Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação
Departamento de Comunicações

CONTRIBUIÇÕES E AVALIAÇÕES DAS ARQUITETURAS PARA AS VPNS CONVERGENTES COM ESCALABILIDADE, SEGURANÇA E QUALIDADE DE SERVIÇO

Autor: Adão Boava

Orientador: Prof. Dr. Yuzo Iano

Tese de Doutorado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para a obtenção do título de Doutor em Engenharia Elétrica. Área de concentração: **Telecomunicações e Telemática.**

Banca Examinadora

Prof. Dr. Yuzo Iano/FEEC/UNICAMP (Presidente)
Prof. Dr. Osamu Saotome — ITA
Prof. Dr. Omar Carvalho Branquinho — PUCC
Prof. Dr. Akebo Yamakami — DT/FEEC/UNICAMP
Prof. Dr. Rangel Arthur - FT/UNICAMP

29 de Julho de 2011, Campinas – SP

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

B63c

Boava, Adão
Contribuições e avaliações das arquiteturas para as VPNs convergentes com escalabilidade, segurança e qualidade de serviço / Adão Boava. --Campinas, SP: [s.n.], 2011.

Orientador: Yuzo Iano.
Tese de Doutorado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Comunicação móvel. 2. Redes de comunicação. 3. Sistemas de comunicação sem fio. 4. Redes de computadores - Medidas de segurança. I. Iano, Yuzo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Contributions and assessments for converging VPN architectures with scalability, security and quality of service
Palavras-chave em Inglês: Mobile communication, Communication networks, Wireless communication systems, Computer networks - Security measures
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora: Osamu Saotome, Omar Carvalho Branquinho, Akebo Yamakami, Rangel Arthur
Data da defesa: 29-07-2011
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidato: Adão Boava

Data da Defesa: 29 de julho de 2011

Título da Tese: "Contribuições e avaliações das arquiteturas para as VPNs convergentes com escalabilidade, segurança e qualidade de serviço"

Prof. Dr. Yuzo Iano (Presidente): _____

Prof. Dr. Omar Carvalho Branquinho: _____

Prof. Dr. Osamu Saotome: _____

Prof. Dr. Akebo Yamakami: _____

Prof. Dr. Rangel Arthur: _____

Resumo

Os próximos anos prometem ser os das tecnologias das redes de nova geração para as operadoras de telecomunicações, fornecedores de equipamentos e usuários, com ênfase na integração das redes móveis sem fio, como 3G e 4G, com as redes fixas tradicionais, integração essa chamada às vezes de convergência das redes. Como consequência da convergência, vive-se um momento em que várias operadoras de telecomunicações fixas e móveis começaram a oferecer alguns serviços básicos de banda larga e os fornecedores de equipamentos iniciaram o processo de homologação de tais serviços, sendo que basicamente o único serviço disponível pelas operadoras que utilizam as redes de banda larga móveis e fixa é o acesso à *internet*. Esta tese apresenta alternativas para integrar as redes fixas com as redes móveis das operadoras a fim de oferecer serviços de VPNs (*Virtual Private Network*) fixo – móveis para aplicações que exijam mobilidade, baixo custo, qualidade de serviço, conectividade e segurança com alta escalabilidade. Para oferecer a mobilidade, são apresentadas as principais soluções de acesso banda larga para a formação de MVPN (*Mobile Virtual Private Network)*. Essas são analisadas e avaliadas a fim de mostrar suas deficiências para utilização em acessos das VPNs. A qualidade de serviço, conectividade, segurança e escalabilidade serão alcançadas com a implementação do protocolo MPLS (*Multi-Protocol Label Switching*) no núcleo da rede. A implementação do MPLS no núcleo da rede consolida o transporte para as diversas tecnologias de acesso sem fio e com fio, reduzindo os custos operacionais das operadoras e tornando a redes mais escaláveis e confiáveis, preparando, assim, a operadora para as redes de acesso de quarta geração (4G). A partir dos requisitos das aplicações que irão trafegar na VPN, são propostas novas contribuições para as VPNs fixo - móveis para que estas atendam a esses requisitos com alta escalabilidade,

mobilidade, segurança, conectividade e qualidade de serviço para o usuário e a operadora. Para validar as novas contribuições propostas, foi implementado um ambiente de teste para avaliar a conectividade e isolamento das VPNs e a qualidade de serviço. Duas propostas para resolver o problema de escalabilidade das VPNs são apresentadas, uma baseada em lista de controle de acesso ACL (*Access Control List*) e outra baseada em *firewall*. Também é apresentada uma proposta de IPSec (*IP Security Protocol*) sobre MPLS para resolver o problema de erros de configuração quando cometidos pelas operadoras de telecom.

Palavras-chave: MPLS, MVPN, VPN, comunicações móveis, qualidade de serviço e segurança.

Abstract

The following years will be dominated by next generation network technology for telecommunication providers, equipment suppliers and users who emphasize the integration of mobile wireless networks such as 3G and 4G with traditional fixed networks – an integration often dubbed as network convergence. As a consequence of convergence, it is possible to observe that various fixed and mobile telecommunication providers are beginning to offer basic broadband services and equipment suppliers have initiated corresponding homologation processes, in which the only service made available by providers that utilize mobile and fixed broadband networks is *internet* access. This thesis presents alternatives to integrate the fixed and mobile network of providers so as to offer MVPN (Mobile Virtual Private Network) and fixed services for application that require mobility, low cost, quality of service, connectivity and security with high scalability. The main solutions for broadband access for MVPN formation are presented to offer mobility. These solutions are analyzed and assessed in order to show their deficiencies for the utilization in VPN accessing. Quality of service, connectivity, security and scalability will be reached with the implementation of MPLS (Multi-Protocol Label Switching) in the core network. The implementation of MPLS in the core network consolidates transportation for several wireless and fixed access technologies, reducing the operational costs of providers, making networks more scalable and trustworthy, thereby preparing the provider for fourth generation (4G) access networks. Based on the requirements of the applications that will travel in the VPN, new contributions are proposed for fixed-mobile VPNs so that it meets these requirements with high scalability, mobility, security, connectivity and quality of service, both for the user and the provider. To validate the proposed contributions a test environment was implemented to evaluate the connectivity and isolation of the VPNs and the quality of service.

Two proposals to solve the VPN scalability problems are presented, one based on ACL (Access Control List) and the other based on firewall. An IPSec (IP Security Protocol) on MPLS proposal is also presented in order to solve configuration errors made by telecommunication providers.

Keywords: VPN, MPLS, MVPN, *mobile communication, quality of service and security*.

Dedicatória

"Em memória do meu pai"

Agradecimentos

Aos familiares, pelo incentivo e apoio durante todo o trabalho.

À minha filha, Bárbara Alano Boava.

Ao Professor Yuzo Iano, pela sua orientação e amizade.

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

Aos funcionários da Faculdade de Engenharia Elétrica e Computação da Unicamp.

Agradeço aos órgãos de incentivo à pesquisa CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e CNPq (Conselho Nacional de Desenvolvimento e Tecnológico) pelo apoio para que este trabalho pudesse ser realizado.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

ADSL – *Asymmetric Digital Subscriber Line*

AF – *Assured Forwarding*

ANSI – *American National Standards Institute*

AS – *Autonomous System*

ATM – *Asynchronous Transfer Mode*

ASBR – *Autonomous System Boundary/Border Router*

BA – *Behavior Aggregate*

BGP – *Border Gateway Protocol*

BSC - *Base Station Controller*

BW – *BandWidth*

CATV – *Community Antenna TV*

CE – *Customer Edge*

CMTS – *Cable Modem Termination Systems*

CPE – *Customer Premise Equipment*

DiffServ – *Differentiated Service*

DLCI – *Data-Link Connection Identifier*

DNS – *Domain Name System*

DOCSIS – *Data Over Cable Service Interface Specification*

DSCP – *DiffServ Codepoint*

DSLAM – *Digital Subscriber Line Access Multiplexer*

DVB-RC – *Digital Video Broadcasting - Reverse Channel*

DVD – *Digital Video Disc*

EBGP – *External BGP*

ECN – *Explicit Congestion Notification*

EDGE – *Enhanced Data rates for GSM Evolution*

EF – *Expedited Forwarding*

ESP – *EXPerimental*

FCC – *Federal Communications Commission*

FDM – *Frequency Division Multiplexing*

FEC – *Forwarding Equivalence Class*

FTP – *File Transfer Protocol*

FTTH - *Fiber - to-the-Home*

FWA – *Fixed Wireless Access*

GPRS – *General Packet Radio Service*

GRE – *Generic Routing Encapsulation*

GSM – *Global System for Mobile*

HDSL – *Hight-Level Data Link Control*

HDTV – *High-Definition Television*

HFC – *Hybrid Fibre-Coaxial*

HSPDA – *High-Speed Downlink Packet Access*

HTTP – *HyperText Transfer Protocol*

GTP – *GPRS Tunneling Protocol*

IEEE – *Institute of Electrical and Electronics Engineers*

IETF – *Internet Engineering Task Force*

ILEC - *Incumbent Local Exchange Carrier*

IntServ – *Integrated Services*

IP – *Internet Protocol*

ISP – *Internet Service Provider*

IPSec – *IP Security Protocol*

ISDN – *Integrated Services Digital Network*

IS-IS – *Intermediate System to Intermediate System*

ITU-T – *International Telecommunication Union*

LAC – *L2TP Access Concentrator*

LAN – *Local Area Network*

LDP – *Label Distribution Protocol*

LEO – *Low Earth Orbit*

LNS – *L2TP Network Server*

LSP – *Label Switched Path*

LSR – *Label Switch Router*

LTE – *Long Term Evolution*

L2TP – *Layer 2 Tunneling Protocol*

MAN – *Metropolitan Area Network*

MIMO - *Multiple-Input Multiple-Output*

MPEG – *Moving Picture Experts Group*

MPLS – *Multiprotocol Label Switching*

MVPN – *Mobile Virtual Private Network*

MMDS – *Multichannel Multipoint Distribution Service*

NGN – *Next Generation Network*

NGN-SDH – *Next Generation Network - Synchronous Digital Hierarchy*

OAM – *Operation Administration Maintenance*

OFDMA – *Orthogonal Frequency Division Multiple Access*

OSPF – *Open Shortest Path First*

P – *Provider*

PDU – *Protocol Data Unit*

PE – *Provider Edge*

PHB – *Per-Hop Behavior*

PPPoA – *Point-to-Point Protocol over ATM*

PPPoE – *Point-to-Point Protocol over Ethernet*

PSTN – *Public Switched Telephone Network*

PVC – *Permanent Virtual Circuit*

QoS – *Quality of Service*

RD – *Route Distinguisher*

RED – *Random Early Detection*

RFC – *Request For Comments*

RIP - *Routing Information Protocol*

RPR – *Resilient Packet Rings*

RR – *Route Reflector*

RT – *Rotas Targets*

RTP – *Real-time Transport Protocol*

RTT – *Round-Trip Time*

RSVP – *Resource Reservation Protocol*

SDH - *Synchronous Digital Hierarchy*

SDSL – *Synchronous Digital Subscription Line*

SDTV – *Standard Digital Television*

SLA – *Service-Level Agreement*

SMC – Serviço Móvel Celular

SMP – Serviço Móvel Pessoal

SNR – *Signal - to - Noise Ratio*

SP – *Service Provider*

STM – *Synchronous Transmission Module*

TCP – *Transmission Control Protocol*

TDM – *Time Division Multiplexer*

ToS – *Type of Service*

TPL – Comprimento do Pacote

TPTT – Tempo de Transferência Total do Pacote

TTL – *Time To Live*

TVoIP – *TV over IP*

UDP – *User Datagram Protocol*

UMTS – *Universal Mobile Telecommunication System*

VAS – *Value-Added Services*

VCI – *Virtual Channel Identifier*

VDSL – *Very high bit-rate Digital Subscriber Line*

VoIP – *Voice over IP*

VPI – *Virtual Path Identifier*

VPLS – *Virtual Private Lan Service*

VPN – *Virtual Private Network*

VPWS – *Virtual Private Wire Service*

VRF – *VPN Routing and Forwarding*

WiMax – *Worldwide Interoperability for Microwave Access*

Publicações:

A. Boava, Y. Iano. “A Methodology to build VPN IP MPLS with Connectivity and Security transport layer for Next Generation Network.” In: Journal of Information Assurance and Security, ISSN:1554-1010,Volume 6 Pages 176-185. 2011. www.mirlabs.net/jias/index.html.

A. Boava, Y. Iano. “A Methodology to Build VPN IP MPLS with Performance and Quality of Service.” In: Journal of Information Assurance and Security, ISSN:1554-1010,Volume 6 Pages 379-388.2011. www.mirlabs.net/jias/index.html.

A.Boava, Y. Iano. “Conectividade e Segurança na camada de transporte das VPNs IP MPLS para as redes NGN”. Unisal, Ciencia e Tecnologia, V12, Paginas 71-76, 2010, ISSN:167-9649.

A.Boava, Y. Iano. “Avaliação da Qualidade de Serviço das VPNs IP MPLS para redes de nova geração”. Unisal, Ciencia e Tecnologia, V11, Paginas 1-15, 2009, ISSN:167-9649.

Capítulo 1

Introdução

1.1 **Visão geral do mercado de telecomunicações e tecnologias**

Nas últimas décadas, duas grandes tecnologias, o protocolo IP e as redes de acesso banda larga, vêm convergindo para a definição de um ambiente total de comunicação, que é a integração das redes fixas com as redes móveis. Essa integração da rede fixa com a rede móvel é também chamada de convergência das redes [1]. A integração das redes fixas com as redes móveis consiste na utilização de acessos móveis e fixos para a formação de VPNs (*Virtual Private Network*). Algumas operadoras de telecomunicações chamam essas VPNs que integram os acessos fixos com os móveis de VPN fixo-móvel ou MVPN (*Mobile Virtual Private Network*)[1]. As MVPNs combinam a capilaridade do protocolo IP com a flexibilidade proporcionada pela mobilidade do acesso móvel.

A convergência das redes baseadas nas MVPNs com acesso banda larga representará, para o setor de telecomunicações nos próximos anos, a ampliação da oferta de novos serviços sobre as redes de acesso banda larga. A figura 1.1 mostra a tendência do crescimento dos acessos banda larga móvel em relação ao total de acessos móveis disponíveis.

[1] O termo *VPN móvel* é utilizado habitualmente pelas operadoras de telecomunicações para definir uma VPN que interliga os *sites* das empresas, sendo que ao menos um desses *sites* possui um acesso sem fio.

A possibilidade de acessar informação e serviços a qualquer momento e em qualquer lugar está demandando novas aplicações, que necessitam formas diferenciadas de tecnologias de acesso para utilizar o protocolo IP (*Internet Protocol*). Entretanto, o protocolo IP convencional não foi concebido para trabalhar com as características de QoS (*Quality of Service*), segurança, escalabilidade e, principalmente, em um ambiente onde os usuários se movimentam conectados à rede através de um enlace sem fio.

Os protocolos TCP/IP convencionais não são apropriados para as redes convergentes de nova geração, pois introduzem muito *overhead* e exigem que muitas mensagens sejam trocadas entre cliente e servidor para estabelecer uma configuração. Além desse problema, o IP convencional apresenta mais alguns problemas que inviabilizam a sua utilização como o protocolo para as redes convergentes de nova geração. Tais problemas estão relacionados com a qualidade de serviço, segurança e conectividade com escalabilidade. Esta tese propõe contribuições para as arquiteturas das redes de nova geração para resolver esses problemas. Para alcançar esses objetivos, é fundamental que o protocolo IP trabalhe em conjunto com o protocolo MPLS[2], que permitirá construir VPNs MPLS convergentes.

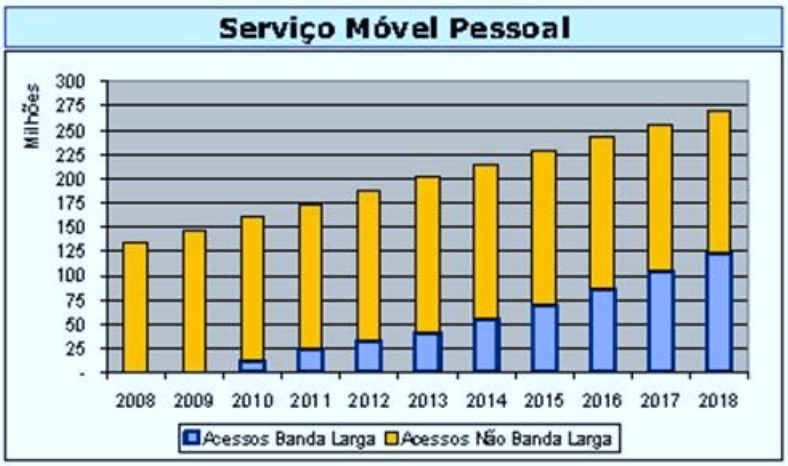

Figura 1.1 – Tendência de crescimento dos acessos banda larga, extraído de [2].

[2] MPLS é um protocolo de comutação baseado em *labels*, sendo recomendado sua implementação quando o objetivo é alcançar qualidade de serviço, segurança e escalabilidade.

As NGNs (*Next Generation Networks*) estão evoluindo, com o objetivo de dar suporte às aplicações de redes virtuais privadas fim a fim de acordo com a QoS necessária a determinadas aplicações. Isso é possível através de novas tecnologias de acesso banda larga, que proporcionam maior velocidade no enlace da rede de acesso que interliga o usuário ao núcleo da rede, e da utilização do protocolo MPLS em conjunto com o IP no núcleo da rede para prover a qualidade de serviço, a segurança, a escalabilidade e a conectividade necessárias às aplicações atuais e novas das redes convergentes.

Aumento da receita dos serviços por usuário, competição baseada em custo e foco na fidelização dos clientes são alguns requisitos básicos para as empresas de telecomunicações manterem-se no mercado atualmente. Nesse contexto foi que as operadoras de telecomunicações viram nas redes de acesso banda larga, principalmente nas tecnologias sem fio, a possibilidade de agregar novos serviços fixos e móveis aos usuários, sendo a *internet* móvel o principal serviço nesse cenário, que permite aos provedores de serviço um retorno positivo que justificasse seus investimentos em novas tecnologias.

Porém, no contexto atual, somente o serviço de acesso à *internet* não justifica o investimento significativo em novas tecnologias pelo provedor de serviço. Como resultado, as operadoras trabalham em novas pesquisas para oferecer novos serviços que justifiquem os altos investimentos na convergência da rede móvel com a rede fixa, ou seja, precisa-se investir em desenvolvimento de novos produtos que tenham demanda e tragam retorno do investimento para a operadora.

De forma simplificada, é possível definir convergência como sendo a integração da rede fixa com a rede móvel, formando o que será chamado nesta tese de Redes Virtuais Privadas Móveis (MVPN) ou VPN fixo-móvel. Portanto, a MVPN é definida como uma emulação de uma rede virtual privada formada por acessos móveis e fixos sobre uma rede compartilhada.

São características fundamentais das MVPNs a qualidade de serviço, segurança e conectividade. A MVPN é formada por *sites* sem fio, mas nem todos os *sites* precisam ser necessariamente sem fio. As soluções mais comuns de implementação de MVPN são aquelas onde o *site* concentrador da MVPN tem um acesso fixo dedicado com tecnologias *frame relay*[3], ATM ou *ethernet* e os *sites* remotos acessam através de outras tecnologias de rede sem fio.

Em alguns países, como no Brasil, o número de telefones celulares já ultrapassou o número de telefones fixos. A figura 1.2 apresenta o grande avanço da telefonia celular em relação à telefonia fixa, mostrando o grande potencial para a exploração de serviços de MVPN sobre essa forma de acesso [3].

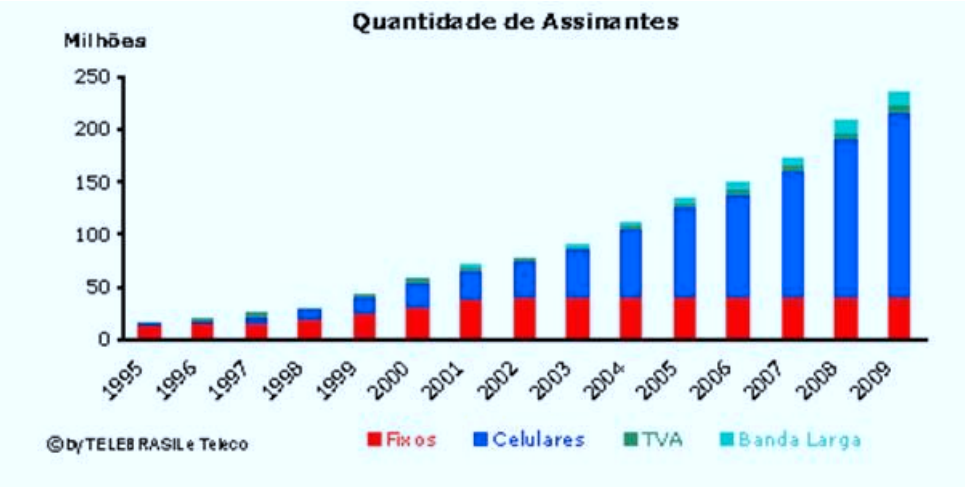

Figura 1.2 – Evolução dos acessos: fixos, móvel, TVA e banda larga, extraído de [3].

