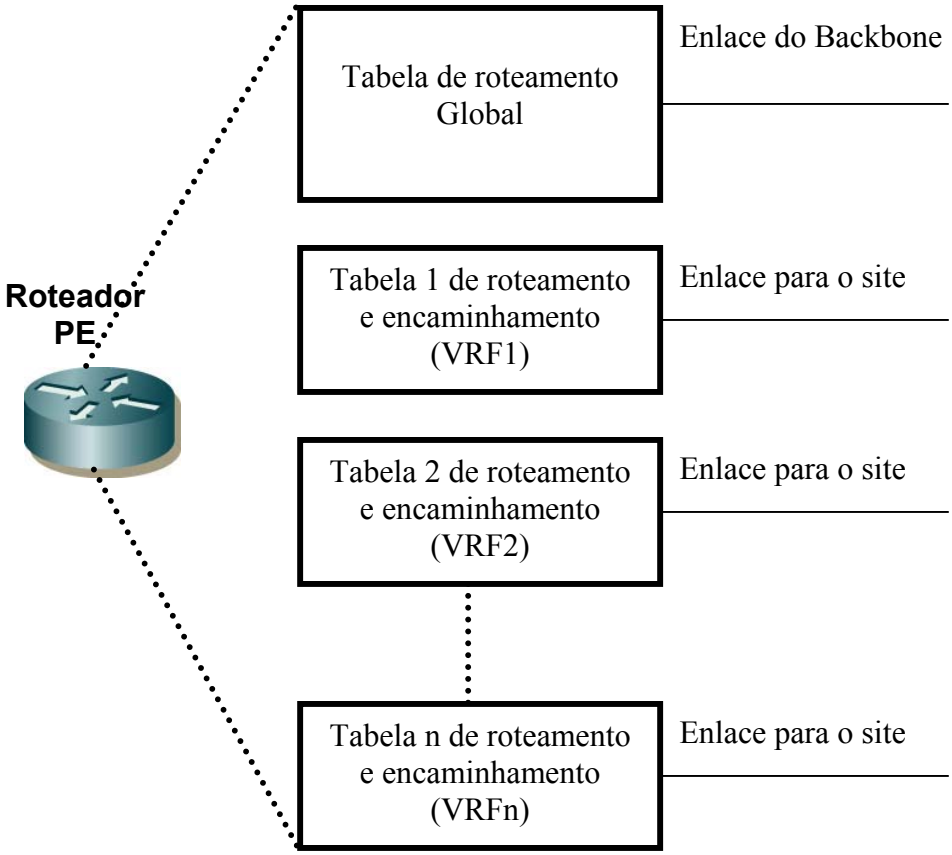

Figura 2.13 - Criação de VRF

2.4.2.2 - Modelo Operacional

Dois fluxos fundamentais de tráfego ocorrem em uma VPN BGP MPLS:

- Um fluxo de controle que é usado para distribuição de rotas VPN e estabelecimento de LSPs (Label Switched Paths);
- Um fluxo de dados que é usado para os usuários encaminharem seu tráfego de dados.

Topologia de Rede Simples

A figura 2.14 mostra uma topologia de rede simples, em que um provedor de serviço entrega um serviço de VPN BGP MPLS para diferentes empresas. Nessa rede há dois roteadores PEs conectados com quatro diferentes redes de clientes.

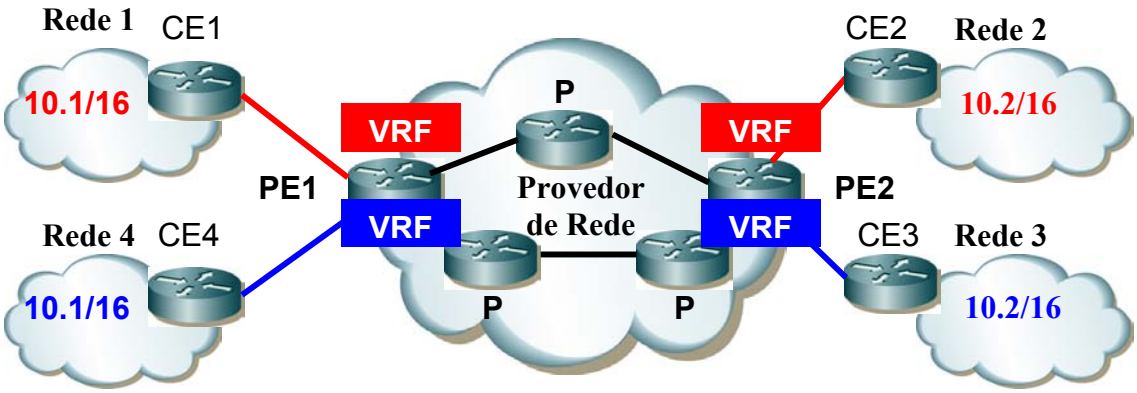

Figura 2.14 - Componente de Rede

A conectividade entre as redes dos usuários pode ser descrita pelas seguintes regras:

- Um computador na rede 1 pode enviar tráfego para um computador na rede 2 e vice-versa;
- Um computador na rede 3 pode enviar tráfego para um computador na rede 4 e vice-versa.

Fluxo de Controle

Em uma VPN BGP/MPLS, o fluxo de controle consiste de dois subfluxos:

- O primeiro subfluxo de controle é responsável para a troca de informação de roteamento entre os roteadores CE e PE no backbone do provedor e entre os roteadores PEs;
- O segundo subfluxo de controle é responsável pelo estabelecimento dos LSPs entre os roteadores PEs do provedor de serviço.

a) Troca de Informação de roteamento

Nesse exemplo, PE1 é configurado para associar a VRF vermelha com a interface ou subinterface sobre as rotas aprendidas do CE1. Quando CE1 anuncia a rota do prefixo 10.1/16 para PE1, esta última habilita uma rota local para 10.1/16 na VRF Vermelha.

PE1 anuncia a rota 10.1/16 para PE 2, usando IBGP. Antes de anunciar a rota, PE1 seleciona um rótulo (por exemplo, 222) para anunciar com a rota e designar o endereço de *loopback*[12] como o próximo salto do BGP.

A RFC 2547bis suporta espaço de endereçamento overlapping (Endereço privado definido na RFC 1918) pelo uso de rotas distinguidas (RD – Ver capítulo 4, passo 5) e a família de endereço de VPN-IP4. A RFC 2547bis constrói a distribuição de informação de roteamento também nos roteadores PEs pelo uso de rotas baseadas em filtros dos atributos estendidos do BGP (rotas *targets*).

Quando o PE2 recebe as rotas do PE1, determina se deverá instalar a rota para o prefixo 10.1/16 dentro da VRF vermelha através dos filtros baseados nos atributos estendidos do BGP. Se PE2 decide instalar as rotas na VRF vermelha, então ele anuncia a rota pelo prefixo 10.1/16 para o CE 2.

b) Estabelecimento do LSP

[12] Loopback – Cada roteador PE necessita de um endereço único (Usualmente chamado de loopback) que é utilizado para alocar um rótulo e habilitar o encaminhamento dos pacotes da VPN através do backbone.

Os roteadores PEs estabelecem sessões MP-BGP entre os roteadores de bordas PEs para trocar rotas de clientes. O tráfego da rede do provedor passa através do LSP (*Label Switched Path* – Caminho Comutado de Rótulo) pré-estabelecido através dos protocolos de sinalização LDP ou RSVP-TE. O roteador PE adiciona dois rótulos como prefixos para cada pacote do tráfego IP do cliente. O "rótulo mais externo" identifica o próximo "salto" ao longo do LSP do provedor de rede, enquanto o "rótulo mais interno" identifica a VPN particular do cliente, conectada no roteador de destino. A informação do rótulo é trocada durante a sessão de configuração MP-BGP.

Uma limitação do uso convencional do BGP4 para o suporte às VPNs BGP/MPLS é que ele foi originalmente designado para transportar informação somente da família de endereçamento IPv4. Em função dessa limitação, o IETF está trabalhando para padronizar o *Multiprotocol Extensions for BGP4* – Extensão do Multiprotocolo BGP4. Essa extensão foi originalmente definida na RFC 2283 e mais tarde atualizada na RFC 2858. A extensão permite ao BGP4 transportar informação de roteamento de múltiplos protocolos (IPv6, IPX, VPN-IPv4,etc.) da camada de rede entre os PEs da VPN BGP/MPLS. As VPNs BGP/MPLS permitem a troca de informação de roteamente da família de endereços VPN-IPv4 entre os PEs do backbone da rede, sendo conhecido como MP-BGP. A referência [8] aborda com mais detalhes esse tema.

Para usar o MPLS para o encaminhamento do tráfego da VPN por meio do backbone do provedor, Um LSPs deve ser estabelecido entre o roteador PE que aprende a rota e o roteador PE que anuncia a rota. A figura 2.15 ilustra esse conceito.

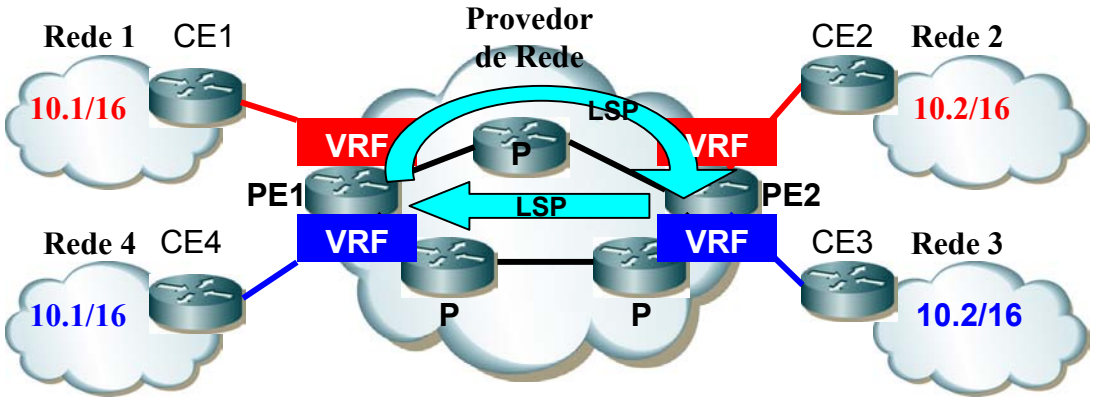

Figura 2.15 – Estabelecimento do LSP

LSPs podem ser estabelecidos através das redes dos provedores de serviço, usando Protocolo de Distribuição de Rótulo (LDP) ou Protocolo de Reserva de Recursos (RSVP).

- O provedor usa LDP se deseja estabelecer um LSP de melhor esforço entre dois roteadores PEs.
- O provedor usa RSVP se deseja desempenho por largura de banda no LSP, ou usar engenharia de tráfego para selecionar um caminho explícito para o LSP. Suporte de LSP baseado em RSVP permite definição a uma qualidade de serviço específica.

Para garantir interoperabilidade, todos os roteadores PE e P devem estar preparados para suportar, no mínimo, LDP.

- Se o provedor definiu usar LDP, uma topologia em malha completa (*full-mesh*) de LSPs melhor esforço (*best effort*) é estabelecida por meio do *backbone* para suportar conectividade PE-PE.
- Se o provedor definiu usar RSVP, LSPs baseados em RSVP têm maior prioridade que os baseados em LDP. LSPs baseados em LDP ou RSVP devem existir entre um par de roteadores PE.

Fluxo de Dados

A figura 2.16 apresenta o fluxo de dados da VPN através do backbone do provedor de serviço de um ponto de presença do usuário para um outro. Assume-se que o computador 10.2.3.4 na rede 2 deseja comunicar-se com o servidor 10.1.3.8 na rede 1.

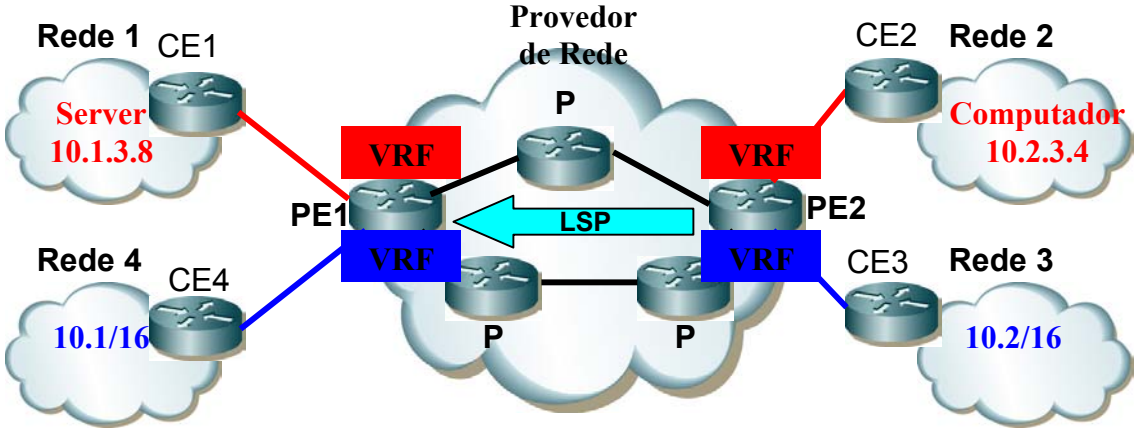

Figura 2.16 – Fluxo de Dados

O computador 10.2.3.4 encaminha todos os pacotes de dados para o servidor 10.1.3.8 (*gateway default*). Quando chegam os pacotes no CE2, este realiza uma longa procura de rotas e encaminha os pacotes IPv4 para o PE2. PE2 recebe os pacotes e realiza uma procura de rota na VRF Vermelha, obtendo a informação de encaminhamento:

- O rótulo do MPLS anunciado pelo PE1 com as rotas (rótulo=222);
- O next hop (próximo salto) BGP para a rota (O endereço de loopback do PE1);
- Subinterface de saída para o LSP de PE2 para PE1;
- O rótulo inicial MPLS para o LSP de PE2 para PE1;

Conforme comentado anteriormente, o tráfego dos usuários são encaminhado de PE2 para PE1, usando MPLS, com a pilha de rótulo (label stack) contendo dois rótulos. Para esse fluxo de dados, PE2 é o LSR de ingresso para o LSP e PE1 é o LSR de egresso para o mesmo LSP. Antes de transmitir o pacote, o PE2 coloca o rótulo 222 dentro da pilha, marcando como último rótulo. Como visto, este rótulo é originalmente instalado na VRF vermelha quando PE2 recebe, via IBGP anúncios do PE1 para a rota 10.1/16. O PE2 coloca o rótulo associado ao LSP para o PE1 dentro da pilha marcando no rótulo mais externo (*top label*).

Depois de criada a pilha de rótulo (label stack), PE2 encaminha o pacote MPLS através da interface no primeiro roteador P ao longo do PE2 para PE1. Os roteadores Ps comutam pacotes por meio do núcleo da rede do backbone do provedor de serviço baseado no rótulo mais externo da pilha. No penúltimo roteador com relação a PE1, o rótulo mais externo da pilha (top label) é retirado e o pacote encaminhado para o PE1.

Quando o PE1 recebe o pacote, ele retira o rótulo criando o pacote nativo IPv4. PE1 usa o último rótulo (222) para identificar o CE correspondente ao próximo pulo para 10.1/16. Finalmente, o PE1 encaminha o pacote IPv4 nativo para CE1 que encaminha os pacotes para o servidor 10.1.3.8 na rede 1.

2.5 – Implementação de DiffServ em VPN MPLS

Entre as alternativas disponíveis para oferecer qualidade de serviço às VPNs MPLS, temos atualmente duas arquiteturas em uso:

- **Serviços Integrados – IntServ [15]**
- **Serviços Diferenciados - DiffServ [18]**

A arquitetura *IntServ* apresenta problemas de escalabilidade, limitando-se a redes de pequeno a médio porte. DiffServ, por outro lado, provou ser bastante escalável pois a maior parte do trabalho é feita na borda e, consequentemente, não precisa manter qualquer estado de microfluxo no núcleo como no caso da arquitetura IntServ.

A característica aleatória da chegada de fluxos em diferentes classes de serviço obriga a utilização de alguma técnica para fornecimento da QoS. As principais técnicas são: provisionamento em excesso dos recursos e provisionamento dinâmico. A grande vantagem do provisionamento em excesso é a facilidade de implantação, pois aproveita a infra-estrutura existente, apenas aumentando a taxa de transmissão ou a capacidade de armazenamento nos dispositivos de comutação. A característica dessa técnica é que normalmente não há classes de serviços diferentes e todos os fluxos desfrutam do mesmo recurso e QoS. A principal desvantagem é que manter um canal de comunicação com capacidade acima da demanda produz um aumento de custo, induzindo maiores tarifas na prestação do serviço.

O aprovisionamento dinâmico consiste em utilizar canais de comunicação compatíveis com a demanda e executar mecanismos de reconfiguração que ofereçam a QoS desejada para determinados fluxos. A grande vantagem é que há um aproveitamento maior da capacidade da rede através do oferecimento de um serviço de melhor qualidade mantendo a infra-estrutura dimensionada de acordo com a demanda. Assim, é possível dizer que o aprovisionamento dinâmico pode oferecer QoS com um custo menor. A desvantagem desse mecanismo é que exige alteração nos equipamentos de rede, além de introduzir uma complexidade adicional.

Em virtude da complexidade dos mecanismos de aprovisionamento dinâmico e principalmente em função do excesso de banda em seus backbone, a maioria das operadoras tem preferido superdimensionar os recursos para obter a QoS desejada. Esse procedimento, no entanto, apresenta um custo muito alto, tanto pela capacidade não utilizada na maior parte do tempo (deve-se aprovisionar pelo pico) como pela necessidade

de planejar o crescimento, já que construir infra-estrutura de telecomunicações exige uma estimativa de tráfego futuro, que tende a ser imprecisa.

Com o advento das redes de acesso banda larga xDSL, os backbones das operadoras estão encontrando dificuldades para manter os níveis de serviços para seus clientes usando apenas superprovisionamento. Também a necessidade de oferecer serviços com menor custo e preços mais competitivos estão levando as operadoras a implementarem aprovisionamento dinâmico. O superprovisionamento se mostrou um modelo adequado no período de monopólio do Setor de Telecomunicações.

A utilização de mecanismos de aprovisionamento dinâmico não são suficientes para garantir a qualidade de serviço em toda a VPN. É necessário executar o controle de aprovisionamento, bem como um gerenciamento sobre todo o domínio da VPN, isto é, em todo o conjunto de equipamentos da operadora e do cliente (CE a CE).

A diferenciação de Serviços (*DiffServ*) é uma proposta de arquitetura para oferecer recursos de QoS sem o problema da escalabilidade. Nesse caso, os fluxos são agregados em classes de serviço com um padrão de QoS específico. Com uma quantidade de classes limitada, a necessidade de recursos computacionais nos roteadores é reduzida pela menor quantidade de estados a tratar.

Nos backbones onde a operadora deseja disponibilizar soluções de VPN BGP/MPLS com classes diferentes de serviço para os seus clientes recomenda-se a utilização de aprovisionamento dinâmico com DiffServ. No capítulo 5 são realizados testes do serviço VPN com QoS baseados na arquitetura DiffServ.

A identificação da classe de serviço (no modelo sugerido serão seis) é feita pela marcação no campo DS – Serviços Diferencial, antigo campo TOS (Tipo de Serviço) no cabeçalho IP. O campo DS contém um valor chamado *codepoint* que é associado a cada classe de serviço. O tratamento que uma determinada classe recebe depende de um conjunto de regras aplicadas a essa agregação, que inclui formas de classificação, escalonamento e tratamento de fila. Esse conjunto de regras é chamado PHB – *Per Hop Behavior*, isto é, comportamento por nó. Um operador de rede que oferece serviço DiffServ tem um contrato de serviço SLA com o usuário e deve cumprir parâmetros de QoS para o tráfego do usuário que cruza a VPN, isto é, parâmetros como retardo, variação do retardo (*jitter*) e descarte.

2.5.1 - Arquitetura DiffServ

Para evitar o problema de escalabilidade da arquitetura IntServ, na qual os roteadores de núcleo não conseguem tratar uma grande quantidade de fluxos, a arquitetura DiffServ foi dividida em dois tipos de roteadores de acordo com a sua posição no domínio: de núcleo ou de borda. Os roteadores de borda ficam na fronteira do domínio e têm a função de fazer a comunicação com roteadores de outras operadoras de backbone ou clientes. Os roteadores de núcleos encontram-se todos no núcleo da rede, sem contato com outros backbones de operadoras ou clientes, e onde o tráfego e a quantidade de fluxos são maiores devido à agregação dos tráfegos originários de vários roteadores de borda. A figura 2.17 mostra esquematicamente a arquitetura de um domínio DiffServ.

Na arquitetura DiffServ, os roteadores de borda realizam toda a complexidade de classificação, marcação, suavização e policiamento. Como esses roteadores tratam uma quantidade menor de fluxos, essas funções, computacionalmente intensas, poderão ser realizadas sem prejuízo da escalabilidade.

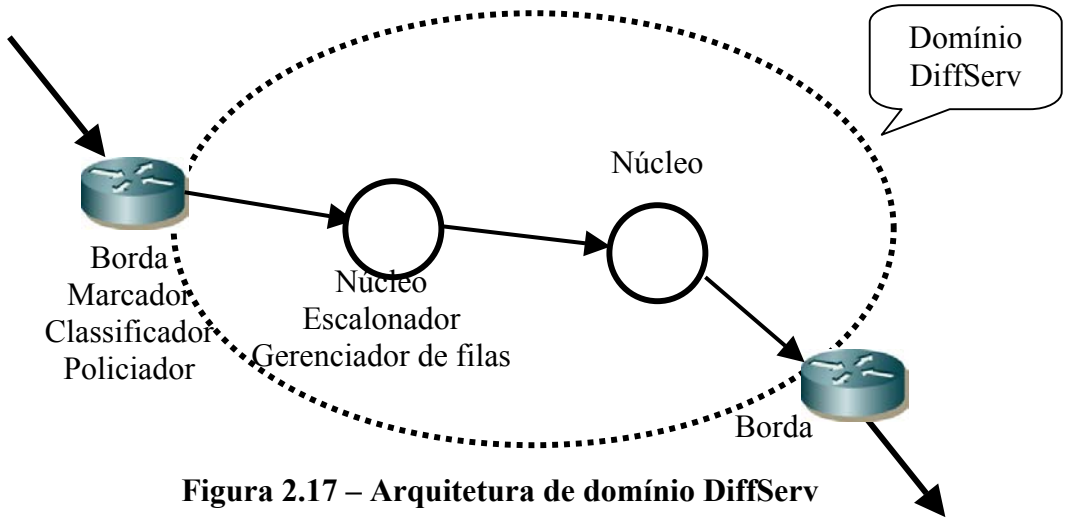

Figura 2.17 – Arquitetura de domínio DiffServ

Os roteadores de núcleo realizam apenas as funções de classificação, escalonamento e gerenciamento de filas. Como o problema de escalabilidade é crítico nos roteadores de núcleo devido a quantidade de fluxos e a demanda de processamento, esses roteadores apenas tratam individualmente cada PHB.

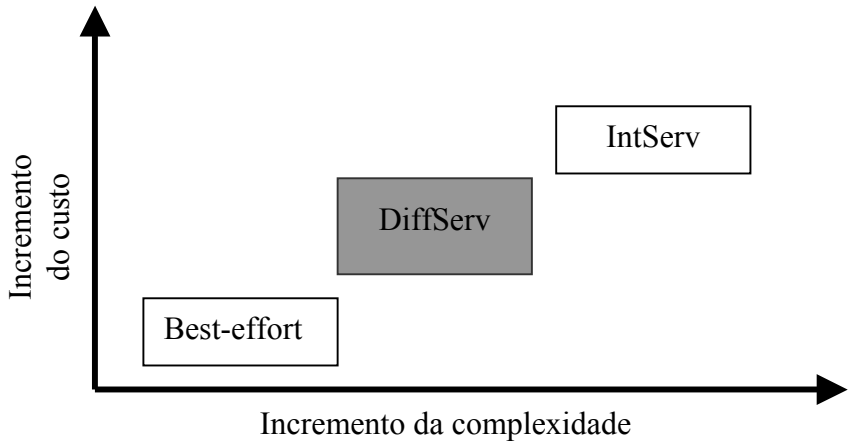

Figura 2.18 – Custo e complexidade de Soluções de Serviços Diferenciados

2.5.2 - PHBs DiffServ

Os dois principais PHBs padronizados são: Encaminhamento Expresso (EF) e Encaminhamento Assegurado (AF). Os tráfegos não classificados nessas classes são chamados de melhor esforço (BE), isto é, tráfego sem nenhuma garantia de QoS.

- **Encaminhamento Expresso (EF)**

O serviço denominado de Encaminhamento Expresso (EF), definido na RFC 2598, permite a adaptação do modelo de serviço garantido da arquitetura IntServ à arquitetura de serviços diferenciados. Ele oferece garantias de QoS elevadas , com baixos valores de perda, atraso e jitter, fornecendo o equivalente a uma linha privada virtual, com largura de banda fixa entre dois computadores. É indicado para aplicações de telefonia sobre IP, videoconferência e para a criação de linhas dedicadas em redes privadas virtuais (VPNs). Sua vantagem sobre o serviço equivalente na arquitetura IntServ está na simplicidade de implementação, pois não é necessário manter nos roteadores nenhuma informação relativa a fluxos. Geralmente, não deve ser usado RED como o mecanismo de gerenciamento da fila, quando suportando o PHB EF, porque a maioria do tráfego é baseada em UDP, e UDP não responde à diminuição dos pacotes pela redução da taxa de transmissão.

- **Encaminhamento Garantido (AF)**

A classe de serviço Encaminhamento Garantido (Assured Forwarding —AF), definida na RFC 2597, destina-se às aplicações que demandam da rede um serviço mais

confiável que aquele de melhor esforço, mas sem todas as garantias de QoS oferecidas pelo encaminhamento expresso. Este serviço não oferece limites superiores para o atraso e jitter, mas garante um tratamento preferencial ao tráfego que dele se utilize. Ele é indicado quando se deseja obter da rede um serviço de entrega de pacotes mais consistentes, a fim de oferecer, por exemplo, uma melhor QoS a agregados de tráfego, consistindo de rajadas de curta duração com destinos diferentes (o tráfego na Web) [51].

O princípio aqui é a divisão do tráfego em N classes, cada uma com algum nível de precedência de descarte (M). A especificação atual define N = 4 e M = 3 (Figura 2.19), embora, em uma situação real, nem todas sejam necessárias. O serviço fornecido por uma certa classe independe do serviço das demais classes, sendo função apenas dos recursos alocados para cada classe pelo sistema [35].

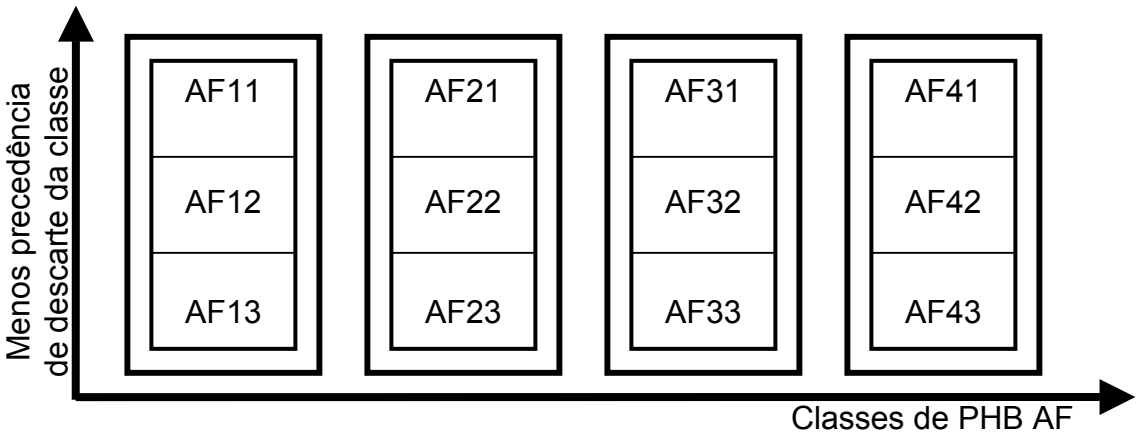

Figura 2.19 - Classes AF

Um usuário pode contratar de um provedor um dos quatro serviços de encaminhamento diferenciado, cada um com três níveis de prioridade de descarte. Em situações de sobrecarga, o tráfego de uma classe superior tem menor probabilidade de sofrer congestionamento que o tráfego de uma classe inferior. O mecanismo de diferenciação aqui utilizado se baseia na prioridade de descarte: quando este for inevitável, primeiro se descartam os pacotes pertencentes ao serviço de melhor esforço e, só então, passa-se para os pacotes associados ao serviço de encaminhamento garantido, segundo sua classe e nível de precedência. Portanto, os pacotes pertencentes ao serviço AF são os últimos a serem descartados em situações de congestionamento.

A tabela 2.1 apresenta os DSCPs recomendados para os quatros grupos AF PHB.

	Classe AF1	Classe AF2	Classe AF3	Classe AF4
Precedência Baixa	0001010	010010	011010	100010
Precedência Média	001100	010100	011100	100100
Precedência Alta	001110	010110	011110	100110

Tabela 2.1 – Recomendação dos valores DSCP AF.

2.5.3 - DiffServ e pacotes MPLS

A combinação de DiffServ e MPLS apresenta uma estratégia muito atrativa para os provedores de serviços oferecerem serviços de VPN MPLS com Qualidade de Serviço (QoS).

Algo que pode ser observado é que existem 6 bits DSCP e somente 3 bits EXP. Como existem apenas oito valores EXP e 64 valores DSCP (dos quais 21 estão definidos atualmente), como oferecer, então, serviços DSCP no MPLS ?.

Em uma rede no modo *frame*[13] (quadro) é possível até três bits EXP; é necessário mapear várias classes DSCP para esses bits EXP. Contudo, na prática, isso não provou ser um problema em redes de produção, pois praticamente nenhuma instalação de Qualidade de Serviço (QoS) oferece serviços que não possam ser providos com os 3 bits EXP MPLS. Está sendo realizado um trabalho no sentido de definir uma outra solução denominada de L-LSP, mas não será abordado neste trabalho. A RFC 3270 [23] trata desse tema.

2.6 - Benefícios das VPNs BGP/MPLS

O maior objetivo das VPNs BGP/MPLS é simplificar a operação da rede para os usuários, enquanto permite ao provedor de serviço oferecer escalabilidade e serviços de

[13] Mode Frame é o termo usado quando é encaminhado um pacote com um rótulo inserido ao pacote, na frente do cabeçalho da camada 3 (o cabeçalho IP, por exemplo).

valor adicionado. As VPNs BGP/MPLS têm muitos benefícios. Serão destacados, aqui, os principais:

- Não há restrição do plano de endereços utilizados em cada VPN do usuário. O usuário pode usar outros endereços, globais ou privados. Na perspectiva do provedor do serviço, clientes diferentes podem ter endereços sobrepostos (*Overlapping*).
- Os roteadores CEs de cada ponto de presença do usuário não trocam informação de roteamento diretamente com outros roteadores CEs. Os usuários não têm de se preocupar com questões de roteamento entre redes porque estas são de responsabilidade do provedor de serviço.
- Usuários não precisam administrar o backbone virtual e nem gerenciar acessos para os roteadores PE ou P.
- Provedor de Serviço não tem um backbone separado ou virtual para administrar cada VPN do usuário.
- Segurança equivalente ao Frame Relay e ATM
- Provedor de Serviço pode utilizar uma infra-estrutura comum para entregar serviços de conectividade Internet e VPN
- Flexibilidade e Escalabilidade para serviços de QoS são suportadas por meio do uso do EXP no *shim header* (cabeçalho MPLS) do MPLS ou pelo uso de engenharia de tráfego.

2.7 – Comparando as diversas tecnologias de VPNs

	ATM/Frame Relay	**GRE**	**IPSEC**	**L2TP**	**MPLS**
Topologia	Estrela e *Full Mesh*	Estrela e *Full Mesh*	Estrela e *Full Mesh*	Estrela	Estrela e *Full Mesh*
Escalabilidade - Configuração e gerenciamento	Limitada em configuração *full mesh*	Limitada em configuração *full mesh*	Limitada em configuração *full mesh*	Não existem limitações na topologia Estrela	Nenhum limite
Segurança	Alta segurança	Nenhuma segurança, poderá ser combinado com IPsec	Alta Segurança	Usa algoritmo de autenticação; pode ser combinado com IPSec para tráfego com criptografia	Altamente segura, similar a ATM e Frame Relay, pode ser combinado com IPSec
Estático e Dinâmico	PVC e SVC	Estático	Estático	Dinâmico	Estático e Dinâmico
QoS	ATM Fórum através de classes de serviços (CBR, ABR, VBR, UBR); Frame Relay usa CIR	QoS IP	QoS IP	QoS IP	MPLS EXP
Dependência da tecnologia de acesso	Limitada em Frame Relay e ATM	Não limitada	Não limitada	Depende de uma tecnologia de acesso PPP	Não limitada

Tabela 2.2 – Quadro Comparativo das VPNs

2.8 - Resumo de Capítulo

Este capítulo apresentou os conceitos básicos da arquitetura VPN BGP/MPLS e DiffServ, que são os assuntos base dessa dissertação. Inicialmente foram apresentados os conceitos de VPNs, modelo overlay e peer. Em seguida, foram apresentadas as características, vantagens e limitações de cada modelo para a partir daí apresentar a RFC

2547 (VPN BGP/MPLS). Ainda neste capítulo, foram apresentadas algumas formas de implementação da RFC 2547. Finalmente, DiffServ foi apresentado para permitir a integração com as VPNs BGP/MPLS e dessa forma ser possível oferecer para o usuário qualidade de serviço. O próximo capítulo tratará de uma estratégia de projeto de VPN que irá integrar VPN BGP/MPLS com DiffServ.