O impacto causado nas redes pela introdução de serviços banda larga em grande quantidade apresenta um valor significativo para as operadoras e para seus clientes. Será principalmente nas tecnologias de acesso das redes banda larga sem fio e *metroethernet*[4] que isso acontecerá de forma mais intensa, levando a uma quebra de algumas premissas utilizadas tradicionalmente no planejamento das redes das operadoras e, como consequência, à necessidade de uma nova abordagem para viabilizar o uso pleno das redes de acesso sem fio,

[3] *Frame Relay* é a tecnologia que dominou o mercado para implementação de VPNs de nível 2 até 2000. Essa tecnologia surgiu no fim da década de 80 como uma simplificação do protocolo X.25, para aumentar, principalmente, a vazão e reduzir o atraso.
[4] *Metroethernet* é uma forma de entregar serviços com interfaces IP em alta velocidade e granularidade.

como as redes de terceira geração (3G), integradas com as redes de outras tecnologias, como *metroethernet*, ATM, ADSL, *frame relay* e cabo, para novas aplicações que necessitam de integração com qualidade de serviço, conectividade, segurança e alta escalabilidade.

O grande mercado potencial de acesso banda larga 3G pode ser verificado observando-se a figura 1.3, que mostra a quantidade atual de banda larga[5] comparada com o DSL (*Digital Subscriber Line)*. A figura 1.3 mostra que, dos 11,4 milhões de acessos banda larga em serviço no Brasil, 7,7 milhões utilizam DSL.

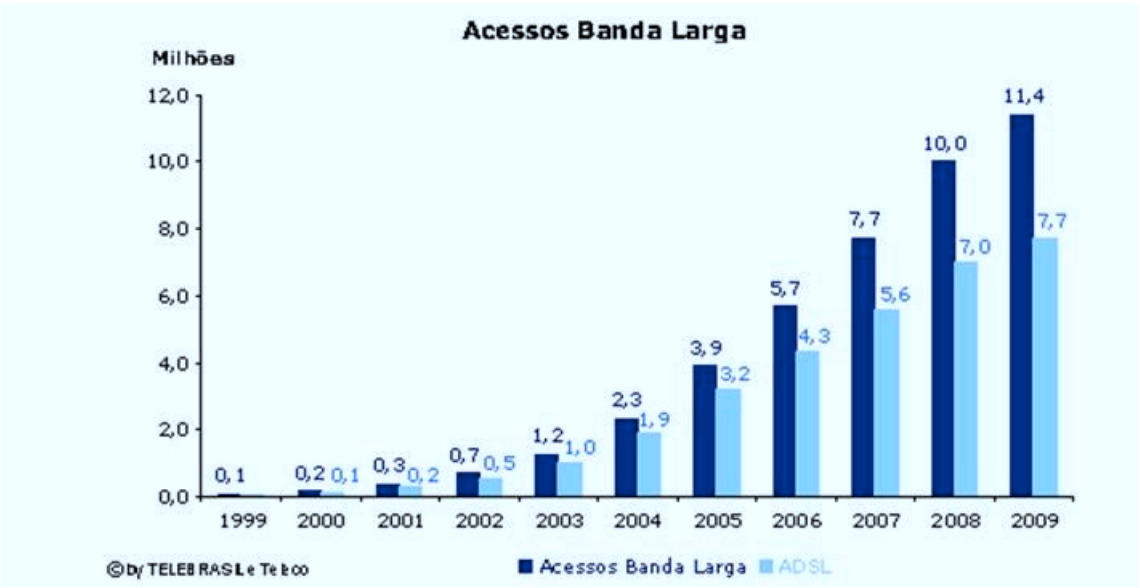

Figura 1.3 – Acesso banda larga x ADSL, extraído de [3].

O trabalho apresenta as principais tecnologias para a evolução das redes de banda larga e como as principais operadoras de telecomunicações poderão implementar soluções de convergência baseadas em VPNs fixo – móveis com acesso banda larga. A partir das principais tecnologias de banda larga, o trabalho mostra uma visão sobre o tema, propondo novas alternativas para tornar viável o uso dessas tecnologias de banda larga sem fio e com fio para a

[5] Banda larga, conforme a definição da UIT, significa acessos com velocidades superiores a 2 Mbits/s, mas essa definição tem apresentado significados distintos, conforme a região. No Brasil, convencionou-se chamar de banda larga todo acesso com velocidade superior a 128 Kbits/s, enquanto na Europa chama-se de banda larga todo acesso com velocidade superior a 256 Kbits/s.

formação de VPNs fixo - móveis convergentes que requerem QoS (Quality of Service - Qualidade de Serviço), conectividade e segurança com grande escalabilidade.

Existem grandes expectativas de que as novas tecnologias de acesso banda larga sem fio (3G, 4G e *WiMax*) e *metroethernet*, em conjunto com o protocolo MPLS no núcleo da rede, venham para mudar o cenário da limitação em velocidade e qualidade de serviço. Novos equipamentos para o usuário e para a rede do provedor que maximizam o uso da tecnologia e tornam os preços do Megabit/s cada dia menores são colocados no mercado periodicamente em grande velocidade.

No entanto, as demandas dos usuários não ficarão limitadas à conectividade com a *internet* apenas ou ao envio de mensagens com o celular. Já se observa entre os usuários uma necessidade de novos serviços como vídeo sob demanda que vão além da conectividade e da *internet*, somente. Os limites para oferecer serviços além da conectividade, com segurança e qualidade de serviço, estão levando as operadoras de telecomunicações e institutos a desenvolver pesquisas em novas tecnologias que possam atender a essas necessidades de mercado com escalabilidade.

Com o advento das novas tecnologias de banda larga sem fio e com fio, aliada às VPNs fixo - móveis, aumentará a oferta de novos aplicativos e serviços (IPTV e VoIP) e de produtos de valor agregado. Esses novos serviços geralmente estão baseados em convergência (voz, dados e imagem), segurança e QoS.

Os VAS[6] (Serviços de Valor Agregado) são serviços que as operadoras oferecem aos seus clientes sobre uma infraestrutura já instalada. Nesse contexto, pode-se cita por exemplo, o caso de uma operadora oferecer aos seus clientes o serviço de gerenciamento de VPN, que poderia possibilitar aos seus clientes certificar os SLAs (níveis de serviços contratado) junto à

[6] VAS ou SAV são formas muito comuns de as operadoras agregarem receita sobre uma rede ou serviço já implementado.

operadora, ou seja, verificar se aquilo que ele contratou é realmente aquilo que está sendo entregue.

Além de fontes de novas receitas, as operadoras de Telecom avaliam o VAS como a principal ferramenta para fidelização de seus clientes. Para que as operadoras possam oferecer os Serviços de Valor Agregado de VPNs fixo - móveis, é fundamental que o núcleo da rede trabalhe com MPLS, pois ele possibilita a implementação de VPNs baseadas em rede, ou seja, aquela VPN em que o provedor é responsável por toda a configuração. Com a funcionalidade do MPLS para VPNs, toda e qualquer alteração dessas VPNs implica acionar o provedor para fazê-la; isso cria uma dependência do cliente ao provedor, a qual normalmente se consolida como fidelização desse cliente.

No entanto, somente a qualidade de serviço, conectividade e segurança não são suficientes para que as operadoras consigam atender às necessidades dos seus clientes e se mantenham no mercado; é necessário rapidez no momento da implementação de uma nova demanda de serviço pelo mercado, e isso é possível somente com uma rede que suporte alta escalabilidade para oferecer novos serviços baseados em VPNs específicas. As contribuições propostas nesta tese são no sentido de implementar o MPLS no núcleo da rede com o intuito de resolver essas novas demandas do mercado com alta escalabilidade.

O objetivo principal desta tese é apresentar novas contribuições para as arquiteturas de integração que possam viabilizar às operadoras de telecomunicações a implementação de novos serviços com rapidez, QoS e segurança, utilizando as tecnologias de banda larga como forma de acesso.

1.2 **Análise dos contextos nacional e internacional**

Este tópico apresenta o histórico das redes de telecomunicações. Busca avaliar o que vem ocorrendo no país e no exterior e apresentar uma análise dos aspectos que necessitam ser

considerados nas novas arquiteturas de redes convergentes baseadas no protocolo MPLS no núcleo da rede e várias tecnologias de banda larga como formas de acesso. Também são avaliadas as necessidades das principais demandas das aplicações do mercado, principalmente aquelas relacionadas com vídeo, voz e dados, pois é importante saber se serão aderentes aos novos ambientes de convergências [2].

O posicionamento mercadológico das grandes empresas de telecomunicações, que não mais se limitam às fronteiras das suas áreas de concessão de origem, e as oportunidades de novos nichos para atender ao mercado de massa ou ao mercado corporativo, que demandam aplicações específicas, são aspectos que necessitam ser entendidos na implementação das novas tecnologias de acesso em banda larga e MPLS. O foco nas necessidades dos novos serviços e a preparação das redes que possam atender aos futuros desafios das telecomunicações são as essências das novas tecnologias que permitirão a convergência. Porém, além da aderência aos futuros serviços, a tecnologia proposta deve ser capaz de preservar os investimentos feitos pelas operadoras no passado. Para isso, a implementação do protocolo MPLS no núcleo da rede é fundamental, pois ele permite a integração com as mais diversas tecnologias, inclusive com aquelas que não são mais consideradas inovadoras, como o *frame relay* e ATM[7].

Novas formas de oferta de aplicações convergentes, que fazem uso de voz, dados, textos e multimídia, apoiadas por infraestrutura multiuso de banda larga, dominada pelas grandes operadoras, requerem o desenvolvimento de novos serviços que tirem proveito das novas tecnologias de banda larga e que atendam à necessidade e rapidez de implementação para a oferta dos novos serviços ao mercado [2,4]. As VPNs MPLS são atualmente a forma mais econômica para as operadoras disponibilizarem novos serviços com a agilidade e velocidade que o mercado exige. Deve-se considerar um nível aceitável para a qualidade de serviço requerida pelas aplicações com segurança. Aplicação somente de acesso à *internet* já não mais

[7] As redes baseadas em ATM não obtiveram sucesso comercial, pois seu alto custo e complexidade inviabilizaram sua utilização na maioria dos projetos. Hoje, sua utilização é somente na forma de acesso e quando não existe alternativa.

atende às necessidades dos usuários, principalmente o corporativo, sendo necessário criar novos serviços para as aplicações das futuras redes.

1.2.1 SITUAÇÃO ATUAL DAS TELECOMUNICAÇÕES NO BRASIL

As empresas de telecomunicações realizaram o maior plano de investimento da história na expansão, modernização e melhoria na qualidade da prestação de serviços. Entre 2001 e 2006, por exemplo, a penetração da telefonia fixa e móvel, como percentual dos domicílios, evoluiu de 58,9% para 74,5%. Atualmente, mais de 35 mil localidades brasileiras dispõem do serviço telefônico. Uma importante conclusão observada a partir da análise dos dados de investimentos das prestadoras realizados no período 1998-2007 refere-se à sua diversificação em relação ao portfólio de serviços. Assim, constatou-se a ampliação e consolidação da oferta do Serviço Móvel Pessoal – SMP[8], TV por assinatura, transmissão de dados em diversas modalidades [4]. É evidente uma tendência de crescimento nos investimentos dos serviços de banda larga e de valor agregado.

Após um ciclo de desenvolvimento no Brasil, em que a universalização da telefonia fixa foi o carro-chefe, as operadoras de telecomunicações atualmente focam em serviços que ofereçam maior valor agregado, como os serviços de VPN de voz, dados e vídeo. A oferta desses serviços convergentes em forma integrada começa a tomar vulto, passando do denominado *triple play* (telefonia, banda larga e TV por Assinatura) e evoluindo para incluir a mobilidade ("*quadruple play*"). O maior dinamismo dos mercados de comunicação sem fio e de comunicações de dados e a estabilização do crescimento dos serviços de telefonia fixa revelam uma transformação estrutural das tendências em telecomunicações. Por um lado, a extraordinária expansão dos serviços que utilizam as tecnologias sem fio expressa a afirmação da mobilidade como um atributo essencial às comunicações interpessoais. Por outro, faz-se necessária a ampliação das soluções multisserviços de dados corporativos através das diversas tecnologias (3G, *metroethernet, WiMax*, etc.) que poderão ser disponibilizadas pelos provedores

[8] SMP foi o sucessor do serviço de comunicação móvel celular (SMC) no Brasil.

de serviços de Telecom para colocar um fim nas diversas formas de transporte de informações de voz, dados e vídeo pelas empresas através de várias plataformas de redes distintas. Essa substituição de várias redes distintas por uma plataforma única de serviço caracteriza o que chamamos de convergência dos serviços [4].

O sucesso das operadoras estará, a cada dia, mais diretamente relacionado à capacidade de atender a esses serviços convergentes. Em função disso, as operadoras têm feito um grande esforço para implementar um único protocolo no núcleo da sua rede que suporte todos os serviços. Inicialmente, o protocolo que apareceu como um grande candidato foi o ATM, mas seu elevado custo de implementação e dificuldade de trabalhar em conjunto com o protocolo IP fizeram com que as operadoras o abandonassem como protocolo de núcleo da rede e o utilizassem somente em projetos especiais na forma de acesso e, quando não existem alternativas, com outro protocolo da rede de acesso.

Nesse contexto, já é consenso entre as operadoras e os principais fornecedores de equipamentos que o protocolo IP deve ser o protocolo do núcleo das redes convergentes. Contudo, também há um entendimento de que o protocolo IP tradicional, baseado no modelo *best effort*,[9] sem qualidade de serviço e sem segurança, não atende aos requisitos das redes convergentes, em função dessas deficiências intrínsecas do protocolo IP. Como consequência dessas deficiências do protocolo IP e da necessidade da convergência dos serviços, este trabalho propõe a implementação de MPLS no núcleo da rede e acesso de banda larga de alta capacidade para a formação de VPNs MPLS fixo - móveis, de acordo com os requisitos dos novos serviços convergentes, como qualidade de serviço e segurança.

Essas tecnologias de banda larga em alta capacidade não dizem respeito somente às redes 3G, ADSL e cabo, mas também a novas tecnologias em processo de homologação e teste pelas operadoras, como o *WiMax* e *metroethernet*. Todas essas tecnologias são avaliadas nos

[9] *Best effort* é um modelo de tráfego da *internet* onde todos os aplicativos são tratados da mesma forma, sem nenhum tipo de diferenciação; por exemplo, voz é tratada da mesma forma que *e-mail*.

próximos capítulos para, em conjunto com o protocolo MPLS, formar novos serviços convergentes, como as VPNs fixo móveis.

1.2.2 SITUAÇÃO DA BANDA LARGA NO MUNDO

Atualmente, os dois tipos de acesso residencial banda larga predominantes são a linha digital de assinante (DSL) ou a cabo. Em muitos países desenvolvidos, mais de 50% das residências possuem acesso banda larga, sendo que a Coreia do Sul, Islândia, Holanda, Dinamarca e Suíça lideram o mercado, com mais de 74% de penetração nas residências em 2008. Nos Estados Unidos, as tecnologias DSL e a cabo têm a mesma participação no mercado para acesso banda larga. Fora dos Estados Unidos e do Canadá, a DSL domina particularmente na Europa, onde, em muitos países, mais de 90% das conexões banda larga são DSL [5].

O Brasil, em relação a outros países, apresenta um baixo percentual da população que possui acesso à *internet*, principalmente em função do alto custo do *Megabit* por segundo, conforme a figura 1.4.

Países como os Estados Unidos, que atualmente têm maior concentração de banda larga em cabo e DSL, vêm promovendo várias licenças de faixas de frequências através da FCC[10] com o objetivo de tornar mais eficiente o uso do espectro, bem como de incentivar o aumento do mercado de banda larga sem fio. O maior exemplo foi a licitação recente da faixa de 700 MHz, que tem como objetivo construir uma infraestrutura de *internet* de alta velocidade de alta capilaridade. Os países europeus, representados em sua maioria por grandes empresas, como a Telefônica (Espanha), France Telecom (França), Deutsch Telecom (Alemanha), Bridge Telecom (Inglaterra) e Itália Telecom (Itália), têm caminhado na direção do incentivo à comunicação sem fio, mas também existe uma forte tendência, nesses países, de haver uma separação entre o acesso ao serviço e o seu conteúdo. Essa separação implica que pessoas jurídicas diferentes podem oferecer o serviço de acesso e conteúdo [5].

[10] A FCC (*Federal Communications Commission)* equivale à Anatel nos Estados Unidos. A FCC é que regulamenta e autoriza os serviços de telecomunicações nos Estados Unidos.

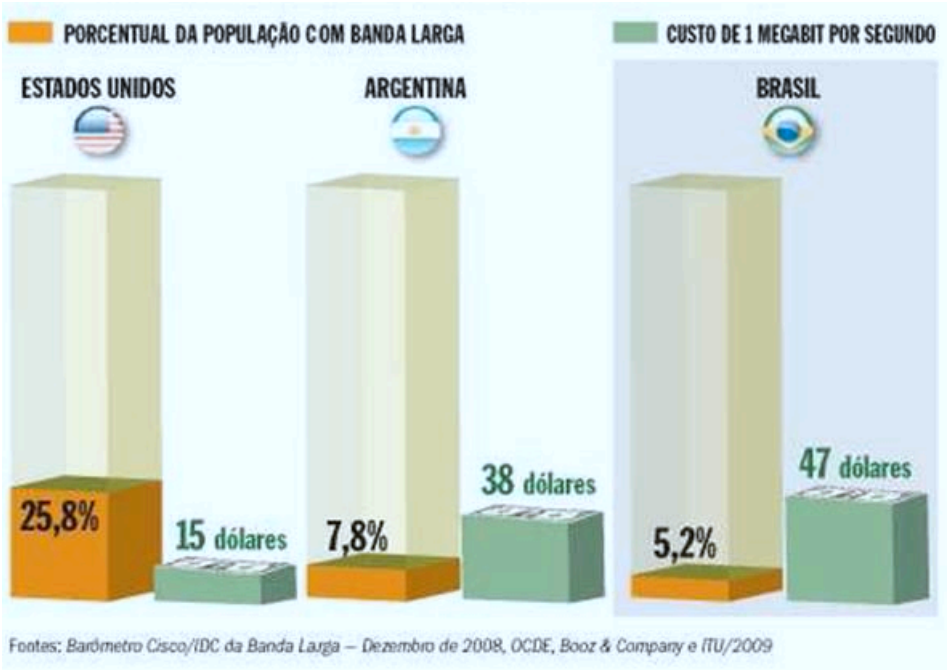

Figura 1.4 – Custos nos Estados Unidos, Argentina e Brasil, extraído de [6].

A figura 1.5, apresentada a seguir, mostra o desempenho, em vários países, do tempo necessário para baixar um filme com qualidade de DVD. O Japão apresenta um melhor desempenho, em função de usar *metroethernet* como forma de acesso à *internet*. Essa tecnologia está começando a ficar comercialmente disponível no Brasil e é detalhada no próximo capítulo.

Figura 1.5 – Desempenho da transmissão de vídeo, extraído de [7].

1.3 O mercado de telefonia móvel

A comunicação móvel celular no Brasil completou, em 2009, 19 anos. Teve início em 1990 com a designação de Serviço de Radiocomunicação Móvel Terrestre Público-Restrito Celular. Por preceito legal, esse serviço foi transformado, em 1996, em concessão, com a designação de SMC(Serviço Móvel Celular), sendo posteriormente, em 2002, substituído pelo SMP(Serviço Móvel Pessoal), serviço de telecomunicação móvel terrestre de interesse coletivo e prestado no regime privado. O SMP, além de representar considerável evolução regulatória, incrementou a expansão da telefonia móvel, marcada por expressivos avanços, como mais uma vez ficou evidenciado no exercício de 2007. O SMP pré-pago, introduzido no Brasil em 1998, teve contribuição acentuada nesse cenário evolutivo, pois, seguindo tendência mundial, o número de usuários continuou crescendo a taxas mais elevadas que o número de usuários do SMP pós-pago [4].

1.3.1 EVOLUÇÃO DA PLANTA

Desde o início das operações do serviço móvel, o número de acessos em serviço cresceu de 4,5 milhões, em 1997, para 174 milhões de acessos no final de 2009.