Capítulo 3

Estratégia de implementação proposta

Neste capítulo é apresentada uma estratrégia para construir VPN MPLS para aprovisionamento de recursos de rede em um domínio IP. A estratégia tem como ponto de partida a especificação das classes de serviços para uma determinada aplicação. A estratégia é formada de 7 passos principais.

Antes de ser apresentada a estratégia, será mostrado um quadro resumo das principais limitações de IP sobre ATM (IPoATM) encontradas normalmente em um ambiente do provedor que oferece serviço baseado em infra-estrutura de IPoATM. A razão da apresentação dessa discussão no contexto desse trabalho é porque grande parte dos backbones (Telemar, Telefônica, Embratel e Brasiltelecom) dos provedores de VPN atualmente trabalham com a tecnologia IPoATM. Para a formação de VPN MPLS é necessário que o provedor faça uma migração para MPLS. A tabela 3.1 a seguir faz uma comparação entre as principais diferenças entre as opções disponíveis. São apresentadas duas opções que devem ser avaliadas em uma migração de IPoATM para MPLS: MPLS baseado em Célula e MPLS baseado em Roteador. O anexo B apresenta informações relacionadas a esse tema.

3.1 – Comparação entre IPoATM, MPLS baseado em Célula e MPLS baseado em Roteador

- MPLS baseado em Célula refere-se ao conjunto de procedimento que define como um comutador ATM pode funcionar como um LSR[14] e comutar células, baseado no conteúdo dos campos VPI ou VPI/VCI das células.

- MPLS baseado em Roteador refere-se ao conjunto de procedimentos que definem como um roteador IP pode funcionar como um LSR, comutando pacotes baseado no rótulo mais externo transportado no *shim header* (cabeçalho MPLS) do pacote.

	IP over ATM	MPLS baseado em célula	MPLS baseado em Roteador
Um plano de controle simples de gerência	**Não**	**Sim**	**Sim**
Um único tipo de equipamento para gerência.	**Não**	**Não**	**Sim**
Eliminação do overhead Célula da ATM	**Não**	**Não**	**Sim**
Suporte nativo para IP DiffServ CoS	**Não**	**Não**	**Sim**
Eliminação do IGP	**Não**	**Sim**	**Sim**

Tabela 3.1 – Comparação: IPoATM, MPLS baseado em célula e roteador

[14] Um Label-Switching Router (LSR) é um equipamento que implementa na rede MPLS os planos de controle e encaminhamento

3.1.1 - Questões de transição

Para a definição de qual é a melhor opção de transição é necessário avaliar os benefícios de cada uma das arquiteturas.

Em termos de custos, uma transição direta para MPLS baseado em roteador é mais cara que uma transição para MPLS baseada em célula, porque será necessário comprar novos LSRs baseados em *frames*. Entretanto, após completar essa transição, a rede irá imediatamente receber os benefícios de desempenho e escalabilidade, não precisando passar por uma nova transição.

Uma transição inicial de IP sobre ATM para comutação de célula MPLS tem menor investimento que uma transição para MPLS baseado em roteador, porque é possível fazer uma atualização de software e adicionar um módulo de roteamento nos comutadores ATM. O desafio dessa proposta é que em algum momento, eventualmente, será necessário fazer uma segunda transição de MPLS baseado em célula para MPLS baseado em roteador quando a limitação de desempenho e escalabilidade de uma estrutura ATM impactar a operação da rede. A combinação do custo de duas transições será significantemente maior do que se for feita uma transição direta de IP sobre ATM para MPLS baseado em roteador.

Para a estratégia apresentada será considerado um backbone de MPLS baseado em roteador para formação de VPN MPLS. Os passos que fazem parte da estratégia para a construção de VPN baseada em MPLS são:

Passo 1 - Especificação dos requisitos da aplicação

- Classificação dos principais aplicativos e seus parâmetros.

Passo 2 - Mapeamento e Divisão dos aplicativos em múltiplas Classes de Serviços

- Dados (Best Effort)[15] – Classe 0
- Dados de Missão Crítica – AF4 – Classe 1
- Dados de Gerenciamento – AF3 – Classe 2
- Dados de Suporte a Negócio – AF2 – Classe 3
- Dados Não Críticos – AF1 – Classe 4
- Voz (EF) – Classe 5

[15] Essa classe de serviço, mesmo sendo Best Effort, trabalha sobre um backbone IP privativo e não Internet

Passo 3 - Seleção da Tecnologia de acesso

- Frame Relay
- ATM
- DSL
- Linha Dedicada

Passo 4 - Seleção do Tipo do CPE/CE

- Com QoS
- Sem QoS

Passo 5 - Configuração da VPN IP MPLS

- Definir as configurações dos Roteadores Virtuais (VRF).
- Definir e configurar o Identificador de rotas[17] (Identificador da VPN do usuário)
- Definir e configurar as políticas de importação e exportação de rotas (RT)
- Configurar o enlace PE-CE
- Associar a interface CE previamente definida nas VRF's
- Configurar o Multiprotocolo BGP.

Passo 6 - Teste de Conectividade e Isolamento da VPN

Passo 7 - Teste de QoS e CoS da VPN

O passo 1 tem o objetivo de identificar os principais aplicativos encontrados atualmente no ambiente das organizações e seus requisitos. O passo 2 sugere o mapeamento dos aplicativos em 6 classes de acordo com o padrão DiffServ. O passo 3 apresenta uma novidade em relação as VPNs tradicionais que é a implementação de VPN com acesso xDSL. O passo 4 avalia os requisitos dos parâmetros mais importante dos CE/CPE em função das classes de serviços.Esse passo apresenta uma novidade em relação aos CEs tradicionais, que é a nova implementação nos roteadores cisco de VRFs no próprio CE conhecida como "Multi – VRF". O passo 5 trata da configuração da VPN. Esta configuração de VPN é uma das partes mais importante do projeto de VPN MPLS, pois qualquer erro de configuração pode refletir em um usuário de uma determinada VPN ter acesso indevido a outra VPN. Em função da importância do passo anterior é sugerido o teste de conectividade e isolamento da VPN no passo 6. O passo 7 tem o objetivo de avaliar

[17] O termo identificador de rotas (RD) equivale nesse texto a rotas distinguishers ou identificador da VPN

se a VPN está priorizando os pacotes e oferecendo os níveis de serviço de acordo com a classificação realizada no passo 2. Para isso será utilizado um software de domínio público conhecido como *iperf* e um ambiente montado para avaliação de desempenho

A figura 3.1 apresenta o fluxo da estratégia[18] proposta para a formação de VPNs IP MPLS.

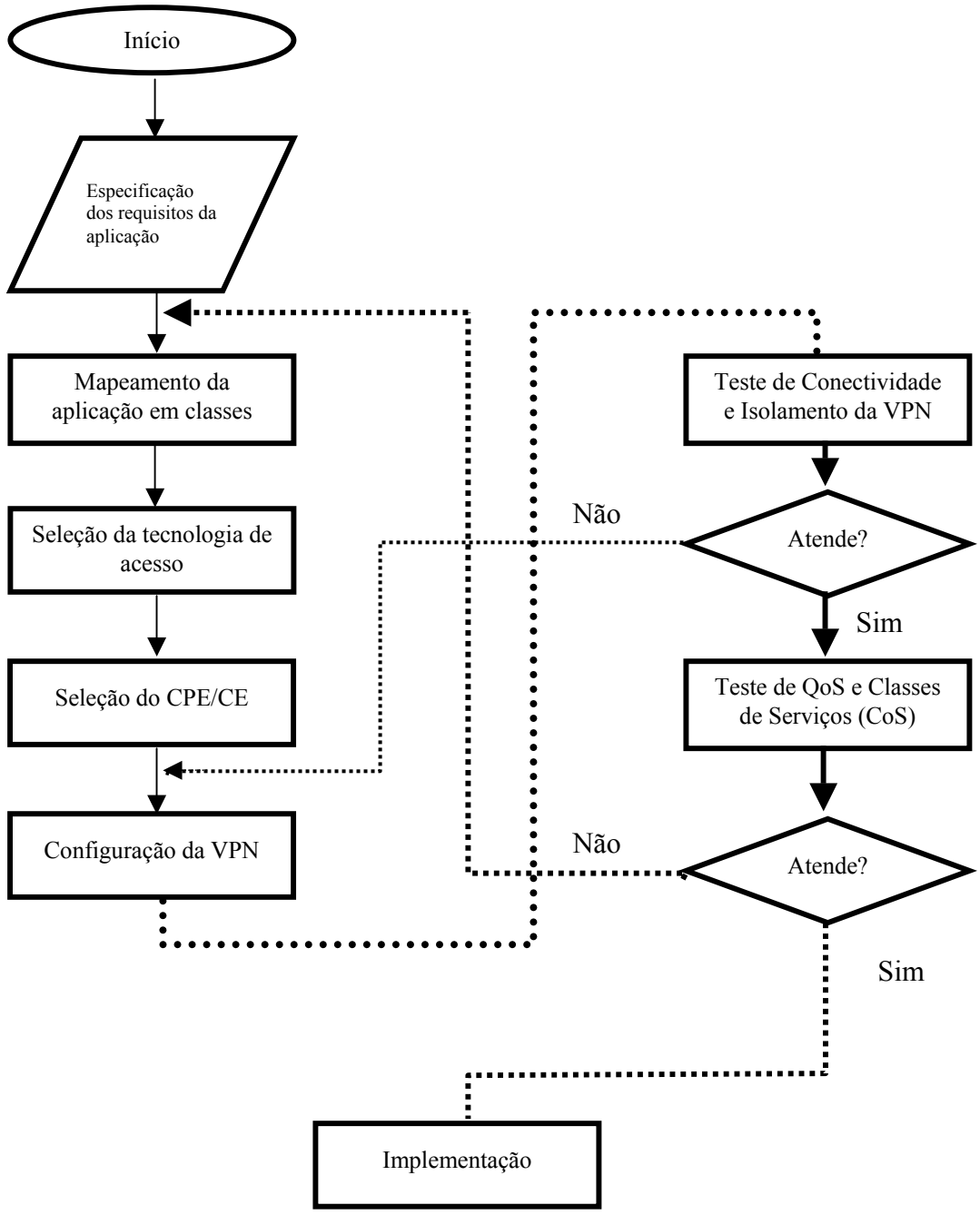

Figura 3.1 – Fluxo de Formação de VPNs MPLS

[18] Essa estratégia é conseqüência de vários projetos e de acordo com as RFCs

As VPNs tradicionais têm se preocupado em fornecer, basicamente, conectividade entre os pontos de presença dos usuários usando as tecnologias de acessos tradicionais. Uma das contribuições deste trabalho é oferecer uma estratégia de projeto de VPN BGP/MPLS que contemple Qualidade de Serviço (QoS) e Classes de Serviços (CoS) de CE a CE, utilizando várias tecnologias de acesso, principalmente xDSL[19].

3.2 - PASSOS

Aqui serão apresentados os 7 passos que fazem parte da estratégia da formação de VPN BGP/MPLS.

3.2.1 – PASSO 1 – Especificação dos Requisitos dos Aplicativos

Para determinar a que classe de serviço (CoS) que os aplicativos devem ser classificados é necessário determinar seus requisitos para depois realizar a associação com uma das 6 classes que fazem parte da proposta apresentada.

Os aplicativos serão identificados pelas suas respectivas portas UDP/TCP. Alguns aplicativos como FTP (21) e WWW (80) já possuem suas portas padronizadas.

3.2.1.1 – Caracterização dos fluxos de tráfego

Um fluxo de rede pode ser caracterizado por sua direção e sua simetria. A direção especifica se os dados viajam em ambas as direções ou apenas em uma direção. A direção também especifica o caminho percorrido por um fluxo em sua viagem, da origem até o destino, por uma inter rede. Muitos aplicativos de rede têm requisitos diferentes em cada direção. Algumas tecnologias novas de transmissão, como a ADSL, tiram proveito de requisitos assimétricos.

A seguir serão definidos os principais aplicativos que normalmente são encontrados no ambiente do usuário para posterior classificação de acordo com o modelo de 6 classes apresentado.

- **VoIP**

[19] A tecnologia de acesso xDSL permite oferecer VPN MPLS com baixo preço para o mercado.

Voz sobre IP (Protocolo Internet) é a convergência da tradicional rede de voz e a rede de dados. A implementação de VoIP em uma VPN MPLS requer atenção com alguns parâmetros: disponibilidade de banda, perda de pacotes, atraso e jitter (variação do atraso).

- **Videoconferência**

Videoconferência é a transmissão de áudio e vídeo entre dois ou mais pontos, em ambas as direções e em tempo real, permitindo interatividade entre os participantes. Ela permite ainda o compartilhamento de dados (textos, planilhas, gráficos, etc) junto com a transmissão de áudio e vídeo.

- **Emulação de Terminal**

O tráfego de Emulação de Terminal é usualmente assimétrico. O terminal envia alguns caracteres e o host envia muitos caracteres. O Telnet é um exemplo de aplicativo de emulação de terminal que gera tráfego terminal/Host.

- **Servidor de Nome e Domínio**

Este é o protocolo que torna possível que qualquer computador encontre qualquer outro na Internet. O fluxo do tráfego DNS segue o modelo cliente servidor.

- **Gerenciamento da rede e sistema**

Pode existir caso em que o usuário da VPN deseja que seu tráfego de gerência seja tratado de forma diferente em relação a outros tráfegos. O perfil de tráfego do gerenciamento da rede e sitema seguem o modelo dos protocolos ICMP, SNMP e Telnet.

- **Protocolos de Transferência de Arquivo (FTP)**

O FTP, especificado através da RFC959, baseia-se no modelo Cliente x Servidor e provê serviços de transferência, renomeação e remoção de arquivos. Provê também a criação, remoção e modificação de diretórios, entre outros. Para a prestação de tais serviços, são estabelecidas duas conexões TCP entre o cliente e o servidor: uma conexão de controle, usada na transferência de comandos, e outra de dados. A confiabilidade das transferências de arquivos realizadas fica por conta do TCP, já que o FTP não implementa nenhum controle adicional sobre os arquivos, a não ser a exigência da senha do usuário para permitir a transferência.

- **E-mail**

O Sistema de Correio Eletrônico constitui-se de uma série de servidores cooperantes interagindo através do protocolo SMTP. Essa transmissão é feita mediante o estabelecimento de um canal de comunicação, conexão TCP, pelo qual transitarão as mensagens conduzidas por meio do protocolo SMTP.

- **Grupo de Discussão**

Grupo de discussão envolve grande quantidade de pessoas. O tráfego nesse tipo de aplicação não é normalmente crítico ao negócio da organização.

- **HTTP**

O HTTP (Protocolo de transferência Hipertexto) é provavelmente o protocolo cliente/servidor de utilização mais ampla no momento. Os clientes utilizam um aplicativo navegador da Web para se comunicar com os servidores Web. O fluxo de tráfego é bidirecional e assimétrico.

O fluxo de tráfego HTTP nem sempre ocorre entre o navegador da Web e o servidor da Web, devido ao cache.

- **NFS**

NFS (Sistema de Arquivo de Rede) é um conjunto de protocolos de sistema de arquivos distribuídos desenvolvido pela Sun Microsystems e que permite acesso a arquivos remotos através de uma rede.

De acordo com as prioridades e níveis de SLA desejados pelo usuário, os diferentes tipos de aplicativos e tráfego que irão trafegar nas Redes VPN MPLS devem ser classificados em uma das 6 classes de serviços, segundo as RFCs 2474 e 2475 (DiffServ) conforme a figura 3.2, complementados pela RFC 2597 (Assured Forwarding PHB) e pela RFC 2598 (Expedited Forwarding), além de todo tráfego não explicitamente definido nas referidas RFCs:

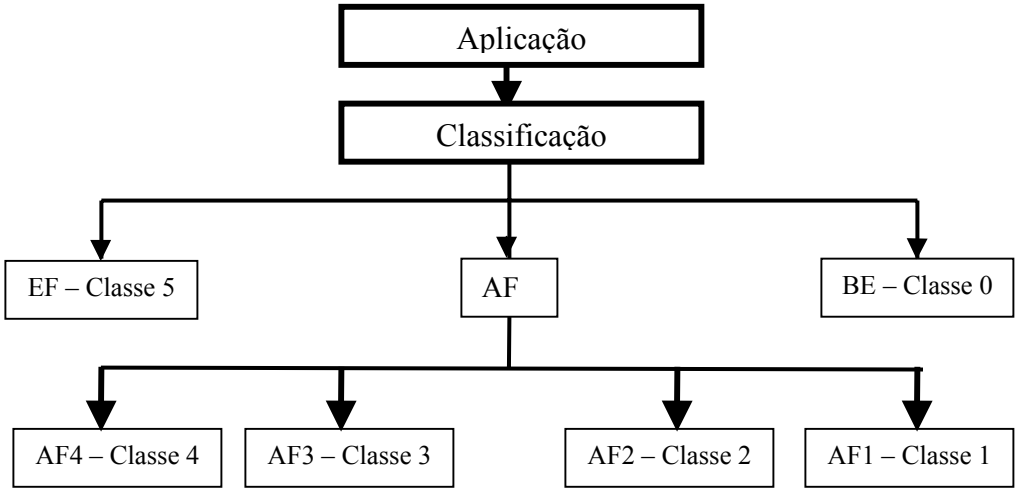

Figura 3.2 – Classificação das aplicações de acordo com DiffServ

É importante que o provedor de serviço implemente algumas alternativas para situações de contigência na rede. Uma das possíveis implementações seria uma configuração mínima para as classes de serviço Missão Crítica (AF4) e Gerenciamento (AF3), e todo o tráfego restante ser classificado como melhor esforço (B_E).

A tabela 3.2 mostra os requisitos de QoS para algumas aplicações típicas.

Aplicações Típicas	Requerimentos de QoS			
	Bandwidth	Latência	Jitter	Perda de Pacote
e-mail	Baixo	-	-	-
FTP	Altas rajadas	-	-	-
Telnet	Baixas rajadas	Moderado	-	-
Mídia Streaming	Média à moderada	Sensível	Sensível	Sensível
Videoconferência	Alta	Crítica	Crítica	Sensível
VoIP	Moderada	Crítica	Crítica	Sensível

Tabela 3.2 – Requerimentos das Aplicações tradicionais

3.2.2 – PASSO 2 – Divisão dos Aplicativos em múltiplas classes

Esse passo apresenta a estratégia de classificação de pacotes com base nos aplicativos dos usuários A política de classificação será de acordo com a requisição do

usuário. A tabela 3.3 apresenta os principais aplicativos. Á medida que outras aplicações sejam necessárias, novas regras de mapeamento precisam ser criadas.

Para oferecer serviços diferenciados de acordo com a aplicação do usuário, os tráfegos devem ser agrupados em classes segundo os requisitos das aplicações. Cada classe deve ser diferenciada pela rede de acordo com o serviço definido na configuração da QoS (Qualidade de Serviço) para essa classe. A classificação é o ato de examinar os pacotes da aplicação/porta do usuário para decidir por qual valor o DSCP deve ser definido no pacote e mapeado em EXP na rede do provedor. Essa classificação ocorre na borda da rede MPLS (equipamento PE).

Na estratégia proposta são recomendadas 6 classes de serviços as quais se encontram indicadas a seguir:

3.2.2.1 – Padrão BE - Classe Dados Padrão Best Effort (BE) – Classe 0

Classe de serviço correspondente ao tráfego de menor prioridade. É equivalente ao serviço Melhor Esforço disponível na Internet. Essa classe de serviço oferece, basicamente, conectividade com nenhuma garantia. Muitas aplicações de dados, tais como o Protocolo de Transferência de Arquivo (FTP), trabalham adequadamente com o serviço Melhor Esforço.

Todo tráfego não explicitamente atribuído às quatro classes AF e à classe EF ficará nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes. Isso garante que tais tipos de tráfego possam fluir se houver recursos disponíveis na rede, porém, impede que estes afetem negativamente as demais classes.

3.2.2.2 – Classe Dados com prioridades - AF

Classe de serviço que provê uma priorização de tráfego das aplicações críticas do usuário em relação a dados Melhor Esforço. Isso significa para o provedor de serviço a possibilidade de oferecer níveis de serviços diferentes por cliente e aplicação. A proposta apresentada neste trabalho sugere a divisão da classe de dados com prioridades em 4 subclasses:

- **AF1 – Aplicações não Críticas – Classe 1**

Aplicações com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato aos usuários. Embora se trate de conteúdo importante, não são aplicações que podem esperar por disponibilidade de recursos da rede da classe padrão BE. Todas aplicações classificadas nessa classe terá prioridade em relação as aplicações padrão – BE.

- **AF2 – Aplicações de Negócios – Classe 2**

Aplicações não interativas, com grande volume de dados importantes para o atendimento complementar aos usuários da organização, porém, sem necessidade de um tempo de resposta reduzido. Essas aplicações serão consideradas prioritárias em relação às aplicações não críticas e de melhor esforço.

- **AF3 – Gerenciamento – Classe 3**

Aplicações de gerenciamento de redes e de sistemas, que necessitam de uma banda mínima para atividades de suporte técnico, mesmo em situações de congestionamento severo da rede. Não ocupam banda suficiente para interferir nos demais tráfegos em condições normais de operação. Essa classe terá prioridade em relação as anteriores.

- **AF4 – Missão Crítica – Classe 4**

Aplicações interativas críticas para o negócio e tráfego DNS que exigem entrega garantida e tratamento prioritário. A aplicação multimídia também será incluída nessa classe. Multimídia possui requisitos de qualidade de serviços diferentes de aplicações tradicionais como *Simple Mail Transfer Protocol* (SMTP), que trabalham bem com a classe de dados Melhor Esforço.

A figura 3.3 apresenta o resultado da influência das perdas de pacotes [53] para uma classe multimídia de uma simulação realizada para análise das perdas de pacotes de 1%, 3% e 8%.

a – 1% . b – 3% c – 8%

Figura 3.3 – Efeitos da perda de pacotes

3.2.2.3 – Classe Tempo Real – EF – Classe 5

Aplicações sensíveis a retardo (*delay*) e variações de retardo da rede (*jitter*), que exigem priorização de pacotes e reserva de banda são adequadas para essa classe.

Um serviço que pode ser oferecido pela arquitetura VPN MPLS é o tráfego diferenciado de pacotes de voz. Esse tráfego possui requisitos de Qualidade de Serviço (QoS) que raramente podem ser atendidos por uma rede IP Melhor Esforço. Os parâmetros de QoS relevantes para o tráfego de voz são o atraso, a variação do atraso (*jitter*) e a taxa de perdas de pacotes. Esses parâmetros refletem a continuidade de um fluxo de voz. Dada a natureza de interatividade do serviço telefônico, o atraso é o fator mais crítico.

3.2.2.4 – Mapeamento dos aplicativos/portas em Classes

Este item apresenta a estratégia de classificação de pacotes, onde os pacotes serão classificados baseados nos aplicativos/portas utilizados pelos usuários.

Após uma análise de quais os principais aplicativos disponíveis no mercado e utilizados pelas organizações, foi realizada a classificação abaixo. Cada aplicativo é identificado por um número de porta TCP/UDP. As portas TCP/UDP são mapeadas em uma das 6 classes apresentada acima. No capítulo 5 serão mostradas alguns testes realizados. Para isso foi utilizado uma ferramenta conhecida como *iperf*, basicamente essa ferramenta implementa a arquitetura cliente/servidor, e permite criar conexões TCP/UDP, sendo os números das portas para os testes as definidas na tabela abaixo.

Classe de Serviço	Aplicativo	Porta/UDP/TCP	Portas para teste
Tempo Real (EF) Classe 0	Voz – RTP/RTCP	*	5001
Missão Crítica (AF4) Classe 1	Transacional – Sistema on line	**	5002
	Multimídia – RTP/RTCP	*	
	DNS	53	
Gerenciamento (AF3) Classe 2	Gerenciamento da Rede e Sitema	**	
	SNMP	161/162	
	Telnet para controle remoto	23	
	http/https	80/443	
Suporte a Negócio (AF2) Classe 3	CADView-3D	649	5003
	SQL-Net	150	
	Oracle	1525	
	Sybase	2439	
	e-learning	**	
Não crítico (AF1) Classe 4	Correio Eletrônico (SMTP)	25	
	Browser (Intranet/Internet)	**	
	Grupos de discussão	**	
Padrão (BE) Classe 5	FTP	21	5004
	Vídeo Streaming	**	
	NFS		

Tabela 3.3 – Classificação das aplicações

(*) Aplicações real-time baseadas em RTP/RTCP necessitarão que o cliente informe qual o intervalo de portas UDP que será utilizado.

(**) Utilização de portas não autorizadas pelo IANA.

3.2.2.5 – Mapeamento dos campos DSCP em EXP

A proposta apresentada possui seis Classes de Serviço previstas (voz-tempo real, missão crítica, gerenciamento, aplicações de negócios, aplicações não críticas e dados

padrão melhor esforço) conforme tabela 3.3. Para cada uma destas classes é previsto um tratamento diferente ao longo de toda a VPN.

O modelo de QoS adotado está baseado em DiffServ. A classificação e marcação de DSCP dos pacotes IP será realizada pelos CPEs/CEs, e a marcação de EXP dos pacotes MPLS será feita pelos PEs envolvidos. A partir destas marcações serão realizadas as classificações em filas em cada roteador da Rede IP do Provedor. Cada fila está associada a uma Classe de Serviço (CoS), onde serão definidas características de prioridade para transmissão (WFQ, WRR), tamanho da fila (buffer), políticas de controle de fluxo (WRED). As marcações IP no DSCP serão mapeadas no campo EXP (MPLS), conforme tabela 3.4:

Classes de Serviço (CS)	Porta	Valores de DSCP (IP)		EXP (MPLS)
Voz – Tempo Real	X1	EF PHB	001 010	001
Não Crítica	X2	AF11 PHB	001 010	001
Suporte a Negócio	X3	AF21 PHB	010 010	010
Gerenciamento	X4	AF31 PHB	011 010	011
Missão Critica	X5	AF41 PHB	100 010	100
Dados Best Effort (BE)	X6	DF PHB	000 000	000

Tabela 3.4 – Mapeamento do DSCP em EXP

3.2.3 – PASSO 3 - Determinação da tecnologia de acesso

Os serviços oferecidos pelas VPNs MPLS foram inicialmente providos através de conexão permanente do CPE/CE[20] do usuário com o roteador PE. Exemplos de tecnologias de acesso disponíveis são as Linhas Dedicadas (*Leased Lines*), *Frame Relay* ou *Asynchronous Transfer Mode* (ATM), a figura 3.4 a seguir mostra essas alternativas.

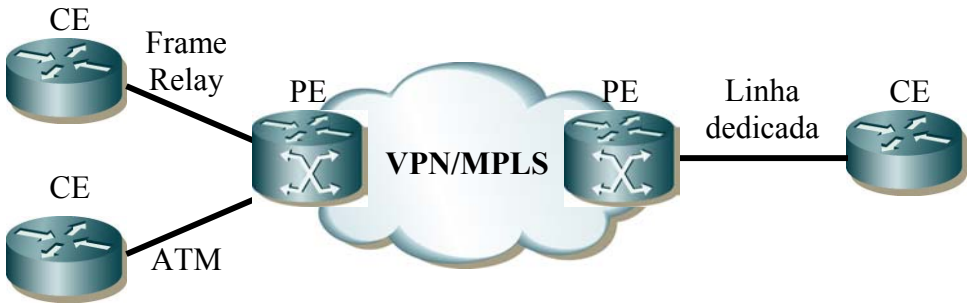

Figura 3.4 – Formas de acessos tradicionais das redes VPN/MPLS

[20] O termo CPE é utilizado normalmente pelos provedores de serviços, enquando CE é utilizado nas RFCs

Para prover serviços escaláveis de VPN MPLS fim a fim, o provedor de serviço deve possuir uma infra-estrutura de rede que suporte a integração de diferentes tecnologias de acesso em uma VPN MPLS.

Acessos Frame Relay, ATM e Linha Dedicada são tecnologias bem conhecidas. O próximo item focará em um novo método de acesso a VPN MPLS conhecido como xDSL.

3.2.3.1 – Provendo acesso xDSL para as VPNs MPLS

DSL usa ATM como um mecanismo básico de transporte. Podem ser utilizados vários métodos de encapsulamento, dependendo do tipo de aplicação requerida. Todos os encapsulamentos usam a camada de adaptação 5 do ATM para segmentar dados em células e a RFC 1483 [13] para permitir o transporte de múltiplos protocolos sobre o mesmo PVC ATM. A RFC 1483 trabalha com dois métodos. O primeiro método permite que múltiplos protocolos sejam transportados sobre o mesmo PVC; o segundo faz a multiplexação implícita do protocolo por PVC, isto é, um protocolo por PVC. Os possíveis métodos de encapsulamento são apresentados na figura 3.5.

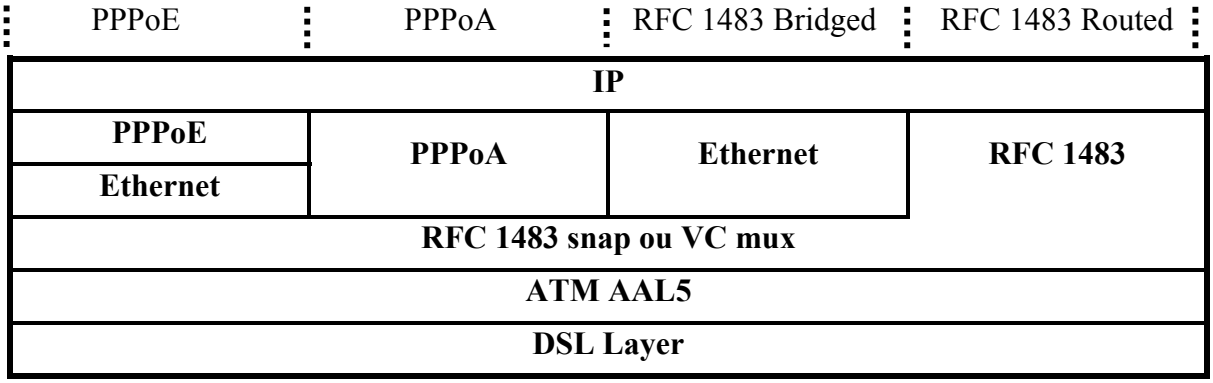

Figura 3.5 – Formato de Encapsulamento DSL

Cada um desses métodos de encapsulamento e seu funcionamento com uma rede VPN MPLS para acesso remoto será abordado no anexo C.

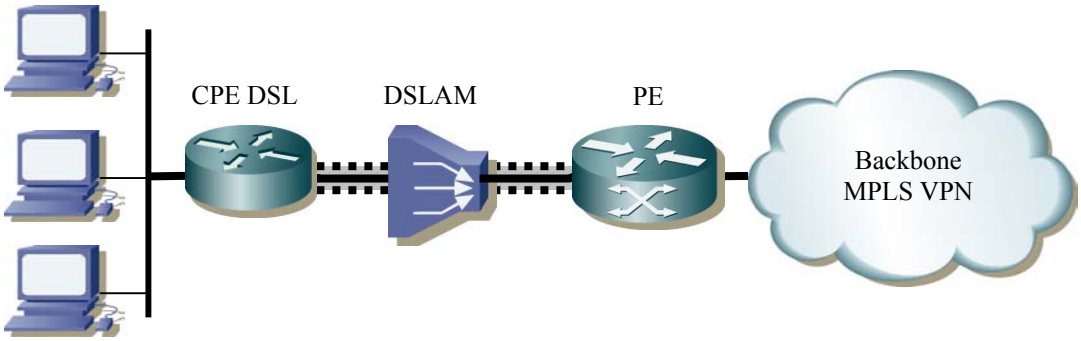

Figura 3.6 – VPN/MPLS com acesso ADSL

As formas de conexão DSL com a VPN MPLS basicamente consistem de um PVC entre o CPE DSL e o PE. O DSLAM é o concentrador dos acessos xDSL, o anexo C detalha essas formas de conexões.

3.2.3.2 – Procedimento para atendimento com várias tecnologias de acesso VPN MPLS

A simplificação na interoperabilidade das redes com tecnologias heterogêneas por meio do MPLS veio possibilitar que as VPNs MPLS sejam atendidas por várias formas de acesso[21], como: Frame Relay, Leased Line, ATM e xDSL. Os custos de implementação dessas tecnologias são, no entanto, muito diferentes entre si. Como conseqüência, é sugerido o modelo de atendimento descrito abaixo para uma operadora que tem como objetivo maior rentabilidade na construção e venda do serviço.

- A primeira alternativa é o atendimento via xDSL, caso seja possível atender os requisitos das aplicações (Ex: Velocidade) dos usuários e haja disponibilidade de acesso na localidade onde o usuário se encontra.
- Caso não seja possível o atendimento por xDSL, a segunda alternativa visando o menor custo seria uma linha dedicada do cliente até o PE mais próximo.
- A terceira alternativa é o atendimento através de acesso Frame Relay

[21] Além das formas de acesso mostrado acima, as operadoras começam a trabalhar com acesso metroethernet.

- A última alternativa é o acesso ATM, em função do alto custo da tecnologia dos equipamentos do usuário para implementar o protocolo ATM.

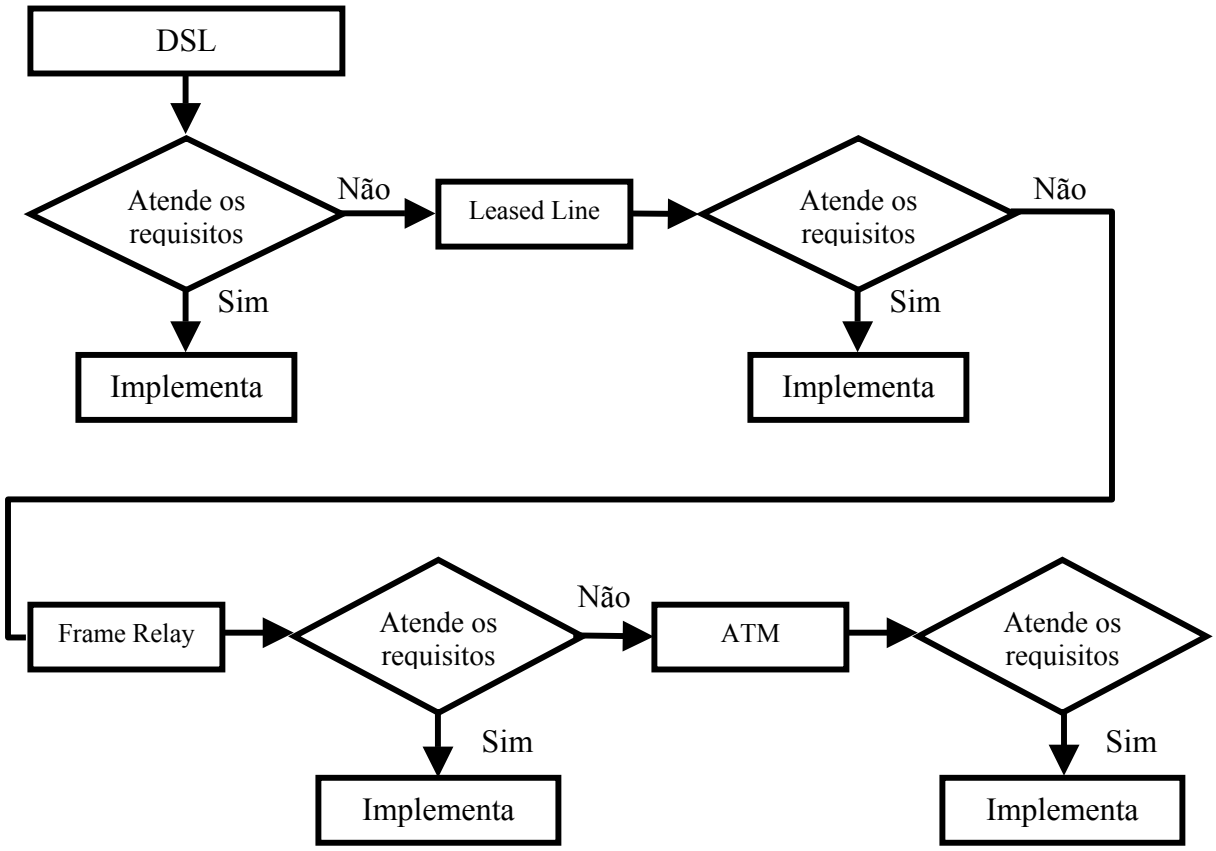

Figura 3.7 – Fluxo de escolha do melhor acesso

3.2.4 – Passo 4 - Determinação do CPE

Nesse ponto do trabalho analisar-se-á os principais aspectos no dimensionamento do CPE para determinadas classes de serviços. Nos testes (capítulo 5) realizados foram utilizados o modelo Cisco 827 com maior ênfase nas caracterisísticas apresentadas no item 3.9.2. A razão da análise do CPE é porque a QoS da VPN depende da marcação do pacote no CPE. Também, será apresentado nesse contexto a implementação recente da Cisco em CPE, conhecida como *VRF lite*, ou seja, habilita a configuração de Múltiplas VRFs nos CPEs.

Os CPEs podem ser divididos de acordo com as seguintes classes de serviços:

3.2.4.1 – Acessos sem QoS – Classe BE – Best Effort

Para as classes de dados padrão – Melhor Esforço (*Best Effort*), os CPEs/CEs tradicionais sem capacidade de classificação dos pacotes poderão ser utilizados. Em função da simplicidade do CPE, o seu custo é bastante reduzido. As funções normalmente exigidas por esses CPEs são:

- Interfaces Wan: DSL (PPPoA e DHCP) e Frame Relay
- Interfaces Lan: Fast Ethernet 10/100
- Protocolos de Roteamento: RIPv2 e OSPF
- Gerência: SNMP
- Translação de Endereços de Rede: NAT

3.2.4.2 – Acessos com QoS – Classes AF (Missão Crítica, Gerenciamento, Suporte a Negócios e Aplicações não críticas) e EF (Voz):

Para acessos com QoS para as Classes AFs e EF, os CEs devem apresentar algumas características que são fundamentais para o desempenho de uma VPN MPLS com qualidade de serviço:

- Possibilidade de definição das classes de serviços de acordo com a aplicação do usuário.
- O CPE deve possuir mecanismos de classificação dos pacotes, podendo ser combinados em:
    - Endereço IP de origem/destino;
    - Porta TCP / UDP de Origem / Destino;
    - Protocolos (p.ex. http, ftp e RTP/RTCP);;
- Mecanismos de Priorização por CoS, abaixo ou equivalentes:
    - WFQ (*Weighted Fair Queuing*) ou WRR (*Weighted Round Robin*);
    - LLQ *(Low Latency Queuing*) ou *Strict Priority*;
- Fragmentação em Layer 2:
    - FRF.12 (*Frame Relay Fragmentation Implementation Agreement*);
- *Buffer* para armazenamento de pacotes em caso de congestionamento, com possibilidade de controle do dimensionamento por Classe de Serviço;

- Suporte a voz:
    - Suporte a H232
    - Suporte a SIP
    - Suporte a MGCP

3.2.4.3 – Múltiplas VRFs nos CPEs (Multi – VRF CE)

Os CPEs das VPNs MPLS tradicionais não têm nenhum mecanismo para garantir privacidade da rede atrás do CE. Normalmente a privacidade é garantida através da colocação de um novo *Switch* (Comutador), onde é configurada uma VLAN para cada departamento (Figura 3.8).

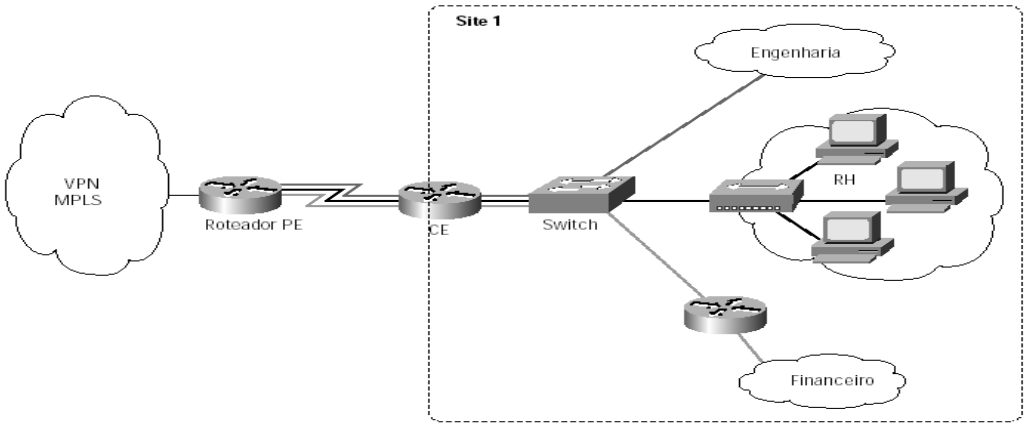

Figura 3.8 - Usando um Switch para segmentar uma LAN

Outra possibilidade é adicionar um novo roteador para cada departamento como mostra a figura 3.9.

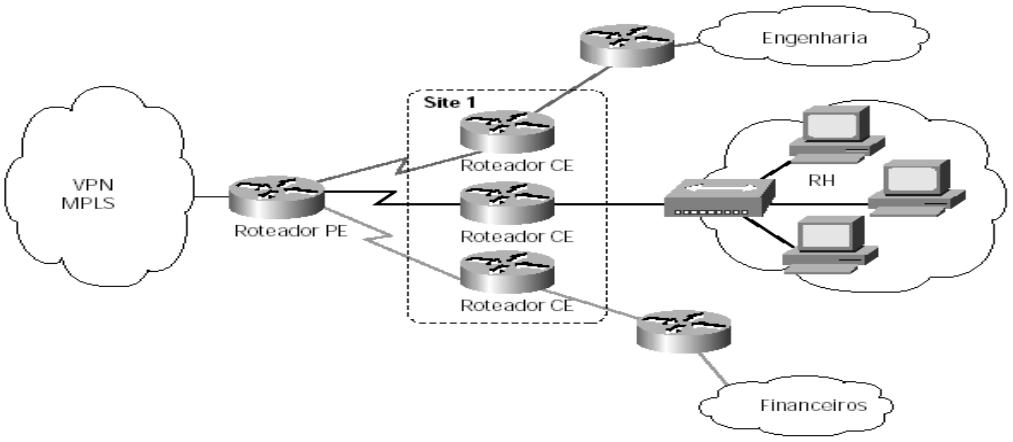

Figura 3.9 – Segmentação da Lan através de um roteador

Essas soluções envolvem a instalação de novos equipamentos como switch/comutador e roteador, além de aumentar a necessidade de gerenciamento.

Uma alternativa elegante para superar as dificuldades acima foi desenvolvida através de Múltiplas VRFs. As Multi-VRF (Múltiplas VRFs) no CPE/CE é uma nova facilidade introduzida recentemente nos equipamentos Cisco. Multi-VRF expande a capacidade de VRF no roteador PE para o roteador CE no modelo da VPN MPLS. O roteador CE fica habilitado em manter várias tabelas separadas (VRFs). Isso permite oferecer o nível de segurança e privacidade das VPN MPLS dentro do ambiente da LAN do usuário. Os roteadores CEs utilizam as VRFs para criar VLANs no ambiento da rede local do usuário. Cada VRF no roteador CE é mapeada em uma VRF no roteador PE. Não existe nenhuma troca de "rótulo" entre PE e CE. A conexão entre PE e CE não suporta LDP.

Na figura 3.10 são configurado algumas VRFs por departamento. Cada subinterface está vinculada a uma VRF da VPN respectiva.

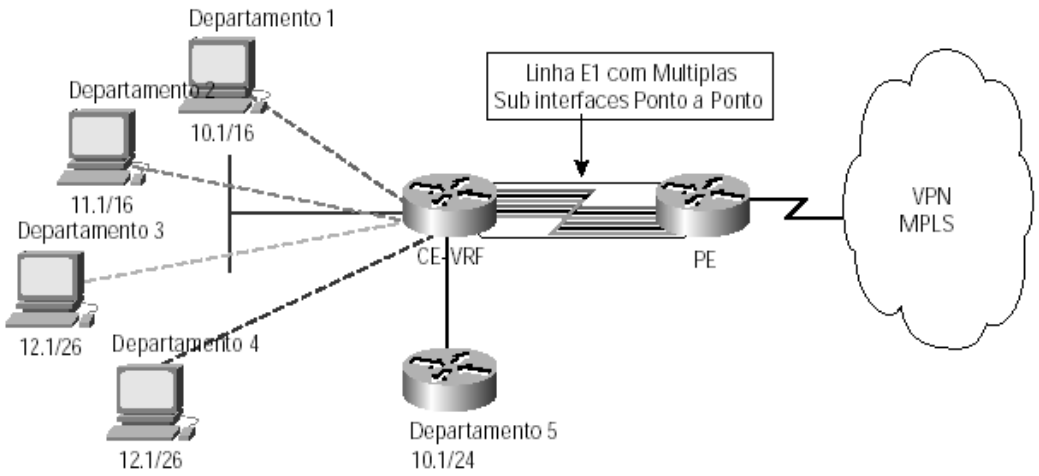

Figura 3.10 – Configurando VRF no CE por departamento

A figura 3.10 ilustra um exemplo em que as Multi-VRF CE podem ser usadas nos roteadores CEs. A conexão entre o roteador PE e a rede MPLS usa os mesmos mecanismos apresentados no capítulo 2. Nesse exemplo, o roteador CE associa uma VRF específica para cada departamento conectado na interface e troca informações com o roteador PE, em seguida as rotas são instaladas dentro da Multi-VRF do CE.

3.2.5 - PASSO 5 – Configuração da VPN MPLS

No próximo capítulo será analisada a configuração da VPN, esse passo é o mais crítico, pois qualquer configuração indevida da VPN pode significar um acesso não autorizado de um cliente de uma determinada VPN em outra.

3.2.6 – Passo 6 – Teste de Conectividade e Isolamento das VPNs MPLS

Esse passo será analisado em detalhes no capítulo 5. Os mecanismos necessários a este passo foram apresentados no capítulo 2 e, na estratégia proposta, permitam que as VPNs MPLS implementem perfeito isolamento e conectividade entre as

mesmas. Para certificar essa funcionalidade é necessário realizar alguns testes para validar esse passo.

3.2.7 – Passo 7 - Teste de QoS das VPNs MPLS

Esse passo será analisado em detalhes no capítulo 5, pois como a estratégia proposta é baseada em oferecer QoS fim a fim na VPN de acordo com os aplicativo, é necessário que os roteadores CE e PE seja avaliados em condições normais e anormais de congestionamento.

3.3 - Resumo do Capítulo

Este capítulo apresentou uma estratégia de construção de VPN MPLS com qualidade de serviço fim a fim. Para que isso fosse possível, a estratégia foi dividida em 7 passos. Inicialmente foi feita uma avaliação que deve ser realizada pelo provedor de serviço com o objetivo de identificar qual é a melhor forma de implementar VPN MPLS no núcleo da Rede. O primeiro passo foi voltado para a análise básica dos requisitos das aplicações do usuário, pois como o método é baseado em diferentes níveis de serviços, a rede precisa conhecer quais os aplicativos/portas que devem ser priorizados em relação a outros. O segundo passo é o mapeamento dos aplicativos em uma das classes EF, AF (AF1, AF2, AF3 e AF4) ou BE. No terceiro passo é definida a tecnologia de acesso. No caso das VPNs MPLS são possíveis várias formas de acesso, sendo que a estratégia apresenta uma nova forma de acesso xDSL que, baseado principalmente no seu baixo custo, tem a tendência de oferecer serviço de VPN/MPLS com preços bastante inferiores em comparação aos tradicionais. A determinação do CE ou CPE é realizada no passo 4 e o objetivo é simplesmente certificar que os CEs irão atender às especificações das aplicações (Ex: VoIP) e do acesso. Também é apresentada uma recente implementação nos CE/CPE que permite a criação de múltiplas VRFs. O passo 5 é o mais importante em um projeto de VPN MPLS. Em função disso será dado maior ênfase a ele no capítulo 4. Os passos 6 e 7 tratam da questão de conectividade, isolamento e qualidade de serviço. O objetivo é validar se a VPN é segura e oferece o desempenho definido pelo SLA.

Capítulo 4

Configuração da VPN

No capítulo 3 foi apresentada a estratégia de projeto de VPN MPLS, sendo a mesma formada de 7 passos. Neste capítulo será exposto um estudo de caso com o objetivo de validar o passo 5 que trata a configuração da VPN MPLS. A configuração será tratada em um capítulo exclusivo em função de sua importância e criticidade, pois uma configuração indevida de uma rota de determinada VPN em outra, significa o acesso a mesma por usuário não autorizado. Os conceitos de RD[22] e RT[23] que são fundamentais na arquitetura de VPN MPLS serão apresentados.

4.1 - Passo 5 – Configuração da VPN IP MPLS

A partir dos conceitos básicos da arquitetura da VPN BGP/MPLS apresentados nos capítulos anteriores, é possível entender como implementar essa arquitetura em termos da configuração da VPN MPLS do estudo de caso abaixo.

Para prover serviços de VPNs por meio de backbone VPN/MPLS as seguintes configurações são necessárias:

- **Definir as configurações dos Roteadores Virtuais (VRF);**
- **Definir e configurar o identificador de rotas/VPN (RD);**
- **Definir e configurar as políticas de importação e exportação de rotas (RT);**

[22] RD – Route Distinguisher identifica a VPN de cada usuário
[23] RT – Route Targets identifica as rotas que a VRF pode importar ou exportar

- **Configurar os enlaces PE-CE;**
- **Associar a interface CE previamente definida nas VRFs;**
- **Configurar o Multiprotocolo BGP.**

A configuração do estudo de caso mostrará as principais preocupações que devem ser consideradas na configuração de VPN MPLS.

Estudo de Caso:

A topologia apresentada na figura 4.1 é uma estrutura de VPN básica que provê conectividade um a um entre as redes dos usuários, usando o modelo *peer* discutido no capítulo 2.

A figura 4.1 apresenta o caso de um usuário que migrou para a topologia de VPN MPLS, e essa será usada para mostrar as principais etapas de configurações da VPN MPLS.

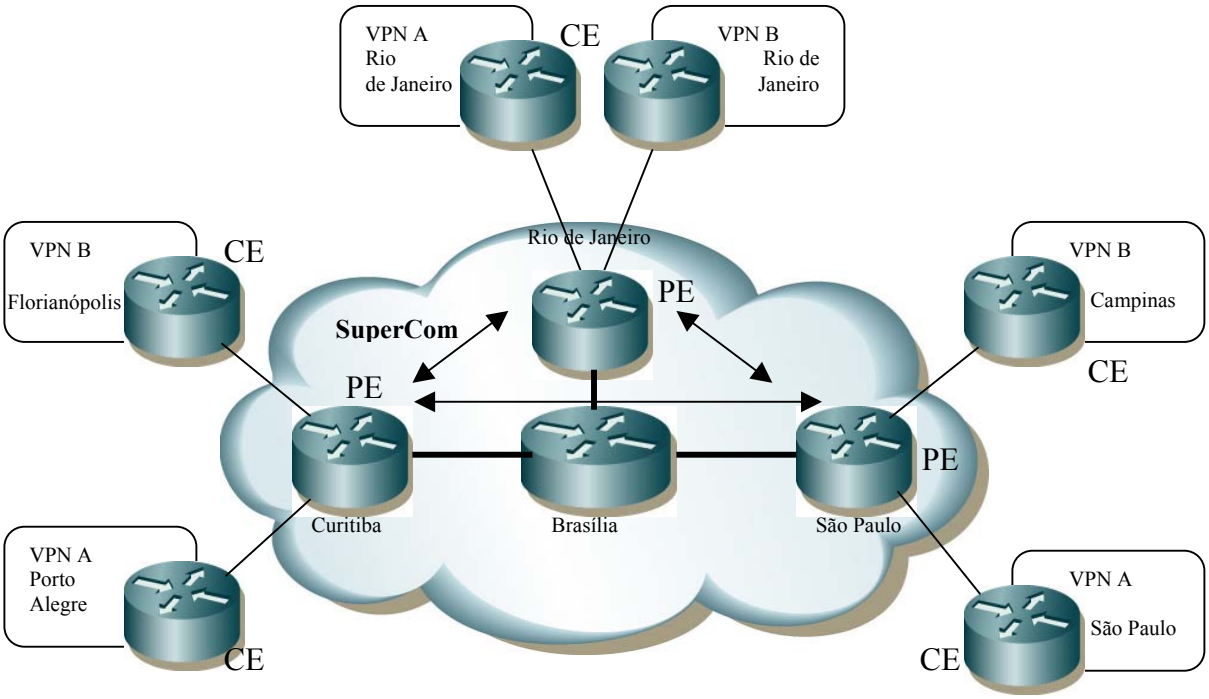

Figura 4.1 – Topologia VPN/MPLS Intranet

Na figura 4.1 acima, o Backbone VPN/MPLS do provedor de serviço SuperCom tem duas VPNs definidas como VPN A e VPN B.

O provedor de serviço utiliza os protocolos de roteamento RIPv2 e rota estática para aprender as rotas das VPNs dos usuários. Os sites das VPN A em Porto Alegre e a

VPN B em Florianópolis usam RIPv2 para se comunicarem com o backbone MPLS/VPN. Os sites das VPN B no Rio de Janeiro e Campinas, VPN A em São Paulo e Rio de Janeiro usam roteamento estático.

A tabela 4.1 mostra os endereços para as VPNs dos usuários e os endereços de loopback[24] usados pelo provedor de serviço para as sessões de BGP.

Empresas

Empresas	Ponto de Presença	Subnet	Prot. de Roteamento
VPN B	Florianópolis	195.12.2.0/24	RIPv2
	Rio de Janeiro	10.2.2.0/24	Roteamento estático
	Campinas	10.2.1.0/24	Roteamento estátivo
VPN A	Porto Alegre	10.2.1.0/24	RIPv2
	Rio de Janeiro	10.1.2.0/24	Roteamento estático
	São Paulo	196.7.25.0/24	Roteamento estático
SuperCom	São Paulo (Loopback)	194.22.15.1/32	
	Curitiba (Loopback)	194.22.15.2/32	
	Rio de Janeiro (Loopback)	194.22.15.3/32	

Tabela 4.1 – Endereços das VPNs dos usuários e loopback do provedor

4.1.1 – Configuração dos Roteadores Virtuais

O primeiro passo no projeto de um serviço de VPN, baseado na arquitetura MPLS, é definir e configurar o roteamento e encaminhamento virtual (VRF). No caso acima, isso significa configurar VRFs para cada VPN A e VPN B. Cada roteador PE deve ser conectado ao roteador CE do usuário que deseja receber rotas de uma VPN específica. Os roteadores PEs da SuperCom em Curitiba, Rio de Janeiro e São Paulo são todos conectados às VPN A e VPN B. As configurações das VRFs devem existir em todos os roteadores PEs.

Os PEs suportam múltiplos roteadores dentro de um único sistema. Isso permite ao provedor de serviço configurar múltiplos roteadores separados dentro de um único chassi. A aplicação para essa função inclui a criação de roteadores individuais dedicados

[24] Loopback – Cada roteador PE necessita de um endereço único (Usualmente chamado de loopback) que é utilizado para alocar um rótulo e habilitar o encaminhamento dos pacotes da VPN através do backbone.

para os usuários. O roteador pode suportar até 1000 (Agregador – PE da Juniper) roteadores virtuais por módulo ou por chassi.

O CPE/CE conectado no roteador PE vê uma interface de roteador. O equipamento (CE) conectado não tem noção do roteador virtual atrás da interface. Por exemplo, um enlace Frame Relay pode ter circuitos que são conectados a diferentes roteadores virtuais. A camada física e enlace não ficam cientes que há múltiplas instâncias de roteadores.

O PE implementa o roteador virtual pela separação de cada estrutura de dado e permite a cada protocolo (TCP/UDP, RIP, OSPF, BGP-4, IS-IS) ser habilitado caso a caso. Há uma tabela do roteador para associar a conexão do usuário (Exemplo: PPP ou Frame Relay), com uma ou mais interfaces IP dentro de um roteador virtual.

Como mencionado acima, o protocolo de roteamento do PE provê todo o suporte para BGP-4, OSPF, IS-IS e RIP. Esses protocolos podem ser habilitados ou desabilitados para cada instância de um roteador no PE. Esses protocolos serão tratados com maior detalhe nas próximas secções.

4.1.2 – Definir e Configurar os "Indentificadores de Rotas - RD" e endereços VPN-IPv4

Multiprotocolo BGP (MP-BGP) é um protocolo usado para distribuir rotas das VPNs entre os roteadores PEs. Antes de apresentar como as rotas são distribuídas entre os PEs, deve-se primeiro analisar como as VPNs BGP/MPLS facilitam o roteamento original dos usuários. Nas VPNs BGP/MPLS as rotas dos usuários são independentes e isoladas de outras VPNs. Além disso, as rotas são separadas pelo provedor de serviço no backbone, sendo possível mais de uma VPN usar o mesmo endereço da rede privada. A única forma de realizar isso é garantir que essas rotas possam ser distinguidas de outras. As VPNs BGP/MPLS conseguem isso por adicionarem um Identificador de Rotas (RD) nos endereços IPv4. O RD é adicionado pelo PE. O resultado é chamado VPN-IPv4.

4.1.2.1 - RDs e as famílias de endereçamentos VPN-IPv4

O objetivo das VPNs BGP/MPLS é ter um endereço único para cada VPN. As Rotas dos clientes devem ser tratadas em diferentes caminhos, dependendo de qual VPN

elas pertencem. A extensão do protocolo BGP [9] permite ao BGP transportar rotas de múltiplas "famílias de endereços" [49]. Uma VPN-IPv4 é composta de 12 bytes, iniciando com 8 bytes que corresponde ao RD e terminando com 4 bytes que se referem ao endereçamento IPv4. O anexo A avalia os tipos de RDs em detalhes.

Um RD consiste de três campos: dois bytes que especificam o Tipo do Campo, um Campo do Administrador e um Número do Campo Atribuído (ASN). O valor do tipo de campo determina o comprimento dos outros dois campos, assim como, a semântica do campo administrador.

O principal requisito da arquitetura VPN MPLS exige que todas as rotas dos usuários sejam únicas dentro do backbone, e que não restrinja o uso de endereçamento privado. O MP-BGP seleciona um único caminho entre todos os possíveis, descrevendo uma rota para um dado destino (rede e máscara). Entretanto, o MP-BGP, por si só, não pode operar corretamente se os usuários utilizam os mesmos planos de endereços.

Na figura 4.2 é apresentado o problema quando o roteador PE da SuperCom no Rio de Janeiro recebe dois endereços idênticos IPv4, ou seja, o roteador PE do Rio de Janeiro não consegue distinguir entre as VPNs A e B. Para que o PE consiga distinguir e escolher a melhor rota entre as duas rotas recebidas é necessário utilizar o mecanismo de identificador de rotas (RD).

Esse mecanismo consiste de uma seqüência de 64 bits na frente do endereço IPv4, que está contido no MP-BGP. Essa seqüência de bits é conhecida como RD, e é diferente para cada VPN, sendo única dentro do backbone MPLS/VPN. A figura 4.3 ilustra como o roteador PE do Rio de Janeiro consegue agora distinguir entre duas rotas IPv4 e pode tratá-las como entidades separadas e pertencentes à devida VPN.

A combinação dos endereçamentos IPv4 e os Identificadores de Rotas fazem com que as rotas IPv4 sejam únicas através da rede VPN MPLS.

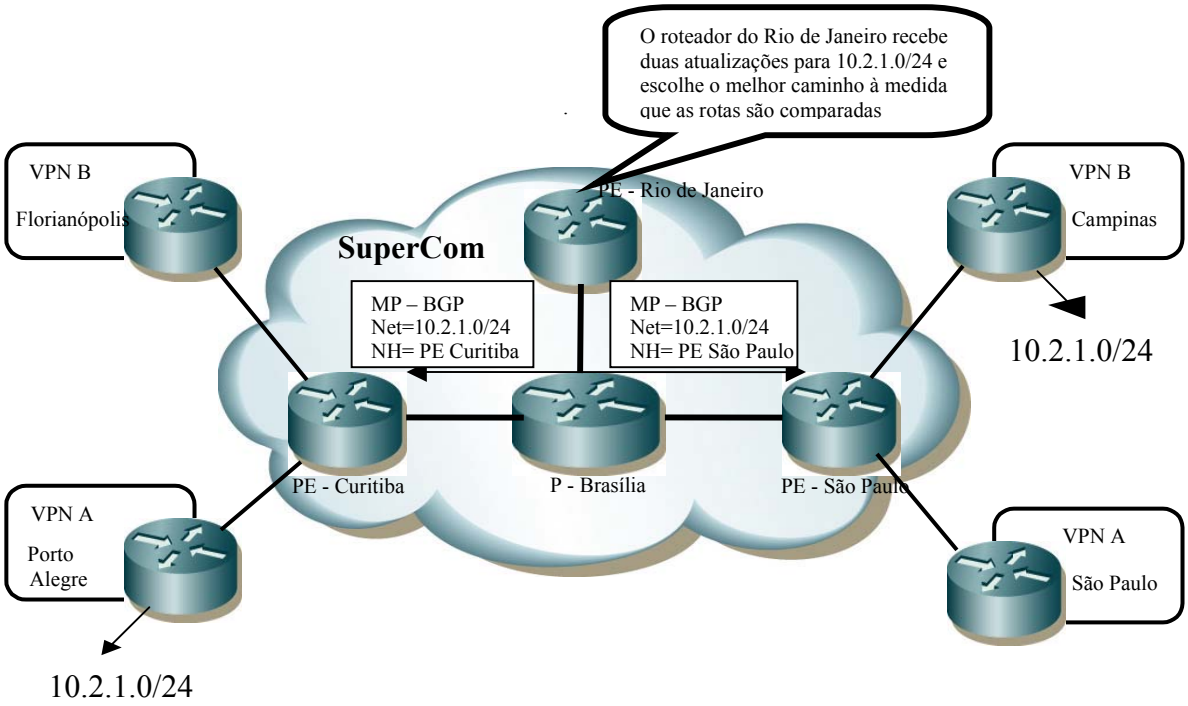

Figura 4.2 – Roteador PE do Rio de Janeiro compara as mesmas rotas Ipv4

A figura 4.3 mostra que, quando o PE do Rio de Janeiro recebe os dados 10.2.1.0/24 dos roteadores PEs de Curitiba e São Paulo, esses dados são agora distinguidos, pois um "Identificador de Rotas - RD" foi criado. Para os dados recebidos do roteador PE de Curitiba foi criado um prefixo **100:26: 10.2.1.0/24** e os dados recebidos do roteador PE de São Paulo um prefixo **100:27: 10.2.1.0/24**.

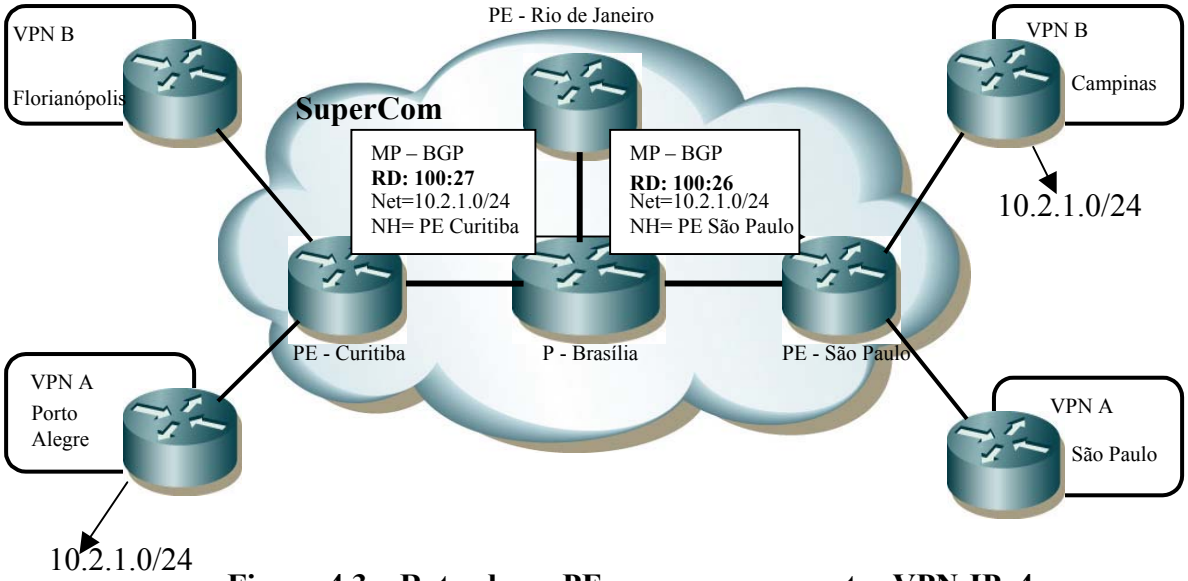

Figura 4.3 – Roteadores PEs comparam as rotas VPN-IPv4

Pelo mecanismo do RD (RD por VPN) é possível aos clientes de diferentes VPNs o uso dos mesmos endereços privados. Isso não resolve o problema de múltiplos clientes dentro da mesma VPN usarem o mesmo endereçamento entre suas redes. A solução para esse problema é possível através de implementação de NAT ou criando RDs por VRFs. Na prática, as operadoras têm optado pela solução através de NAT e implementar RD somente por VPN e não por VRF. A criação de RD por VRFs demanda grande incremento de memória e processamento dos PEs.