Dentre os fatores que contribuíram para esse crescimento, destacam-se: a entrada de novos prestadores em São Paulo e no Nordeste, o início da operação da 3ª Geração, que promoverá o aparecimento de novos serviços e a expansão da banda larga, e os pacotes promocionais de minutos para chamadas na rede da própria operadora a preços cada vez mais baixos. No final de 2009, 97,0% da população tinham acesso ao serviço de comunicação móvel celular, sendo que [4]:

- ✓ 78,6% da população eram servidos por quatro ou cinco prestadoras;
- ✓ 6,3% da população eram servidos por três prestadoras;
- ✓ 4,8% da população eram servidos por duas prestadoras; e

- ✓ 7,3% da população eram servidos apenas por uma prestadora.

No final de 2009, 86,3% dos municípios já contavam com o serviço de comunicações móvel celular [3].

1.4 Por que Qualidade de Serviço (QoS) e MPLS são fundamentais para as operadoras de telecomunicações móveis e fixas

As operadoras de telecomunicações móveis estão enfrentando grandes desafios, que incluem os altos valores das licenças para exploração do serviço móvel, o momento de concorrência entre as operadoras de telefonia móvel e fixa, o alto custo de investimento em equipamentos na rede, o aprovisionamento dos serviços e, principalmente, serviços que possam ser disponibilizados rapidamente ao mercado, sem grandes dificuldades técnicas e baixo investimento. A QoS (*Quality of Service*) e MPLS têm se apresentado como a solução mais conveniente e eficiente para superar esses desafios. Utilizando as vantagens da QoS e MPLS, as operadoras móveis poderão explorar facilidades não-disponíveis com as tecnologias atuais [8].

1.4.1 MAXIMIZAR O RETORNO DO INVESTIMENTO DA INFRAESTRUTURA NO ACESSO DE RÁDIO

A rede de acesso a rádio não é apenas a parte que exige maior investimento das operadoras de telecomunicações; é um dos principais elementos responsáveis pela satisfação da qualidade de serviço percebida pelo usuário. Além disso, a boa escolha da rede de acesso é fundamental para que a operadora possa otimizá-lo, de modo a oferecer a seu cliente vários serviços em um único meio.

1.4.2 ALTO RETORNO PARA SERVIÇO DE VALOR ADICIONAL

A capacidade das redes de acesso 3G, em conjunto com o MPLS no núcleo da rede, para a formação de VPNs fixo - móveis permite oferecer soluções com qualidade de serviço diferenciada por cliente.

1.4.3 OFERTA DE SERVIÇO ALÉM DA SIMPLES CONECTIVIDADE

A oferta de VPNs fixo - móveis permite às operadoras de telecomunicações oferecerem ao mercado serviços que não sejam orientados somente à conectividade, por exemplo os serviços de conteúdos. As MVPNs baseadas em MPLS e acesso 3G fazem com que todo o roteamento das redes seja realizado e controlado pelas operadoras de telecomunicações em seu núcleo de rede, e não mais pelos seus clientes em seus roteadores. Esse aspecto é de fundamental importância para a operadora fidelizar seus clientes, pois qualquer mudança em suas redes locais implicará alterações no ambiente da operadora. Isso tem como consequência principal uma dependência do cliente em relação à operadora.

1.4.4 REDUÇÃO DO CUSTO ATRAVÉS DA CONSOLIDAÇÃO DE UMA REDE ÚNICA

A oferta de serviço móvel baseado em uma rede com núcleo MPLS permitirá que essa mesma rede seja consolidada para a convergência dos serviços. Qualquer serviço poderá ser transportado através do núcleo da rede, habilitando uma determinada classe de serviço específica que atenda aos requisitos das aplicações que trafegarão na rede.

1.5 Trabalhos relacionados

Vários trabalhos foram realizados através de simulações com o objetivo de avaliar algumas especificações das redes convergentes de maneira isolada. Basicamente, as simulações eram realizadas com dois *softwares* de simulação de rede, mais precisamente, o NS e o *Opnet*. Já os resultados que são apresentados neste trabalho são consequências de um ambiente real montado para coletar os dados e posterior avaliação.

Andrew Viterbi [9] apresentou em seu livro que o sucesso de uma rede de comunicação convergente está fundamentado em quatro leis básicas: Maxwell, Shannon, Moore e Metcafe. Mostra-se, neste trabalho, que as premissas de Viterbi em relação à Metcafe não são mais aplicáveis para o cenário atual. Conforme Viterbi em seu livro, os custos para formação de uma rede são proporcionais à quantidade de *sites* ao quadrado (n^2), mas neste trabalho apresenta-se

uma proposta que utiliza MPLS no núcleo das redes convergentes, o que faz com que o custo seja proporcional somente à quantidade de *sites n*.

Em Davie, Bruce e Y.Rekhter [10], são avaliados os aspectos mais importantes da segurança em redes de comunicação que utilizam as tecnologias ATM e *frame relay*. São apresentados os mecanismos de segurança baseados em CVP (Circuitos Virtuais Permanentes) e DLCI (*Data-Link Connection Identifier*).

Segundo Marcos A. de Siqueira [11], as VPNs MPLS podem ser realizadas através da conectividade de túneis seguros entre os equipamentos do usuário. Após uma vasta investigação, os autores chegaram à conclusão de que a arquitetura VPN MPLS poderá apresentar o mesmo nível de segurança oferecido pelas tecnologias de camada de enlace, como *frame relay* e ATM, desde que as VPNs MPLS sejam devidamente configuradas pelo provedor de serviço.

Vasconcelos [12] apresentou, em sua tese, um trabalho que avaliou a qualidade de serviço em ambientes móveis, concentrando-se nas questões relativas à rede de núcleo dos sistemas celulares de terceira geração. Essas redes devem ser capazes de oferecer suporte a serviços com requisitos rígidos em alguns parâmetros de QoS, como o exigido pelas aplicações de tempo real de voz e vídeo interativos. O autor observou que as principais soluções de QoS propostas para a *internet*, que trabalha com o IP tradicional, nem sempre possibilitarão o atendimento dos requisitos do núcleo da rede. As soluções tradicionais baseadas em IntServ e DiffServ não resolvem as dificuldades técnicas provocadas pela mobilidade. A movimentação dos nós exigiria frequente renegociação de recursos na alternativa do IntServ e também tornaria difícil a realização de um provisionamento estático na alternativa do DiffServ. Foi então proposta pelo autor uma arquitetura de serviços voltada para o ambiente de mobilidade, baseando-se em classes de serviços que permitem a degradação de alguns parâmetros de qualidade de serviço para a garantia de outros. No entanto, essa proposta trabalhou com

alocação das classes em determinadas filas para determinados requisitos de QoS, e os resultados foram certificados através de simulações, enquanto esta tese propõe a implementação de MPLS no núcleo da rede para trabalhar em conjunto com o IP para oferecer as vantagens de escalabilidade, segurança, QoS às VPNs convergentes sobre um núcleo IP MPLS em um ambiente real.

Hanshi [13] sugere um algoritmo para proteção da QoS em redes MPLS, explorando a facilidade do rápido rerroteamento (*fastrerouter*)[11] da tecnologia MPLS. A queda de enlace sempre ocasiona um aumento do atraso e perdas de pacotes, portanto, a rede tem que restabelecer o tráfego, transferindo-o da rota afetada para uma alternativa. O autor propõe um método de proatividade de QoS para o tráfego protegido através da configuração de caminho alternativo com antecedência. Com o objetivo de realizar o roteamento rápido para o caminho alternativo, os critérios de seleção são baseados em largura de banda e atraso fim a fim.

Hung e Wang [14] apresentam, em seu artigo, uma proposta de tudo sobre MPLS (All-MPLS) para o núcleo da rede 3G UMTS. Túneis GTPs têm sido definidos pelo 3GPP como um mecanismo de transporte para UMTS. Para cada pacote de transmissão, são necessários 40 *bytes* (GTP, UDP e IP) extras para a transmissão. Para pequenos pacotes, como o de VoIP, o *overhead* é considerável. Em resposta a esses inconvenientes, os autores propõem integrar a tecnologia MPLS com a tecnologia 3G UMTS. Os túneis GTP são substituídos por túneis MPLS (8 *bytes*), representando uma diminuição de 40 *bytes* para 8 *bytes*. Ao diminuir o *overhead*, a nova abordagem melhora a eficiência de transmissão de 63% para 89,5% para o pacote VoIP. Além disso, a nova proposta oferece melhor balanceamento de carga, maior disponibilidade do serviço e melhor qualidade de serviço em comparação com as abordagens atuais.

Em Sasan e Shervin [15], a proposta é a administração e operação das redes móveis IP MPLS. Os autores apresentam uma arquitetura para avaliar a integridade das redes e suas

[11] *Fastrerouter* é uma das facilidades da rede MPLS que permite o reroteamento entre caminhos estabelecidos.

interoperabilidades com as infraestruturas de outras redes existentes. A importância da contribuição está no fato de que está mais comum o transporte de tráfego de nível dois como o 802.11 sobre as redes IP MPLS. O trabalho investiga diferentes requisitos de módulos, os esforços de padronização, detecção de falhas, verificação de conectividade e gerenciamento total das funcionalidades. Para alcançar esses objetivos, é proposta uma nova topologia de implementação de ferramentas adequadas de OAM entre as camadas de comunicações para garantir a mobilidade IP MPLS com grande escalabilidade. Essas ferramentas são importantes não somente para detectar prováveis defeitos entre as redes MPLS, mas também para gerenciar os contratos de SLA[12] dos clientes das operadoras. Também é possível com essas ferramentas a implantação eficiente de qualidade de serviço e engenharia de tráfego.

Tingzhou Yang e Dimitrios Makrakis [16] apresentam uma hierarquia *mobile* MPLS para as aplicações sensíveis a *delay* sobre a *internet* sem fio. *Mobile* MPLS integra os protocolos *mobile* IP e MPLS para o suporte de mobilidade MPLS. As operadoras de serviços móveis têm implementado células cada vez menores para aumentar a capacidade do sistema, provocando consequentemente um maior número de *handoff*. Em redes de operadoras que implementam em seu núcleo MPLS o uso do *mobile* IP, não é uma solução ótima. Para resolver as deficiências do *mobile* IP em uma rede MPLS, é sugerido um processo de sinalização rápida "*make-before-break*" no mecanismo de *mobile* MPLS. Um LSP é estabelecido antes de o *host* móvel mover-se para uma nova rede de cobertura. É demonstrado através de simulação que, com a hierarquia *mobile* MPLS, o atraso dos hosts móveis durante o *handoff* é diminuído consideravelmente. Levando em conta a introdução crescente de novos aplicativos (como voz sobre IP e vídeo) e equipamentos (sensores, monitores) que utilizam a rede sem fio, é fundamental que a rede seja capaz de fornecer garantias de baixo atraso.

Ravi Bhagavathula, Nagaraja Thanthry e Ravi Pendse [17] propõem, em seu artigo intitulado "*Mobile* IP e Rede Virtual Privada", que a necessidade de conectividade à *internet* está

[12] SLA é um contrato de níveis de serviço estabelecido entre a operadora e o seu cliente.

conduzindo a aceitação de soluções de mobilidade diferentes das convencionais. *Mobile* IP é uma das propostas amplamente aceitas para atender aos requisitos de mobilidade dos nós móveis. Embora o IP móvel atenda aos requisitos de conectividade dos nós móveis, as questões relativas à qualidade de serviço e segurança permanecem sem solução. Os usuários corporativos têm necessidade de segurança e qualidade de serviço, mesmo como visitantes em outra rede externa. As questões de QoS torna-se mais complicada quando se trata de uma rede em movimento (rede móvel). A VPN (*Virtual Private Network*) pode ser uma solução alternativa para a mobilidade para atender à segurança e à QoS. O trabalho atual investiga a QoS fornecida pelas alternativas tradicionais do *mobile* IP quando comparadas com as VPNs.

Rong Ren, Deng-Guo Feng e Ke Ma [18] apresentam uma proposta de IPSec sobre MPLS para prover segurança contra o ataque de usuário da mesma VPN e, como MPLS não utiliza nenhum tipo de criptografia entre o CE e PE, os autores sugerem a utilização de IPSec em conjunto com MPLS para aumentar o nível de segurança com a implementação de criptografia. É importante dizer que o custo de solução aumenta significativamente com a implementação de IPSec. De acordo com os autores, há quatro formas de implementar segurança em uma VPN: tunelamento, criptografia, gerenciamento de chaves e autenticação. É importante destacar que a proposta dos autores é baseada em IPSec de CE a PE, enquanto esta tese sugere, num dos capítulos, a utilização de CE a CE. A proposta dos autores de IPSec somente entre CE e PE faz sentido para a época, pois a maioria das aplicações era baseada em acessos remotos.

1.6 **Objetivo**

1.6.1 OBJETIVO GERAL

Este trabalho tem como objetivo geral estudar as características dos sistemas móveis e fixos para propor novas contribuições para as arquiteturas das (MVPNs) Redes Virtuais Privadas Móveis e fixas utilizando como acesso as tecnologias de banda larga e núcleo MPLS, oferecendo para o usuário qualidade de serviço, segurança e conectividade, além de alta

escalabilidade para a operadora de telecomunicações. As novas contribuições devem ser capazes de oferecer VPNs com níveis de QoS (*Quality of Service*) necessários às aplicações. O trabalho é voltado para as partes das redes de acesso banda larga e o núcleo da rede. Tanto o acesso quanto o núcleo de rede devem estar preparados para tratar tráfegos diferentes, de acordo com a aplicação do usuário.

1.6.2 OBJETIVOS ESPECÍFICOS.

- ✓ Evidenciar que as tecnologias de banda larga podem ser utilizadas não somente para o acesso à *internet*, mas também para fornecer outros serviços como as VPNs MPLS, tão seguros quanto as redes dedicadas, *frame relay* e ATM, com um custo inferior ao das soluções tradicionais;
- ✓ Apresentar as tecnologias de banda larga para a formação de VPN;
- ✓ Descrever a tecnologia de banda larga a cabo (*net*) que pode ser utilizada como forma de acesso das VPNs MPLS;
- ✓ Mostrar o desempenho das VPNs com acesso *frame relay* em relação às VPNs com acesso ADSL para o transporte de voz;
- ✓ Apresentar os conceitos fundamentais para construção das VPNs convergentes, muitas vezes chamadas de MVPNs;
- ✓ Descrever as principais arquiteturas de qualidade de serviço utilizadas para formação de MVPN;
- ✓ Avaliar a segurança, a conectividade e o isolamento das MVPNs;
- ✓ Apresentar uma proposta para resolver a questão de escalabilidade dos PEs;
- ✓ Propor uma alternativa para resolver os erros de configuração das VPNs MPLS provocados pelas operadoras;
- ✓ Mostrar como as principais operadoras de telecomunicações implementam as MVPNs.

1.7 **Estrutura do texto**

O trabalho está organizado da seguinte maneira. O Capítulo 1 apresenta uma introdução do trabalho através de uma breve história da evolução das comunicações móveis e de banda larga no contexto nacional e internacional. O capítulo 2 explora os aspectos relacionados aos tipos de acessos de banda larga que podem ser utilizados como acesso de VPN (*Virtual Privade Network*) fixo - móvel. O capítulo inicia descrevendo as forma de acessos ADSL, *Cable Modem*, Rádio e Satélite. Em seguida, essas formas de acesso são utilizadas para a construção de VPN. O capítulo é finalizado com uma comparação de desempenho de uma VPN Frame Relay tradicional com a VPN ADSL. O capítulo 3 avalia os aspectos teóricos das construções de redes MVPN(*Mobile Virtual Private Network)* e fixas, com maior ênfase nas VPNs que utilizam o núcleo MPLS. O capítulo 4 mostra a necessidade da introdução de QoS (*Quality os Service*) em VPN por meio de uma análise de um ambiente real montado através de uma topologia que permitiu a avaliação e análise das técnicas da QoS implementadas. A tecnologia MPLS é avaliada para o suporte à QoS em núcleo de redes fixas e móvel e, futuramente, para a utilização em *backhaul*. No capítulo 5, é apresentado como são realizados a conectividade e o isolamento das MVPNs. O capítulo 6 mostra os problemas decorrentes de escalabilidade dos PEs e apresenta algumas propostas para resolvê-los. Finalmente, o capítulo 7 apresenta a conclusão e os trabalhos futuros.

Capítulo 2

VPNs MPLS com acesso banda larga

Neste capítulo, são propostas e discutidas algumas alternativas de construção de redes virtuais privadas móveis e Fixas através das várias opções de tecnologias banda larga. O capítulo tem como principal objetivo mostrar que as tecnologias de banda larga podem ser utilizadas como forma de acesso de outros serviços, como as VPNs, e que banda larga não significa somente conexão à *internet*. Os problemas decorrentes das novas tecnologias das VPNs fixo - móveis serão avaliados e comparados. Essas novas propostas requerem diferentes arquiteturas de rede. O objetivo é identificar e comparar as diversas tecnologias, modelos e suas integrações.

Este capítulo está organizado da seguinte forma. A seção 2.1 discute a evolução dos acessos banda larga para a formação de VPN, que são: ADSL, cabo, *WiMax* e satélite. Nessa seção, apresentam-se as VPNs com acesso a cabo (*net*); essa é uma nova proposta que poderá ser explorada no futuro pelas empresas de TV a cabo no Brasil e outras empresas no mundo. A seção 2.2 descreve as principais características dos acessos para formação das redes virtuais privadas *frame relay* para serem comparadas com as das redes virtuais privadas ADSL. A seção 2.3 mostra implementações baseadas em combinações das tecnologias ADSL com *frame relay* e ATM para a formação de redes virtuais privadas. Esses modelos de implementação de VPN com acesso banda larga ADSL são uma novidade tecnológica e somente começaram a ser

disponibilizados no Brasil recentemente. A seção 2.4 descreve as principais tecnologias de acesso sem fio para formação das MVPNs (*Mobile Virtual Private Network*), bem como seus sistemas e serviços de dados, e apresenta o cálculo da capacidade de canal para as principais tecnologias de rede sem fio que serão utilizadas como acesso das MVPNs. A seção 2.5 apresenta uma nova forma de acesso para formação de VPNs de banda larga, chamada *metroethernet*. A seção 2.6 apresenta uma análise de desempenho, comparando as tecnologias *frame relay* com a tecnologia ADSL. Finalmente, a seção 2.7 traz uma nova proposta para arquiteturas de *backhaul* com base em MPLS *ethernet*.

2.1 **Redes de acesso banda larga para formação de VPN**

Na década de 1990, grandes iniciativas foram tomadas pelas operadoras de redes públicas de telecomunicações no sentido de que fosse viável o fornecimento de serviços de televisão interativa nas residências. Várias tecnologias foram desenvolvidas, e experimentos práticos de campo e bancadas foram implementados pelas operadoras de telecomunicações, como a aplicação de vídeo sob demanda. No entanto, em meados da mesma década, ficou claro que essa não era uma aplicação cuja demanda estimada justificasse os altos investimentos necessários à sua disponibilização naquela época. Houve então uma tendência ao abandono das pesquisas em curso pelas operadoras de telecomunicações que tinham interesse na exploração do serviço. Em contrapartida, foi nessa mesma época que a demanda por acesso à *internet*, em especial à WWW, explodiu. Assim, as operadoras de telecomunicações começaram a investir em acesso banda larga para conexão à *internet* para justificar novos investimentos em novas tecnologias da rede de acesso [19]. No contexto atual das telecomunicações, a tendência é utilizar as redes banda larga para viabilizar o acesso a todos os aplicativos. Este capítulo propõe-se a apresentar novos métodos para implementar redes virtuais privadas móveis e fixas através das atuais e futuras tecnologias de banda larga.

No Brasil, assim como na maioria dos outros países, existem quatro principais meios de acesso em banda larga [5,6] e outro em processo de homologação pelas operadoras, que é a tecnologia *metroethernet:*

- ✓ xDSL: tecnologia para a transmissão de dados por fios de cobre da infraestrutura que conecta o aparelho telefônico à central telefônica;
- ✓ Cabo: tecnologia para a transmissão de dados por cabos coaxiais normalmente usados na infraestrutura de transmissão de TV paga;
- ✓ FWA / Rádio: transmissão de dados com infraestrutura sem fio na última milha;
- ✓ Satélite: tecnologia para transmissão de dados via satélite;
- ✓ *Metroethernet:* tecnologia que entrega a interface *ethernet* diretamente ao usuário em alta velocidade.

A figura 2.1 apresenta diversos tipos de tecnologias de acesso ao roteador de borda do provedor. Esta seção analisa as principais tecnologias de rede de acesso disponíveis pelos provedores de serviços de telecomunicações.