4.1.2.2 - Configuração dos Identificadores de Rotas (RD)

Cada VRF no roteador PE necessita ter um Identificador de Rotas associado, que pode estar relacionado a um site/ponto ou VPN. No caso mais comum, em que um ponto pertence unicamente a uma VPN intranet, é tecnicamente recomendável o uso de um único identificador de rotas para a VPN. Entretanto, esse ponto no futuro poderá ser membro de uma VPN extranet. Por exemplo, suponha-se um identificador de rotas que é utilizado por VPN. Se um ponto particular (site 2 da figura 4.4) de rede desejar ser membro de múltiplas VPNs, não será possível determinar que identificador de rotas usar para esse ponto específico, porque o mesmo pertence a mais que uma VPN. Entretanto, para uma topologia de um modelo Intranet simples (tabela 4.2), usa-se o mesmo identificador de rotas por VPN para reduzir o uso de memória do roteador PE.

Quando certas topologias (como a Extranet apresentada na figura 4.5) são criadas, pode ser necessário estender os identificadores de rotas por VRF/Site para um determinado modelo de projeto.

Pode-se estabelecer a atribuição de um valor particular do Identificador de Rotas para cada VRF no roteador PE. A estrutura desse valor pode ser no formato ASN: nn ou endereço: nn IP. Recomenda-se o uso do ASN: nn com o Número do Sistema Autônomo (ASN), que é atribuído pela Internet Assigned Numbers Authority (IANA) e que é único entre os provedores de serviço.

O provedor de serviço atribui o valor da segunda parte do Identificador de Rotas. Como recomendado, esse valor normalmente deverá ser único por VRF. Em alguns casos, tais como o exemplo apresentado na figura 4.1, poderá ser único por VPN quando se trata de Intranet. A tabela 4.2 mostra os valores para cada VPN da SuperCom dos usuários.

VPN do usuário	ASN	Valor Único	Identificador de Rota/VPN (RD)
VPN B	100	26	100:26
VPN A	100	27	100:27

Tabela 4.2 – Definição dos identificadores de rotas por VPN

4.1.2.3 – Rotas Targets - RT

O atributo RT identifica uma coleção de VRFs pelo qual um roteador PE distribui as rotas. Um roteador PE usa esse atributo (RT) para restringir a importação e exportação de rotas para as VRFs.

Cada VRF tem uma política de configuração para importação e exportação das rotas. O roteamento que é distribuído para outros PEs são marcados como atributos RT de exportação. As rotas que são recebidas pelo outro roteador PE são checadas se seu atributo RT de importação aceita inserir essa rota dentro da VRF. Esse mecanismo flexível permite a construção de diferentes topologias de VPNs e modelos de negócios. Esse atributo é definido em *BGP Extended Communities Atribute [9]*.

Observe a figura 4.4, onde é apresentado duas VPNs e três sites, sendo a **VPN A** formada pelos sites 1 e 2, a **VPN B** formada pelos sites 2 e 3. É importante observar que os identificadores de rotas (RD) na figura abaixo serão por site e não por VPN, caso contrário (RD por VPN) o site 2 ficaria indeterminado entre o RD da VPN A e VPN B.

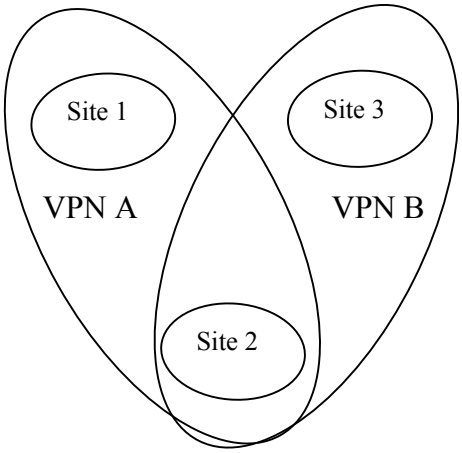

Figura 4.4 – Exemplo de topologia através do RT

Essa topologia é formada pela matriz (tabela 4.3) de configuração das VRFs RTs, onde a VRF2 para o site 2 está configurada para importar e exportar as rotas das

VPNs A e B. A VRF1 importa e exporta rotas somente da VPN A. A VRF3 importa e exporta rotas somente da VPN B.

VRF	RT VPN A	RT VPN B
1	Importa e Exporta	X
2	Importa e Exporta	Importa e Exporta
3	X	Importa e Exporta

Tabela 4.3 – Matriz de configuração das RT por VRF

Através dos conceitos de RT e RD por site foi possível determinar que o site 1 pertença somente à VPN A, o site 3 à VPN B e o site 2 a ambas VPNs.

4.1.2.4 – Extranet

Através dos conceitos básicos de RD e RT (apresentados anteriormente) é possível implementar uma Extranet.

Extranets (como apresentado no capítulo 2) são redes de determinados usuários que podem compartilhar informações com outras redes corporativas. Por exemplo, empresas de cartão de crédito, ASPs (Provedores de Serviços de aplicação) podem permitir o acesso a determinados servidores a partir de outras redes corporativas.

A figura abaixo apresenta um exemplo com o suporte inicial para formação de VPNs Extranet. Neste exemplo, os acessos "PBX1" e "PBX2" fazem parte, simultaneamente, da VPN de suas respectivas redes corporativas e da VPN VoIP.

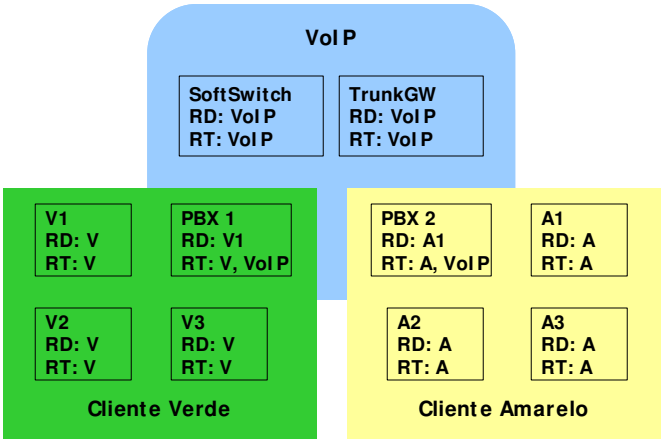

Figura 4.5 – Modelo de Extranet

Para que isto seja possível, é necessário que sejam criadas duas VRFs exclusivamente para os acessos pertencentes ao PBX1 (com rotas das VPNs VoIP e Verde) e PBX2 (com rotas das VPNs VoIP e Amarelo).

4.1.3 – Configuração das políticas de importação e exportação de rotas

O último passo na configuração de cada VRF é a adição das políticas de importação e exportação (RT) para cada usuário da VRF.

A rota *target (RT) BGP Extended Community* apresentada no item anterior dita a política de importação e exportação usada pela VRF.

4.1.4 – Configurar o enlace CE-PE

Para prover um serviço de VPN, o roteador PE precisa ser configurado para que a informação de roteamento aprendida de uma VPN do usuário possa ser associada a uma determinada VRF. Isso é possível de ser feito por meio do processo padrão do protocolo de roteamento, que é conhecido como **contexto de roteamento**. Cada VRF usa um contexto de roteamento separado.

Algumas rotas aprendidas por meio de uma interface que está associada a um protocolo de contexto de roteamento particular são instaladas dentro da VRF associada. Outras rotas aprendidas das interfaces que não fazem parte de algum contexto do roteamento são colocadas na tabela de roteamento global. Isso permite a separação da informação dentro de diferentes contextos, embora a informação seja aprendida pelo mesmo protocolo de roteamento.

A informação de roteamento é propagada de um ponto de rede do usuário para o provedor do serviço. Mais precisamente, a informação é propagada de um roteador CE para o roteador PE, para que o roteador CE seja conectado. Há várias opções de propagar essas informações, tais como: RIP, roteamento estático, OSPF ou BGP. Para que uma VPN funcione corretamente, é necessário que seja levantado qual o melhor protocolo de roteamento que deve ser utilizado e os parâmetros associados em função da necessidade do usuário.

- **PE-CE - Roteamento Estático**

A primeira opção é executar roteamento estático entre os roteadores PE e CE. O roteamento estático é distribuído para dentro do BGP para anunciar, por meio de sessões MP-BGP, que conectam os roteadores PEs. Isso é uma boa escolha quando o usuário tem um único ponto de entrada na rede do provedor de serviço, porque há pouco para ser realizado pela dinâmica de aprendizagem das rotas dos usuários por meio do enlace PE-CE.

No estudo de caso da figura 4.1, o roteador PE da SuperCom, em São Paulo, precisa ser configurado com rota estática para as VPN A e VPN B. Cada roteador CE do usuário aponta para o *default* no roteador PE. Nesse caso, não é necessário considerar as configurações no roteador CE. O primeiro passo nesse processo é configurar todas as rotas estáticas relevantes e colocá-las na VRF correta do PE, em vez da tabela de roteamento global.

- **Configuração do Link PE-CE – Rip Versão 2**

Essa opção de conectividade provê a facilidade de executar RIP versão 2 entre os roteadores PE e CE. A informação recebida por meio do RIP de alguma VPN do roteador CE do usuário é anexada dentro da VRF e então é anunciada por meio da VPN/MPLS, entre os roteadores PEs.

O roteador PE do provedor SuperCom de Curitiba, no estudo de caso da figura 4.1, executa o RIP versão 2 com o site/ponto da VPN A em Porto Alegre e o site/ponto da VPN B em Florianópolis.

- **Configuração do enlace PE-CE através de BGP**

Certos usuários que irão se conectar ao backbone da VPN BGP MPLS poderão executar BGP com o provedor de serviço e trocar rotas VPN por meio dessas sessões BGP. Com essa opção de conectividade, todas as rotas que são aprendidas de um CE do usuário serão anunciadas por meio da VPN MPLS, usando as sessões existentes entre os roteadores PEs do provedor de serviço. A figura 4.6 mostra esse tipo de conectividade.

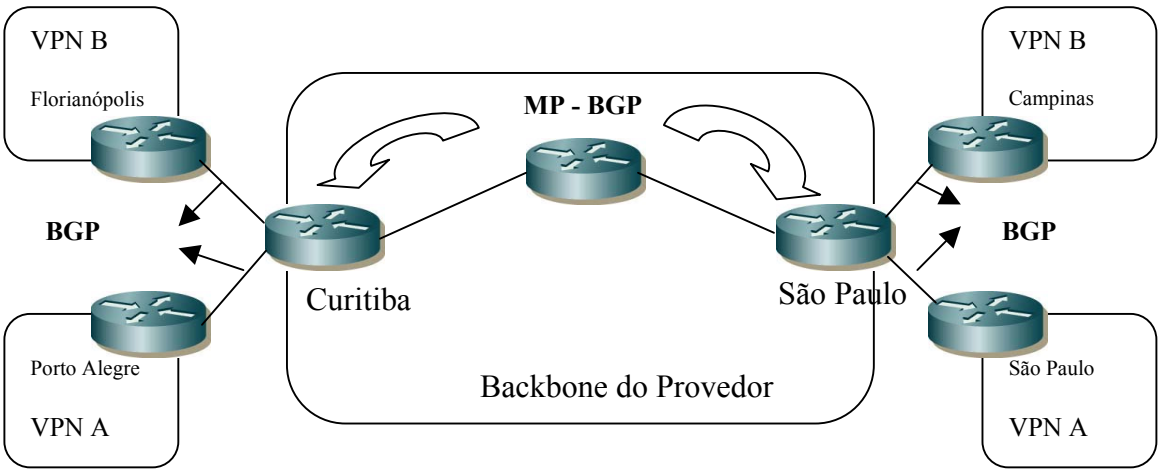

Figura 4.6 – BGP entre CE e PE

Como pôde ser visto na figura 4.6, ambos os clientes das suas respectivas VPNs conectam com o provedor da VPN MPLS por meio de BGP. Com essas configurações, quailquer rota aprendida por meio de sessões com o roteador CE do cliente VPN A será incluída dentro da VRF associada desse cliente. Assim como qualquer rota aprendida por meio das sessões com o roteador CE do usuário VPN B será colocada dentro da VRF do respectivo usuário.

Há dois requisitos principais para configurar BGP em um ambiente VPN MPLS. O primeiro, é a configuração da sessão entre os roteadores PEs, conhecida também como MP-BGP; o segundo, é a configuração do BGP entre os roteadores PE e CE. Para alcançar esse segundo objetivo, a família de endereçamento deve ser configurada sob o processo BGP para cada VRF, que receberá rotas da VPN do cliente usando BGP.

- **Protocolo de Roteamento OSPF entre PE-CE: Configuração do enlace PE-CE com OSPF**

A última opção de conectividade que será analisada é o OSPF. Essa opção pode ser atraente para clientes que já utilizam OSPF em cada site de sua rede através, por exemplo de *frame relay,* e ainda deseja trocar informações de roteamento OSPF entre os mesmos, sem ter que mudar para outros protocolos de roteamento como BGP ou RIPv2. Se o backbone da VPN MPLS é utilizado para conectar as redes, não é necessário mudar o protocolo de roteamento OSPF, pois o backbone MPLS pode ser usado para trafegar a informação.

Usando o modelo Overlay, os provedores de serviços têm capacidade de oferecer a infra-estrutura que poderá ser útil para as trocas de informações de roteamento entre os ambientes dos usuários de forma transparente ao protocolo de roteamento. Com esse modelo, os roteadores das redes dos clientes formam roteamentos adjacentes com os outros roteadores remotos por meio dos circuitos virtuais Frame Relay ou ATM, sendo que eles trocam informações IP diretamente entre os roteadores CEs por meio desses CVPs, usando o protocolo OSPF. Com a introdução das VPNs MPLS e o modelo de VPN peer-to-peer, as trocas de informação de roteamento tornam-se um desafio. Roteamentos adjacentes diretos através de CVPs entre redes dos usuários não podem mais serem formados, porque não existe mais um circuito virtual direto entre os sites. Isso significa que é necessário um mecanismo que permita ao OSPF funcionar nesse ambiente.

A nova solução deve prover as mesmas funcionalidades que o modelo overlay oferece para OSPF, com a exceção que esta funcionalidade deve ser oferecida pelo modelo de VPN MPLS.

As informações de roteamento aprendidas dos usuários por meio do OSPF são colocadas dentro da VRF. Essas rotas são então anunciadas por meio do backbone VPN MPLS, entre os roteadores PEs, usando MP-BGP, e são importadas para dentro das VRFs de outros PEs.

Para suportar conectividade OSPF de PE a CE em um ambiente VPN MPLS, um nível adicional de hierarquia de roteamento é necessário das redes dos usuários da VPN para executar processos de OSPF. Os protocolos OSPF já provêm dois níveis de hierarquia do backbone, que são área 0 e algumas áreas conectadas. O terceiro nível de hierarquia é provido para que as redes possam ser conectadas com o backbone da VPN MPLS. Esse nível extra de hierarquia é o topo da área 0. A referênncia [5] trata esse tema com mais detalhes.

4.1.5 – Associação de interfaces CE nas VRFs definidas

Após definir todas as VRFs no roteador PE, é necessário dizer ao PE qual interface pertence a qual VRF e, portanto, deverá popularizar as rotas VRFs com os pontos conectados. Mais de uma interface pode pertencer à mesma VRF.

Quando a interface é associada com uma VRF particular, o endereço IP é removido da tabela de roteamento global, pois um acesso feito naquele endereço não será

mais válido por meio de múltiplas tabelas de roteamento e deverá ser reconfigurado após a interface se tornar membro da VRF.

4.1.6– Configuração do Multiprotocolo BGP

A configuração do BGP requer vários passos e comandos de configuração. O BGP tem sido configurado para sessões MP-BGP PE a PE por meio do backbone VPN/MPLS, e para algumas sessões BGP PE a CE para usuários que desejam trocar BGP com o provedor de serviço.

Normalmente, a configuração padrão nos roteadores é IPv4, sendo necessário ativar as sessões VPN-IPv4.

Depois de ativar os roteadores para VPN-IPv4, o próximo passo na configuração do MP-BGP é definir e ativar as sessões BGP entre os roteadores PEs.

- **Processo de decisão para as VPN-IPv4**

As rotas RT e RD do BGP controlam a seleção das rotas VPN-IPv4. Esse processo ocorre após as rotas serem aprendidas de outros roteadores PEs, por meio das sessões MP-BGP, mas antes essas rotas são importadas para dentro de alguma VRF.

O primeiro passo no processo de decisão BGP é agrupar todas as rotas relevantes tal que elas possam ser comparadas. Antes do roteador PE selecionar as rotas, ele tem de conhecer que rotas da VPN existem e quais dessas rotas devem ser comparadas pelo processo de seleção BGP. Quando o roteador PE é aprovisionado para serviços de VPN, cada VRF é configurada com declaração, que diz ao roteador PE quais rotas devem ser importadas para dentro da VRF (RT). Com essa informação, o roteador PE faz o seguinte:

- Analisa todas as rotas com as mesmas RT, com alguma declaração de importação de rotas para dentro da VRF;
- Considera todas as rotas que têm as mesmas RD como a designada para o processamento inicial da VRF;
- Cria novos caminhos BGP com um RD que é igual para os RDs configuradas para a VRF que está iniciando o processo.

Agora, todas as rotas são comparadas e, nesse ponto, o processo de seleção BGP é executado.

Em função dos motivos acima é possível entender por que esse processo pode influenciar a quantidade de memória requerida para reter as rotas da VPN no roteador PE. Se cada roteador PE usa uma RD diferente para cada VRF de uma VPN particular, a quantidade de memória necessária para armazenar todas as rotas da VPN aumentaria.

4.2 - Resumo do Capítulo

Esse capítulo apresentou um estudo de caso para validar o passo 5 que trata da configuração da VPN. A maior ênfase neste capítulo foi na configuração da VPN. O passo 5 detalhou os cuidados que devem ser tomados em um projeto de VPN MPLS que são: criar a VRF; criar um Identificador de Rotas (RD); especificar políticas de importação e exportação das VRFs (RT); estabelecer conectividade BGP entre os PEs; estabelecer MP-BGP entre os roteadores e permitir a troca de VPN-IPv4 entre os roteadores. O capítulo também avalia a possibilidade de criar RD por site ou por VPN. A escolha do melhor protocolo de roteamento é analisada na última seção do trabalho. O próximo capítulo análisa os testes de conectividade, isolamento e qualidade de serviço da VPN. Esses testes referem-se aos passos 6 e 7.

Capítulo 5

Testes e análise dos Resultados Obtidos (Passos 6 e 7)

Os testes contidos neste capítulo têm o objetivo de validar a Estratégia proposta para projeto de VPNs MPLS com "6" classes de serviços. A validação será realizada por meio de três testes:

- **Teste de Conectividade das VPNs**
- **Teste de Isolamento das VPNs**
- **Teste de QoS das VPNs**

Para os testes de QoS no CE e PE são utilizados quatro cenários (tabela 5.1).

Cenário 1: Voz (EF) e Dados Best Effort (BE), com a soma das bandas geradas (30 + 120) para cada classe menor que a velocidade do acesso (256).

Cenário 2: Voz (EF) e Dados Best Effort (BE), com a soma das bandas geradas para cada classe (30 + 300) maior que a velocidade de acesso (256).

Cenário 3: Voz (EF), Dados Best Effort (BE), Missão Critica (AF11) e Suporte a Negócio (AF31), com a soma das bandas geradas (30 + 50 + 30 + 20) menor que a velocidade de acesso (256).

Cenário 4: Voz (EF), Dados Best Effort (BE), Missão Critica (AF11) e Suporte a Negócio (AF31), com a soma das bandas geradas (30 + 50 + 30 + 200) maior que a velocidade de acesso.

Cenário	Classe de serviço	Banda Configurada (Kbps)	Tráfego Gerado (Kbps)	Tamanho Pacote (bytes)	Protocolo	Porta
1	Voz (EF)	54	30	60	UDP	5001
	Missão crítica (AF11)	-	-	-	-	-
	Suporte a negócio (AF31)	-	-	-	-	-
	Dados (BE)	138	120	500	UDP	5004
				1200		
2	Voz (EF)	54	30	60	UDP	5001
	Missão crítica (AF11)	-	-	-	-	-
	Suporte a negócio (AF31)	-	-	-	-	-
	Dados (BE)	138	300	500	UDP	5004
				1200		
3	Voz (EF)	54	30	60	UDP	5001
	Missão crítica (AF11)	68	50	500	UDP	5002
				1200		
	Suporte a negócio (AF31)	43	30	500	UDP	5003
				1200		
	Dados (BE)	27	20	500	UDP	5004
				1200		
4	Voz (EF)	54	30	200	UDP	5001
	Missão crítica (AF11)	68	50	500	UDP	5002
				1200		
	Suporte a negócio (AF31)	43	30	500	UDP	5003
				1200		
	Dados (BE)	27	200	500	UDP	5004
				1200		

Tabela 5.1 – Configurações das Classes

5.1 – Classes de Serviços diferenciados

Níveis de Serviços Diferenciados são suportados pela manipulação de atributos chaves de certos fluxos que mudam a percepção do usuário da qualidade de serviço que a rede está entregando. Esses atributos incluem:

- A quantidade de dados que podem ser transmitidos por unidade de tempo (*thtoughput*);
- O atraso para transmissão dos dados de um ponto para outro ponto na rede (*delay* ou latência);
- A variação do atraso (*jitter*) para um dado fluxo.
- O percentual de dados transmitidos que não chegam ao destino corretamente (*loss*).

A necessidade de oferecer múltiplas classes de serviços para várias aplicações dos usuários deve-se à competição por recursos gerada pela multiplexação estatística dos pacotes. Com o objetivo de oferecer diferentes resultados relativamente à vazão, atraso, *jitter* e perdas, é necessário que os pacotes recebam tratamento diferenciado.

Para testar os parâmetros de Qualidade de Serviço (QoS), são necessárias algumas entidades de teste. O transmissor introduz o tráfego de teste (iperf – cliente) de modo a emular a geração de tráfego por parte da aplicação. O receptor (iperf – servidor) consome o tráfego de teste e responde se necessário. Um monitor captura os fluxos de dados nos pontos de interesse para futura análise.

5.2 - Organização dos Testes

Este capítulo organiza os testes por grupo, baseado na estratégia apresentada anteriormente. Cada grupo começa com um breve comentário sobre os testes, seguido por uma série de blocos descritivos; cada bloco descreve um único teste. Cada bloco descritivo segue o seguinte formato:

Nome do Teste: O nome do teste é formado pela concatenação da sigla do teste. O número do grupo e o número de teste dentro do grupo, separados por (.). Dessa forma, o teste CON1.2 se refere ao segundo teste do primeiro grupo dentro do conjunto CONECTIVIDADE. O número do teste é 1.2

Propósito: O propósito é uma sentença curta descrevendo o objetivo do teste. Descreve sucintamente a funcionalidade ou capacidade a ser testada.

Test Setup: Descreve a configuração de todos os equipamentos antes do início do teste. Se o valor de um dado parâmetro de protocolo não for especificado, o valor default do protocolo será usado para o parâmetro.

Procedimento: Contém instruções passo-a-passo para a execução do teste. Os passos incluem itens como: habilitar interfaces, desconectar equipamento da rede ou enviar pacotes de uma estação de teste. O procedimento de teste também sugere que o testador faça observações que são interpretadas de acordo com os resultados observáveis para aquela seção de teste.

Dados a serem registrados: Relaciona as informações a serem coletadas e registradas durante a execução dos testes.

5.3 – Recursos utilizados

Hardware:

- 3 Agregadores (PE)
- 3 Roteadores Cisco 827 (CE) – Acessos ADSL
- 2 Roteadores Cisco 827-4V – Teste de VoIP
- 2 Laptops com Windows 2000 ou XP, com placa Ethernet 10/100

Software:

- Gerador de tráfego - Iperf

Os hardware e software são utilizados para os testes de conectividade, isolamento (figura 5.1) e QoS (figura 5.2).

5.4 – A topologia para o teste de conectividade e isolamento está representada na figura abaixo

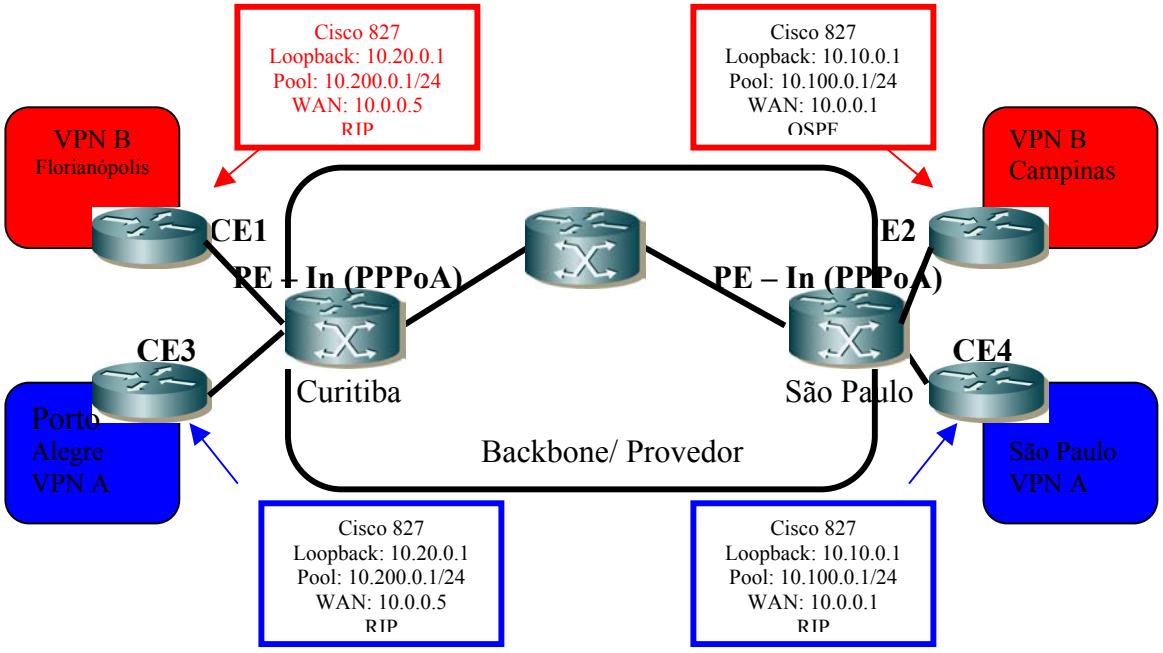

Figura 5.1 – Topologia para teste de conectividade e isolamento

Procedimento:

Configurar os agregadores PEs e roteadores Cisco 827, conforme scripts de configuração definidos previamente.

5.5 – Grupo 1 : Conectividade

5.5.1 – Teste CON1.1 – Conectividade IntraVPN

Propósito: Testar conectividade entre pontos de uma mesma VPN (figura 5.1). Nos testes, basicamente, tem-se um cenário de duas VPNs (VPN A e VPN B). Os testes foram realizados por meio dos comandos ICMP.

Procedimento:

1 – A partir de cada CE, tentar enviar mensagens de PING para os endereços IP de loopback[23] dos outros CEs na mesma VPN. Será executado este passo para as duas VPNs.

[23] Os endereços de loopback aqui utilizado é para o teste, normalmente em ambiente de produção da rede o backbone MPLS não permite o transporte de endereços loopback. Essa é uma estratégia que depende de cada provedor.

Dados a serem registrados:

- Capturar log com resultado dos pings

Resultados obtidos:

```
612346962@vpn1#ping 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/153/156 ms

612346962@vpn1#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/149/156 ms
```

Conclusão do teste:

Um dos pontos fundamental em uma solução de VPN MPLS é que seja possível conectividade entre VPNs que utilizam inclusive os mesmo endereços (Os PEs de Curitiba e São Paulo apresentam duas VPNs com endereços iguais). Os resultados do teste mostram que existem conectividade entre os CEs da mesma VPN, mesmo que os endereços das duas VPNs sejam iguais (propositadamente) nos PEs.

5.5.2 – Teste CON1.2 – Isolamento de tráfego entre VPNs

Propósito: Verificar que existe isolamento de tráfego entre VPNs por meio da separação dos espaços de endereçamento e roteamento. Verificar que quando há duas VPNs no mesmo roteador PE o tráfego fica isolado. Em outras palavras, quando dois CEs com o mesmo espaço de endereço em VPNs diferentes, somente o CE na mesma VPN recebe o tráfego da fonte.

Procedimento:

Usando a configuração de base, verificar e capturar as seguintes informações a partir da console de cada roteador CE:

- Verificar que cada CE somente pode ter acesso a outros membros de sua VPN.

Dados a serem registrados:

- Capturar log com resultados.

Resultados Obtidos:

VPN A (10.20.0.1) tenta se conectar com o CE2 (10.0.0.1)

```
d:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

VPN A (10.20.0.1) tenta se conectar com o (10.10.0.1)

```
d:\>ping 10.10.0.1

Pinging 10.10.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Conclusão do teste:

Nesse teste de VPN MPLS foi mostrado a sua capacidade de separação de endereçamento e roteamento. A única possibilidade de ter acesso em outra VPN por meio de um núcleo MPLS é se esse está configurado devidamente para isso (exemplo são as configurações Extranet). No primeiro PING, tentou-se conectar ao endereço da interface WAN do roteador CE2. No segundo PING o objetivo era chegar ao endereço loopback, mas nenhum dos objetivos foi alcançado. Quando o ping foi gerado da VPN1 para a VPN2, foi medido na VPN1 se a mesma não recebia os mesmos endereços destinos. Certificando que os planos de endereços estão completamente isolados.

5.6 – Grupo 2 : Teste de Qualidade de Serviço (QoS)

5.6.1 – Teste QoS2.1: Avaliação de QoS no CE (Cisco 827)

A razão de realizar os testes de QoS também no CE, é porque na estratégia proposta os pacotes são classificados a partir do CE, e não como as VPNs MPLS tradicionais, onde os pacotes são classificados somente no PE.

Propósito: Avaliar o comportamento dos parâmetros de QoS para as classes de serviço Voz (EF), Missão Crítica (AF11), Suporte ao Negõcio (AF31) e Dados Melhor Esforço (BE), implementados no CE cisco 827, na presença de uma demanda de tráfego superior à banda nominal disponível no acesso. Ou seja, o teste deve mostrar que os pacotes classificados como EF tenham prioridade em relação às classes AF e BE; que AF11 tenha prioridade em relação ao AF31 e BE; e finalmente que AF31 seja prioritário em relação aos pacotes BE.

Para esses testes foram utilizados os seguintes componentes:

- Gerador de tráfego

Nesse tipo de teste específico, é usado o Iperf (www.iperf.com), instalado nas máquinas geradora e receptora.

- Unidades de Capturas

As unidades de capturas serão os monitores dos 2 computadores, onde serão gerados o tráfego e os arquivos com todos os logs capturados.

Test Setup:

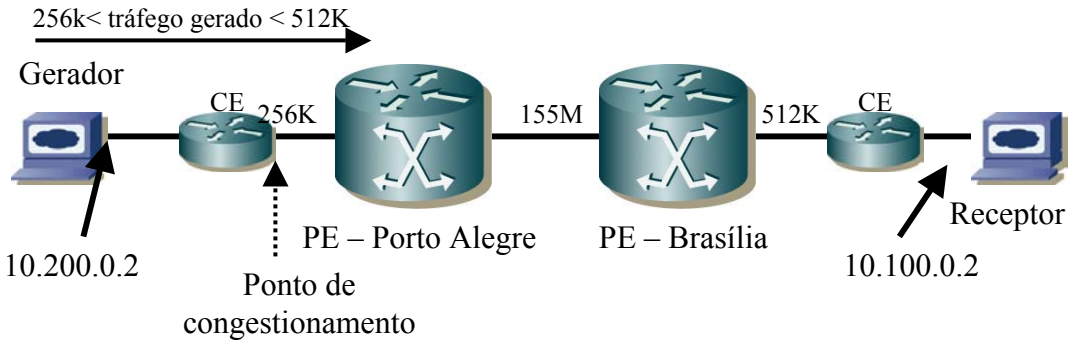

Figura 5.2 – Topologia para o teste de QoS do CE

Procedimento:

Gerar fluxos de tráfego para cada classe de serviço de acordo com a tabela 5.1. Nessa tabela, a banda configurada refere-se ao CE; tráfegos gerados, tamanhos de pacote, protocolo e porta são parâmetros de entrada do Iperf (gerador).

Dados a serem registrados:

- Valores dos parâmetros de QoS – Vazão, atraso, perdas de pacotes e jitter.

Será mostrado, a título de exemplo, o procedimento para capturar os dados da classe voz no caso do cenário 1. Para os demais cenários e classes foram realizados os mesmos procedimentos, sendo plotados somente os gráficos.