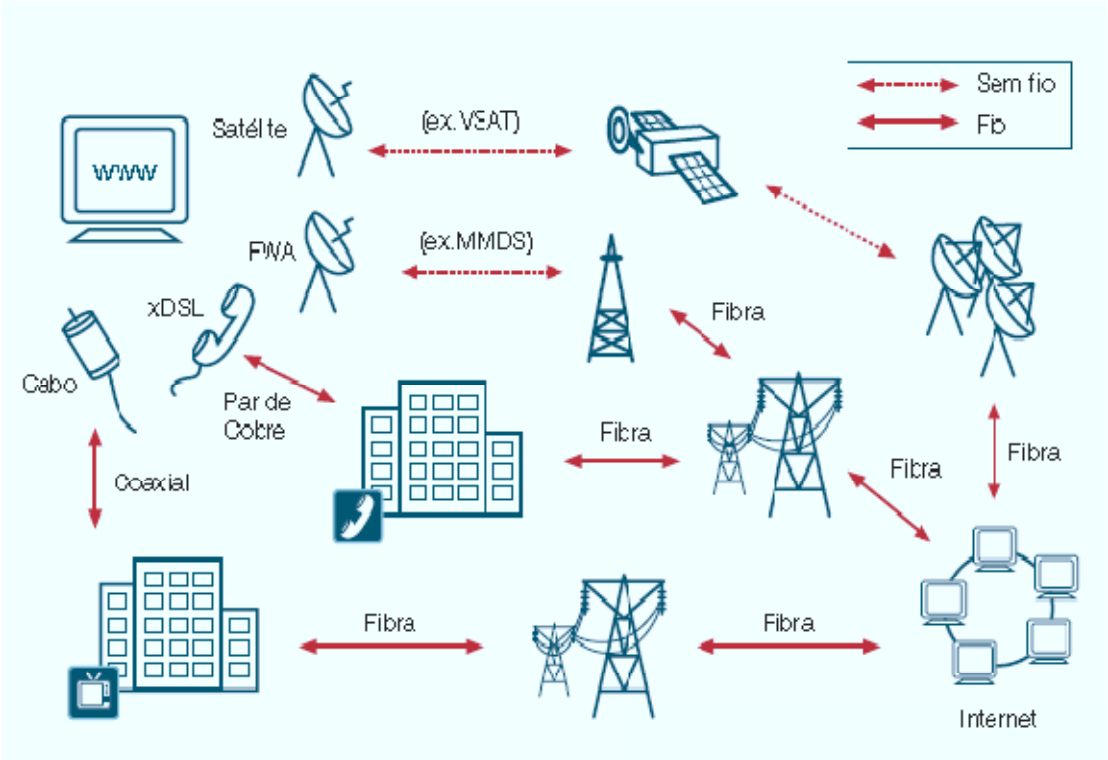

Figura 2.1 - Meio de acesso para banda larga, extraído de [6].

As redes de acesso são os enlaces físicos que conectam o equipamento do usuário ao primeiro roteador da operadora, também conhecido como roteador de borda. Tradicionalmente, sempre existiu o conceito de que acesso banda larga é sinônimo somente de conexão à *internet*. Porém, nas próximas seções, mostra-se que os acessos banda larga podem ser utilizados pelas operadoras para disponibilizar vários serviços ao mercado, por exemplo, as VPNs.

A seguir, é mostrado que muitas dessas tecnologias empregam, em níveis que variam, parcelas da tradicional infraestrutura telefônica com fio. Essa infraestrutura é fornecida por um provedor de serviços de telecomunicações, como a Verizon nos Estados Unidos, a France Telecom na França e a OI e Telefônica no Brasil.

2.1.1 TECNOLOGIA XDSL

Uma das redes mais acessíveis e com maior abrangência é a rede telefônica, formada por pares de condutores elétricos de cobre. Em função de sua alta capilaridade, as linhas telefônicas têm sido foco de grandes estudos para disponibilizar acesso de dados em alta velocidade. As modernas técnicas de PDS (Processamento Digital de Sinais) foram adaptadas especialmente para esse desafio e resultaram no que hoje é conhecido como xDSL (*Digital Subscriber Loop*), constituído de várias tecnologias que disponibilizam acesso à rede telefônica em alta velocidade: ADSL, HDSL, SDSL e VDSL.

A tecnologia HDSL (*High-bit-rate Digital Subscriber Loop*) fornece comunicação duplex em um ou dois pares de assinante com taxa T1 (1,544Mbit/s) ou E1 (2,048Mbit/s). A tecnologia HDSL atualmente fornece a solução mais rápida e de menor custo para oferecer canais digitais E1/T1 ao usuário com qualidade comparável à de fibra ótica. O HDSL permite que organizações públicas e privadas façam uso otimizado de um dos seus maiores valores, o par de fios de cobre implantado. O HDSL transforma o par de fios de cobre, que era apenas visto como uma simples linha para telefone, em canais digitais de alta velocidade com capacidade de prover serviços avançados, não somente para corporações e pequenos negócios, mas também para residências. Hoje, a aplicação mais destacada do HDSL é na provisão de serviços digitais avançados em

enlaces de usuários finais das corporações. O HDSL utiliza eletrônica avançada, permitindo às organizações privadas e empresas de telecomunicações usarem o par de fios de cobre, com qualidade comparável à da fibra ótica, sem ter que condicionar de alguma forma o par de fios já existente. Ultimamente, o HDSL tem encontrado sua maior aplicação entre usuários finais e na redução de custos, porque ele quadruplica a distância que um sinal digital pode viajar sem a necessidade de amplificação ou regeneração. A tecnologia SDSL *(Symmetric Digital Subscriber Loop* ou *Single Digital Subscriber Loop)* fornece tráfego bidirecional (*duplex*), simultâneo de voz e dados em altas taxas, que vão desde 160 kbits/s até 2,048 Mbit/s. As tecnologias SDSL e ADSL(*Asymmetric Digital Subscriber Loop)* aliviam o congestionamento na rede de tráfego de voz. Ambos, voz e dados, não passam pela rede de comutação de circuitos, como é feito com os *modems* analógicos e os serviços ISDN. Ao contrário, as companhias telefônicas fazem o roteamento do tráfego de voz para a rede de comutação de circuitos e dos dados para a rede de comutação de pacotes [20].

O VDSL (*Very-high-bit-rate Subscriber Loop*) é a tecnologia DSL mais rápida sobre um par de fios de 12,96 a 51,84 Mbit/s para envio e de 1,5 a 2,3 Mbit/s para recebimento (Tabela 2.1). É uma alternativa econômica para a solução FTTH. O problema dessa tecnologia de transmissão assimétrica é o baixo alcance, que varia entre 300m a 1,5km. Além de suportar as mesmas aplicações que ADSL, permite que um NSP ofereça transmissão de HDTV e vídeo sob demanda [20].

Tabela 2.1 – Velocidade de *download* x distância admissível.

Distância em KM	Velocidade (Mbit/s) – *Down*
0,3	52
0,9	26
1,5	13

Percebendo essa capacidade de alta velocidade da linha telefônica e de toda uma rede já implementada, as operadoras começaram a questionar o porquê de não utilizar a tecnologia DSL como forma de acesso de outros serviços em substituição às formas de acessos tradicionais, como *frame relay* e ATM.

A primeira utilização da tecnologia DSL para outro serviço que não a *internet* foi em VPN de nível 2, onde existe uma combinação das tecnologias *frame relay*, ADSL e ATM dos acessos que faziam parte da VPN. O item 2.3 mostra essa forma de implementação, que foi iniciada no Brasil em 2004. É importante destacar que algumas operadoras ainda não disponibilizam essa solução, talvez pela falta de percepção dos benefícios e de conhecimento técnico necessário para a sua implementação.

A segunda utilização da tecnologia DSL depois da *internet* e a mais significativa é como forma de acesso das VPNs baseadas em MPLS. Isso representou uma redução significativa dos custos para a operadora e, consequentemente, dos preços do serviço para o usuário final. O item seguinte apresenta as implementações baseadas em DSL e MPLS.

2.1.1.1 VPN MPLS ADSL

Os serviços oferecidos pelas VPNs MPLS foram inicialmente providos através de conexão permanente do CPE/CE do usuário com o roteador PE. Exemplos de tecnologias de acesso disponíveis são as linhas dedicadas (*leased lines*), *frame relay* ou ATM (*Asynchronous Transfer Mode*). A figura 2.2, a seguir, mostra essas alternativas.

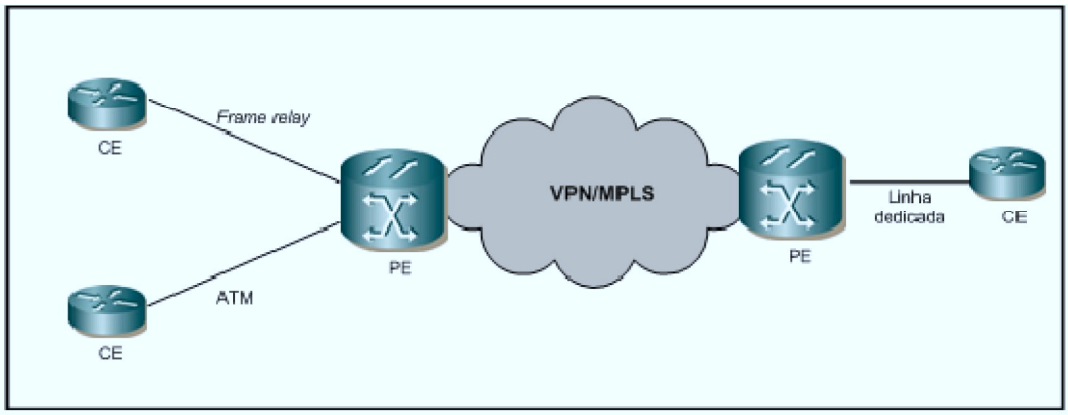

Figura 2.2 – Formas de acessos típicos das VPN MPLS.

Como o *frame relay*, ATM e linha dedicada são métodos tradicionais de acesso às VPNs, este item é direcionado para as VPNs com a tecnologia ADSL como forma de acesso. A figura 2.3 mostra a formação de uma VPN com acesso ADSL e núcleo MPLS.

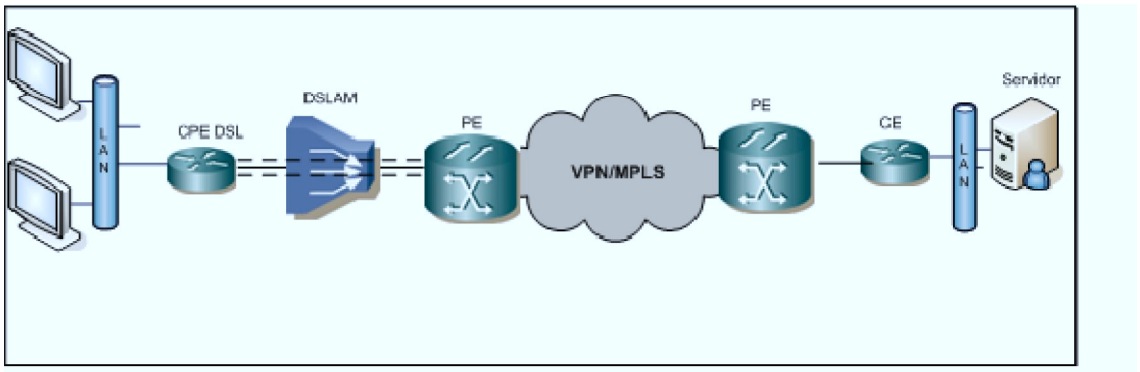

Figura 2.3 – VPN com acesso DSL.

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 DSLs. Essa modalidade de VPN MPLS com acesso DSL foi um dos motivos de seu sucesso comercial; outro grande motivo é a complexidade dessa solução, que é função de n, enquanto as tradicionais são função de n^2. O próximo capítulo desenvolve matematicamente esse tópico, relacionado à complexidade das VPNs baseadas em MPLS em relação às VPNs tradicionais.

2.1.2 CABO

Na transmissão de dados através dos cabos coaxiais de banda larga, utiliza-se a tecnologia já disponível para a televisão a cabo ou CATV (*Community Antenna TV*). O equipamento que é instalado no ambiente do usuário é chamado *cable modem*.

O *cable modem* é um serviço de acesso à *internet* em alta velocidade, baseado na infraestrutura de transmissão de TV por assinatura. Essa estrutura é viabilizada pela utilização do *cable modem*, um equipamento de comunicação que permite a transmissão de dados em altíssima velocidade através da infraestrutura de CATV, por cabos coaxiais e HFC. A velocidade de conexão varia muito, dependendo do sistema de *cable modem* adotado, da arquitetura da rede de TV a cabo e do tráfego em si. O fluxo de dados *downstream* pode atingir velocidades de até 27Mbit/s, o que resulta em velocidades de recebimento de dados de cerca de 1 a 3 Mbit/s, se for considerado o fato de a largura de banda ser compartilhada por vários usuários. Na direção de envio de dados, as velocidades podem atingir até 10 Mbit/s. O modelo mais comum é o assimétrico, devido à própria natureza assimétrica das aplicações. O termo *cable modem* refere-se a um "*modem*" que opera sobre a rede de TV a cabo. Ele acumula funções associadas a um *modem*, sintonizador, encriptador/decriptador, *bridge,* roteador, interface de rede, agente SNMP e *hub ethernet* [21].

Um dos inconvenientes do sistema surge se o usuário desejar utilizar o *cable modem* para criar um servidor de HTTP ou FTP. Para que isso seja possível, deve-se contornar o fato de que o ISP fornece sempre um endereço IP dinâmico. Existem alguns programas que contornam isso implementando um DNS dinâmico e associando um nome de domínio permanente a um endereço IP dinâmico. O provedor pode também bloquear portas, impedindo o uso de certos serviços. Como os assinantes compartilham a largura de banda disponível durante suas sessões, existe a preocupação de que o desempenho da rede caia à medida que mais usuários se conectam. Em um primeiro momento, pode-se pensar que, quando 200 usuários compartilharem uma largura de banda de 27 Mbit/s, sobrarão aproximadamente 135 kbit/s para cada um –

ligeiramente maior que os 128 kbit/s de uma conexão ISDN. Isso não é, necessariamente, verdade. Diferentemente da rede telefônica comutada, onde é alocada uma conexão dedicada para cada usuário, os usuários do *cable modem* não ocupam uma parcela fixa da largura de banda durante o tempo em que permanecem conectados. Os recursos da rede são alocados somente na transmissão e recepção de dados em rajadas. Ao invés de cada usuário ter disponível uma taxa fixa de 135 kbit/s, a este é permitido usar toda a largura de banda disponível durante o tempo de transmissão de seus pacotes de dados – tempos da ordem de milissegundos [21].

2.1.2.1 Redes HFC e redes IP

A transmissão de dados sobre a rede de TV a cabo é uma tecnologia que usa a infraestrutura da rede HFC para o transporte do tráfego de dados. Há três grandes padrões em uso: DOCSIS (*Data-Over-Cable ServiceInterface Specification*), Euro-DOCSIS e DVB-RC (*Digital Vídio Broadcast – Return Channel)*. Esses três padrões têm dois canais diferentes que são utilizados para a transmissão de dados bidirecional entre o provedor e o usuário. Em todos os padrões, o canal de *downstream* refere-se ao canal entre o provedor e o usuário, e o canal de *upstream* refere-se à conexão entre o usuário e o provedor. A tabela 2.2 especifica cada um dos padrões [22].

A figura 2.4 apresenta a arquitetura e os componentes básicos de uma rede para acesso a cabo. Nessa arquitetura básica, *o cable modem* atua como uma ponte entre a rede de cabo e a LAN do usuário. O *cable modem* trabalha na camada de nível 2 do modelo OSI e opcionalmente pode trabalhar na camada de nível 3 com o protocolo IP[22].

Tabela 2.2 – Padrões para acesso através de cabo, extraído de [22].

FEATURE	DOCSIS 1.x	Euro-DOCSIS	DVB-RC
Taxas de *Downstream*	64-QAM: 27 Mbps 256-QAM: 42 Mbps 6 MHz de canalização	64-QAM: 38 Mbps 256-QAM: 52 Mbps 8 MHz de canalização	64-QAM: 38 Mbps 256-QAM: 52 Mbps 8 MHz de canalização
Taxas de *Upstream*	QPSK: até 5,12 Mbps 16-QAM: até 10,24 Mbps	QPSK: até 5,12 Mbps 16-QAM: até 10,24 Mbps	QPSK Diferencial até 3,088 Mbps
Performance	Eficiência maior que 80% sobre uma conexão de voz e dados no *link* de *upstream* de 10 Mbps	Eficiência maior que 80% sobre uma conexão de voz e dados no *link* de *upstream* de 10 Mbps	Eficiência entre 50 e 72% em 3,088 Mbps
Serviços	Acesso à *internet* e voz sobre IP (VoIP)	Acesso à *internet* e voz sobre IP (VoIP)	Acesso à *internet*
Protocolo básico	IP com QoS	IP com QoS	Transporte ATM.

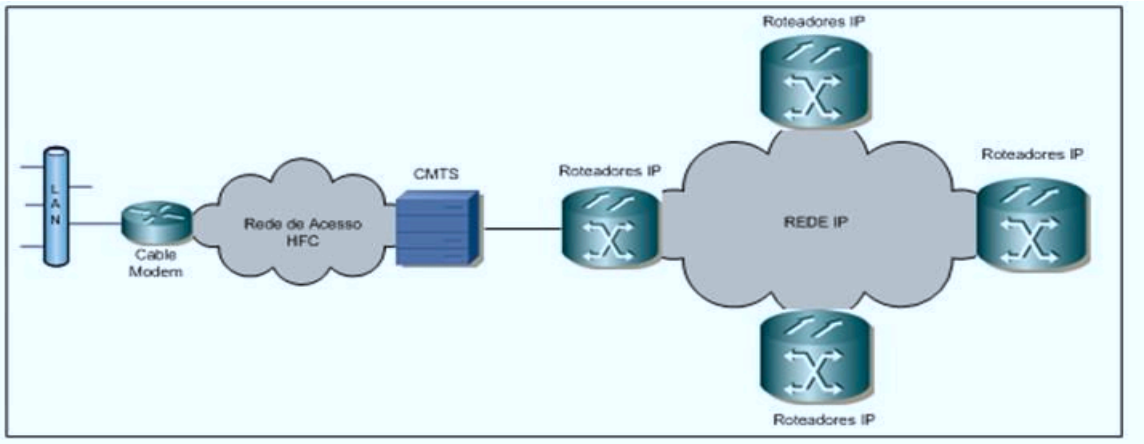

Figura 2.4 – Elementos básicos de uma rede HFC para conexão IP.

2.1.2.2 VPN com acesso a cabo

Há dois principais motivos para a implementação de VPN MPLS com acesso a cabo. O primeiro motivo é a demanda de novos negócios pelas operadoras a cabo, que têm crescido rapidamente nos últimos anos. Atualmente, a tecnologia de acesso através do cabo é realizada principalmente pelos usuários residenciais, em função do pequeno valor da assinatura. No entanto, se o provedor de serviço conseguir implementar qualidade de serviço e segurança, o acesso a cabo poderá ser utilizado como forma de acesso das VPNs MPLS para o mercado corporativo. O segundo motivo para a formação de VPN MPLS com acesso a cabo tem relação com a regulamentação de alguns países sobre os serviços de comutação de circuitos. Existem países em que a infraestrutura é monopólio da concessionária local, e VPN MPLS a cabo poderá ser uma alternativa para oferecer novos serviços baseados em VPN MPLS [22].

Vamos analisar agora como uma VPN MPLS poderá ser implementada sobre uma infraestrutura de cabo existente e que funcionalidades deverão ser configuradas. A figura 2.5, a seguir, apresenta uma topologia básica de integração da rede de cabo sobre uma rede MPLS.

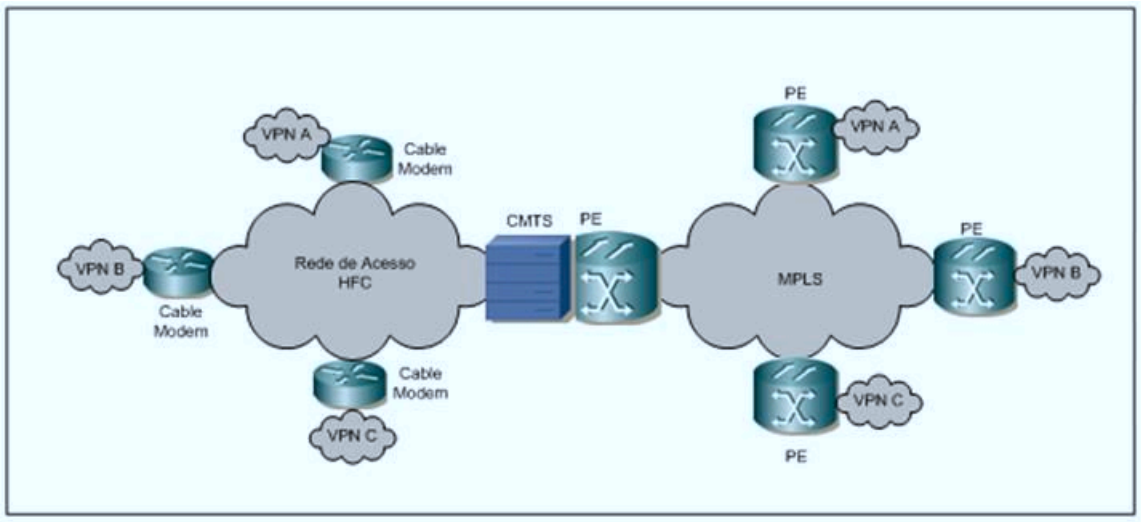

Figura 2.5 – Integrando a rede HFC com a rede MPLS, extraído de [22].

Assim como os *modems* ADSL, as funcionalidades de VRFs são necessárias nos *modems* a cabo para que seja possível a implementação de VPN com MPLS fim a fim (desde o

equipamento do usuário). A implantação dessa funcionalidade no modelo é um desafio em termos de escalabilidade, tanto do ponto de vista econômico quanto do de projeto.

Para a implementação de VPN com acesso a cabo, é necessário que um dos equipamentos execute a função de PE; esse elemento a ser considerado é o CMTS. O CMTS tem a funcionalidade de um PE, ou seja, o CMTS funciona como um roteador. O CMTS precisa ter a facilidade de suportar a separação de *cable modem* dentro de diferentes grupos para que possa vincular a VRF apropriada. Como o *cable modem* usa a rede HFC como um meio compartilhado, os usuários podem ter alguns problemas com segurança com essa tecnologia. Facilidades avançadas, como a habilidade de prevenir clientes que estão atrás do *cable modem* de *spoofing* de seus endereços IP, tanto quanto a implementação de lista de acesso no *cable modem*, podem também prevenir os problemas de segurança. O uso adicional de criptografia na camada MAC ou na camada de rede poderá ser apropriado se um nível maior de segurança na VPN com acesso a cabo for necessário. A figura 2.6 mostra como construir VPN MPLS com acesso a cabo de forma adequada para usuário corporativo. Também essa topologia apresenta como um provedor pode otimizar a sua estrutura de rede para fornecer acesso à *internet* para usuários residenciais e VPNs seguras para usuários corporativos [22].

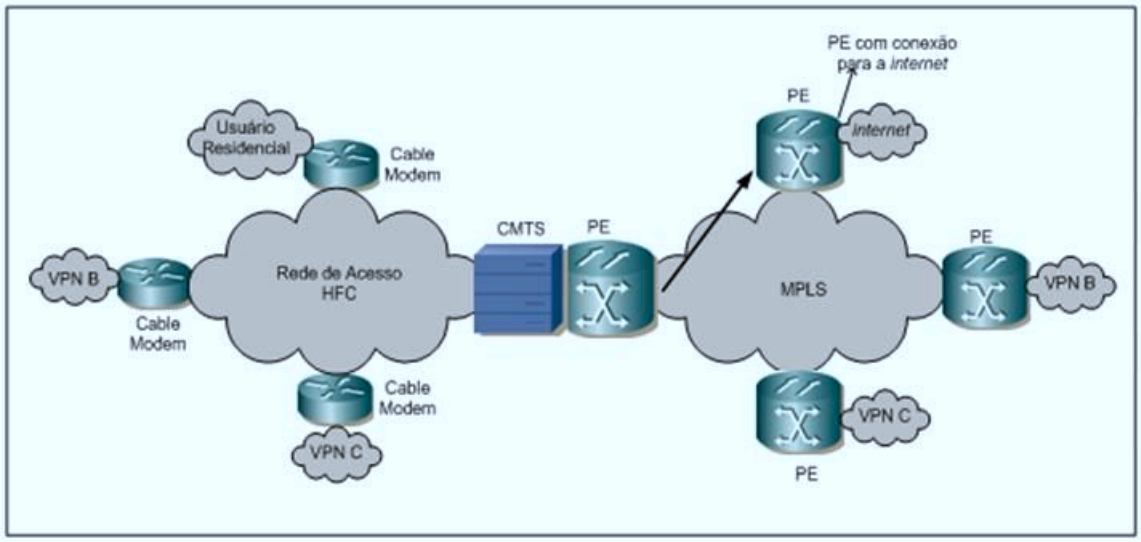

Figura 2.6 – Integrando a rede HFC com a rede MPLS e acesso à *internet.*

Também é possível que uma operadora a cabo possa competir em uma região diferente da sua, onde atua através da interconexão da sua rede com outros provedores de serviços. Uma alternativa para oferecer acessos com o mesmo nível de serviço, mas que pertencem a provedores diferentes, é usar políticas baseadas em roteamentos no CMTS.

2.1.3 RÁDIO – SOLUÇÕES SEM FIO

As tecnologias de redes de comunicação sem fio têm apresentado um avanço significativo nos últimos anos e estão se tornando cada vez mais populares.

O propósito de uma rede sem fio é facilitar aos usuários o acesso a várias aplicações disponíveis e novas que virão como consequência da convergência dos serviços. Voz sobre IP (VoIP), correio eletrônico, Vídeo sobre IP e *World Wide Web* precisam ser agora acessíveis através das novas redes de comunicação sem fio com QoS (*Quality of Service*) e segurança. Para aplicações que requerem uma alta qualidade de serviço, como as de vídeo sob demanda e algumas aplicações de tempo real, um ambiente sem fio pode trazer grandes problemas e comprometer o desempenho de aplicações desse tipo. Em função dessa necessidade, será avaliado neste tópico uma nova proposta de criar VPNs MPLS, utilizando como acesso a tecnologia *WiMax*.

2.1.3.1 A tecnologia *WiMax*

Na mesma linha da tecnologia *Wi-Fi*, o IEEE especifica as bases da tecnologia *WiMAX*, através do padrão IEEE 802.16 [23]. Trata-se de uma tecnologia de rede metropolitana sem fio, com suporte à cobertura na ordem de quilômetros e taxas de transmissão de até 74 Mbit/s, além de QoS e interfaces para redes IP, ATM, E1/T1 e *ethernet*.

O termo *WiMAX* (*World Interoperability for Microwave Access*) refere-se ao *WiMAX Forum*, que tem como missão principal garantir a interoperabilidade entre os equipamentos baseados no

padrão IEEE 802.16 e é composto predominantemente por fabricantes de equipamentos e *chipsets* [24].

É importante destacar que no Brasil a licença de exploração do serviço *WiMax* está suspensa em função de um recurso pelas operadoras de Telecom, depois que a Anatel publicou o edital de licitação. Hoje, o serviço de *WiMax* no Brasil basicamente é oferecido por apenas algumas operadoras que trabalham na faixa de frequência não-licenciada, mas muitas operadoras estão aguardando o novo edital de licitação para oferecer os serviços com base na tecnologia *WiMax*.

O padrão 802.16 é baseado na técnica OFDM (*Orthogonal Frequency Division Multiplexing*), que é muito eficiente para a transmissão de dados. O padrão 802.16 é formado pelos padrões 802.16a, 802.16c, 802.16d, 802.16f e 802.16g. A figura 2.7 apresenta os principais padrões utilizados no 802.16. Esse padrão foi originalmente publicado em 2001 para rede de banda larga para acesso fixo, onde a interface aérea trabalhava na faixa de frequência de 10 – 66 GHz, sendo que sua aplicação era específica para conexões ponto a ponto. Em 2004, foi publicado 802.16d para suportar aplicações portáteis operando na faixa de frequência entre 2 e 66 GHz. O padrão 802.16e aumentou as facilidades da mobilidade em alta velocidade e comunicação entre áreas de serviços diferentes, permitindo o *roaming* [23].

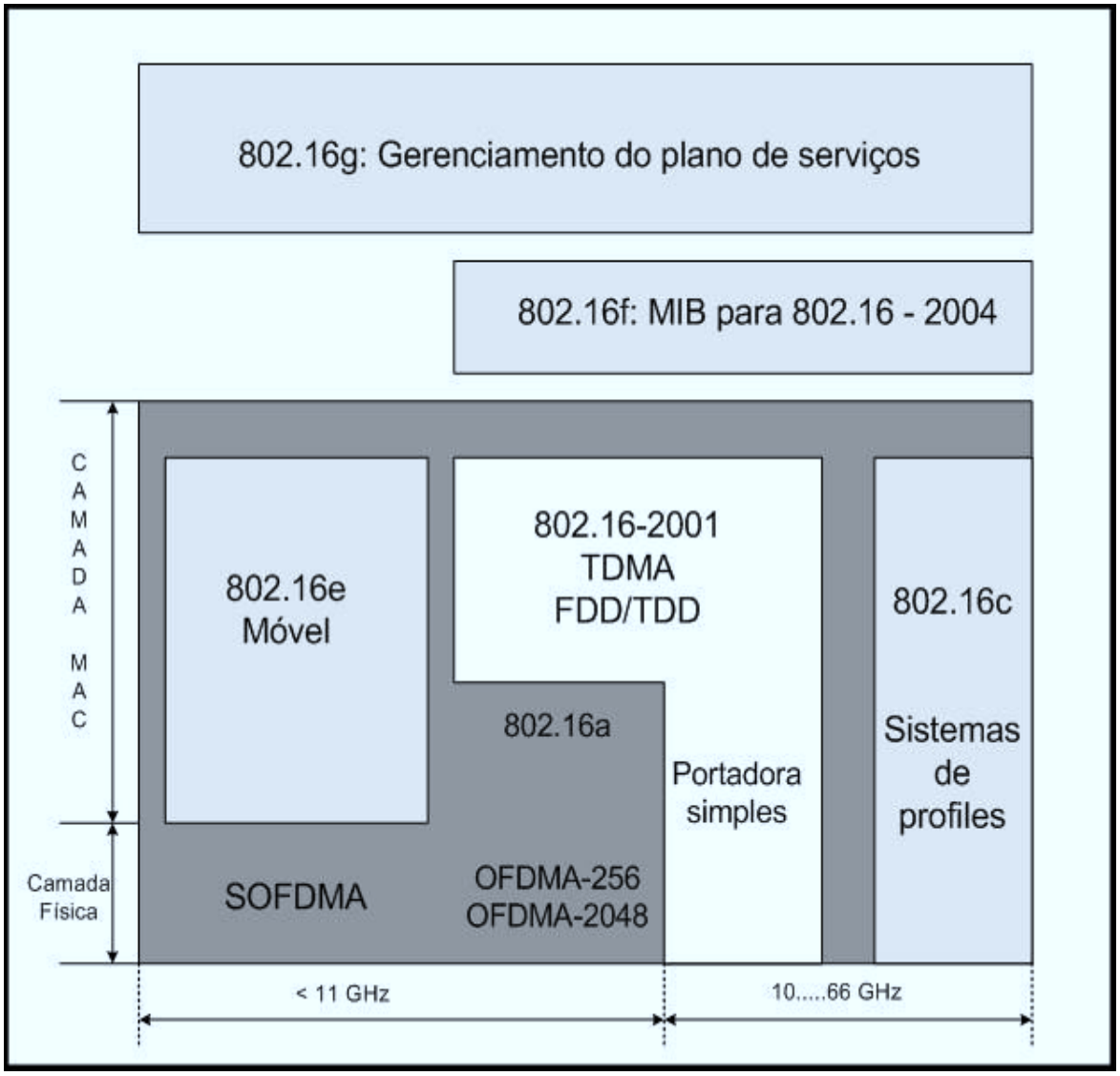

Figura 2.7 – Padrão 802.16, adaptado de [23].

2.1.3.2 *WiMax* para formação de VPNs móveis (MVPN)

As empresas de telecomunicações têm encontrado dificuldade em oferecer soluções de VPNs para locais que não possuem infraestrutura de rede para fazer o atendimento ou para entrar em regiões fora de sua área de concessão, pois isso demanda alto investimento em construção de uma nova rede a partir do zero. Nesse contexto é que surge o *WiMax* como uma solução para a formação de VPNs móveis (MVPN) seguras como uma alternativa às soluções de VPNs fixas com acesso DSL. Na solução de MVPN com acesso *WiMax*, o usuário remoto poderá acessar seus aplicativos em alta velocidade com segurança e qualidade de serviço. Ao contrário

das MVPNs baseadas em acesso DSL ou a cabo, as MVPNs baseadas em acesso *WiMax* suportam a mobilidade e, em algumas situações, a alta velocidade.

Para o *WiMax* suportar as MVPNs, as características de segurança, qualidade de serviço (QoS) e mobilidade são as principais questões a serem resolvidas. Em função dessa necessidade, a topologia apresentada na figura 2.8 mostra uma arquitetura de integração do *WiMax* com um núcleo de rede MPLS que tem como principal objetivo resolver as questões relacionadas a esses requisitos, que são a segurança e a qualidade de serviço (QoS), os quais são avaliados em capítulos posteriores com mais detalhes.

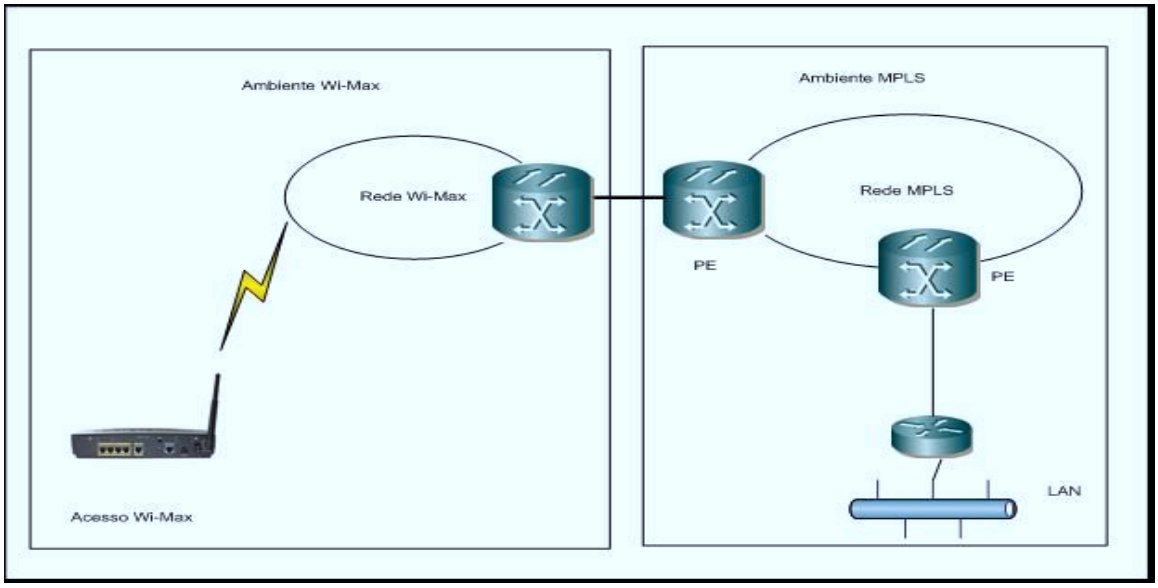

Figura 2.8 – Integração da tecnologia *WiMax* com MPLS para formação de MVPN.

2.1.4 SATÉLITE

Este tópico apresenta uma análise sobre a utilização dos satélites. Essa é uma forma de acesso de VPN em rede de comunicação integrada para o fornecimento do serviço de VPN fixo - móvel. Sendo considerados como mais uma opção para possibilitar comunicação de dados entre *sites* de uma organização, os satélites destacam-se por total alcance e rapidez na implantação do acesso e no oferecimento de alta velocidade para a formação de VPN fixo - móvel. Motivadas pela tendência das comunicações com total conectividade e pela possibilidade de acessibilidade

do serviço em qualquer lugar, as empresas do segmento de telecomunicações estão utilizando o satélite como alternativa de acesso das VPNs para localidades sem estrutura que não suportem outra tecnologia.

O uso da forma de acesso via satélite para VPN Móvel necessita da avaliação de diversos requisitos que podem influenciar nas decisões de escolha da tecnologia de acesso da VPN fixo - móvel. Destacam-se os problemas de ordem física e os das tecnologias atualmente existentes, que estariam sendo adaptadas para disponibilização nesse serviço. São verificadas, a seguir, algumas dessas limitações técnicas que podem inviabilizar a sua utilização.

- ✓ **Latência *jitter* e quantidade de satélites**

Até 1980, os satélites eram colocados em órbitas equatoriais, no "*Belt Clark*", situado a 35.000 km de distância da Terra. Nessa distância, são necessários apenas três satélites para cobrir todo o globo, porém, um dos grandes dificultadores para se fazer uso dessa órbita para a *internet*, telefonia e, principalmente, para acessos de VPN fixo - móvel que demandam qualidade de serviço (QoS) deve-se ao retardo causado pela propagação do sinal no espaço livre. O atraso do sinal é da ordem de 250 ms. Para se diminuir o atraso causado pela propagação do sinal e também para proporcionar serviços móveis, que preferencialmente precisam usar terminais pequenos com antenas pequenas, seria necessário o uso de satélites mais próximos da Terra. Quanto mais próximos da Terra, menor a potência requerida pelos satélites e pelos terminais. Isso se deve ao fato de a perda do sinal estar relacionada com a distância. A potência do sinal eletromagnético é atenuada pelo quadrado da distância que o sinal propaga. Por exemplo, se a distância entre o transmissor e o receptor duplica, é necessário quadruplicar a potência no transmissor para se ter o mesmo nível de potência no receptor [25].

Os satélites que estão situados em baixa órbitas (LEOs) estão 60 vezes mais próximos da Terra do que os satélites GEOs. A altitude de LEO varia entre 400 e 1.600 milhas. O problema de se utilizar LEO é que a quantidade de satélites para cobrir toda a Terra é muito maior do que quando se utiliza GEO. No exemplo da *Teledesic*, que fará uso dessa órbita, serão necessários 288

artefatos. As aplicações de *broadcast e multicasting*, que é o caso das TVs via satélites, ou seja, distribuição de vídeo, são comprovadamente boas para serem usadas nas órbitas GEOs, uma vez que o atraso para comunicações de apenas um sentido não causa grandes perturbações no sistema. Os satélites GEOs têm muitas vantagens, tais como ampla cobertura, alta qualidade de comunicação e eficiência econômica. Como eles estão sincronizados com o movimento da Terra, o processo de *tracking* torna-se mais simples do que nas órbitas não-geoestacionárias. Ao se utilizarem órbitas LEOs, o tempo em que o satélite se torna visível da Terra varia de 20 a 30 minutos até sumir no horizonte. Um *link* de comunicação deve ser transferido para outro satélite antes de o primeiro sumir. Dessa forma, o problema é sanado tendo-se sempre pelo menos dois satélites visíveis em qualquer ponto da Terra. O roteamento entre os satélites requer mais inteligência nos equipamentos [25, 26].

Tabela 2.3 – Comparação entre LEO, MEO e GEO, adaptado de [25].

	LEO	MEO	GEO
Tempo de vida do satélite (anos)	3-7	10-15	10-15
Atraso de propagação	Pequeno	Médio	Grande
Perda de propagação	Baixa	Média	Alta
Complexidade da rede	Complexa	Média	Simples
Hand Off	Muito	Médio	Nenhum
Visibilidade do satélite	Curta	Média	Sempre

As formas de acesso das VPNs MPLS DSL, *frame relay*, GPRS, *metroethernet* e satélite não são necessariamente tecnologias concorrentes, mas sim complementares, pois permitem que, conforme a localização dos *sites* do usuário, seja feito um tipo de atendimento. Portanto, aqueles usuários que estão em locais de fácil acesso e que possuem outras tecnologias, por exemplo, DSL, podem ser atendidos por elas, enquanto aqueles *sites* que estão localizados em locais de difícil acesso serão atendidos por satélite.

Um dos maiores problemas do satélite como forma de acesso das VPNs para algumas aplicações é que o IP não exige um serviço de rede confiável, sendo o TCP o responsável pela recuperação de dados perdidos, duplicados, corrompidos ou entregues fora de ordem. O que faz com que pacotes IP sejam retransmitidos é a finalização do tempo no transmissor para receber confirmação do recebimento do pacote enviado. Em situações de congestionamento da rede, o pacote de confirmação (*ack*) vai atrasar e, portanto, será reenviado, podendo gerar a execução da mesma tarefa duas vezes caso o protocolo de transporte não identifique esse problema. O TCP é responsável pela confiabilidade de entrega de dados através do caminho de rede, mas sua eficiência não é a única consideração ao se utilizar a rede de satélite como forma de acesso das VPNs IP. Deve-se levar em consideração o tipo de protocolo utilizado no enlace, o tipo de CPE e, principalmente, os requisitos das aplicações. A principal deficiência do satélite que inviabiliza algumas aplicações é o alto atraso de propagação para confirmação de ida e volta (RTT) de uma mensagem para os satélites geoestacionários, o que fica em aproximadamente 500 ms. Esse RTT torna inviáveis aplicações como as de voz e vídeo sobre VPN IP. A solução normalmente utilizada para resolver o problema do atraso de propagação é utilizar satélite de baixa ou média órbita que apresenta um RTT em torno de 80 ms. Porém, essa diminuição do RTT requer uma maior quantidade de satélites para manter a cobertura. Esse aumento da quantidade de satélites provoca a necessidade de comunicação entre satélites, tendo como consequência um atraso de propagação variável (*jitter*). Aplicações como voz e vídeo não suportam altos valores de *jitter*, como é mostrado no Capítulo 4. Os principais aspectos que prejudicam o desempenho dos satélites como acessos das VPNs fixo - móveis são[25]:

- ✓ Devido ao atraso de propagação por meio do sistema GEO, os satélites levam tempo para determinar se o pacote chegou ou não, inviabilizando muitas das aplicações de VPNs IP interativas.
- ✓ O uso frequente de canais assimétricos dos satélites tende a inviabilizar um bom desempenho das VPNs IP com acesso de satélite.
- ✓ Grande quantidade de *handoff* em órbitas pode gerar perdas de pacotes.
- ✓ Nos sistemas de baixa órbita, a comunicação entre satélites acaba provocando uma variação do RTT (*jitter*).