Ex:

- Configurar o servidor iperf para o fluxo UDP no computador de Porto Alegre.

  Receptor: Iperf –s –u – p5001 – b54k
- Configurar o cliente iperf para o fluxo UDP no computador de Brasília

  Gerador: Iperf –c10.200.0.2 –u –p5001 –b54k

```
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[132] local 10.100.0.2 port 5001 connected with 10.200.0.2 port 1247
[ ID] Interval       Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[132]  0.0- 1.0 sec  3.57 KBytes  29.3 Kbits/sec  16.318 ms 8274/ 8335 (99%)
[132]  1.0- 2.0 sec  3.69 KBytes  30.2 Kbits/sec  15.922 ms    0/   63 (0%)
[132]  2.0- 3.0 sec  3.69 KBytes  30.2 Kbits/sec  16.225 ms    0/   63 (0%)
[132]  3.0- 4.0 sec  3.69 KBytes  30.2 Kbits/sec  16.857 ms    0/   63 (0%)
[132]  4.0- 5.0 sec  3.63 KBytes  29.8 Kbits/sec  15.527 ms    0/   62 (0%)
[132]  5.0- 6.0 sec  3.69 KBytes  30.2 Kbits/sec  15.283 ms    0/   63 (0%)
[132]  6.0- 7.0 sec  3.63 KBytes  29.8 Kbits/sec  16.863 ms    0/   62 (0%)
[132]  7.0- 8.0 sec  3.69 KBytes  30.2 Kbits/sec  15.915 ms    0/   63 (0%)
[132]  8.0- 9.0 sec  3.63 KBytes  29.8 Kbits/sec  19.394 ms    0/   62 (0%)
[132]  9.0-10.0 sec  3.69 KBytes  30.2 Kbits/sec  19.555 ms    0/   63 (0%)
[132] 10.0-11.0 sec  3.75 KBytes  30.7 Kbits/sec  18.660 ms    0/   64 (0%)
[132] 11.0-12.0 sec  3.63 KBytes  29.8 Kbits/sec  18.357 ms    0/   62 (0%)
[132] 12.0-13.0 sec  3.63 KBytes  29.8 Kbits/sec  19.826 ms    0/   62 (0%)
[132] 13.0-14.0 sec  3.63 KBytes  29.8 Kbits/sec  19.300 ms    0/   62 (0%)
[132] 14.0-15.0 sec  3.63 KBytes  29.8 Kbits/sec  19.484 ms    0/   62 (0%)
[132] 15.0-16.0 sec  3.69 KBytes  30.2 Kbits/sec  18.311 ms    0/   63 (0%)
[132] 16.0-17.0 sec  3.69 KBytes  30.2 Kbits/sec  18.257 ms    0/   63 (0%)
[132] 17.0-18.0 sec  3.69 KBytes  30.2 Kbits/sec  18.347 ms    0/   63 (0%)
[132] 18.0-19.0 sec  3.57 KBytes  29.3 Kbits/sec  18.470 ms    0/   61 (0%)
[132] 19.0-20.0 sec  3.75 KBytes  30.7 Kbits/sec  17.999 ms    0/   64 (0%)
```

Tabela 5.2 – Resultados de saída do Iperf que estão plotados na figura 5.3

Considerações de siglas utilizadas nos gráficos: Missão Critica = M_C; Suporte ao Negócio = S_N; Bandwidth em Kbps= B.W; Jitter em ms= Jitter; Loss em %= Loss.

A escala de tempo foi omitida dos gráficos em função de ser a mesma para todos os gráficos. Os valores variam de 1 a 50 segundos em intervalos de 1 segundo.

Cenário 1:

Teste QoS2.1.1 – Teste de QoS2.1(CE) no cenário 1

- **Resultado obtido** para o tamanho dos pacotes de dados de 500Kb
  RTT=173ms

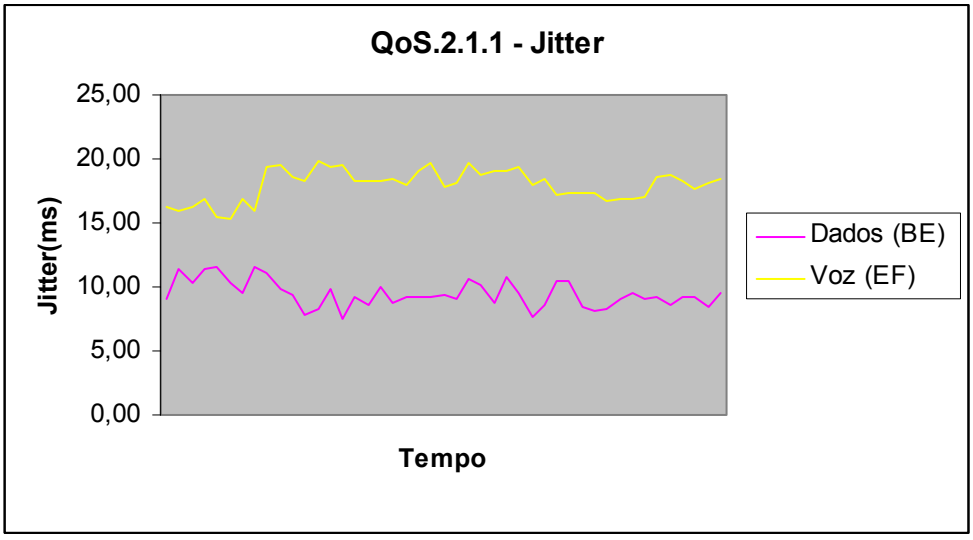

Figura 5.3 – QoS 2.1.1 - Jitter

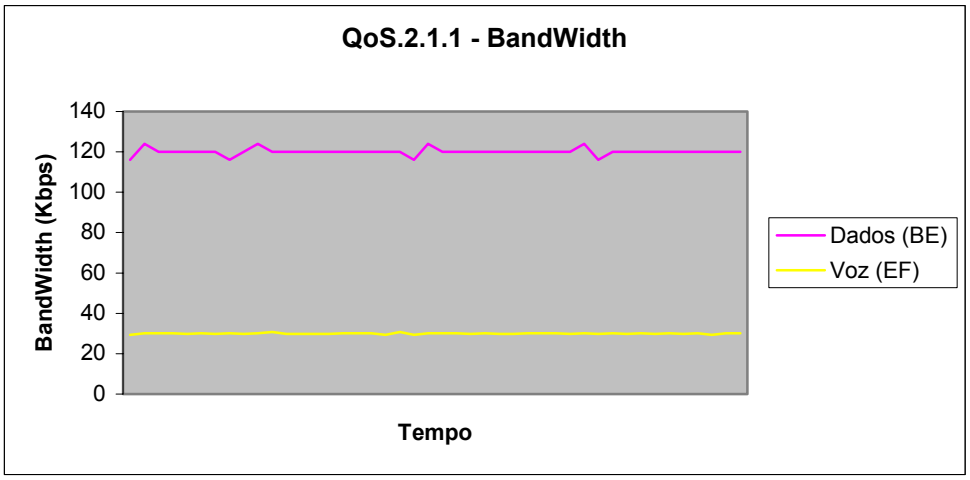

Figura 5.4 – QoS 2.1.1 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 byte RTT=199ms

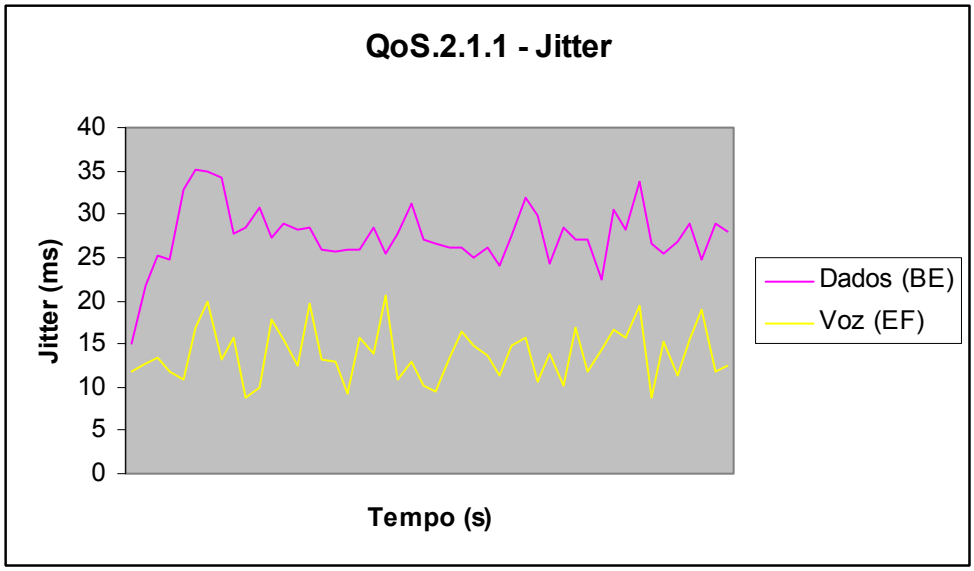

Figura 5.5 – QoS 2.1.1 - Jitter

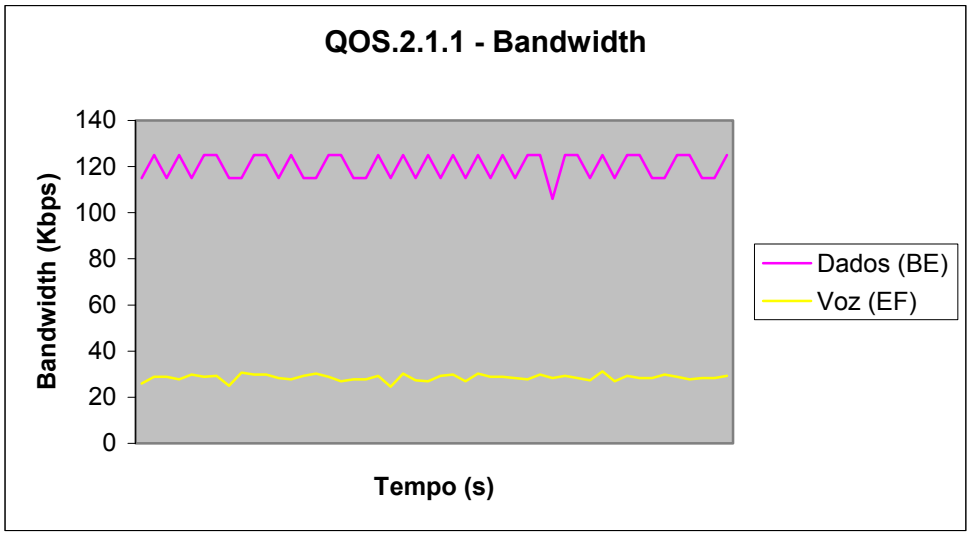

Figura 5.6 – QoS 2.1.1 - Bandwidth

Conclusão do cenário 1:

Os valores de vazão, atraso, jitter e perda de pacotes mantiveram-se em níveis normais, ou seja, em condições sem congestionamento o desempenho das aplicações não é prejudicado. Condições sem congestionamento é aquela em que a soma dos tráfegos gerados (30 + 120) pelas aplicações é menor que a soma no acesso (256Kbps). Os Valores de pacotes perdidos (loss) não foram apresentados nesse cenário, pois não houve perda de pacotes.

Cenário 2:

Teste QoS2.1.2 – Teste de QoS2.1(CE) no cenário 2

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes RTT=340ms

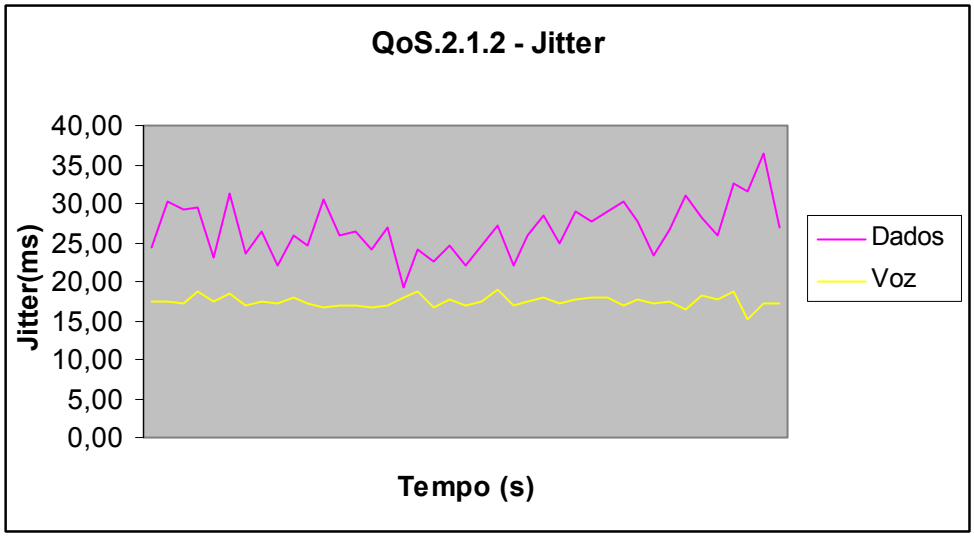

Figura 5.5 – QoS.2.1.2 - Jitter

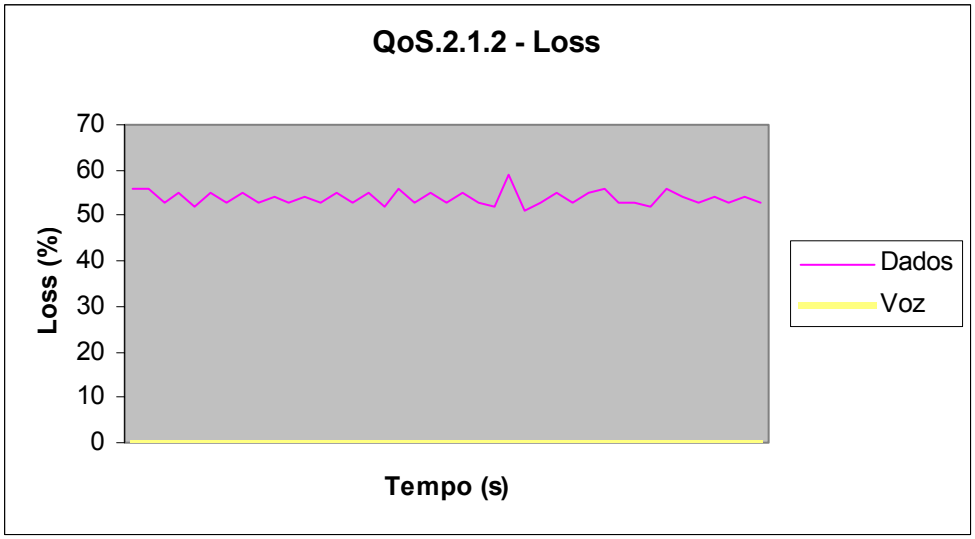

Figura 5.6 – QoS.2.1.2 - Loss

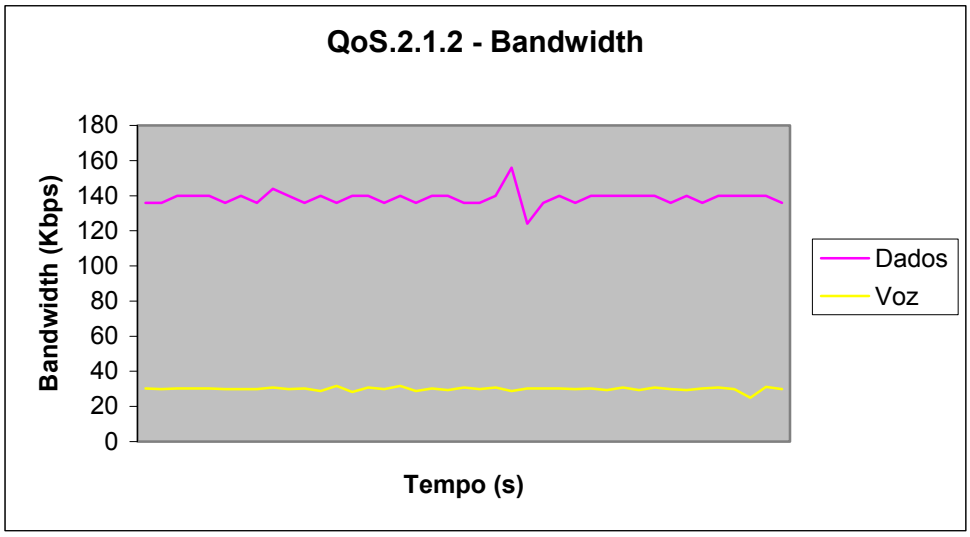

Figura 5.7 – QoS.2.1.2 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes RTT=405ms

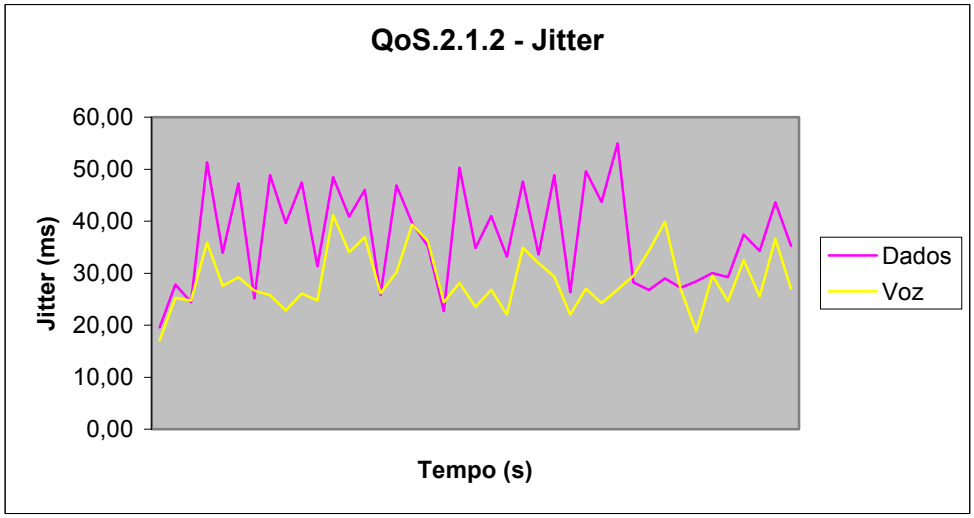

Figura 5.8 – QoS.2.1.2 – Jitter

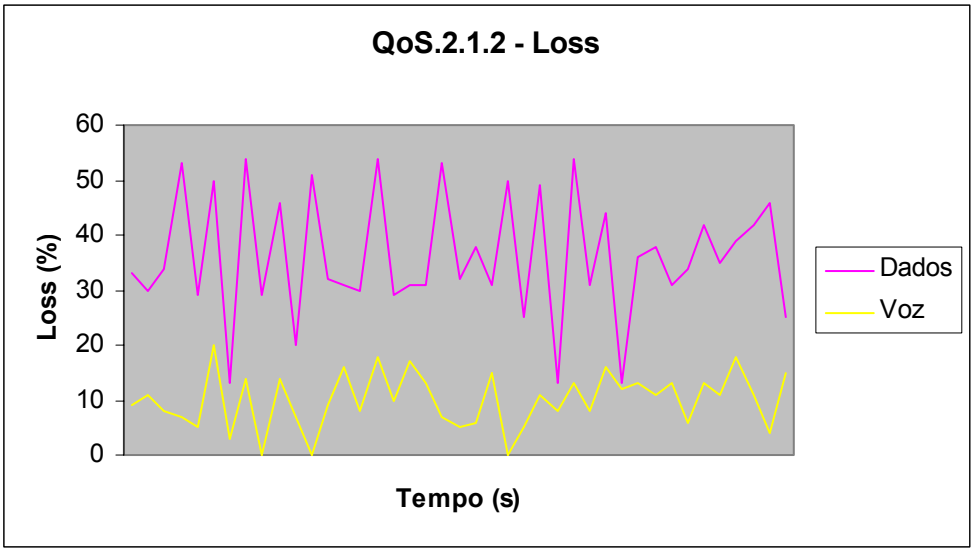

Figura 5.9 – QoS.2.1.2 – Loss

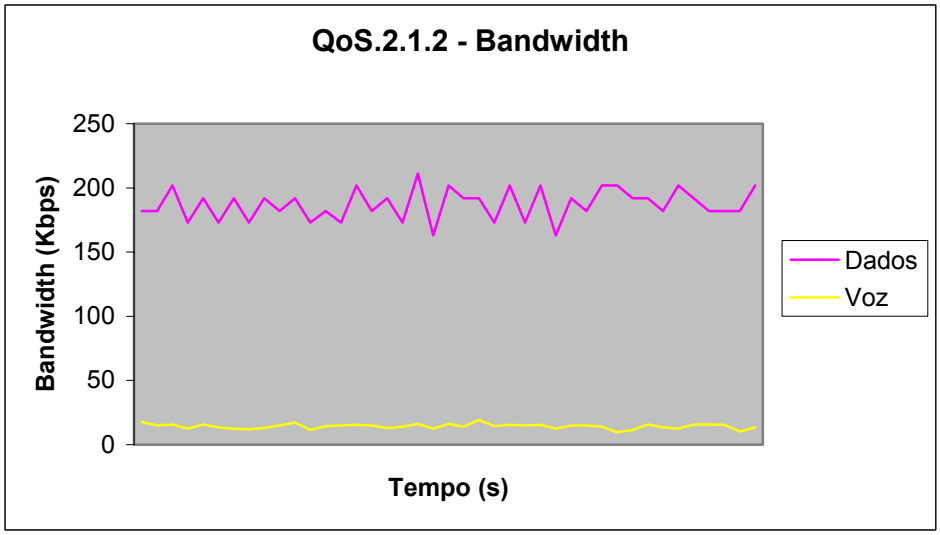

Figura 5.10 – QoS.2.1.2 - Bandwidth

Conclusão do Cenário 2:

Para pacotes de dados de 500 bytes, os valores de vazão, atraso, jitter e perda de pacotes se mantiveram em níveis aceitáveis para a classe VOZ (EF) e Dados mesmo numa situação de congestionamento, sendo uma situação de congestionamento aquela onde o tráfego gerado pelas aplicações (30 + 300) é maior que a velocidade de acesso (256).

Para pacotes de dados de 1200 bytes, nota-se uma diminuição da vazão, a ocorrência de perdas de pacotes e um aumento no jitter para a classe VOZ. Este fato é

conseqüência do tempo que o pacote (pequeno) de voz (60 bytes) tem que aguardar na fila enquanto um pacote (grande) de dados (1200 bytes) é transmitido. Rocomenda-se fortemente o uso de mecanismos de LFI (Fragmentação e Intercalação da Camada de Enlace) nos acessos para manter os valores de jitter em níveis que não prejudiquem a qualidade da comunicação de voz. Deve ser feito um ajuste fino no tamanho da fila de VOZ no 827(CE) e no PE para se reduzir as perdas de pacotes.

Cenário 3:

Teste QoS2.1.3 – Teste de QoS2.1 no cenário 3

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes
  RTT=181ms

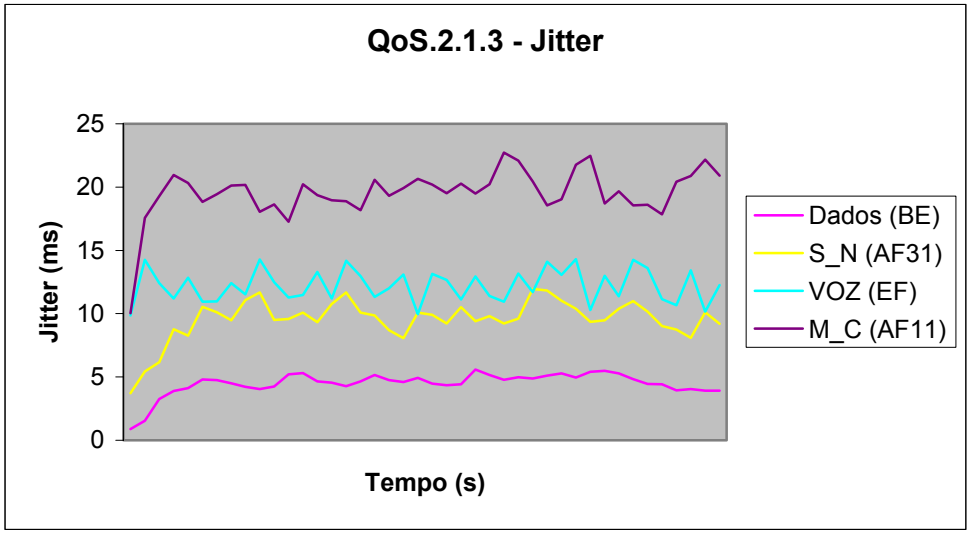

Figura 5.11 – QoS 2.1.3_Jitter

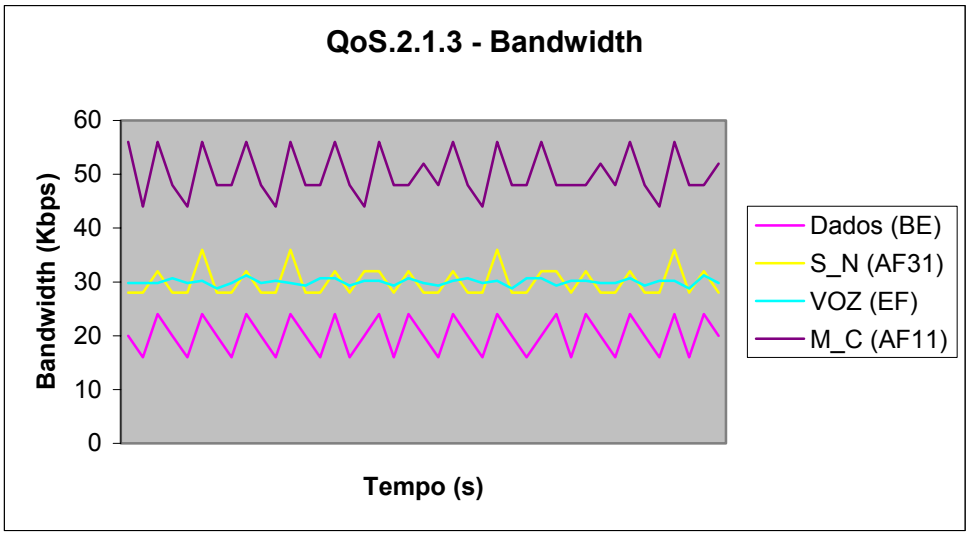

Figura 5.12 – QoS 2.1.3 – Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes RTT=207 ms

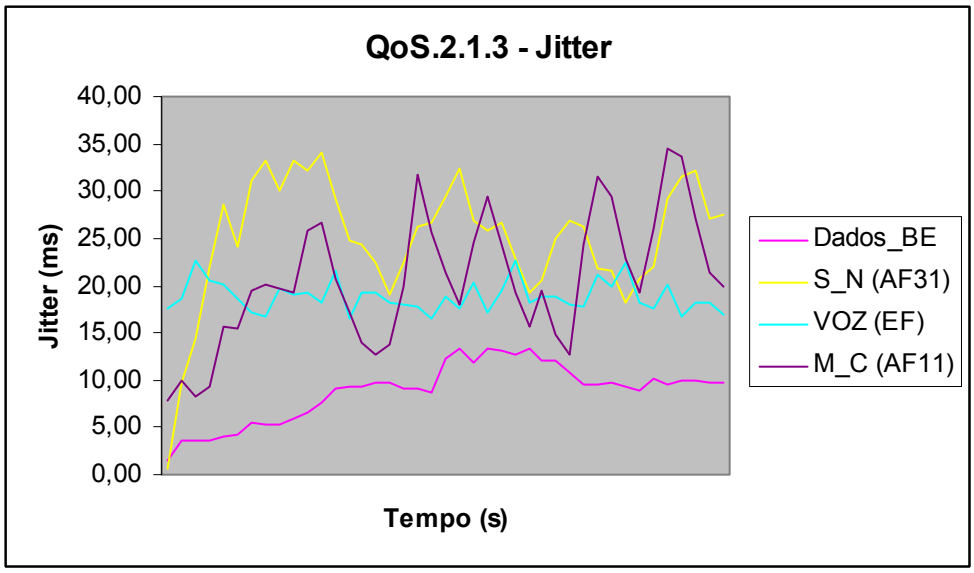

Figura 5.13 – QoS 2.1.3 – Jitter

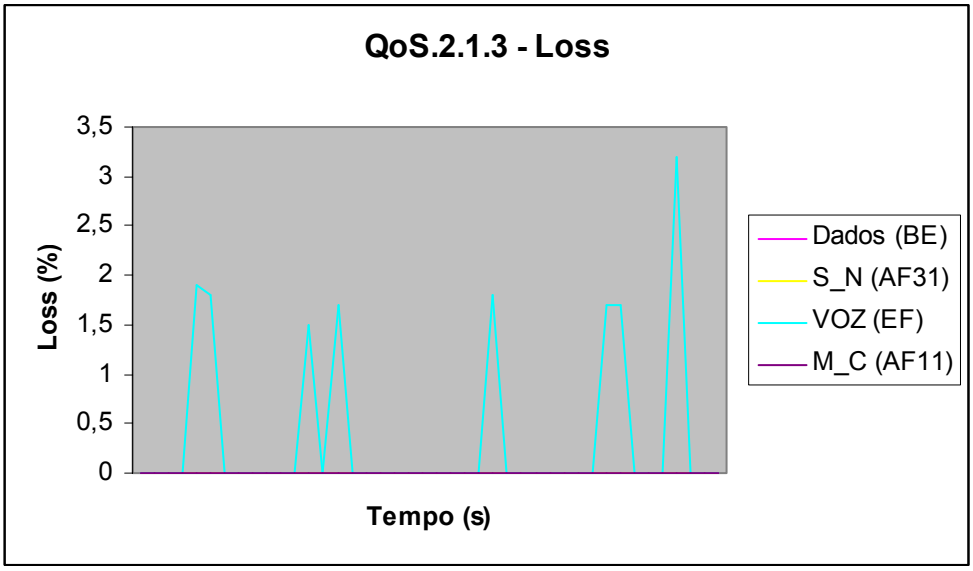

Figura 5.14 – QoS 2.1.3 – Loss

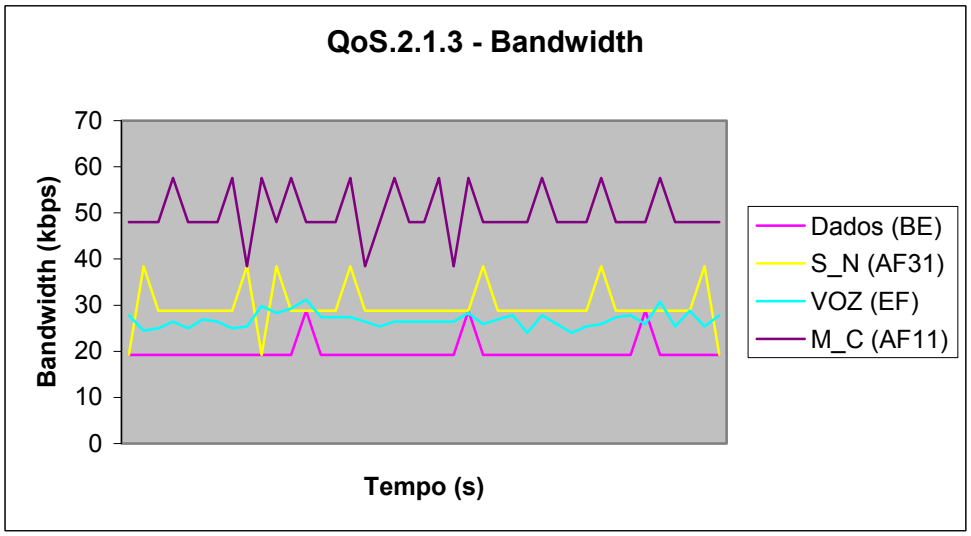

Figura 5.15 – QoS 2.1.3 – Bandwidth

Conclusão do cenário 3:

Os valores de vazão, atraso, jitter e perda de pacotes mantiveram-se em níveis normais para essa situação sem congestiomento. O jitter para a classe voz não ultrapassou os 15ms para o tamanho do pacote de 500 bytes e 20ms para 1200 bytes, esses valores são considerados muito bons para voz. Na prática o valor de até 30ms é considerado excelente. A bandwidth para os tamanhos de pacotes de 500 e 1200 bytes mantiveram na média os

mesmos valores do tráfego gerado. As perdas de pacotes foram mínimas para o tamanho de pacotes de 1200bytes, mas nada que possa preocupar.