2.1.4.1 VPN MPLS com acesso de satélite

O objetivo deste tópico é apresentar uma arquitetura de VPN MPLS com acesso de satélite e avaliar os seus requisitos mínimos para o atendimento das aplicações através de tecnologia de acesso baseada em satélite. A figura 2.9 apresenta a integração das redes MPLS com as redes de satélites. Essa solução poderá ser disponibilizada pelas operadoras de telecomunicações, mas alguns cuidados devem ser tomados para evitar a diminuição de performance para algumas aplicações, principalmente aquelas onde a redução do atraso fim a fim é requisito para um bom desempenho. Além dessa questão, a viabilidade econômica tem grande importância em uma solução de integração de MPLS com satélite, pois atualmente os custos de uma solução baseada em satélite são superiores na média em relação a outras soluções baseadas em tecnologias tradicionais. Em função dessas variáveis de desempenho e custo, a solução do acesso de satélite em redes MPLS para a formação de VPN MPLS tende a tornar-se atrativa para as aplicações de dados e normalmente para os *sites* afastados das áreas urbanas, pois nos locais com alta densidade populacional as operadoras possuem alternativas com melhores custos e desempenho.

A integração da rede MPLS com a rede de satélite é realizada através da conexão de um equipamento de borda da rede MPLS, chamado de PE, com a *hub* do satélite. Essa conexão pode ser realizada através de rede *metroethernet* ou até mesmo de uma conexão ponto a ponto SDH. Dentro da rede MPLS, são facilmente configurados os parâmetros de qualidade de serviço e segurança necessários em uma VPN, que exige esses requisitos. Os capítulos 4 e 5 avaliam esses tópicos. A figura 2.9 apresenta uma proposta de integração de satélite sobre MPLS.

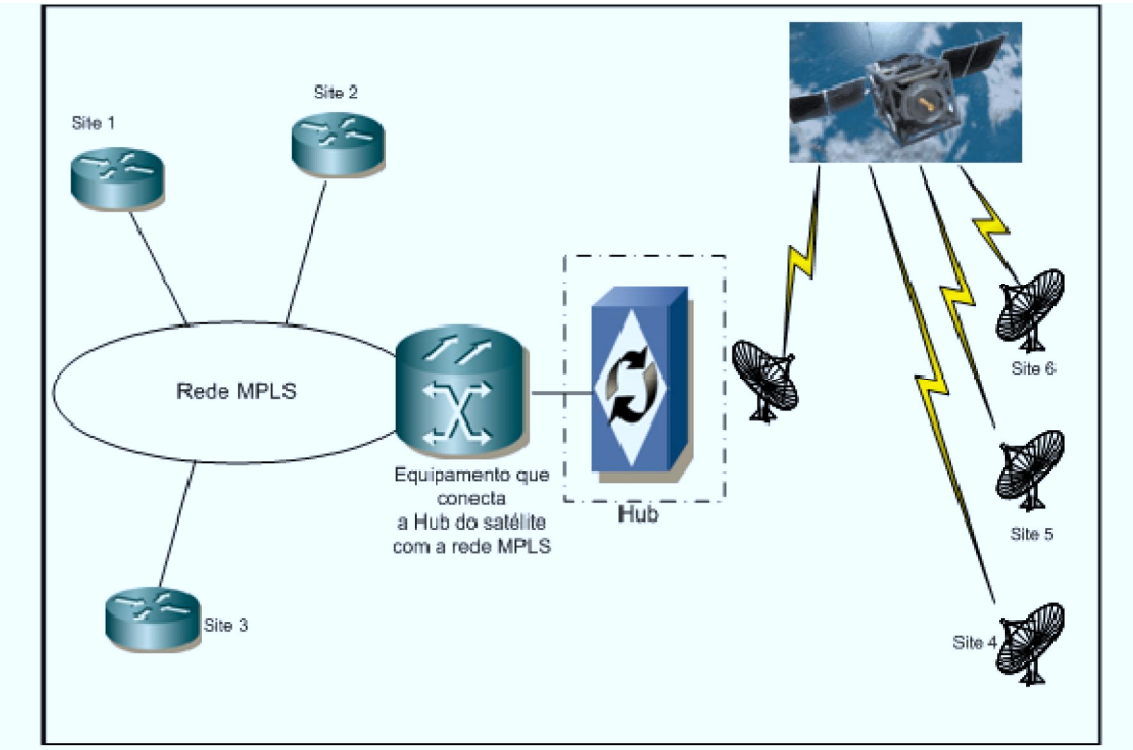

Figura 2.9 – Convergência de satélite com as redes MPLS.

Essa proposta é indicada para soluções de VPN MPLS em que alguns *sites* têm viabilidade técnica de serem atendidos com tecnologias de alto desempenho, como *metroethernet*, e outros estão em locais em que a única alternativa é o satélite. Essa solução permite que a comunicação entre aqueles *sites* que possuem viabilidade técnica para um bom desempenho de comunicação entre eles não precisem utilizar os *sites* que utilizam a tecnologia de satélite.

Os usuários potenciais para essa topologia proposta são as empresas que têm como características geográficas a dispersão de seus *sites*. As VPNs MPLS com acesso via satélite permitem a integração desses *sites* através de um único protocolo, o MPLS, no núcleo da rede.

2.2 VPN *Frame Relay*

A tecnologia *frame relay* surgiu no fim da década de 80 como uma extensão simplificada do protocolo X.25 para aumentar, principalmente, a sua vazão e diminuir seu atraso. O objetivo

principal era obter um suporte de interligação para LANs (*Local Area Network*). Enquanto a vazão teórica de uma rede de pacotes do tipo X.25 situa-se em torno de uma taxa efetiva da ordem de 1 a 3 Mbit/s, o *frame relay* pode apresentar vazões da ordem de 10 a 50Mbit/s[27]. Na prática, foi possível observar que as redes X.25 não oferecem taxas maiores que 64kbit/s, enquanto as redes *frame relay* ofereceram taxas até 2 Mbit/s.

Surgida dos grupos de trabalho especializados da ANSI, a tecnologia *frame relay* teve sua especificação acolhida também por parte do ITU-T, através de um conjunto de recomendações. No final da década de 1990, teve sua importância confirmada ao ser definida como um dos serviços de suporte mais importantes no contexto da N-ISDN [27].

A tecnologia *frame relay* encontrou a sua principal aplicação em redes de dados públicas de longa distância, administradas pelas concessionárias, mas também como suporte em ambientes de redes locais, como solução de interconexão de redes locais em médias e longas distâncias.

Até o final de 2007, aproximadamente todas as VPNs no Brasil utilizavam a tecnologia *frame relay*. Nesse modelo, cada rede do ambiente do usuário tem um roteador, que é conectado, através de enlaces ponto a ponto, a outro roteador remoto do usuário. A figura 2.10 apresenta o modelo. As soluções das VPNs baseadas em *frame relay* eram as predominantes no mercado mundial. Esse tipo de solução apresenta vários problemas que limitam o desenvolvimento em larga escala do serviço VPN:

- ✓ Escalabilidade;
- ✓ Complexidade;
- ✓ Custo proporcional à quantidade de circuitos virtuais privados (CVP).

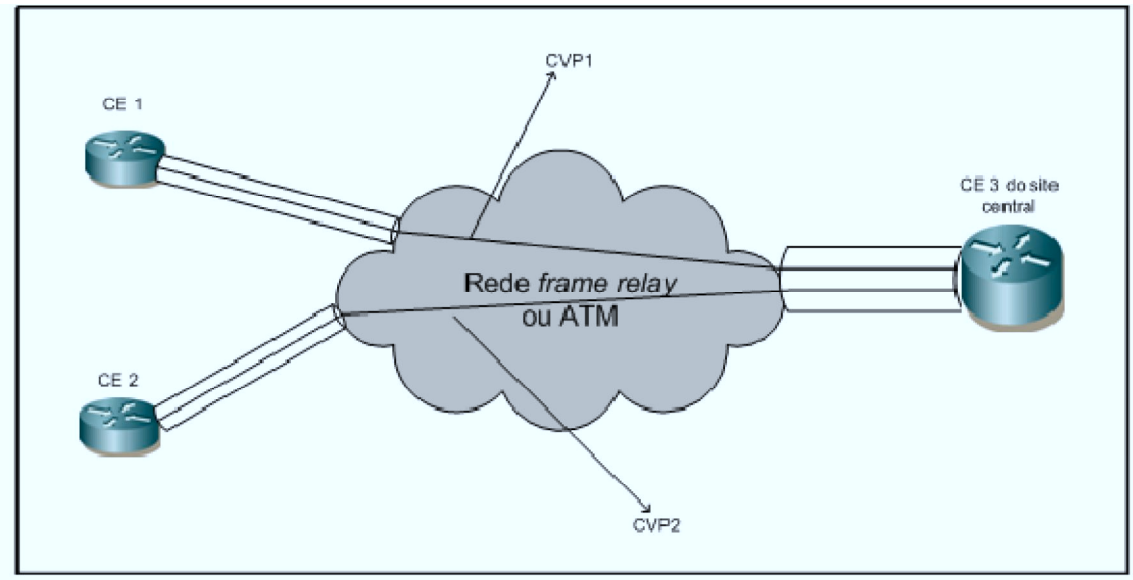

Figura 2.10 – Redes *frame relay* ou ATM.

Nessa implementação, todas as conexões são realizadas ponto a ponto. A rede *frame relay* é totalmente transparente aos protocolos de roteamento, o que tem importante impacto se o usuário decidir mudar o protocolo de roteamento, pois a operadora de telecomunicações não terá nenhum conhecimento da troca. Isso representa uma independência do cliente em relação ao provedor, o que, na maioria das vezes, não coincide com o desejo deste. Atualmente, no mundo das telecomunicações, o provedor deseja ter o controle total da rede do seu cliente, pois isso facilita sua fidelização. Nas próximas seções, mostra-se que a implementação de VPNs MPLS aumenta significativamente o nível de fidelização do cliente pela operadora, pois qualquer alteração necessária na rede de comunicação do usuário exige uma alteração na configuração de rotas pela operadora.

2.3 Combinando acesso ADSL, *frame relay* e ATM

A entrega de serviços de VPNs através da rede de acesso DSL exige mais recursos de rede que a entrega dos serviços tradicionais de *internet* em alta velocidade.

A arquitetura convencional do ADSL utiliza o protocolo PPPoE entre um roteador do usuário e o DSLAM que se conecta ao *backbone internet*. Todo o tráfego entre o roteador do usuário e a *internet* é do tipo *best effort (melhor esforço)*. As contribuições apresentadas a seguir

mostram a possibilidade de construir VPNs de baixo custo e bom desempenho com a utilização dos acessos DSL.

Inicialmente, as redes de DSL (*Digital Subscriber Line)* foram desenvolvidas basicamente para o serviço de acesso à *internet* residencial em alta velocidade. No estágio atual dessa tecnologia, vários fatores estão levando as operadoras de telecomunicações a disponibilizar outros serviços sobre a tecnologia DSL. É proposta, neste tópico, a utilização da tecnologia DSL em conjunto com *frame relay* e ATM para a formação de VPNs que podem transportar vários tipos de tráfegos, como voz, dados e multimídia.

Em função de demandas do mercado por VPNs seguras com alto desempenho e baixo custo e objetivando ampliar suas opções de meios de acesso para formar VPN com baixo custo, as empresas de telecomunicações iniciaram um processo de investigação, a partir de 2003, da possibilidade de inclusão de um serviço diferenciado em seus portfólios de produtos. Esse serviço seria baseado em acessos ADSL combinados com as outras tecnologias, tais como ATM e *frame relay*.

O objetivo dessa combinação é aproveitar toda a capilaridade da malha de acesso banda larga ADSL instalada pelas operadoras, em conjunto com as redes ATM e *frame relay*, para prover conectividade entre vários *sites* da rede, similarmente a um serviço VPN de nível 2 baseado somente em tecnologia *frame relay* e ATM.

A principal aplicação dessa proposta é a interligação das LANs (*Local Area Network*) das empresas de forma simplificada e de rápida implementação. A topologia das propostas que utilizam a combinação dessas três tecnologias será sempre uma rede com topologia em estrela, com um *site* de concentração conectado através das tecnologias *frame relay* e ATM, podendo os outros *sites* ser ADSL, *frame relay* ou ATM.

A implementação dessa solução consiste na instalação nos *sites* de um CPE com interface WAN que trabalhe com os protocolos ADSL, *frame relay* e ATM. Deste CPE é configurado um PVC (*Permanent Virtual Circuit*) para que este possa se comunicar com os demais dispositivos que compõem a VPN. Nesse PVC, é possível oferecer a algumas aplicações QoS (*Quality of Service*), de acordo com o perfil de tráfego do usuário. No caso da QoS, os mecanismos adotados devem ser de nível 3 e devem atuar sobre cada pacote IP em trânsito pelo CPE; portanto, devem suportar as características mais comuns. Normalmente, é configurado nesse PVC o parâmetro CIR, que se refere à velocidade garantida, e o parâmetro EIR, que especifica a velocidade máxima que o acesso suporta.

A gerência é outra questão que merece comentários nessa solução de VPN. O CPE de cada *site* pertencente a uma VPN poderá ser gerenciado local ou remotamente. Para a gerência a distância, pelo menos um PVC deverá ser configurado entre os centros de gerência e um dos CPEs dos *sites* da VPN. Uma vez tendo conectividade com um dos elementos da VPN, todos os demais podem ser acessados. Como regra básica, o CPE a ser conectado ao centro de gerência deverá ser o do ponto de concentração.

Um dos aspectos fundamentais na implementação da solução está associado à qualidade dos pares metálicos disponíveis. É vital que os procedimentos adotados para a disponibilização de acessos ADSL para usuários corporativos sejam seguidos rigorosamente para que se possa garantir uma implementação dentro dos SLAs estabelecidos. Ou seja, diferentemente do acesso ADSL usado somente para a *internet*, o par do ADSL utilizado para o acesso de VPN corporativa deve ser seguido de vários procedimentos de teste de qualidade do par físico.

As formas possíveis de implementação de VPN nível 2 com acesso ADSL são:

- ✓ Concentrador ATM e acessos ADSL e
- ✓ Concentrador *Frame relay* e acessos ADSL.

Essas duas alternativas devem-se à impossibilidade de um acesso ADSL conectar-se com um acesso ADSL.

2.3.1 VPN ADSL COM ATM NO CONCENTRADOR E ACESSOS ADSL

Em função de a própria tecnologia ADSL já fazer uso do ATM como protocolo de nível 2, sua integração com outros CPEs que possuam interface ATM ocorre naturalmente. Esse cenário é formado com vários *sites* remotos utilizando conexões físicas ADSL e uma localidade conectada à rede ATM através de um enlace ATM, como mostrado na figura 2.11.

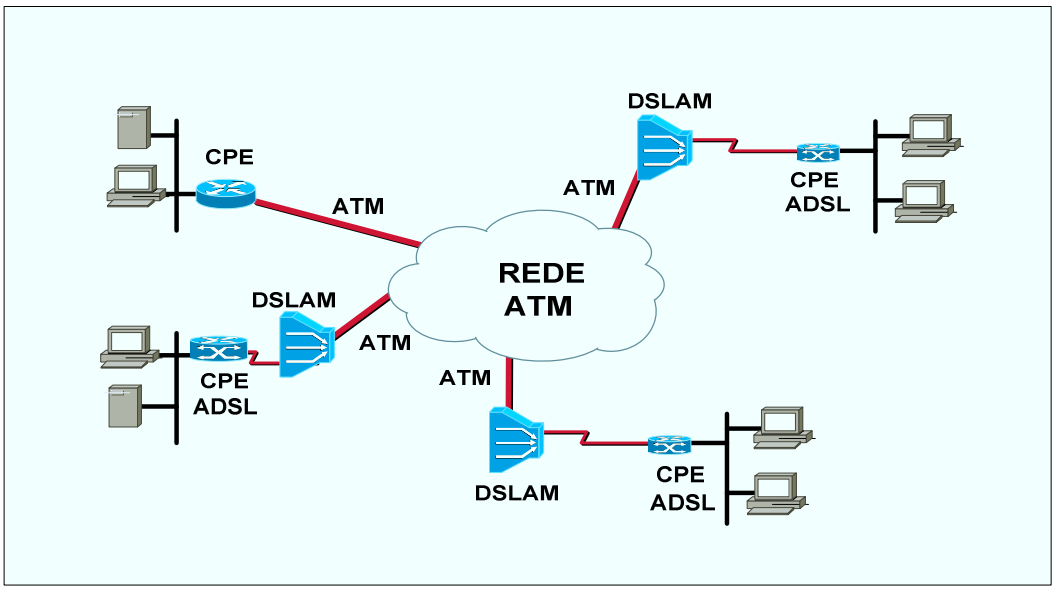

Figura 2.11 – Topologia da VPN com concentrador ATM.

A conectividade entre os vários *sites* será alcançada através da configuração de circuitos virtuais permanentes (PVC) ATM entre os *sites* com CPEs ADSL e o *site* concentrador com CPE ATM. É importante salientar que também poderemos ter acessos *frame relay* ou mesmo ATM onde estão indicados acessos ADSL.

Nesse cenário, o CPE ATM ficará como um *site* de concentração para as várias localidades remotas numa topologia em estrela e poderá usar qualquer tipo de interface ATM para conectar-se à rede, podendo ser E1, E3 e STM-1. É importante, contudo, que uma estimativa do perfil de tráfego para cada localidade remota seja feita para que se possa escolher a interface mais adequada.

Como o CPE ATM é o ponto de concentração de tráfego das localidades remotas, ele deverá suportar a terminação de sessões PPPoE e PPPoA. Os CPEs ADSL poderão ser gerenciados através da configuração de um circuito virtual de gerência para pelo menos um deles. Como colocado anteriormente, a regra básica é que esse CPE seja o do *site* de concentração.

A classe de serviço implementada em nível 2 consiste na configuração de parâmetros ATM associados aos PVCs da interface ADSL do CPE. Os parâmetros mais comuns nesse caso estão relacionados a controle de banda, *delay* e variação de *delay* (*jitter*).

Nesse tipo de controle, todo o tráfego pertencente a um dado PVC é tratado da mesma maneira, ou seja, o CPE não se preocupa efetivamente com fluxos de pacotes IP de diferentes aplicações.

É importante salientar que, durante o provisionamento de uma determinada solução, os elementos da rede ATM deverão ser configurados de forma adequada para que não se tornem gargalos durante os períodos de pico de tráfego, afetando as aplicações dos usuários finais. A figura 2.12 apresenta a topologia com as conexões virtuais ATM.

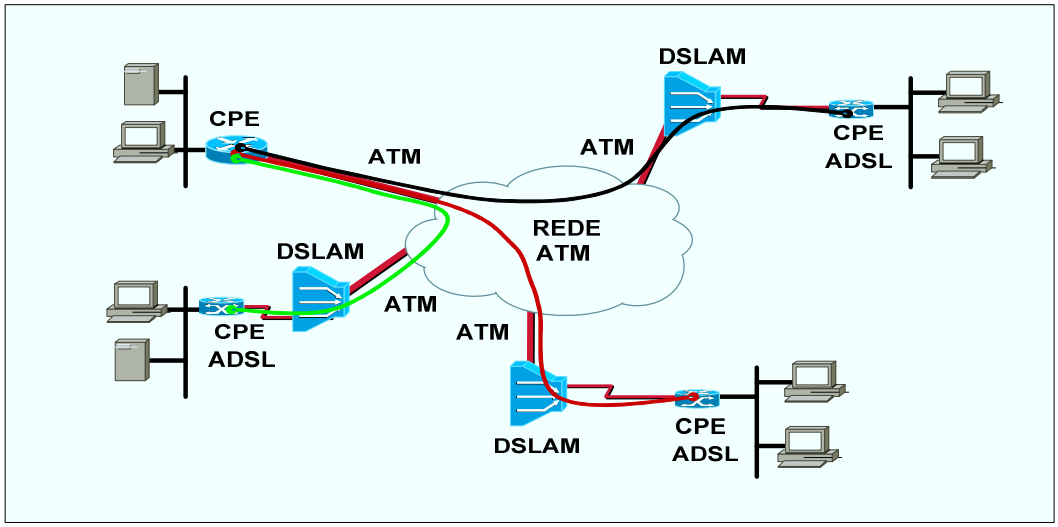

Figura 2.12 – Configuração dos PVCs.

2.3.2 VPN ADSL COM *FRAME RELAY* NO CONCENTRADOR

Como foi apresentado anteriormente, em função de a própria tecnologia ADSL já fazer uso do ATM como protocolo de nível 2 e da possibilidade de interoperabilidade entre o *frame relay* e o ATM através do padrão FRF.8 (*ATM and frame relay Service Interworking*), torna-se possível o provisionamento de um PVC entre um CPE ADSL e um CPE *frame relay*.

Através desse padrão, a rede ATM efetua um mapeamento entre os PVCs de uma interface ATM (VPI/VCI) e seus atributos para DLCIs e respectivos atributos em uma interface *frame relay*. Para os CPEs *frame relay* e ADSL, todo o processo de mapeamento descrito acima se passa de forma transparente, ou seja, não há a necessidade de qualquer configuração especial para operação. Nessa topologia, há vários *sites* utilizando os acessos ADSL (*frame relay* ou até ATM) e um *site* concentrador usando um enlace *frame relay*, como mostrado na figura 2.13.

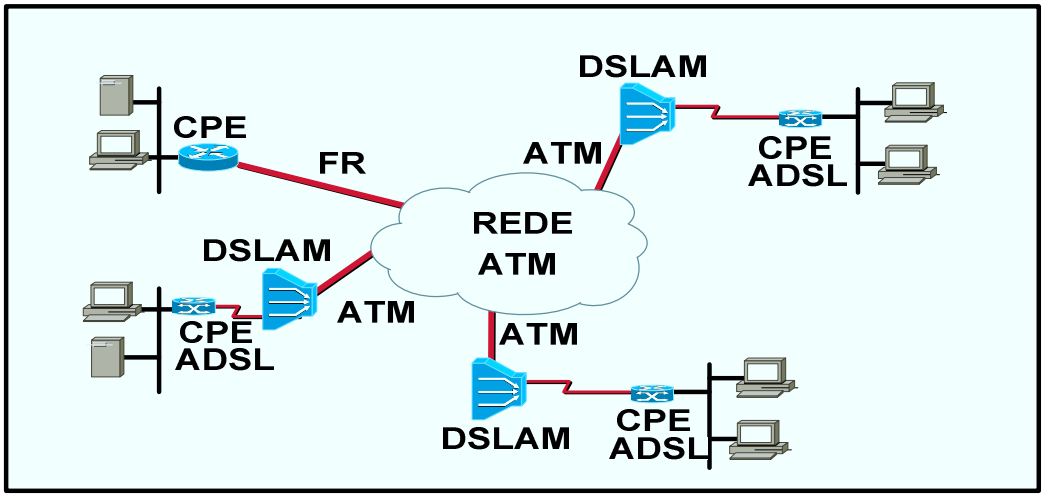

Figura 2.13 – VPN ADSL com concentrador *frame relay*.

A figura 2.14 apresenta os caminhos dos PVCs entre os acessos remotos ADSL e o concentrador *frame relay*.

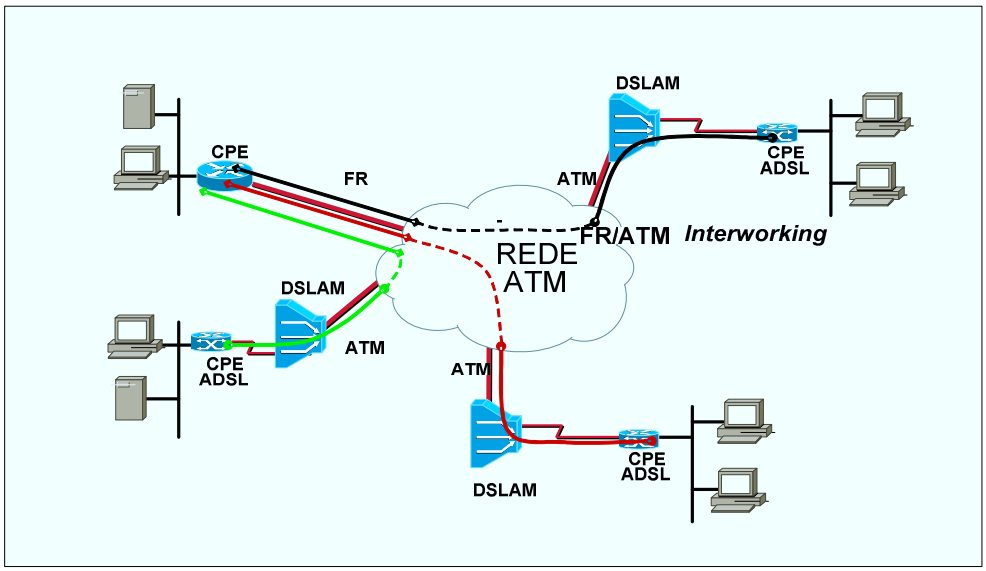

Figura 2.14 – PVCs com concentrador *frame relay*.

Com base nos modelos de VPNs apresentados acima, com acesso DSL, foi possível observar que a proposta oferece uma alternativa de formar uma VPN de baixo custo em função da utilização de acesso DSL no usuário. No entanto, a complexidade do modelo continua variando com a quantidade de acessos ao quadrado n^2, pois o núcleo da rede continua sendo ATM ou *frame relay*. Nos próximos capítulos, propõe-se a utilização de MPLS no núcleo da rede, e isso faz com que a complexidade da rede seja em função de n, e não de n^2.

2.4 VPN com acesso sem fio

Uma das maiores aplicações das redes sem fio é a formação de *intranet* móvel, que é possível através das VPN (Redes Virtuais Privadas com acesso móvel. A *intranet* móvel é o acesso remoto à VPN utilizando um acesso móvel. As Redes Virtuais Privadas Móveis (MVPNs) serão abordadas em detalhes no próximo capítulo. A seguir, apresenta-se uma análise da capacidade de canal das principais tecnologias de acesso sem fio, pois estas atualmente são as tecnologias com maior tendência de mercado. Nos próximos capítulos, trata-se do núcleo da rede, que é independente da tecnologia de acesso escolhida.

2.4.1 CAPACIDADE DO CANAL DE UMA REDE DE ACESSO SEM FIO PARA VPN MÓVEL

O desempenho da solução fim a fim de uma VPN Móvel depende basicamente da rede de acesso e do núcleo da rede. Neste item, avalia-se a capacidade da rede de acesso de algumas tecnologias que podem ser utilizadas como formas de acesso das VPNs Móveis (MVPN).

2.4.1.1 Capacidade de *downlink* das principais tecnologias de acesso sem fio

A taxa de dados no *downlink* de uma célula é normalmente definida como a capacidade da célula. A capacidade máxima teórica da taxa de dados é o parâmetro que muitas vezes é utilizado pelos fabricantes e as operadoras de telecomunicações para demonstrar a capacidade de sucesso comercial das tecnologias e compará-las com as outras disponíveis no mercado. A capacidade é medida em quantos *bits* o sistema pode transmitir por *Hertz* da largura de banda por segundo (*bits* por segundo por *Hertz*). A tabela 2.4 apresenta a taxa máxima de dados, largura de banda do canal, frequência de reuso e eficiência espectral das atuais e futuras tecnologias de redes celulares sem fio [28].

Os valores da tabela 2.4 representam os limites teóricos de cada tecnologia. As velocidades típicas observadas na prática são menores e mais bem avaliadas. Esses valores teóricos demonstram que as novas tecnologias fazem melhor uso do espectro disponível quando as condições dos sinais são consideradas ideais. Isso é devido aos seguintes fatores [28]:

- ✓ Modulação de ordem superior – enquanto GSM utiliza a modulação GMSK, que codifica um *bit* de dado por portadora, as tecnologias de gerações superiores, como LTE e 802.16e, em condições ideais, utilizam 6 *bits* de dado para cada portadora.
- ✓ Codificação reduzida – os sistemas sem fio normalmente protegem as transmissões de dados através da adição de *bit* de detecção e correção de erros. Quanto mais redundância for adicionada, maior é a possibilidade de reconstruir a informação caso ocorra um erro de transmissão. Em boas condições do meio,

menos redundância é necessária, uma vez que a probabilidade de erro de *bit* no meio é menor.

- ✓ MIMO – múltipla entrada e múltipla saída. Essa técnica explora o fato de que o sinal de rádio fica disperso entre o transmissor e o receptor. Um sistema MIMO 2 x 2 utiliza duas antenas transmissoras e duas receptoras ao longo de dois caminhos de rádios independentes. A ideia é dobrar a velocidade sem o uso adicional do espectro.
- ✓ Uso de banda de maior frequência – a utilização de maior banda de frequência aumenta a velocidade de transmissão de dados, mas não aumenta a eficiência espectral.

Na prática, a capacidade da célula é muito menor que os valores mencionados na tabela 2.4. Esses valores são aplicáveis em condições ideais. Os principais fatores que influenciam o alcance da capacidade máxima teórica da célula são: interferência intercélula, tecnologias e capacidade da rede, capacidade dos terminais, localização dos terminais e frequência utilizada.

Tabela 2.4 – Taxa de dados teóricos, largura de banda do canal, frequência de reuso e eficiência espectral de diferentes tecnologias de redes sem fio, extraído de [28].

Tipo de Rede	Taxa de dados teóricos	Largura de Banda do Canal	Reuso de Frequência	Eficiência Espectral
GSM	14,4 Kbit/s	200 KHz	4	0.032
GPRS	171 Kbit/s	200 KHz	4	0.07
EDGE	474 Kbit/s	200 KHz	4	0.2
Cdma2000	307 Kbit/s	1.25 MHz	1	0.25
1xEV-DO Rev_A	3,1 Mbit/s	1.25 MHz	1	2.4
UMTS	2 Mbit/s	5 MHz	1	0.4
HSPDA	14 Mbit/s	5 MHz	1	2.8
HSPA + (2 x 2 MIMO)	42 Mbit/s	5 MHz	1	8.4
802.16e *WIMAX*	74,8 Mbit/s	20 MHz	1	3.7
802.16e 2 x 2	160 Mbit/s	20 MHz	1	8.0
802.16e 4 x 4	300 Mbit/s	20 MHz	1	15.0
LTE	100 Mbit/s	20 MHz	1	5.0
LTE 2 x 2 MIMO	172,8 Mbit/s	20 MHz	1	8.6
LTE 4 x 4 MIMO	326,4 Mbit/s	20 MHz	1	16.3

Apesar de as novas tecnologias trabalharem nas interfaces de rádio com a máxima eficiência espectral possível, é necessário levar em consideração que uma maior eficiência espectral exige uma maior relação sinal ruído (SNR). A relação sinal ruído é determinada pela equação de Shannon Hartley:

$$C = B \log_2 (1+SNR) \quad (1)$$

Nessa equação, C representa a capacidade do canal; B, a largura de banda do canal em *Hertz*; SNR, a relação sinal ruído. A tabela 2.5 representa a eficiência espectral típica para um canal e os valores da relação da potência do sinal pela potência do ruído (SNR) [28].

Tabela 2.5 – Relação sinal ruído requerida para diferentes eficiências espectrais.

Eficiência espectral	SNR requerida em (dB)	SNR requerida (linear)
10	30	1000
5	15	31,6228
2.9	8	6,30957
2	5	3,16228
1	0	1
0,4	-5	0,316228
0,14	-10	0,1
0,04	-15	0,0316228

A análise a seguir mostra a evolução das tecnologias UMTS, HSPDA e LTE da relação sinal ruído que impacta diretamente na capacidade do canal. Na sequência, faz-se o cálculo da capacidade de alguns sistemas atuais e do futuro que foram extraídos da referência [28].

- ✓ Cálculo da máxima capacidade do canal UMTS

A capacidade teórica máxima da célula do sistema 3G UMTS é 2 Mbit/s, considerando que não há interferência entre células vizinhas. A largura de banda para o UMTS ocupa 5 MHz. Portanto, a eficiência espectral do UMTS será igual a:

$$\text{Eficiência Espectral (UMTS)} = \frac{2Mbit/s}{5MHz} = 0{,}4$$

O resultado acima está de acordo com a tabela 2.4. De acordo com o teorema da capacidade máxima do canal de Shannon Hartley e a relação sinal ruído conforme a tabela 2.4, é possível calcular a capacidade máxima do canal UMTS: SRN = -5 dB, conforme a tabela 2.5

$$\text{Capacidade máxima do canal UMTS} = 5Mhz * \log 2(1 + 0{,}316228) = 1{,}9820Mbit/s$$

- ✓ Cálculo da capacidade máxima do canal do HSDPA

A capacidade teórica máxima da célula do sistema 3G UMTS é 14 Mbit/s. Na camada física, isso é implementado utilizando-se modulação de alta ordem e reduzindo-se a taxa de codificação de erros. Para alcançar essa capacidade teórica, a seguinte eficiência espectral é necessária:

$$\text{Eficiência Espectral (HSDPA)} = \frac{14Mbit/s}{5MHz} = 2{,}8$$

De acordo com Shannon Hartley, que determina a capacidade teórica máxima, esta requer uma relação sinal-ruído muito maior em relação a UMTS; de acordo com a tabela 2.5, esse valor é 8dB.

$$\text{Capacidade máxima do canal HSDPA} = 5Mhz * \log 2(1 + 6{,}30957) = 14{,}3Mbit/s$$

- ✓ Cálculo da máxima capacidade do canal do LTE

O LTE especifica uma taxa de pico teórica de 100 Mbit/s em um canal de 20 MHz. Em um canal de 5 MHz, a taxa de pico cai para 25 Mbit/s, que é 6 Mbit/s mais rápido que o HSDPA. Para alcançar essa capacidade teórica, a seguinte eficiência espectral é necessária:

$$\text{Eficiência Espectral (LTE)} = \frac{100Mbit/s}{20MHz} = 5$$

Conforme o Shannon Hartley, a capacidade teórica máxima do canal LTE requer uma relação sinal ruído melhor em comparação com o UMTS; esse valor é aproximadamente 15 dB ou 31,6228, conforme está apresentado na tabela 2.5.

$$\text{Capacidade máxima do canal LTE} = 20Mhz * \log 2(1+31{,}6228) = 100{,}55Mbit/s$$

2.5 **VPN com acesso *metroethernet***

As VPNs com acesso *metroethernet* são uma nova forma de tecnologia de acesso à rede de dados para formação de VPNs e outros serviços devido principalmente à redução de custo de interface para grandes valores de largura de banda, em comparação com as demais tecnologias de acesso disponíveis, especialmente ATM. Em função de a *metroethernet* ser uma tecnologia de acesso em desenvolvimento, as soluções apresentam diferenças de implementações entre si.

Entre as soluções disponíveis atualmente, destacam-se: o modelo MPLS *draft-martini*/VPLS, o modelo baseado em *switches* de nível 2 e 3 (L2/L3), o modelo RPR e o modelo NG-SDH.

2.5.1 MODELO *DRAFT-MARTINI*

Nesse modelo [29], *frames ethernet* são transportados diretamente sobre os túneis MPLS (LSP), que são criados a partir do protocolo de distribuição de *label* (LDP). O modelo apresenta maior escalabilidade em relação aos outros modelos, além de garantir a isolação de tráfego de diferentes VPNs de nível 2, uma característica do MPLS analisada e avaliada no Capítulo 5. Soluções baseadas nesse modelo ainda se encontram em fase de desenvolvimento e, provavelmente, ainda não apresentam custo competitivo quando comparadas com soluções que são baseadas em *switches* L2 / L3 e NG-SDH.

Atualmente no mundo são poucas as redes MPLS que têm implementada a funcionalidade de engenharia de tráfego na rede MPLS (MPLS-TE). Com essa implementação, será possível a utilização otimizada de banda, que é uma forma de reduzir os custos de transporte das operadoras e disponibilizar recursos de *fast-rerouting* para serviços sobre um anel *metroethernet*.

A idéia inicial do modelo Martini surgiu da necessidade de uma operadora transportar o tráfego *frame relay* de um dos seus clientes sobre uma rede MPLS. A ideia foi generalizada para o transporte de outros protocolos de nível 2, como as VLAN *ethernet*, células ATM, Quadros PPP e quadros HDLC (*Hight-Level Data Link Control*). A figura 2.15 apresenta um exemplo de implementação do modelo Martini [30,31].

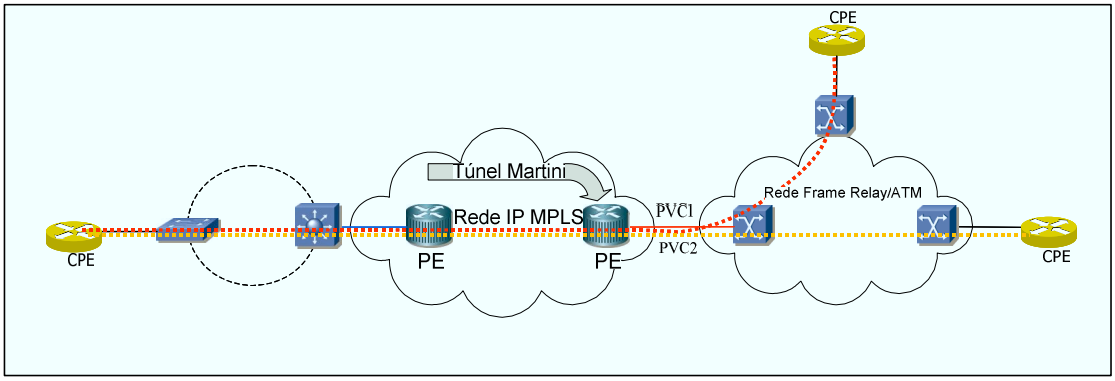

Figura 2.15 – Modelo Martini.

Basicamente, o modelo Martini permite ao provedor entregar dois tipos de serviços:

- ✓ Virtual Private Wire Service (VPWS)

O serviço de VPWS permite ao provedor entregar conexões ponto a ponto aos seus clientes. Nesse serviço, o cliente é responsável pelo roteamento, e o provedor oferece um serviço equivalente a uma linha dedicada.

- ✓ Virtual Private Lan Service (VPLS)

O Serviço VPLS representa a interconexão de dois ou mais pontos de rede através de tecnologia de *bridging ethernet* sobre uma rede MPLS. Como os quadros são transportados pelo *backbone* MPLS, a contribuição do IETF aumenta ao serem considerados os mecanismos de Qualidade de Serviço (QoS), Engenharia de Tráfego, *Fast Reroute* e OA&M (*Operations, Administration & Maintenance*), que contribuem fortemente para a escalabilidade e robustez das redes *metroethernet* [31].

2.5.2 MODELO COM *SWITCHES* L2/L3

Esse modelo fornece a melhor relação de custo por interface, entretanto, com escalabilidade limitada e necessidade de fibra óptica dedicada, sendo indicado principalmente para localidades com perspectivas de alta demanda de interfaces. A figura 2.16 apresenta um exemplo de implementação do modelo de *metrothernet.*

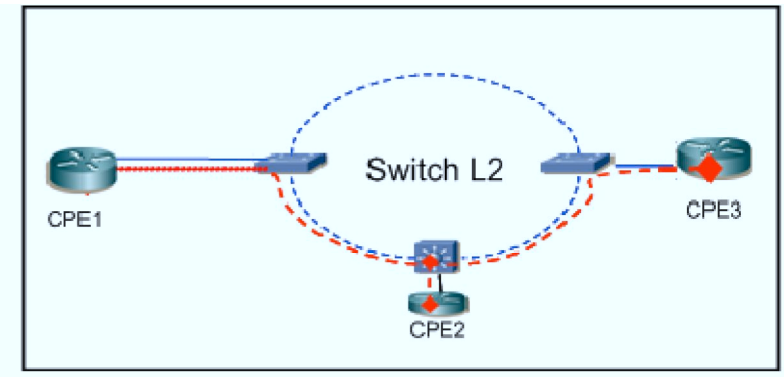

Figura 2.16 – Modelo L2.

2.5.3 MODELO RPR

O IEEE tem trabalhado na especificação do padrão 802.17 – RPR (*Resilient Packet Rings*) [32], tecnologia de anéis que permite o transporte de pacotes *ethernet* ou IP/MPLS com alta disponibilidade e eficiência.

O RPR (*Resilient packet ring*) é um padrão desenvolvido dentro do IEEE para formação de anéis para transporte de pacotes Layer 2, agregando uma série de funcionalidades para uso otimizado de recursos e suporte a diferentes classes de serviço, seguindo um modelo similar ao ATM (PCR, SCR, MBS) e funcionalidades para recuperação rápida do tráfego em caso de falhas em um anel.

Entretanto, a padronização recente, após anos em elaboração, limita a disponibilidades e a compatibilidade entre diferentes fornecedores, tornando duvidosa a adoção desse padrão pelas operadoras.