Cenário 4:

Teste QoS2.1.4 – Teste de QoS2.1 no cenário 4

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes
  RTT=365ms

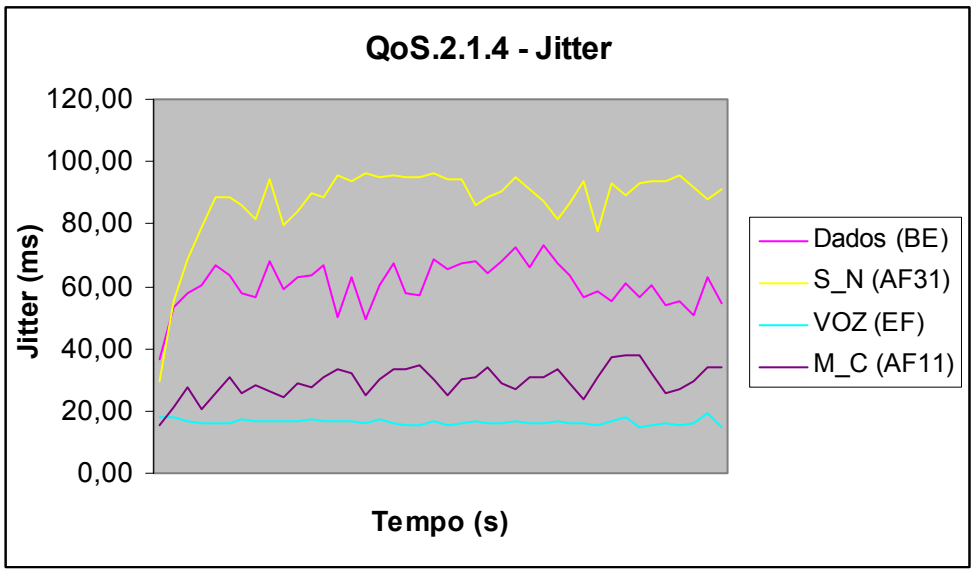

Figura 5.16 – QoS 2.1.4 - Jitter

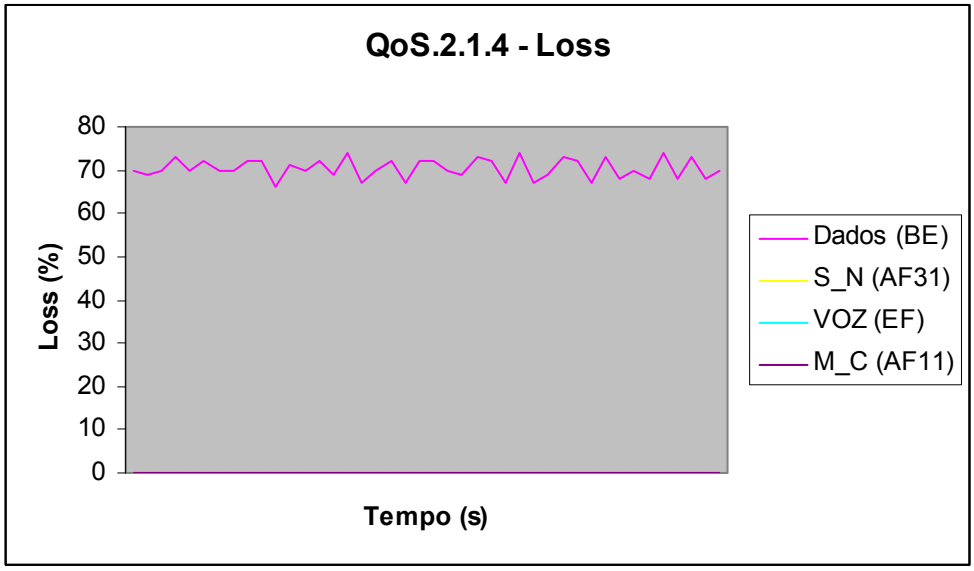

Figura 5.17 – QoS 2.1.4 - Loss

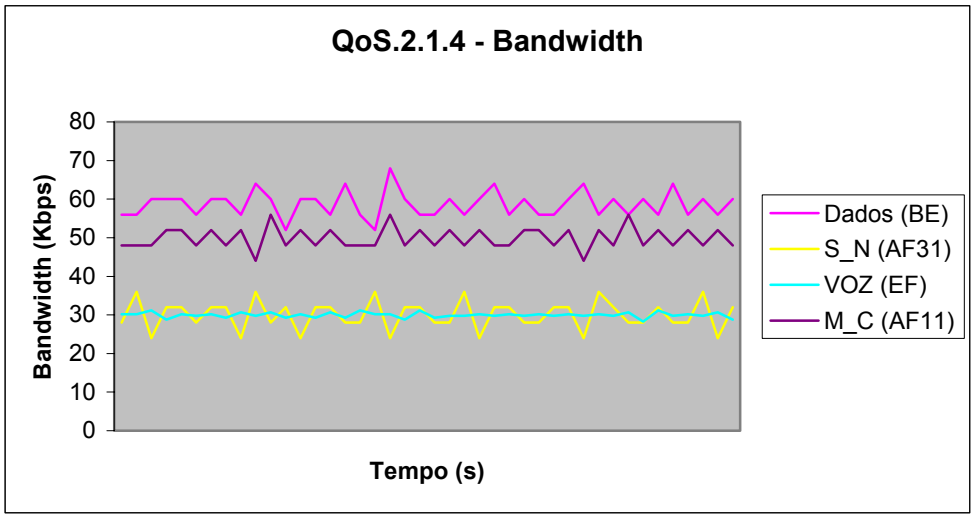

Figura 5.18 – QoS 2.1.4 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes RTT=700 ms

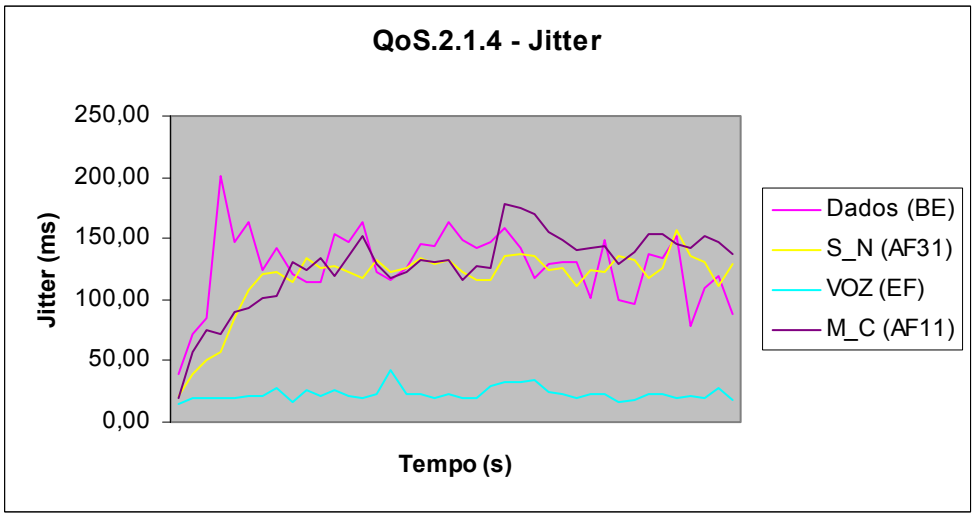

Figura 5.19 – QoS 2.1.4 - Jitter

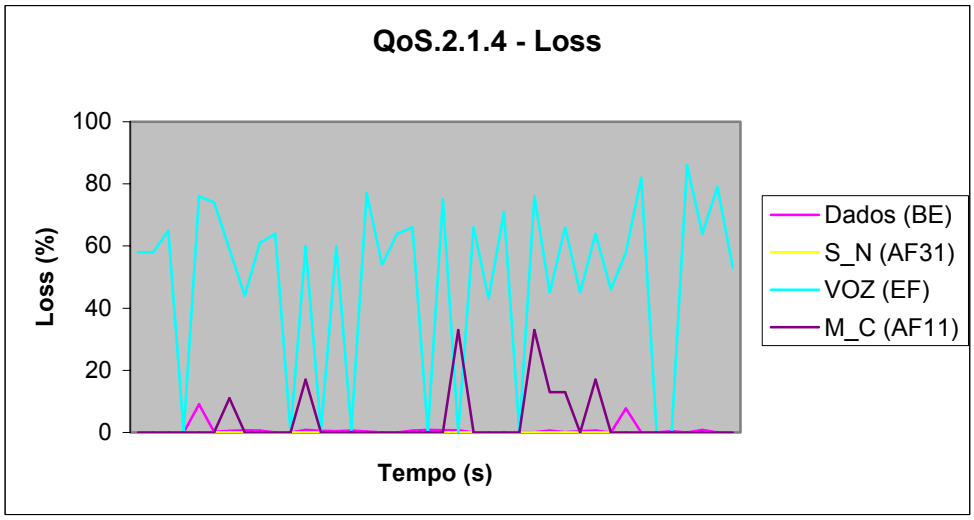

Figura 5.20 – QoS 2.1.4 - Loss

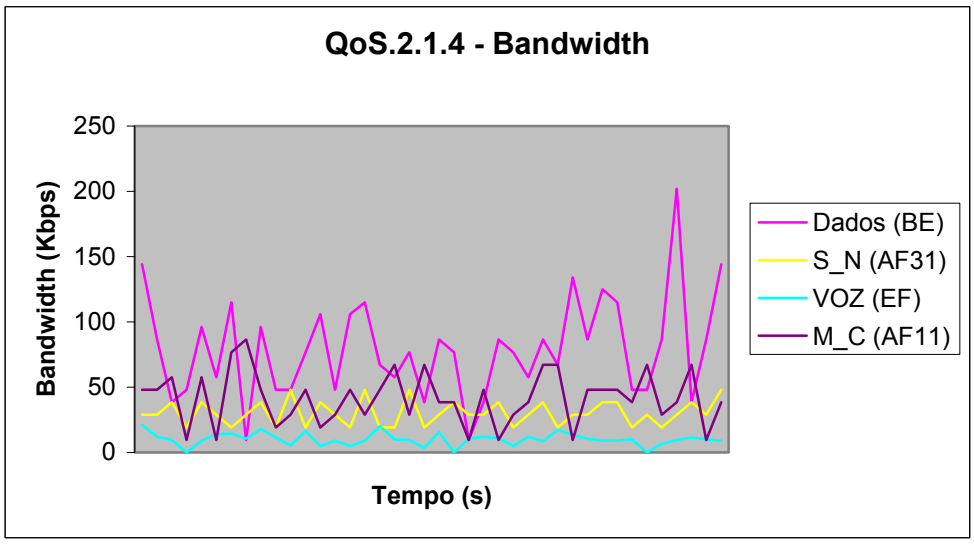

Figura 5.21 – QoS 2.1.4 - Bandwidth

Conclusão do Cenário 4:

Para pacotes de dados de 500 bytes, os valores de vazão, atraso, jitter e perda de pacotes se mantiveram em níveis aceitáveis para as classes, inclusive VOZ, mesmo numa situação de congestionamento. Ocorreu um aumento do RTT em relação ao cenário 3, pois o cenário 4 representa uma situação de congestionamento.

Para pacotes de dados de 1200 bytes, nota-se uma diminuição da vazão, a ocorrência de perdas de pacotes e um aumento no jitter para a classe VOZ. Este fato é conseqüência do tempo que o pacote (pequeno) de voz (60 bytes) tem que aguardar na fila

enquanto um pacote (grande) de dados (1200 bytes) é transmitido. Rocomenda-se fortemente o uso de mecanismos de LFI (Fragmentação e Intercalação da Camada de Enlace) nos acessos para manter os valores de jitter em níveis que não prejudiquem a qualidade da comunicação de voz e também deve ser feito um ajuste fino no tamanho da fila de VOZ no 827 (CE) e no PE para se reduzir as perdas de pacotes. Ou seja, o resultado desse cenário mostra que é necessário além de DiffServ alguns mecanismos extras para oferecer a qualidade de serviço a determinada aplicação

Relação entre a utilização da Bandwidth x RTT

Dado que a única componente do atraso fim a fim que pode se controlado é o atraso da fila, o suporte para diferentes classes de serviço é baseado no controle do tipo de atraso para diferentes classes de tráfegos durante período de congestionamento da rede. Na ausência de alguma técnica de gerenciamento de fila como RED (Random Early Detection), há uma relação direta entre a utilização da bandwidth e o atraso RTT em um enlace que é muito utilizado na prática. Se a utilização do enlace em um intervalo de 5 minutos[24] fica em torno de 10% da largura da banda, será mínima a perda de pacotes e o atraso RTT, porque o enlace estará subutilizada. Entretanto, no caso de um aumento da utilização da banda acima de 50% (figura 5.22) nesse mesmo intervalo de 5 minutos, o RTT médio apresentará um incremento exponencial.

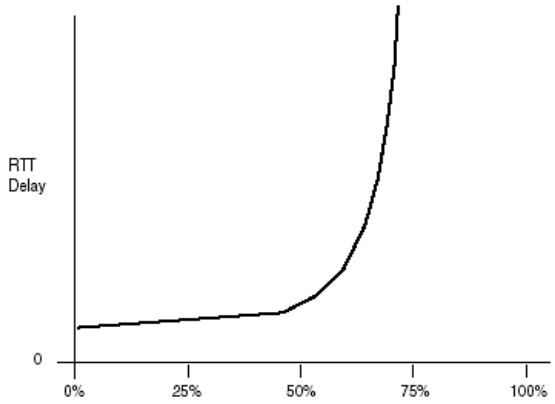

Figura 5.22 – RTT X Utilização durante uma amostragem de 5 minutos

Se o objetivo é otimizar a largura de banda e também gerenciar os atrasos das filas para tráfegos sensíveis a atraso, para encontrar a solução, primeiro deve-se determinar

[24] Com a medição durante 5 minutos, tem-se uma razoável amostragem, esse período de 5 minutos é usado na prática normalmente.

que aplicações na rede podem suportar o incremento e a variação do atraso. Aplicações baseadas em TCP são especialmente projetadas para serem adaptadas e suportarem atrasos, mas há outros tipos de aplicações, tais como voz em tempo real, que não estão habilitadas para operar com grandes atrasos e variação.

Portanto, a solução para melhor utilização da largura de banda e também o melhor controle do atraso da fila, é isolar a aplicação que não pode suportar atrasos de 50 a 60% de utilização. É possível realizar isso, substituindo os pacotes daquelas aplicações dentro de uma fila que não experimente o atraso causado pela alta utilização do circuito. É necessário identificar certo conjuntos de aplicações, isolar essas aplicações de outros tipos de tráfegos, substituí-las dentro de uma fila dedicada, e então controlar a quantidade de atraso por enfileiramentos dessas aplicações específicas.

A fragmentação dos pacotes diminui o desvio padrão dos pacotes manuseados pelas filas de saída, resultando na diminuição do tempo médio de enfileiramento do pacote e do desvio padrão deste tempo.

5.6.2 – Teste QoS2.2:Avaliação de QoS no Agregador (PE)

Propósito: Avaliar o comportamento dos parâmetros de QoS para as classes de serviço Voz (EF), Missão Crítica M_C (AF11), Suporte a Negócio S_N (AF31) e Melhor Esforço , implementadas no agregador **PE**, na presença de uma demanda de tráfego superior à banda nominal disponível no acesso. Ou seja, o teste deve mostrar que os pacotes classificados como EF tenham prioridade em relação a AF e BE; que AF11 tenha prioridade em relação ao AF31 e BE; e finalmente que AF31 seja prioritário em relação aos pacotes BE.

Test Setup:

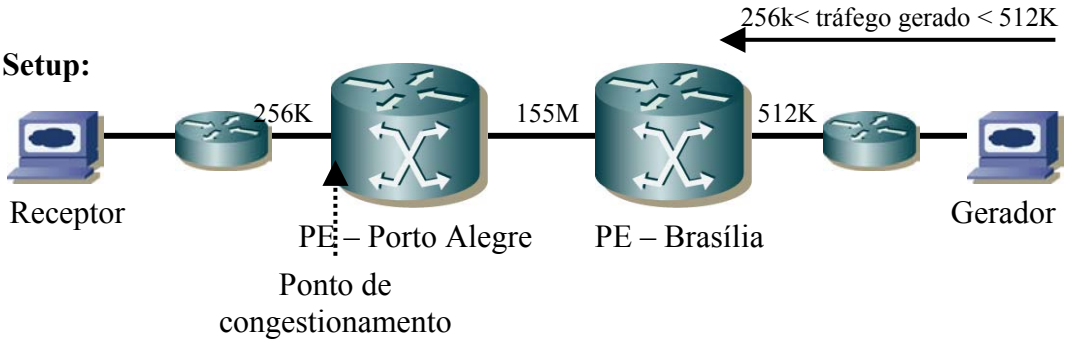

Figura 5.23 – Topologia para o teste de QoS do PE

Procedimento: Gerar fluxos de tráfego para cada classe de serviço de acordo com a tabela a seguir. Cada teste deverá ser executado com tamanhos de pacote de 500 a 1200 bytes para

as classes de serviço, Missão Crítica M_C (AF4) , Suporte a Negócio S_N (AF2) e Dados best effort (BE). A classe voz sempre terá o tamanho fixo em 60bytes.

Cenário	Classe de serviço	Banda Configurada (Kbps)	Tráfego Gerado (Kbps)	Tamanho Pacote (bytes)	Protocolo	Porta
1	Voz (EF)	34	30	60	UDP	5001
	Missão crítica (AF11)	-	-	-	-	-
	Suporte a negócio (AF31)	-	-	-	-	-
	Dados (BE)	350	150	500	UDP	5004
				1200		
2	Voz (EF)	34	30	60	UDP	5001
	Missão crítica (AF11)	-	-	-	-	-
	Suporte a negócio (AF31) – S_N	-	-	-	-	-
	Dados (BE)	350	300	500	UDP	5004
				1200		
3	Voz (EF)	34	30	60	UDP	5001
	Missão crítica (AF11)	80	40	500	UDP	5002
				1200		
	Suporte a negócio (AF31)	80	40	500	UDP	5003
				1200		
	Dados (BE)	190	80	500	UDP	5004
				1200		
4	Voz (EF)	54	30	200	UDP	5001
	Missão crítica (AF11)	80	40	500	UDP	5002
				1200		
	Suporte a negócio (AF31)	80	40	500	UDP	5003
				1200		
	Dados (BE)	170	300	500	UDP	5004
				1200		

Tabela 5.3 – Parâmetros por classes de Serviços

Dados a serem registrados:

- Valores dos parâmetros de QoS – Vazão, atraso, perda de pacotes e jitter.

Considerações: Missão Critica = M_C; Suporte ao Negócio = S_N.

Cenário 1:

Teste QoS2.2.1 – Teste de QoS2.2(PE) no cenário 1

- **Resultado obtido** para o tamanho dos pacotes de dados de 500bytes RTT=160ms

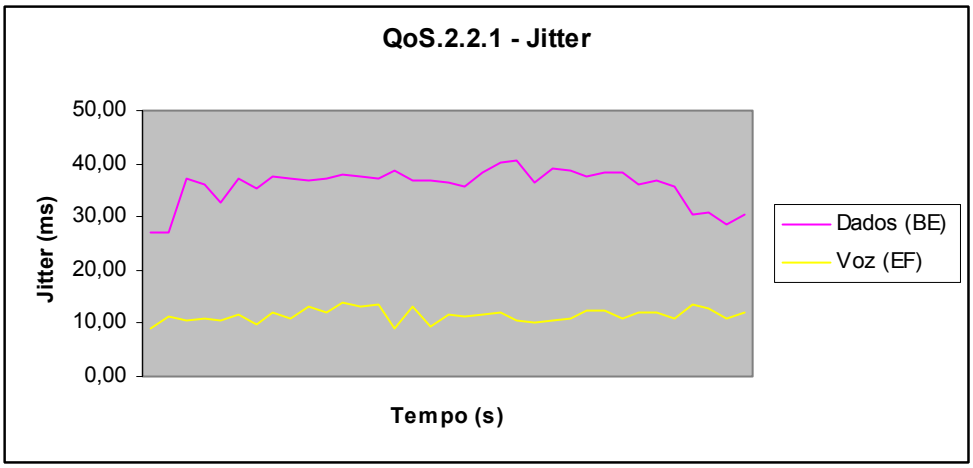

Figura 5.24 – QoS.2.2.1_Jitter

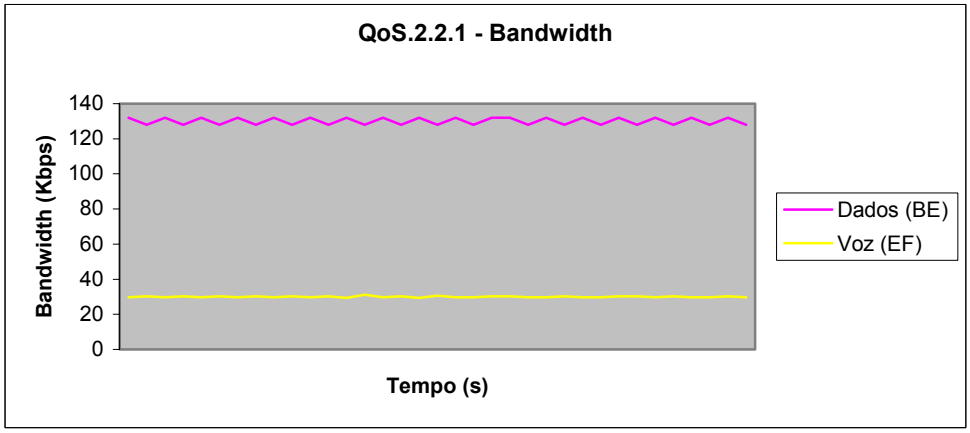

Figura 5.24 – QoS 2.2.1 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes

RTT=173ms

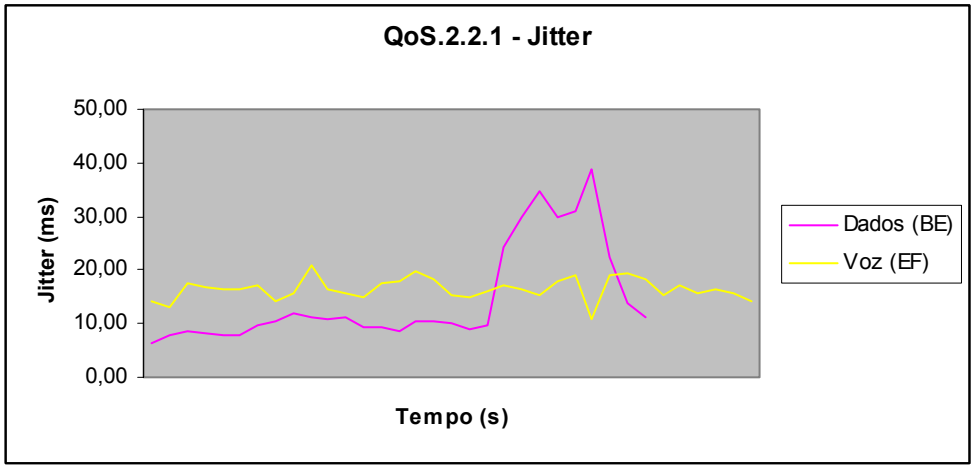

Figura 5.25 – QoS 2.2.1 - Jitter

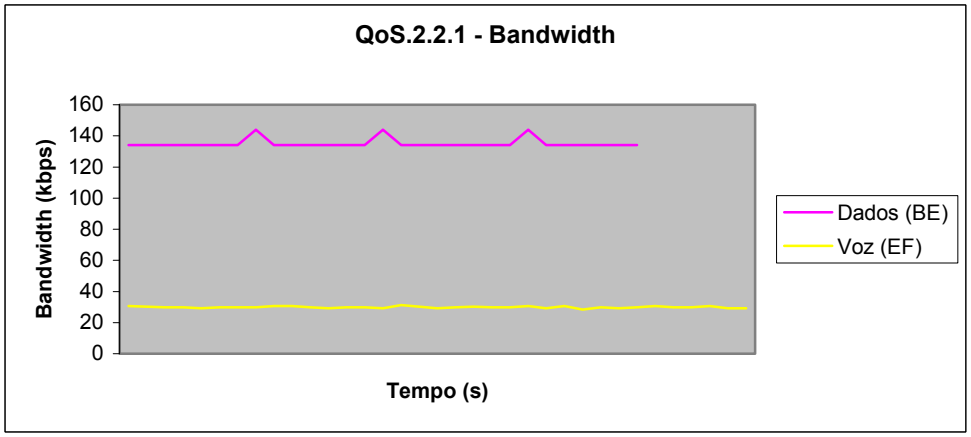

Figura 5.26 – QoS 2.2.1 - Bandwidth

Conclusão do Cenário 1 – Os valores de vazão, jitter, atraso e perdas de pacotes se mantiveram em níveis normais para a situação sem congestionameto. Não ocorreu nenhuma perda de pacotes para esse cenário. O RTT se manteve com valores aceitáveis para vários tamanhos de pacotes.

Cenário 2:

Teste QoS2.2.2 – Teste de QoS2.2(PE) no cenário 2

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes
  RTT=167ms

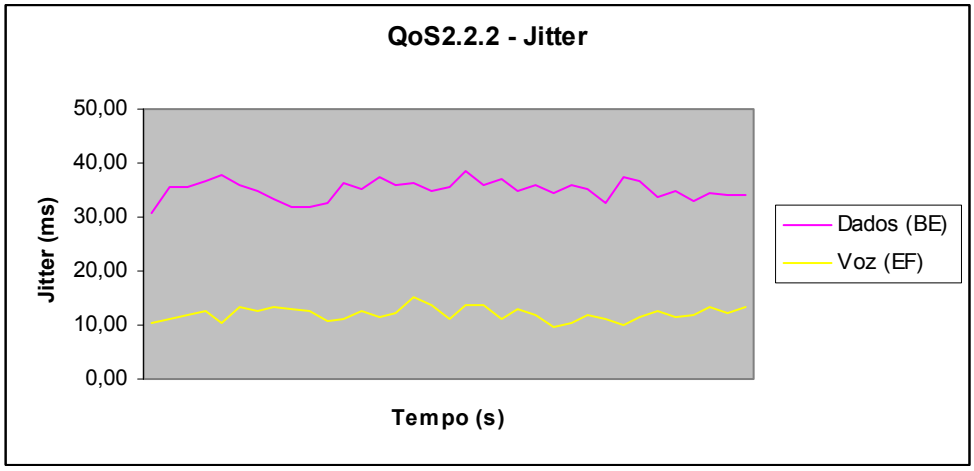

Figura 5.27 – QoS 2.2.2_Jitter

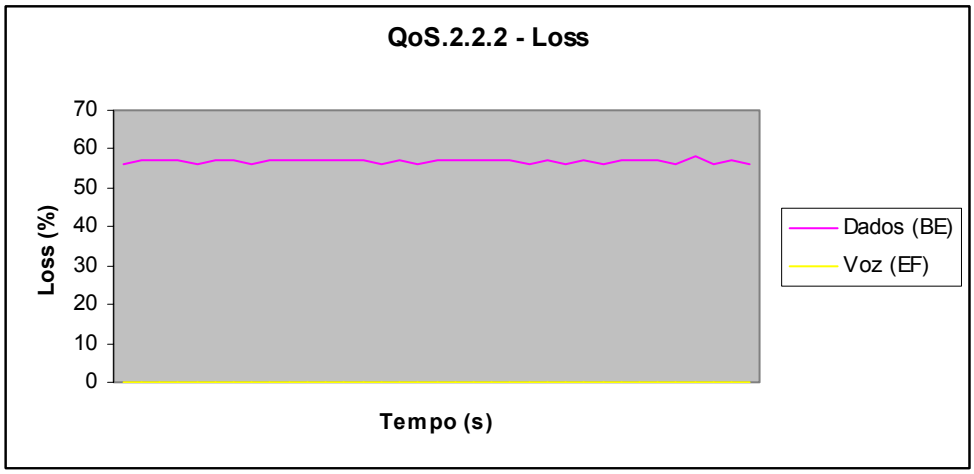

Figura 5.28 – QoS 2.2.2 - Loss

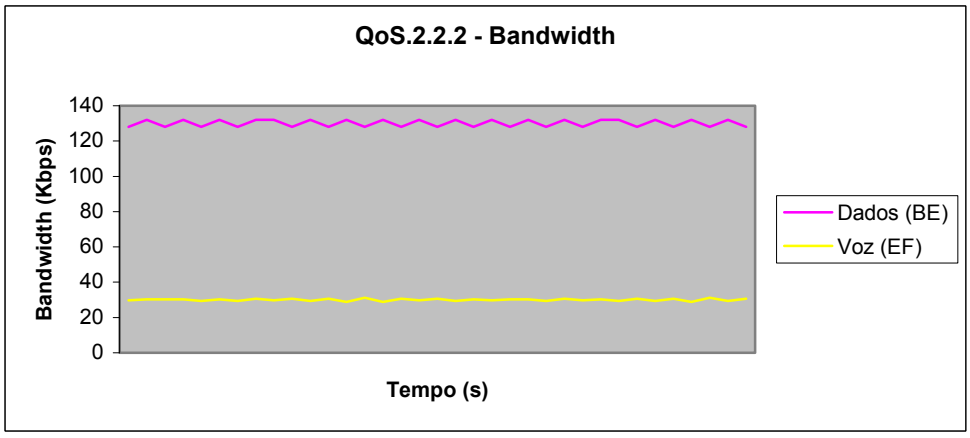

Figura 5.29 – QoS 2.2.2 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200bytes RTT=200 ms

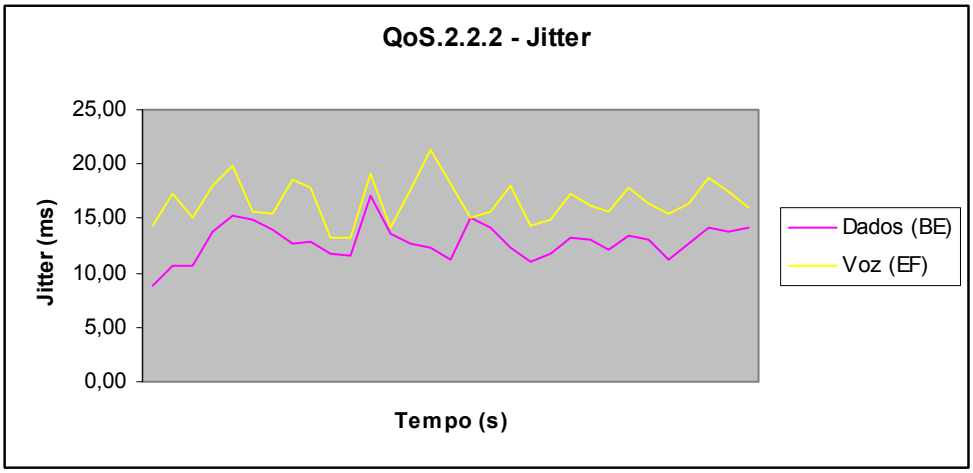

Figura 5.30 – QoS 2.2.2 - Jitter

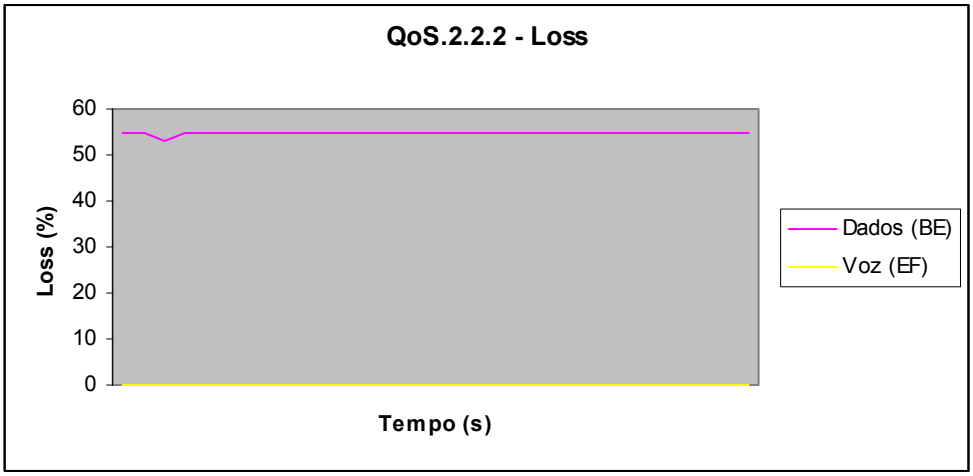

Figura 5.31 – QoS 2.2.2 - Loss

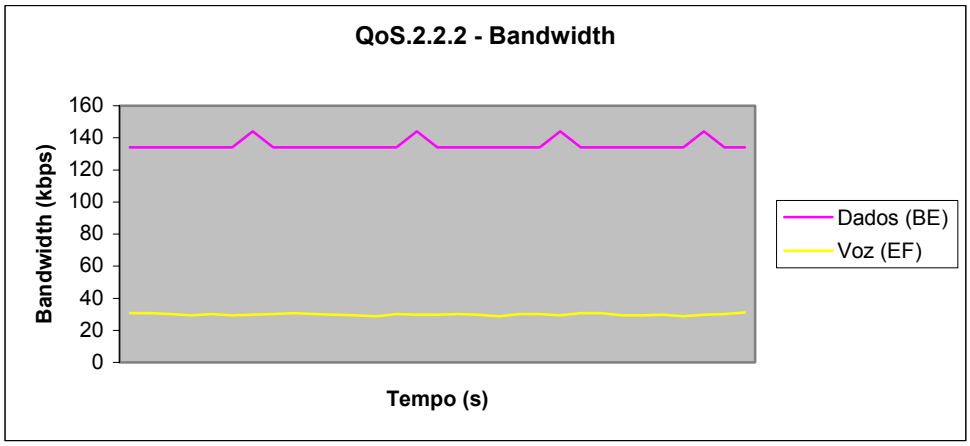

Figura 5.32 – QoS 2.2.2 – Bandwidth

Conclusão do cenário 2: Os valores de vazão, atraso, jitter e perdas de pacotes se mantiveram em níveis normais para a classe VOZ, mesmo em situação de congestionamento. Não ocorreu nenhuma de perda de pacotes (loss) para a classe voz nas situações em que houve variação do tamanho dos pacotes.

Cenário 3:

Teste QoS2.2.3 – Teste de QoS2.2 no cenário 3

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes
  RTT=172 ms

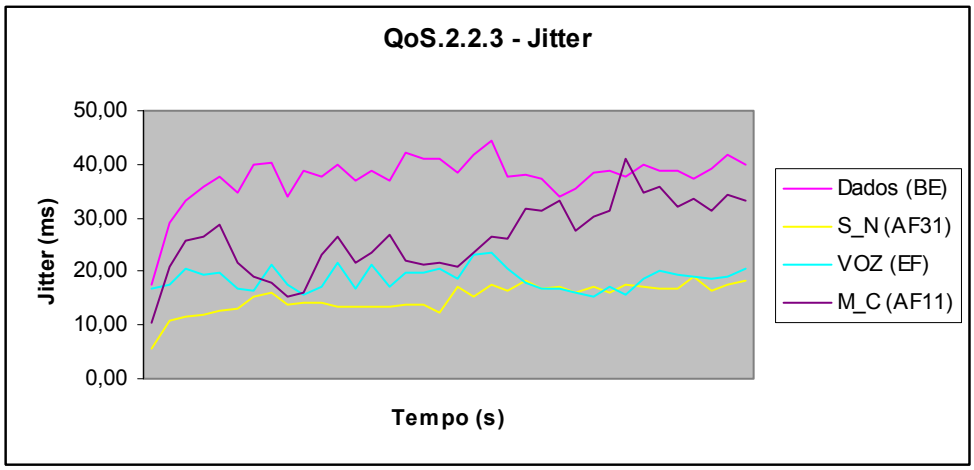

Figura 5.33 – QoS 2.2.2 - Jitter

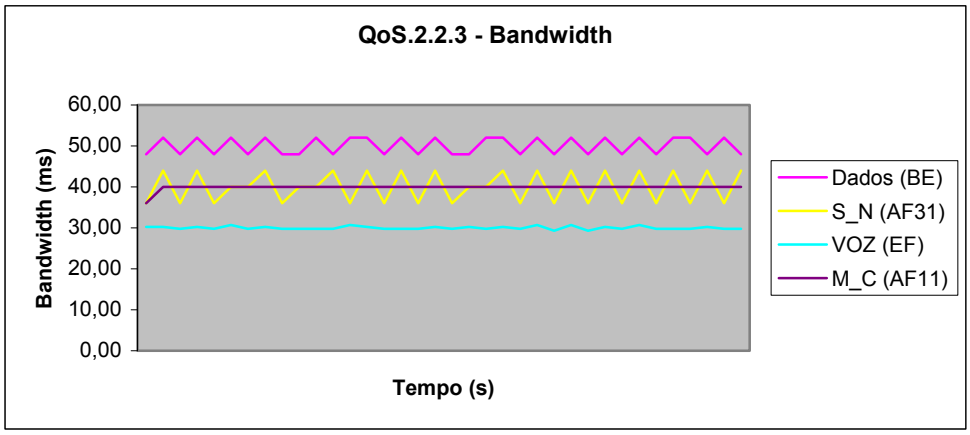

Figura 5.34 – QoS 2.2.2 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes RTT=195 ms

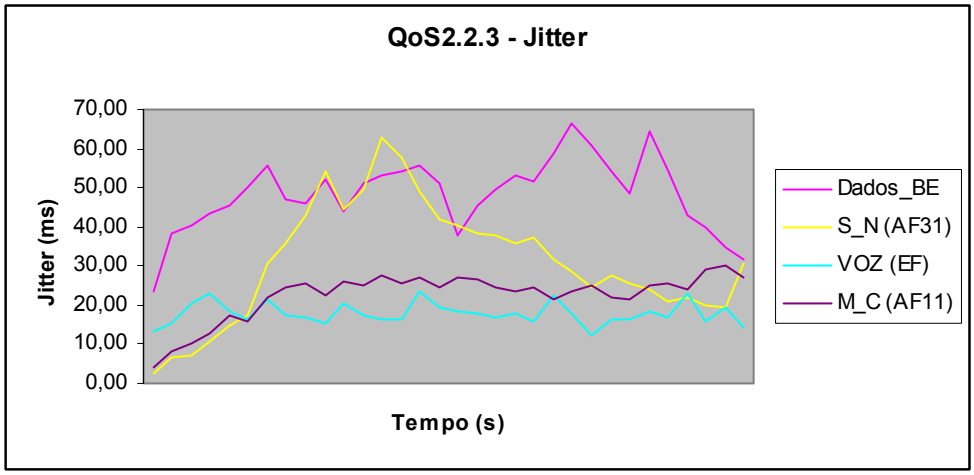

Figura 5.35 – QoS 2.2.2 - Jitter

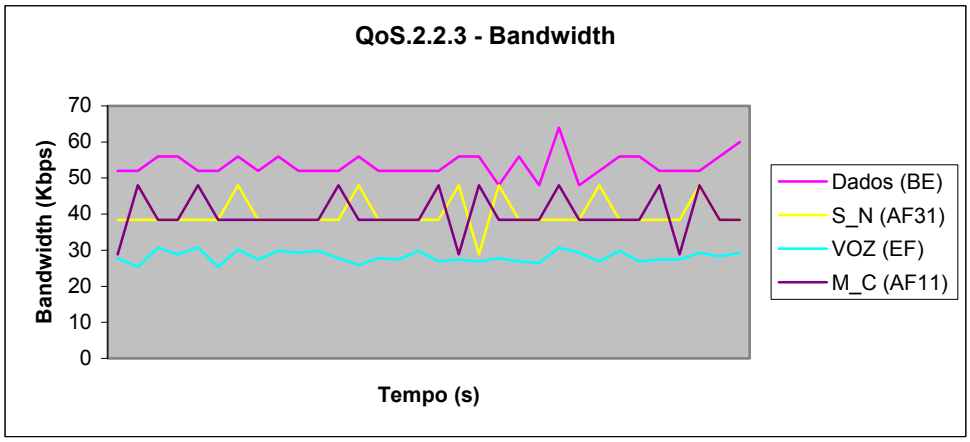

Figura 5.36 – QoS 2.2.3 - Bandwidth

Conclusão do Cenário 3: Os valores de vazão, atraso, jitter e perdas de pacotes se mantiveram em níveis normais. Não ocorreu nenhuma perda de pacotes para as quatro classes nesse cenário.

Cenário 4:

Teste QoS2.2.4 – Teste de QoS2.2(PE) no cenário 4

- **Resultado obtido** para o tamanho dos pacotes de dados de 500 bytes
  RTT=290 ms

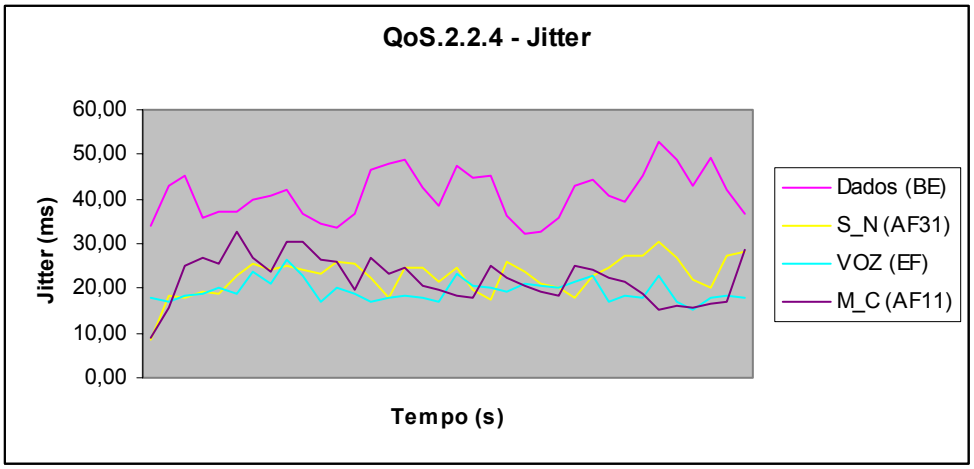

Figura 5.37 – QoS 2.2.4 - Jitter

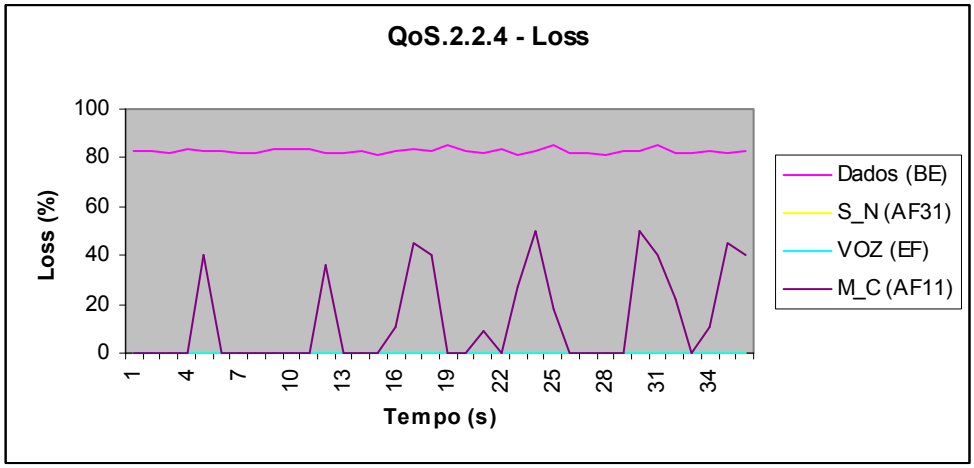

Figura 5.38 – QoS 2.2.4 - Loss

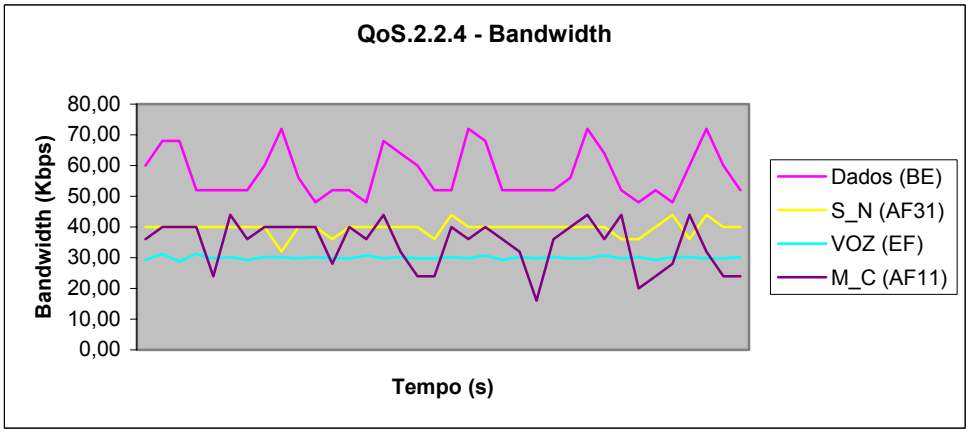

Figura 5.39 – QoS 2.2.4 - Bandwidth

- **Resultado obtido** para o tamanho dos pacotes de dados de 1200 bytes RTT=400 ms

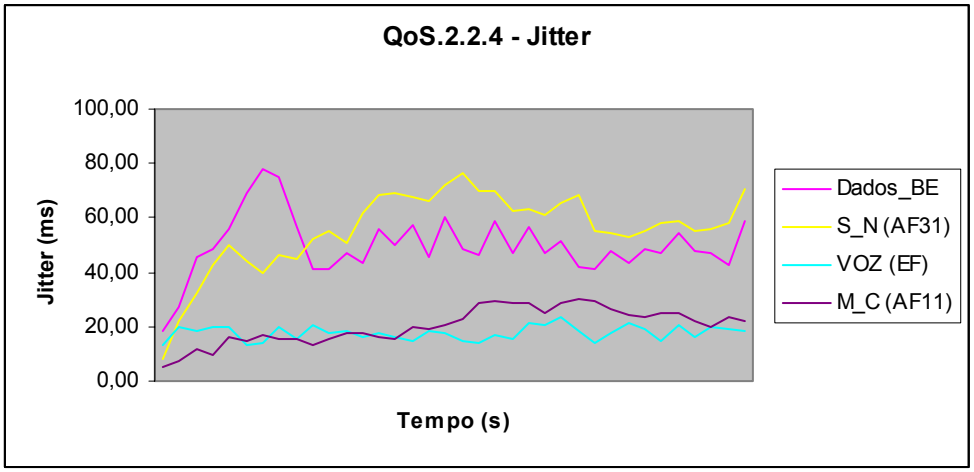

Figura 5.40 QoS.2.2.4 - Jitter

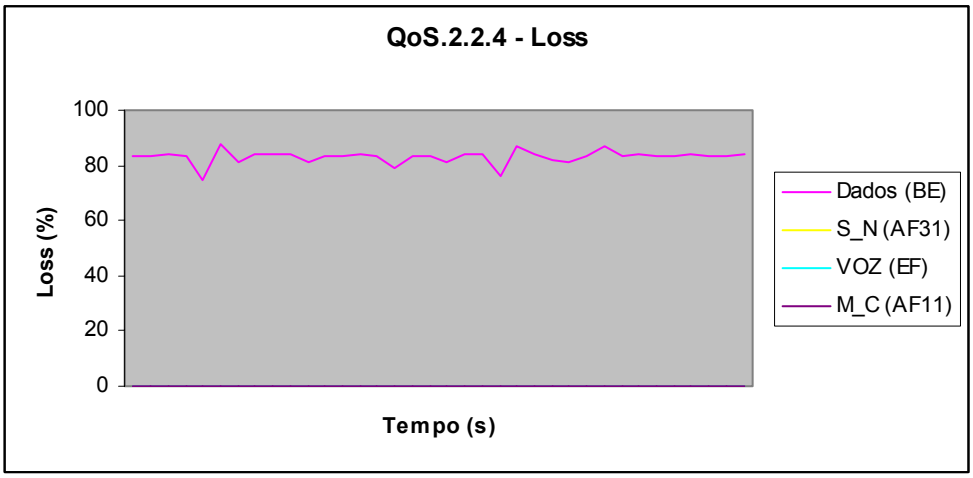

Figura 5.41 – QoS 2.2.4 - Loss

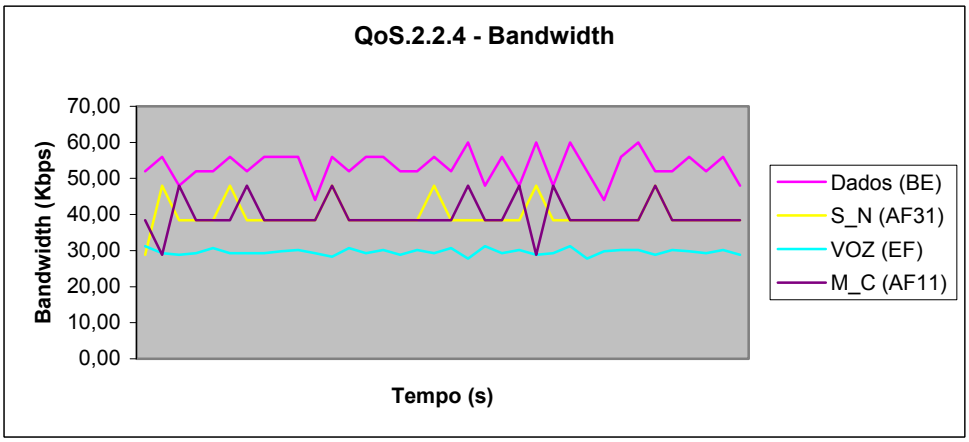

Figura 5.42 – QoS 2.2.4 - Bandwidth

Conclusão do Cenário 4 – Para pacotes de dados de 500 bytes, nota-se a ocorrência de uma pequena perda de pacotes na classe de Missão Crítica. Para as classes voz e dados S_N, os valores de vazão, atraso, jitter e perda de pacotes se mantiveram em níveis normais.

5.7 - Resumo do capítulo

Neste capítulo foram apresentados o ambiente de desenvolvimento utilizado e a implemetação dos três tipos de testes das VPNs. O software utilizado na montagem e verificação dos resultados é totalmente gratuito (Iperf). Os testes constituem da verificação de conectividade, isolamento e qualidade de serviços da VPN. Para o teste qualidade de serviço foram simulados quatro cenários para verficar se tanto o CE como o PE priorizam os pacotes em situação de congestionamento do acesso, de acordo com a classificação dos pacotes.

Os resultados mostraram que os mecanismos de QoS analisados apresentam bom desempenho para os quatros cenários. Alguns cuidados devem ser levados em consideração quando na transmissão da classe tempo real (EF) com relação ao tamanho de pacotes de dados na rede.

Os testes de conectividade e isolamento mostraram que existe uma separação entre espaço de roteamento e endereços por meio de uma tabela de roteamento por VPN.

Os testes realizados foram baseados na estratégia mostrada no capítulo 3, desde a definição da aplicação até o teste de QoS. Para evitar que o capítulo ficasse excessivamente longo, procurou-se enfatizar basicamente os teste, considerando que os passos anteriores como as configurações das VPNs já estivessem realizadas.

Capítulo 6

Conclusão e trabalhos futuros

6.1 - Conclusão

No capítulo 1 foi demostrado a tendência das VPNs MPLS. No Brasil é esperado um grande crescimento no mercado das pequenas e médias empresas. Nos mercados Governo e Corporativos é esperado uma grande migração das VPNs de nível 2 Frame Relay para VPN MPLS.

Após o que se demostra no capítulo 2, é possível concluir que o provedor de serviço pode minimizar seus custos de provisionamento e operação, oferecendo todos os serviços por meio de uma única plataforma de VPNs MPLS.

No capítulo 3 apresentou-se uma estratégia para projeto de VPNs MPLS. A principal contribuição é que para um bom projeto de VPNs MPLS, deve-se partir primeiro das reais necessidades dos aplicativos do usuário até chegar ao passo 6, que é a configuração da VPN. O mapeamento dos aplicativos em classes e a tecnologia de acesso são pontos que devem ser analisados antes de se configurar a VPN. Toda arquitetura tem benefícios e limitações, e o provedor de serviço deve efetuar uma cuidadosa análise dos requisitos dos usuários e selecionar a melhor solução para cada usuário. O capítulo 4 mostrou os principais aspectos na configuração da VPN MPLS: criar uma VRF, Atribuir um único "identificador de rotas - RD"para cada VRF; especificar políticas de importar e exportar para cada VRF - RT; estabelecer conectividade BGP entre os roteadores PEs; estabelecer MP-iBGP entre os roteadores PEs e permitir trocas de rotas VPN-IPv4;

configurar o processo de roteamento por VRF. As configurações dos identificadores das VPNs (RD) e as rotas target (RT) devem ser tratado em especial em um projeto de VPN MPLS. Se o projeto for apenas Intranet é possível considerar os RDs por VPNs, caso seja Extranet a implementação poderá ser de duas maneiras : RD por VRF ou realizando NAT entre as VPNs.

O Capítulo 5 teve como objetivo apresentar uma plataforma simples, de baixo custo e de fácil uso, que permita um estudo da abordagem feita nos capítulos anteriores, ou seja, permita validar a estratégia aplicada, comprovando os níveis de isolamento, conectividade e serviços diferenciados em uma VPN MPLS. Os resultados apresentados nesse capítulo mostram que é possível ter um nível de segurança e principalmente qualidade de serviços para as diversas aplicações que trafegam em uma VPN MPLS com DiffServ. Os experimentos foram feitos para os tipos de tráfegos EF, AF e BE. O que se pode concluir, portanto, desse capítulo é que é possível para o provedor, oferecer VPN segura e com qualidade de serviço.

6.2 – Trabalhos Futuros

- VoMPLS – É sabido que o IP não é um protocolo eficiente para transporte de voz, em função disso, um trabalho muito interessante seria implementar transporte Voz diretamente sobre MPLS.
- Multicast em MPLS – Hoje no Brasil nenhuma rede MPLS ainda suporta Multicast sobre MPLS; portanto um trabalho de como implementar Multicast sobre MPLS será de grande utilidade.
- Voz sobre IPSec sobre LSP – Um trabalho também bastante interessante seria analisar o desempenho dos LSPs quando os dados transportados são pacotes de voz com IPSec.
- IPv6 através de MPLS.

Bibliografia

[1] S.Blake, et. Al., RFC 2475, “An Architecture for Differentiated Services,”December 1998

[2] Vegesna, S. “IP Quality of Service”, Cisco Press 2001.

[3] U.Black., “ MPLS and Label Switching Networks” Prentice Hall Series 2001

[4] I. Pepelnjak, J. Guichard, “MPLS and VPN Architectures – Volume I” Cisco Press 2002

[5] I. Pepelnjak, J. Guichard, J. Apcar. “MPLS and VPN Architectures – Volume II” Cisco Press 2003

[6] E. Osborne, A. Simba, “Engenharia de Tráfego com MPLS” Cisco Press 2003

[7] P. Tonsu, G. Wieser, “MPLS-Based VPNs” Prentice Hall series 2001

[8] Y.Rekhter, E. Rosen, RFC 2574, “BGP/MPLS VPNs,”March 1999

[9] S. Ramachandra, D. Tappan, “BGP Extended Communities Attribute,” [draft-ramachandra-bgp-ext-communities-09.txt], work in progress, June 2001.

[10] E. Rosen, R Callon, A. Viswanathan, RFC 3031, “Multiprotocol Label Switching Architecture,” January 2001.

[11] B. Jamoussi, L. Andersson, R. Callon and R. Dantu: “Constraint-Based LSP Setup using LDP”, RFC 3212, January 2002

[12] Dino Farinacci, Tony Li, A. Conta, Y Rekhter, Dan Tappan, E. Rosen, G. Fedorkom, RFC 3032, “MPLS Label Stack Encoding, “January 2001.

[13] Juha Heinanen, RFC 1483, “Multiprotocol Encapsulation over ATM Adaptation Layer 5,” July 1993.

[14] Bilel Jamoussi, et al, “Constraint-Based LSP Setup using LDP,”[draft-ietf-mpls-crldp-05.txt], January 2001

[15] R. Braden, et al., RFC 2205, “Resource ReServation Protocol (RSVP) – Version 1, Functional Specification, “September 1997.

[16] Yakov Rekhter, Eric Rosen, RFC 3107, “Carrying Label Information in BGP-4,” May 2001

[17] K. Nichols, et al., RFC 2474, “Definition of the Differentiated Services Filed (DS Field) in the IPv4 and IPv6 Headers,” December 1998.

[18] S. Blake, D. Black, M. Carlson, E.Davies: “An Architecture for Differentiated Services”, RFC 2475, December 1998.

[19] Grossman, D. and Heinanem, J., RFC 2684, “Multiprotocol Encapsulation over ATM Adaptation Layer 5.” September 1999.

[20] Conta, A., Doolan, P., and Malis, A, RFC 3034. “Use of Label Switching on Frame Relay Networks.” January 2001

[21] Davie, Bruce and Y.Rekhter “MPLS Technology and Applications” Morgan Kaufmann Publishers 2000

[22] Guichard, Jim and I, Pepelnjak MPLS and VPN Architectures: A Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs Cisco Press 2000.

[23] F.L Faucher, B. Davie, S. Davari, P. Vaananem: “MPLS Suport of Differentiated Services”, RFC 3270, May 2002

[24] Campanella, M., et al., “Specification and Implementation plan for a Premium IP service”, GEANT deliverable D9.1, March 2001.

[25] Kamienski, C.A & Sodok, D., “Qualidade de Serviço na Internet”, minicurso , 18 SBRC, Belo Horizonte/MG, May 2000

[26] Leinen, Leinen, S., Przybylski, M, Reijs, V. & Trocha, S., "Testing of Traffic Measurement Tools",TF-NGN Deliverable D9.4, September 2001.

[27] Nichols, K., Jacobson, V. & Zhang, L., "A Two-bit Differentiated Services Architecture for the Internet", RFC 2638, July 1999.

[28] Pan, P., "Scalable Resource Reservation Signaling in the Internet", Ph.D. Thesis, Columbia University, 2002.

[29] Tanenbaum, A. S., "Computer Networks", Prentice Hall, 3rd edition, 1996.

[30] TEQUILA Project, http://www.ist-tequila.org, 2000.

[31] Xiao, X. & Ni, L. M., "Internet QoS: A Big Picture", IEEE Network, March 1999.

[32] White Paper – "The need for QoS", www.qosforum.com/white-papers/Need_for_QoS-v4.pdf.

[33] White Paper – "Introduction to QoS policies", www.qosforum.com/white-papers/qospol_v11.pdf.

[34] A White Paper by NetScreen Technologies, Inc. - Deploying Scalable, Secure, DynamicVirtual Private Networks, May 2003.

[35] Magalhãaes, M. F.; Cardozo, E. (1999). Qualidade de serviço na Internet. Relatório técnico, UNICAMP/FEEC/DCA, Campinas, SP.

[36] A White Paper by Cisco. - MPLS based VPNs: Equivalent to the security of Frame and ATM, March 2001.

[37] Semeria, Chuck. – "RFC 2547bis: BGP/MPLS VPN Fundamentals", www.juniper.net/techcenter/techpapers/200014, 2001

[38] Semeria, Chuck. – "RFC 2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications", www.juniper.net/techcenter/techpapers/, 2001

[39] Semeria, Chuck.–"RFC 2547bis: Migration Strategies for IP Service Growth:Cell-switched MPLS or IP-routed MPLS", www.juniper.net/techcenter/techpapers/200026, 2002

[40] A White Paper by Soirent – BGP/MPLS: Virtual Private Networks,2002

[41] Semeria, Chuck.; Stewart, W.J. – "Supporting Differentiated Service Classes in Large IP NEtworks", www.juniper.net/techcenter/techpapers/, 2001

[42] Bagasrawala, A. – "Next Generation VPNs", Lucent Technologies

[43] A White Paper by Nortel Networks. - "Deploying IP-VPN services on Passport Multiservice Networks"www.nortelnetworks.com

[44] RFC 2598, "An Expedited Forwarding PHB", http://www.ietf.org/rfc/rfc2598.txt

[45] RFC 2597, "Assured Forwarding PHB Group", http://www.ietf.org/rfc/rfc2597.txt

[46] RFC 2338, "Virtual Router Redundancy Protocol", http://www.ietf.org/rfc/rfc2338.txt

[47] RFC 2917, "A Core MPLS IP VPN Architecture", http://www.ietf.org/rfc/rfc2917.txt

[48] RCF 2983, "Differentiated Services and Tunnels", http://www.ietf.org/rfc/rfc2983.txt

[49] RCF 1265, "BGP Protocol Analysis", http://www.ietf.org/rfc/rfc1265.txt

[50] RCF 1403, "BGP OSPF Interaction", http://www.ietf.org/rfc/rfc1403.txt

[51] Stoika, I.; Zhang, H. (1998). LIRA: An approach for service differentiation in the Internet.Proceedings of NOSSDAV.

[52] McCabe, J.D. Practical Computer Network Analysis and Design. São Francisco, Califórnia: Morgan Kaufmann Publishers, In.; 1998

[53] Igor M. Moraes, Marco Dias D. Bicudo , Kleber V. Cardoso , Saulo V. de Vasconcellos ,José F. de Rezende , Otto Carlos M. B. Duarte – "Desenvolvimento de um Ambiente de Testes com Suporte à Qualidade de Servicço para Transmissão de Vídeo Digital", 2003

Anexo A – Conceitos básicos de BGP

A.1 – BGP

O BGP é um protocolo de roteamento dinâmico, utilizado para comunicação entre sistemas autônomos (ASs). Baseados nessas informações, os sistemas autônomos conseguem trocar informações e determinar o melhor caminho para as redes que formam a Internet. Tal papel é muito importante, sabendo-se que a todo momento as redes podem sofrer alterações, podem ocorrer quedas de suas conexões, receber anúncios inválidos, aplicar políticas, manter a conectividade por outros caminhos, adaptando-se rapidamente e mantendo a consistência de seus anúncios de forma eficiente.

A divulgação das informações de roteamento BGP [50] é feita entre roteadores que estabelecem uma relação de "vizinhança", sempre na forma de pares. Tendo essa relação, são trocadas as informações contidas nas tabelas de roteamento BGP de cada um destes. Para estabelecer uma relação de vizinhança é necessário que dois roteadores tenham uma conexão direta entre eles, ou que algum protocolo IGP trate de garantir a alcançabilidade. Essa relação de vizinhança pode definir aos roteadores uma relação de *speakers ou peers* (pares).

Tratando-se de um protocolo importante que requer confiabilidade em sua comunicação, para garantir a alcançabilidade entre todas as redes da Internet, é necessário que seja utilizada uma forma confiável de troca de informações deste protocolo. Isso é obtido pela utilização do protocolo TCP entre dois roteadores que trocam informações do protocolo BGP. A porta utilizada para a comunicação é 179.

Para diferir e identificar univocamente em cada sistema autônomo (AS), cada AS possui um número que o identifica mediante os demais ASs da Internet. Este número varia entre 1 e 65535, sendo que a faixa entre 64512 e 65535 é destinada a uso privado.

A.2 - SESSÃO BGP

Antes do estabelecimento de uma sessão BGP, os roteadores vizinhos trocam mensagens entre si para entrar em acordo sobre quais serão os parâmetros (ex: tempo máximo de espera entre as mensagens – hold time) da sessão. Não havendo discordância e nem erros durante a negociação dos parâmetros entre as partes, a sessão BGP é estabelecida. Caso contrário, serão enviadas mensagens de erro e a sessão não será aberta.

Quando a sessão é estabelecida entre os roteadores, são trocadas mensagens contendo todas as informações de roteamento, ou seja, todos os melhores caminhos previamente selecionados por cada um, para os destinos conhecidos. Posteriormente, eles trocarão mensagens somente de atualização das informações de roteamento de forma incremental. Essa técnica mostrou-se um avanço no que se refere à diminuição da carga das CPUs dos roteadores e na economia da banda dos enlaces, quando comparada a outros protocolos que, ao comunicarem suas atualizações, enviam, periodicamente, a totalidade de rotas instaladas em suas tabelas.

A.3 - Mensagem BGP

As mensagens trocadas em sessões BGP têm o comprimento máximo de 4.096 bytes, e mínimos 19 bytes. Todas as mensagens são compostas de, no mínimo, um cabeçalho e, opcionalmente, uma parte de dados. O formato do cabeçalho das mensagens BGP está apresentado na figura A1.

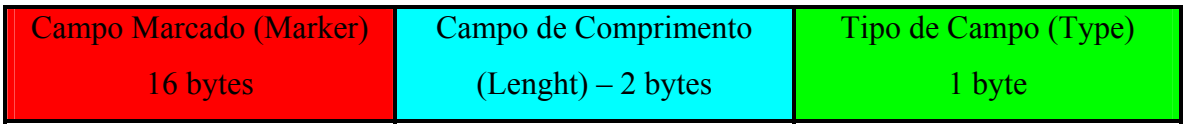

Figura A.1 – Formato da Mensagem do cabeçalho BGP

- **Campo Marcador:**

Serve para verificar a autenticidade da mensagem recebida e se houve perda de sincronização entre os roteadores vizinhos BGP. Pode ter dois formatos: caso a mensagem seja do tipo OPEN (abrir), ou se a mensagem do tipo OPEN não possuir informação de autenticação, o campo deve estar todo preenchido com o número 1; senão, o campo marker terá seu conteúdo baseado em parte no mecanismo de autenticação usado.

- **Campo do Comprimento:**

Deve conter um número que representa o comprimento total da mensagem, incluindo o cabeçalho. Como pode haver mensagens que não possuem dados após o cabeçalho, a menor mensagem BGP enviada é de 19 bytes.

- **Tipo de Campo:**

Esse campo deve conter um número que representa o código de um tipo de mensagem. Os tipos de mensagens são: KEEPALIVE, NOTIFICATION, OPEN e UPDATE

A.4 - Tipos de Mensagens BGP

Os roteadores vizinhos BGP-4 que suportam BGP-4 trocam mensagens de 4 tipos antes ou durante uma sessão BGP. A seguir apresenta-se para que serve cada tipo dessas mensagens.

- **OPEN**

A mensagem do tipo OPEN é enviada para se iniciar a abertura de uma sessão BGP entre os vizinhos BGP. O formato dessa mensagem está apresentado na figura A2.

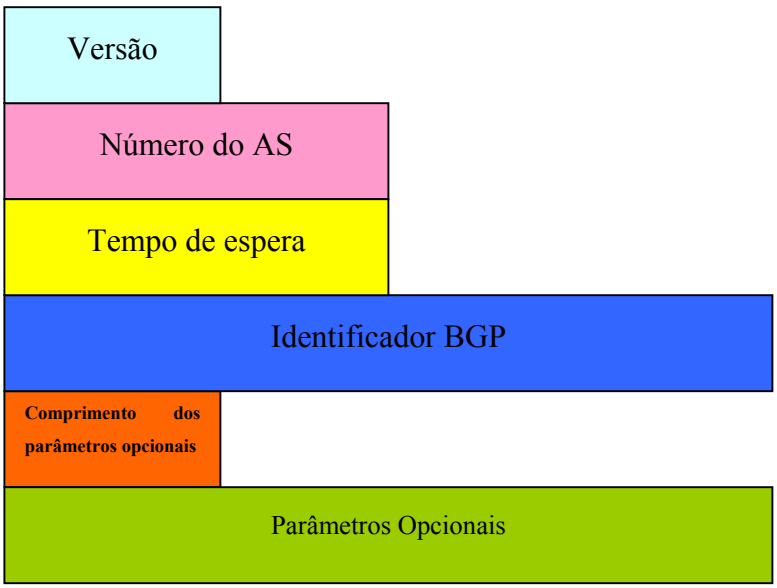

Figura A.2 – Formato da mensagem OPEN

- **NOTIFICAÇÃO:**

Esse tipo de mensagem é enviado no caso da detecção de erros durante ou após o estabelecimento de uma sessão BGP. O formato da mensagem NOTIFICAÇÃO está apresentado na figura A3.

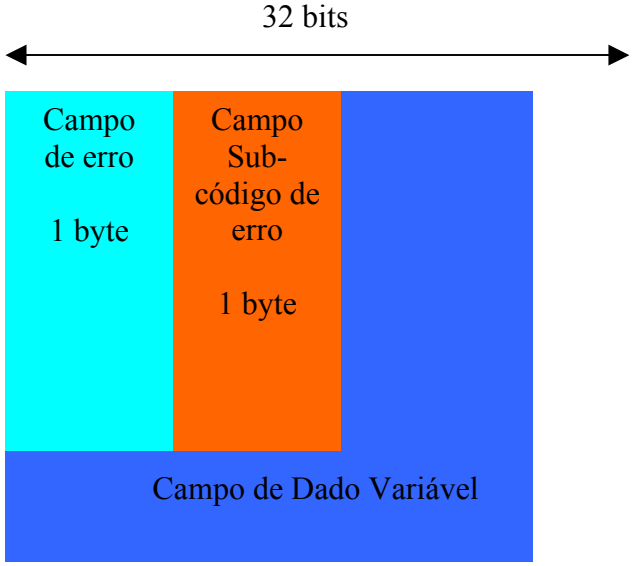

Figura A.3 – Formato da mensagem NOTIFICAÇÃO

- **KEEPALIVE**

São mensagens trocadas periodicamente, com o propósito de verificar se a comunicação entre os vizinhos está ativa. A mensagem do tipo KEEPALIVE é composta apenas de cabeçalho padrão das mensagens BGP, sem dados transmitidos após o cabeçalho. O tempo máximo permitido para o recebimento da mensagem KEEPALIVE é definido pelo hold time.

A.5 - RDs e as famílias de endereçamentos VPN-IPV4

O objetivo das VPNs BGP/MPLS é ter um endereço distinto para cada VPN. Rotas dos clientes devem ser tratadas em diferentes caminhos, dependendo de qual VPN elas pertencem. O multiprotocolo BGP extensão [9] permite ao BGP transportar rotas de múltiplas "famílias de endereços" [49]. Uma VPN-IPv4 é composta de bytes, iniciando com 8 bytes que corresponde ao RD e terminando com 4 bytes que se referem ao endereçamento IPv4 (Ver figura A4). Se duas VPNs usam o mesmo endereçamento IPv4, os PEs transladam, incluindo o prefixo de endereçamento VPN-IPv4, para cada VPN. Isso garante que, se o mesmo endereço é utilizado em duas VPNs diferentes, é possível instalar duas rotas completamente diferentes para o mesmo endereço, uma para cada VPN [8].

Um RD consiste de dois bytes que especificam o Tipo do Campo, um Campo do Administrador e um número do campo atribuído (ASN). O valor do tipo de campo determina o comprimento dos outros dois campos, tão bem como a semântica do campo administrador. O campo administrador identifica um número atribuído à autoridade e o número do campo atribuído contém um número que havia sido atribuído pelo identificador para um propósito particular. Essas duas variantes tinham sido definidas para permitir ao administrador da rede escolher uma única RD, baseada em outro ASN ou endereço IP público. No entanto, as semânticas não influenciam o comportamento do BGP em algum caminho. Quando o BGP compara dois prefixos de endereços, ele ignora a estrutura inteiramente.

O RD consiste de um campo de 8 bytes. Juntos com 4 bytes do endereço IPv4, ele constrói a família de endereços das VPN-IPv4. O RD é dividido em:

- Tipo do Campo: 2 bytes
- Valor do Campo: 6 bytes

A interpretação do valor do campo depende do valor do tipo de campo. Até o presente momento, dois são os valores do Tipo de Campo definido: 0 e 1. Quando o tipo de campo é 0, o valor de campo consiste de dois subcampos (ver figura A5):

- Administrador do Subcampo: 2 bytes
- Número Atribuído ao Subcampo: 4 bytes

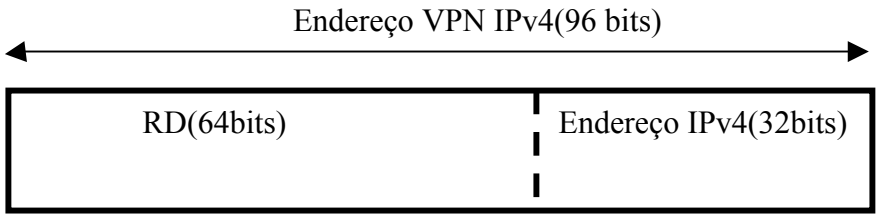

Figura A.4 – VPN/IPv4

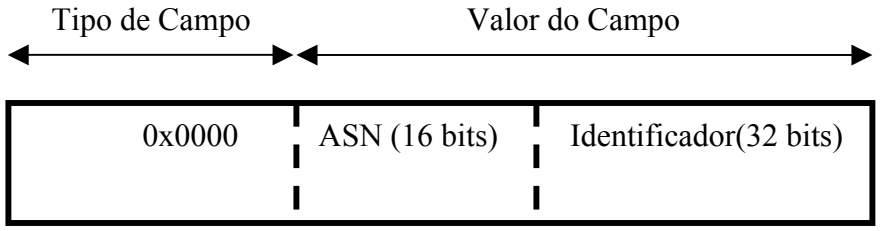

Figura A.5 – RD Tipo=0

O administrador do Subcampo deve conter um ASN. Se esse ASN é de um ASN público, ele deve ser atribuído pela Internet Assigned Numbers Association (IANA). O número atribuído ao subcampo pertence ao plano de numeração que é administrado pela empresa da qual o ASN foi atribuído pela IANA. Quando o tipo de campo for 1, o valor do campo consiste de dois subcampos (vê figura A6):

- Administrador do Subcampo: 4 bytes
- Número Atribuído ao Subcampo: 2 bytes

O administrador do subcampo deve conter um endereço IP. Se esse endereço IP tiver sido atribuído pela IANA para uma empresa particular, o número atribuído ao subcampo contém um número do espaço de numeração, que é administrado pela empresa para a qual o endereço foi atribuído.

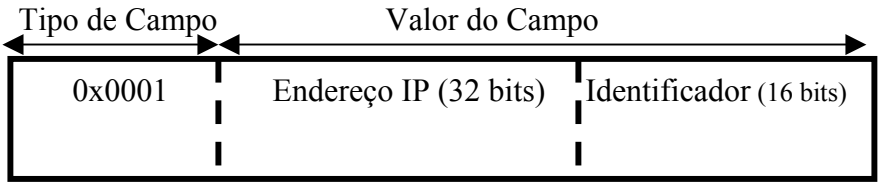

Figura A6 – RD do Tipo=1

Anexo B – MPLS baseado em Célula x MPLS baseado em Roteador

B.1 - Principais limitações do IPoATM:

Há um número de limitações bem conhecidas associadas ao modelo tradicional de IP sobre ATM:

- IP sobre ATM incrementa a complexidade da rede pela necessidade do provedor de gerenciar dois planos de controle e fundamentalmente dois tipos diferentes de equipamentos de rede.
- IP sobre ATM resulta em uma ineficiência do uso da largura de banda da célula ATM, como conseqüência do cabeçalho da célula do ATM que corresponde a aproximadamente 25% de toda a informação transmitida em cada célula (célula TAX)[25].
- As abordagens dos serviços IP diferenciados (DiffServ) para as classes de serviços não são bem mapeados com os mecanismos de QoS do ATM
- IP sobre ATM requer o desenvolvimento de N^2 rotas adjacentes.

Para resolver essas limitações os provedores têm optado entre MPLS baseado em Célula ou MPLS baseado em Roteador. Será apresentado agora as principais contribuições dessas duas arquiteturas para resolver as principais limitações do IPoATM.

[25] Célula TAX se refere a utilização do ATM para transporte, ocasionando um grande overhead e ineficiência da largura de banda da rede

B.2 - MPLS baseado em célula

Basicamente há dois pontos principais em que a transição de IP sobre ATM para Comutação de célula MPLS pode remover a complexidade e simplificar a operação da rede.

- Reduzindo a ênfase em IGP

Um dos maiores problemas que dificulta o crescimento de IP sobre ATM é que a criação de n^2 circuitos virtuais permanentes (CVPs) pode levar a saturação o IGP durante situações de falhas. Através do MPLS baseado em célula é eliminada a necessidade de estabelecer uma topologia de n^2 roteamentos.

- Simplificação no gerenciamento das CoS

MPLS baseado em célula pode simplificar o gerenciamento da classe de serviço (CoS) na rede, pois os planos de controle ATM e MPLS em uma rede IP sobre ATM podem ser substituídos por um único plano de controle IP/MPLS. MPLS baseado em célula suporta CoS IP por meio do estabelecimento de múltiplos LSPs, sendo cada LSP dedicado a uma classe específica de tráfego. A diferença essencial entre IP sobre ATM e Comutação de célula MPLS é que, em vez de usar sinalização ATM para estabelecer PVCs, a sinalização MPLS estabelece os LSPs. Enquanto um único plano de controle tem o benefício quando comparado com uma outra opção formada por dois planos de controle independentes, o desenvolvimento de MPLS baseado em célula não elimina a complexidade de gerenciamento associada ao desenvolvimento de dois tipos diferentes de equipamento – Roteadores IP e Comutadores ATM.

B.3 - MPLS baseado em Roteador:

O desenvolvimento da infra-estrutura MPLS baseada em roteadores IP tem-se mostrado adequado para superar essas limitações do IP sobre ATM.

- MPLS baseado em roteador elimina a complexidade de gerenciamento de dois planos de controle e dois diferentes tipos de equipamentos de rede, porque é requerido um único plano de controle IP/MPLS.

- MPLS baseado em roteador provê mais eficiência no uso da largura de banda da rede, por não usar ATM como transporte.
- MPLS baseado em roteador pode suportar IP DiffServ CoS, pois LSRs baseados em Frame têm a habilidade de ler e escrever bits EXP no rótulo da pilha MPLS, que transporta a informação IP DiffServ. Essa capacidade permite múltiplos níveis de serviço em um mesmo LSP.
- MPLS baseado em roteador elimina a necessidade do estabelecimento de n^2 conexões entre os roteadores de bordas.

Anexo C – Metodos de encapsulamento xDSL

Cada um dos métodos de encapsulamento abaixo e seu funcionamento com uma rede VPN MPLS para acesso remoto será abordado em seguida.

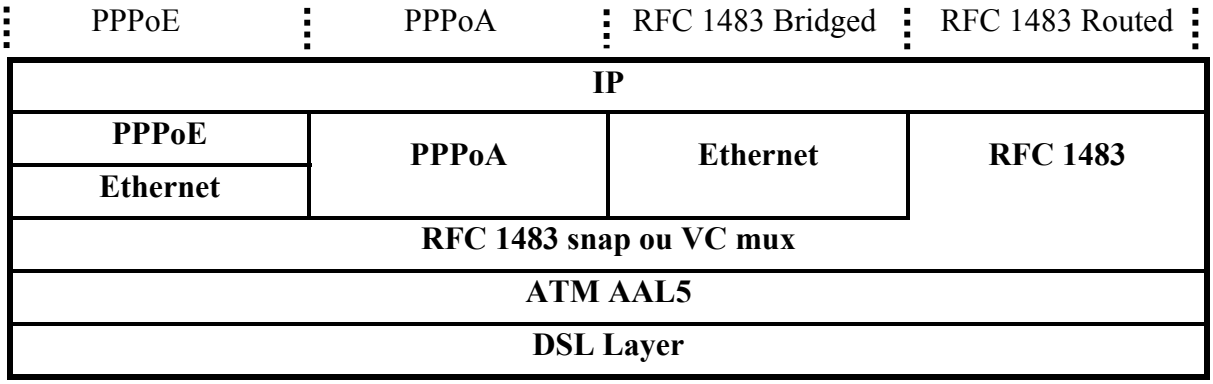

Figura C – Formato de Encapsulamento DSL

C.1 - Acesso DSL usando a RFC 1483 com encapsulamento roteado

Esse método de conexão é particularmente simples e consiste de um PVC ATM entre o CPE do acesso DSL e o roteador PE, como apresentado na figura C.1.

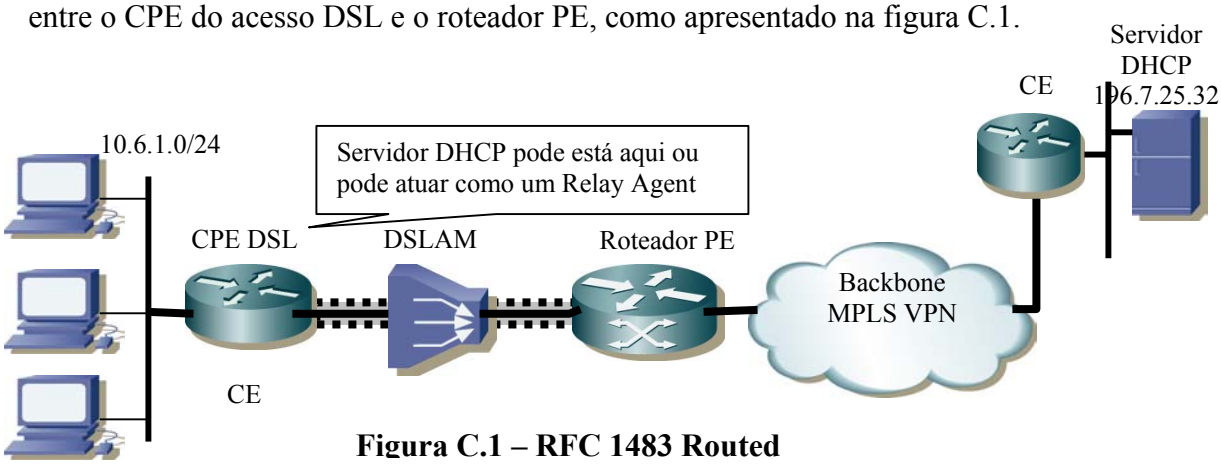

Figura C.1 – RFC 1483 Routed

Nenhuma autenticação e autorização do usuário são necessárias nesse cenário. Na visão da rede MPLS, não há diferença entre essa configuração e um outro circuito virtual permanente (CVP) como Frame Relay ou Linha Dedicada. Em função do CPE ser um roteador, ele pode ser configurado com roteamento dinâmico no roteador PE, se necessário, e atuar como um servidor DHCP na rede local.

C.2 - Acesso xDSL usando RFC 1483 com encapsulamento de nível 2 (*bridged*)

Nesse cenário, todo tráfego entre o acesso DSL do CPE e o roteador PE é processado no nível de enlace. O tráfego é transportado no PVC ATM como na RFC 1483 com a inclusão da informação de nível 2 (Endereçamento Ethernet). Para o roteador apresentado na figura C.2, a subinterface ATM aparece como uma interface Lan.

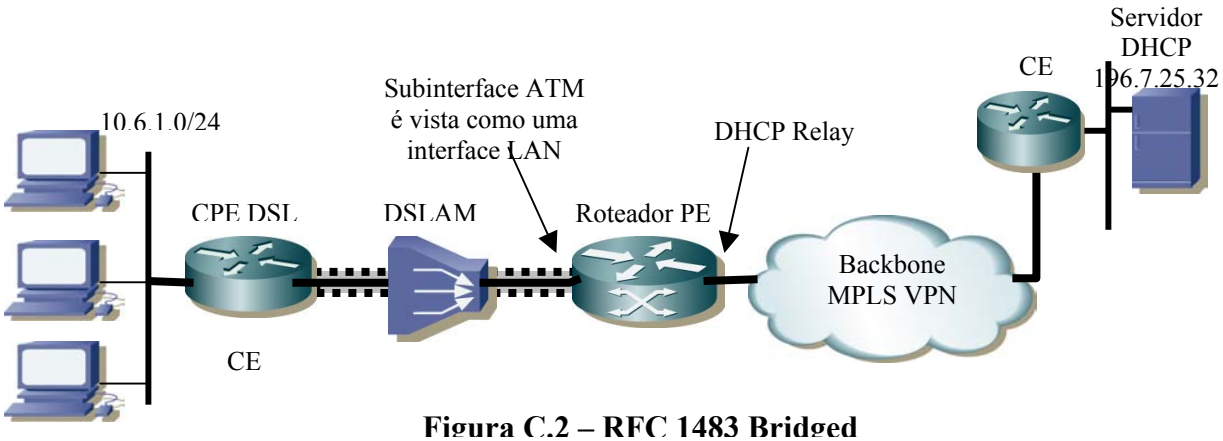

Figura C.2 – RFC 1483 Bridged

Como o CPE do acesso DSL não tem nenhuma funcionalidade de roteamento, ele não pode atuar como um servidor DHCP. Entretanto, se DHCP é requerido, então o servidor DHCP remoto deverá prover o serviço.

C.3 - Acesso xDSL usando PPP sobre Ethernet (PPPoE)

No acesso que utiliza PPP sobre Ethernet (PPPoE), como apresentado na figura C.3, o CPE é conectado no roteador PE usando uma conexão simples, como na RFC 1483 com encapsulamento de nível 2 (bridged) . Sessão PPPoE é normalmente direcionada para PC, clientes com software PPPoE instalado e encapsulado (bridged) sobre PVC ATM, por meio de encapsulamento Ethernet dos quadros . O roteador PE tem uma interface de acesso virtual para cada PC cliente, como uma oposição ao PPPoA. A vantagem do PPPoE é que

o software reside nos PCs clientes. Portanto, os CPEs DSL necessitam somente de capacidade de encapsulamento de nível 2 (bridging). Nenhuma capacidade de roteamento é necessária. Como conseqüência, tem-se um baixo custo de hardware, porque cada PC executa sua própria sessão PPP e autenticação.

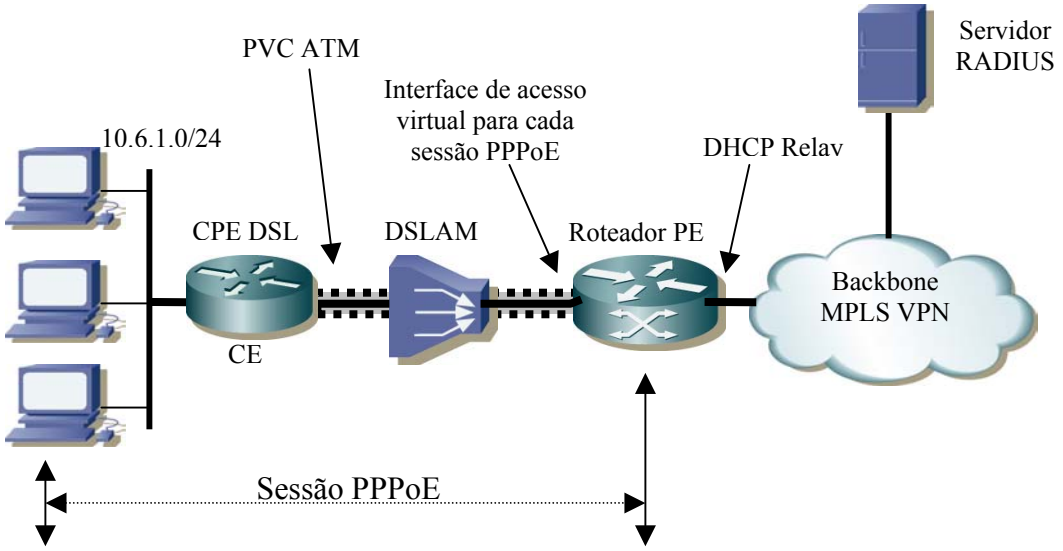

Figura C.3 - PPPoE

C.4 - Acesso xDSL usando PPP over ATM (PPPoA)

No PPP sobre ATM (PPPoA), apresentado na figura C.4, o CPE do usuário tem funcionalidade de roteamento e usa PPP para conectar com o roteador PE. A sessão PPP é executada sobre o PVC ATM entre o CPE DSL e o roteador PE, sendo então chamada de PPP sobre ATM ou PPPoA. As máquinas locais podem também ser configuradas estaticamente com endereçamento IP ou por solicitação ao servidor DHCP, que é configurado no outro CPE DSL ou num servidor remoto na Intranet.

A vantagem de usar PPPoA em um acesso DSL é que pode ser feita uma simples autenticação na conexão DSL para todos os PCs atrás do CPE DSL. Os PCs podem obter seus endereços de um DHCP[26] local, que é configurado no CPE DSL, ou de um servidor DHCP do usuário.

[26] DHCP Relay Agente – Se o servidor DHCP está centralizado em algum lugar da rede, deve-se habilitar um DHCP agente Relay para consigurar a interface LAN do roteador do usuário que irá trocar mensagens entre o usuário e o Servidor DHCP.

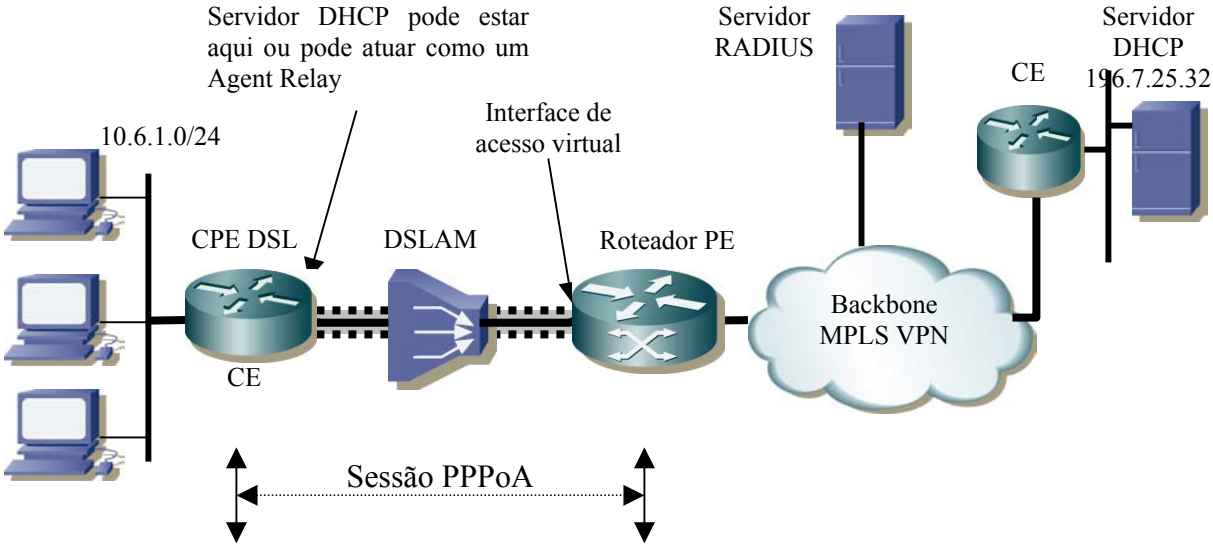

Figura C.4 - PPPoA

Anexo D – Escolhendo o melhor protocolo de roteamento para as VPNs MPLS

É importante entender qual protocolo de roteamento deve ser apropriado para determinado tipo de topologia. Para entender melhor essa análise a topologia da figura D.1 foi alterada para uma topologia simples de VPN de um cliente típico, como mostra a figura D.2.

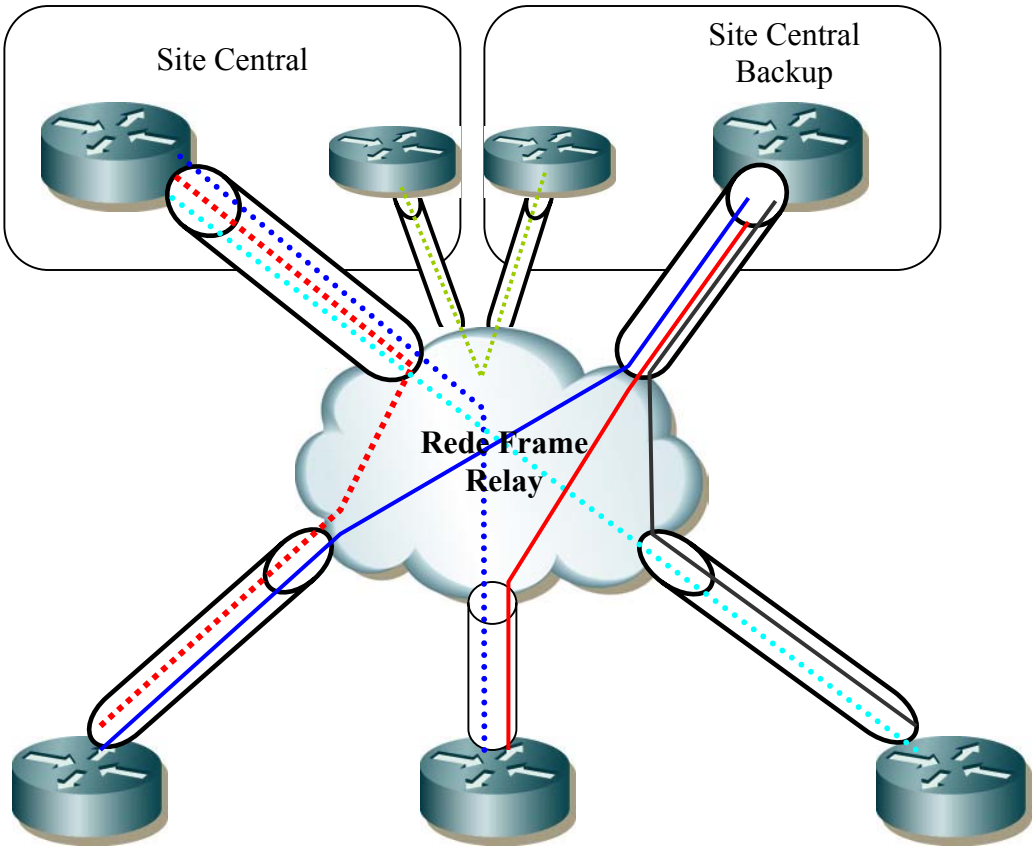

Figura D.1 – Topologia típica de rede das VPN tradicionais

A topologia apresentada acima tem dois pontos centrais, conectados por meio de Frame Relay para vários pontos remotos. Os pontos centrais são conectados entre si e com os pontos remotos por meio de PVC. O roteamento é realizado por meio do protocolo de gateway interior – EIGRP [5].

O cliente decidiu migrar sua rede atual Frame Relay para uma VPN MPLS, com o objetivo de superar a complexidade e limitação do modelo da rede virtual privada Frame Relay, que usa o modelo Overlay. A nova infra-estrutura de rede usará um provedor de serviço que oferece o serviço de VPN MPLS, como pode ser visto na figura D.2.

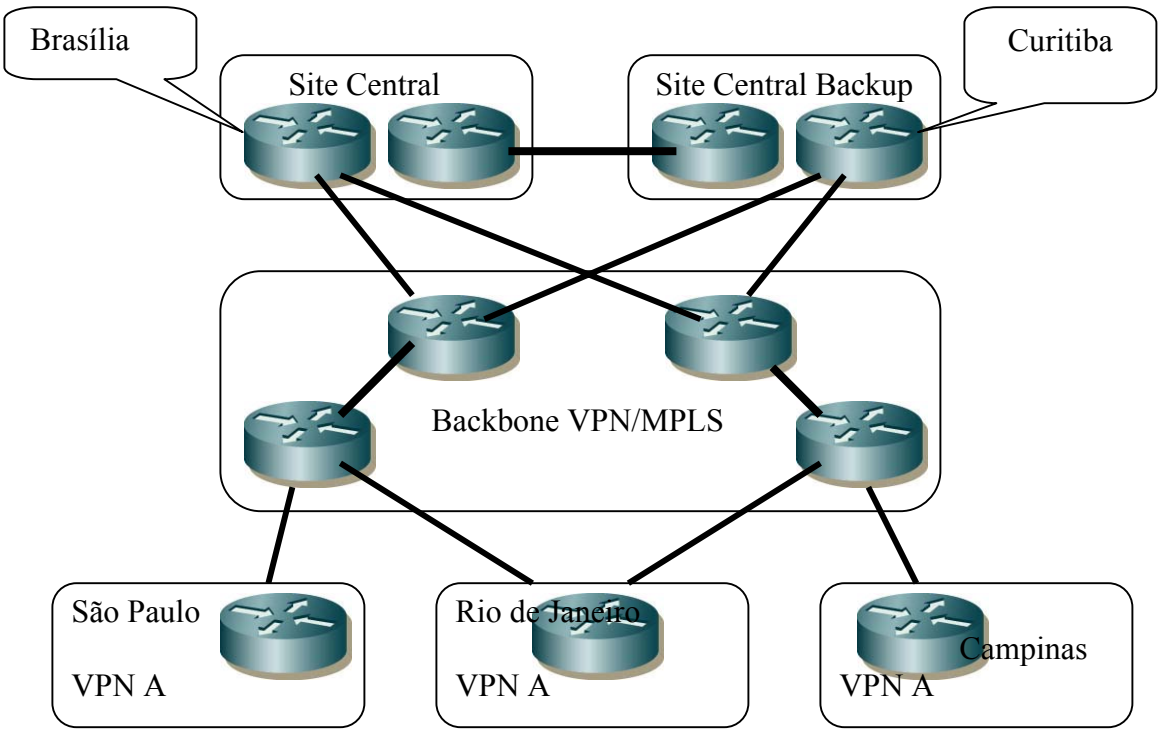

Figura D.2 – Migração para VPN MPLS

A partir dessa topologia de rede é necessário decidir qual das quatros opções de conectividade PE-CE deverá ser usada em cada ponto da rede. Como já foi discutido anteriormente, na seção OSPF, se o cliente já está trabalhando com OSPF entre cada ambiente, ele poderá decidir pela continuidade do uso desse protocolo entre os roteadores PE e CE. Nessa circunstância essa é uma boa escolha de projeto em função dos motivos já discutidos anteriormente.

No exemplo da figura D1, O protocolo utilizado é o EGIRP, portanto, é necessário que o cliente migre o protocolo de roteamento usado por meio do enlace PE-CE para OSPF, BGP-4, RIPv2 ou usar roteamento estático para que as rotas possam ser trocadas entre os pontos da VPN A e o Backbone da VPN MPLS. Dado o fato de que alguns pontos remotos têm um único enlace com o backbone VPN MPLS, o roteamento estático poderá ser utilizado em cada roteador PE no Backbone VPN MPLS. Entretanto, alguns pontos como o central, o backup e Rio de Janeiro possuem mais que um enlace com o provedor da VPN. Roteamento estático não é realmente uma boa opção nesse caso; protocolos dinâmicos de anúncio das rotas são necessários.

A necessidade de roteamento nos pontos remoto e central é diferente. No caso dos ambientes remotos, devem aprender outras rotas da VPN MPLS assim que o roteamento entre os pontos estiver disponível. O ponto Central, entretanto, precisa aprender não somente rotas de outros pontos remotos, mas também precisa aplicar políticas em termos do fluxo de dados. Em adição, ele precisa ser um ponto de concentração em termos de rota (Isso deverá incluir rotas Internet aprendidas da VPN MPLS). Por essa razão, RIP v2 pode ser uma escolha adequada para os pontos remotos, mas BGP é uma boa escolha para o ponto central, em função de sua escalabilidade e políticas.

Do ponto de vista do provedor de serviço, o uso do BGP entre os roteadores CE e PE é o protocolo preferido. Isso porque o uso do BGP oferece várias vantagens para o provedor de serviço:

- Há redução do Overhead, manutenção do roteador PE e as configurações são simplificadas.
- Redistribuição entre protocolos de roteamento não é necessário se as rotas são aprendidas por meio do BGP.