2.5.4 MODELO NG-SDH

Uma das principais formas de capilarização da Rede Metro Ethernet no Brasil deverá ser baseada em redes NG-SDH [33,34] devido à planta de transmissão existente das operadoras de telecomunicações.

2.6 Considerações sobre o dimensionamento de banda para canais de voz das VPNs

As redes de DSL (*Digital Subscriber Line*) foram desenvolvidas inicialmente para prover serviço residencial de acesso à *internet* em alta velocidade; a rede telefônica baseada em comutação de circuito para prover o serviço; e as redes *frame relay* e ATM para prover serviço de transporte de dados. Entretanto, no cenário atual, vários fatores estão levando os provedores de acesso a expandir suas redes DSL para prover novos serviços, como voz, sobre rede de pacotes (VoIP) com a mesma qualidade de serviço oferecida pelas redes tradicionais de telefonia, que

trabalham com a tecnologia de comutação por circuito. O principal fator que está levando as operadoras a optarem por DSL e não pelas tecnologias tradicionais, como *frame relay*, está baseado em custo, ou seja, o custo de implementação da tecnologia DSL é inferior ao da tecnologia *frame relay*. No entanto, cuidados devem ser levados em consideração no momento do dimensionamento da banda necessária por canal de voz.

2.6.1 TRANSMISSÃO DE VOZ EM CANAIS DIGITAIS

A necessidade de CODEC, o encapsulamento nível 2 (PPP, HDLC, *frame relay*), o encapsulamento nível 3 (IP) e controle de atraso e *jitter* utilizado na transmissão digital de voz influenciam diretamente a banda necessária para a transmissão de voz sobre IP (VoIP).

O tipo de CODEC (Codificador/Decodificador) deve ser dimensionado corretamente, pois afeta significativamente a qualidade de voz e o consumo de banda por canal de voz. O que predomina atualmente no mercado para soluções que utilizam enlace WAN é o *codec* G.729, que apresenta uma boa qualidade e uma baixa taxa de transmissão por canal de voz (8kbps) [35].

O RTP (Protocolo de tempo real) e RTCP (Protocolo de controle de tempo real) são protocolos padronizados pela IETF usados para compensar o problema de atraso e *jitter* (variação do atraso). Como os fluxos RTP normalmente transportam tráfego de informações em tempo real, é preferível que seja usado o UDP. Redes de telefonia e vídeo empregam RTP/RTCP. As principais funcionalidades do RTP/RTCP são: sincronismo (RTP), sequenciamento (RTP), identificação da mídia transportada (RTP) e retorno sobre as condições da rede (RTCP) [35].

2.6.2 TRANSMISSÃO DE VOZ SOBRE IP EM CANAIS DIGITAIS

A figura 2.18 mostra os cabeçalhos necessários para a transmissão de canais de voz sobre IP (VoIP). O cabeçalho IP+UDP+RTP produz *overhead* de 40 *bytes*, conforme mostra a figura 2.17 [35,36,37].

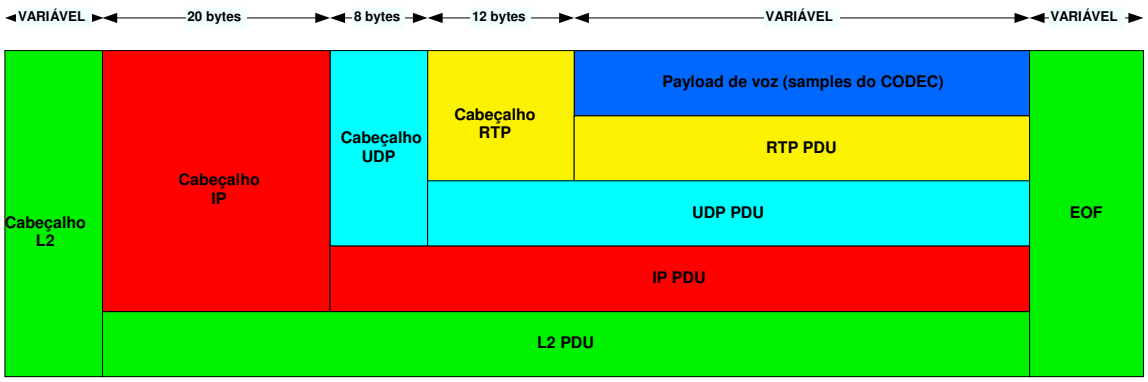

Figura 2.17 – Pacote de VoIP.

2.6.3 BANDA NECESSÁRIA PARA O TRANSPORTE DE UM PACOTE VOIP SOBRE *FRAME RELAY*

Para o correto dimensionamento, é considerado um CODEC G.729 com as seguintes características: taxa de *bits* (8kbps), intervalo de amostragem (10ms), tamanho da amostragem (10 *bytes*), o tamanho do pacote de voz (20 *bytes*), encapsulamento *frame relay* (6 *bytes*) e *end of frame* (1 *byte*) [35,36,37].

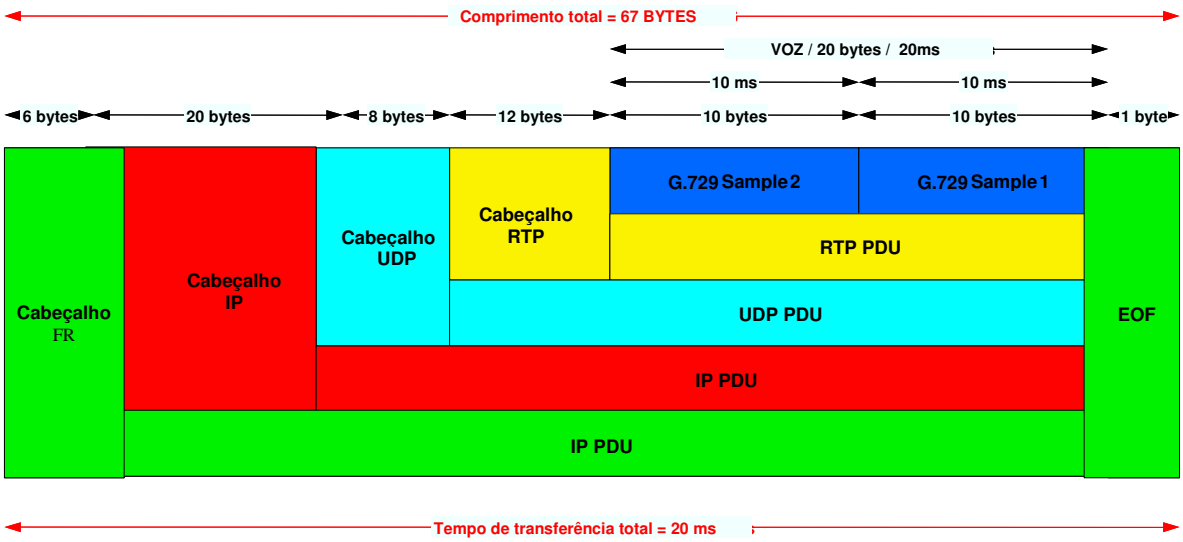

Figura 2.18 – VoIP sobre um enlace *frame relay*, adaptado de [35].

2.6.3.1 Cálculo da largura de banda do canal utilizando *frame relay*

Neste item, calcula-se a largura de banda necessária para o transporte de voz sobre IP (VoIP) sobre acesso *frame relay* com o intuito compará-la aos requisitos da banda necessária para o transporte dos canais de voz[35,36,37].

- ✓ A primeira opção é calcular a largura de banda, considerando-se apenas o encapsulamento IP + UDP + RTP.

$$BW = \frac{TPL}{TPTT} \qquad (2)$$

$$BW = \frac{60bytes}{20ms}$$

$$BW = 24kbps$$

Sendo que BW refere-se à largura de banda; TPL, ao comprimento do pacote; e TPTT, ao tempo de transferência total do pacote.

- ✓ Agora é calculada a largura de banda, considerando-se o cabeçalho do *frame relay*, ou seja, IP + UDP + RTP + *frame relay*

$$BW = \frac{TPL}{TPTT}$$

$$BW = \frac{67bytes}{20ms}$$

$$BW = 26{,}8kbps$$

Com o encapsulamento *frame relay*, a largura de banda ficou 12% superior à banda de 24 Kbps. Ou seja, para um *CODEC* de 8Kbps utilizando VoIP, é necessária uma banda de 24 Kbps devido ao *overhead* do IP, UDP e RTP. Caso seja utilizado um enlace *frame relay* para a conexão WAN, a largura de banda necessária será de 26,8 Kbps.

Uma técnica para reduzir a quantidade de banda é usar a compressão de cabeçalho IP/UDP/RTP, conforme a figura 2.19. O protocolo cRTP (*Compressed Real-time Transport Protocol*) comprime o(s) cabeçalho(s) do pacote que transporta o tráfego de voz. Essa compressão pode ser aplicada somente ao cabeçalho RTP ou à combinação dos cabeçalhos IP+UDP+RTP. Quando aplicado à combinação dos cabeçalhos IP, UDP e RTP, o protocolo cRTP consegue uma compressão de cabeçalho de 40 para 2 *bytes*, ou para 4 se considerarmos o *checksum* UDP[35,36,37]. Essa compressão corresponde a uma redução de até 95% na sobrecarga (*overhead*) referente aos cabeçalhos. Na prática, muitas das operadoras de telecomunicações preferem normalmente não ativar a compressão, pois envolve alto processamento nos roteadores de borda da rede em troca de um sobredimensionamento da rede.

No exemplo anterior, com a utilização do cRTP, a banda será:

$$BW = \frac{29bytes}{20ms}$$

$$BW = 11{,}6Kbps$$

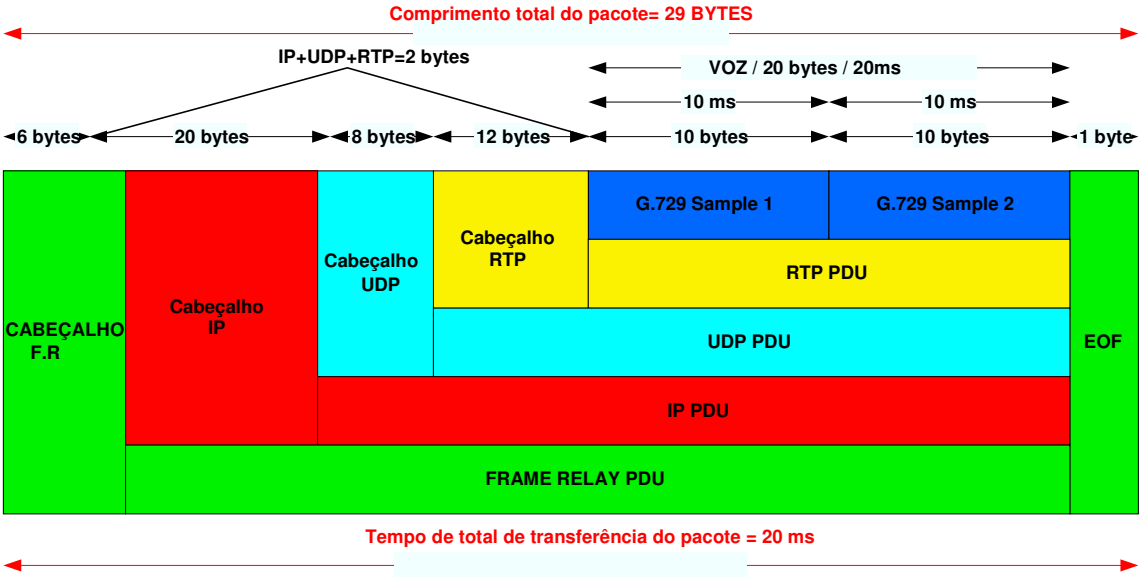

Figura 2.19 – Compressão IP+UDP+RTP.

2.6.4 ENCAPSULAMENTO DE VOIP EM ADSL

Neste tópico, é calculada a largura de banda necessária para o transporte de voz do canal DSL, comparando-se o seu resultado com o do *frame relay*. Avalia-se a banda necessária em um acesso DSL PPPoA. A figura 2.20, abaixo, apresenta os quadros PPPoA utilizados em DSL[35,36,37].

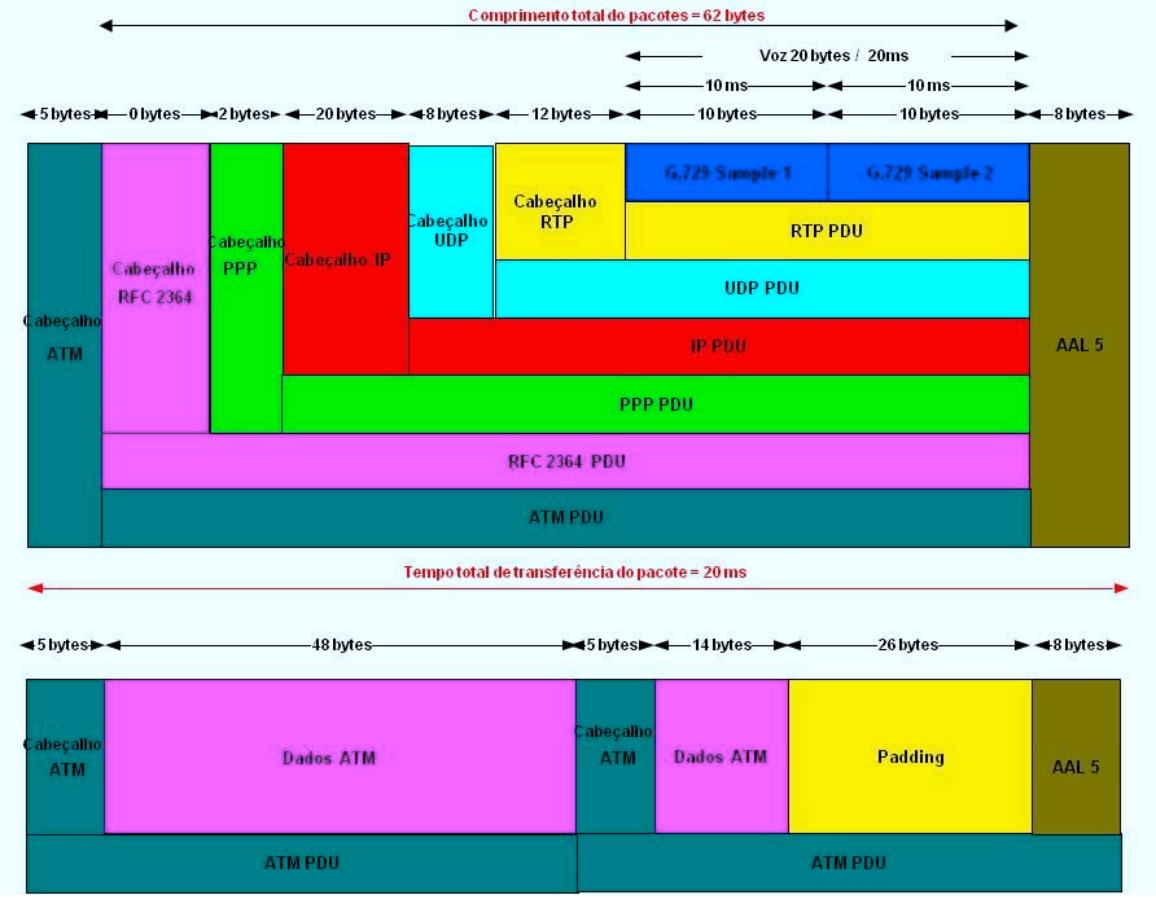

Figura 2.20 – Encapsulamento de VoIP em ADSL.

A banda necessária é:

$$BW = \frac{106bytes}{20ms}$$

$$BW = 42{,}4kbps$$

Esse resultado mostra que, para transportar um canal de voz sobre um acesso DSL, é necessária uma banda de 42,4Kbps, enquanto que, para um acesso *frame relay*, são necessários somente 26,8Kbps. Esse valor representa um ganho em banda de 36,79% da tecnologia *frame relay* sobre o DSL, mas, mesmo diante dessa deficiência do DSL em relação ao *frame relay*, as operadoras de telecomunicações têm demonstrado a preferência pela tecnologia DSL à tecnologia *frame relay*, pois esta apresenta um custo de implementação superior em relação ao da tecnologia DSL.

2.7 Novas arquiteturas de *backhaul* móvel para as redes de nova geração

Nas especificações para a evolução das redes 2G para 2.5G e 3G, o ATM foi especificado no *release* 99 do 3G. Na época, imaginava-se que o ATM fosse a principal solução para integrar voz, dados e vídeo em uma única plataforma, mas, devido aos problemas de escalabilidade, que são avaliados futuramente, o ATM não foi uma solução que motivou a migração do TDM baseado em SDH e PDH, ou seja, no cenário atual, praticamente todos os *cores* das redes móveis continuam trabalhando com TDM. Além da falta de escalabilidade, o ATM não obteve sucesso entre as operadoras móveis em função, principalmente, do alto custo dos acessos de 34 Mbits/s e 155 Mbit/s [38].

O que se pode observar é que a evolução nas redes móveis tem se mostrado com maior frequência nas redes de acesso entre o usuário e as estações bases (BS) do que a evolução das tecnologias de transmissão entre as BSs - BSC, BSC- MSC e entre os outros elementos das arquiteturas de redes móveis. Essa falta de evolução na tecnologia do núcleo das redes tem levado as operadoras a continuar utilizando as técnicas TDM através das tecnologias SDH e PDH até os dias atuais. Ou seja, normalmente, entre as BSCs as MSC, é utilizado 1 x STM1 ou 2 x STM1 e, entre as BSs e as BSC, alguns enlaces de 16 x E1.

A figura 2.21 mostra a evolução natural que deverá acontecer nos próximos anos no núcleo e no acesso das redes móveis. A primeira migração será a implementação do MPLS no

núcleo da rede; em seguida, a implementação será entre a BS e a BSC, ou seja, no *backhaul*. Este trabalho avalia a implementação no *backhaul*, por entender que a implementação no núcleo da rede móvel será muito semelhante à já realizada na migração do núcleo da rede fixa TDM/ATM para a rede IP MPLS.

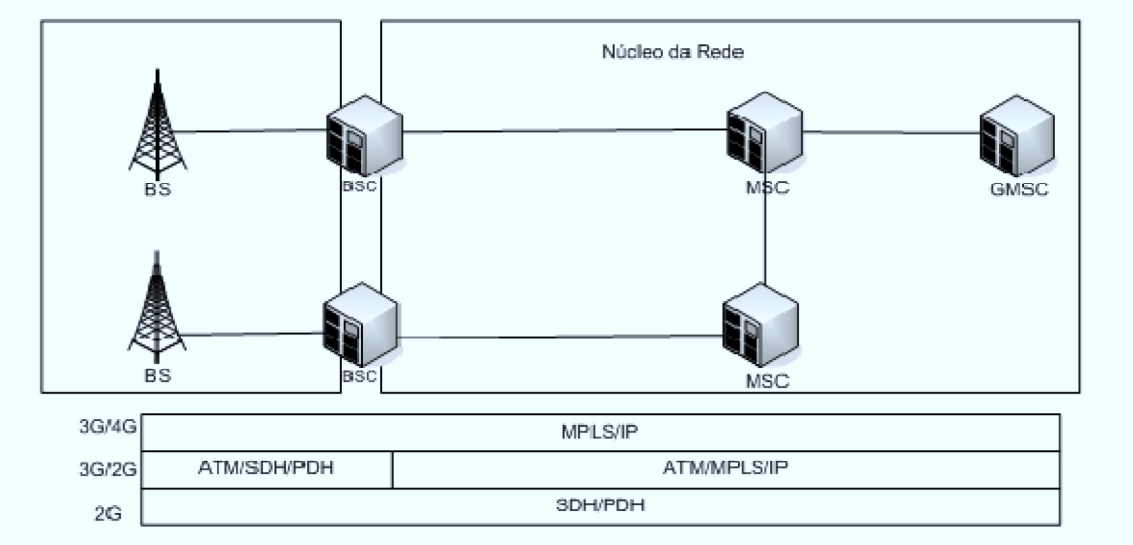

Figura 2.21 – Formas de implementação de MPLS nas redes móveis.

A figura 2.22, apresentada a seguir, mostra a evolução das possíveis implementações de *backhaul* no mundo, sendo que, na Europa e Ásia, predominam as implementações com rádio micro-ondas IP/*ethernet*. É possível observar que os rádios micro-ondas com interface *ethernet* IP são muito utilizados, mostrando a grande tendência de IP no uso em *backhaul* [39].

Um dos grandes problemas das operadoras de comunicações móveis hoje é o custo entre as BSs e as BSCs, seja esse transporte baseado em IP/*Ethernet* sobre PDH, SDH, ATM ou micro-ondas. Uma proposta, então, é implementar IP/*Ethernet* sobre MPLS, pois, como se mostra nos

próximos capítulos, apresenta um custo inferior em relação às tecnologias tradicionais.

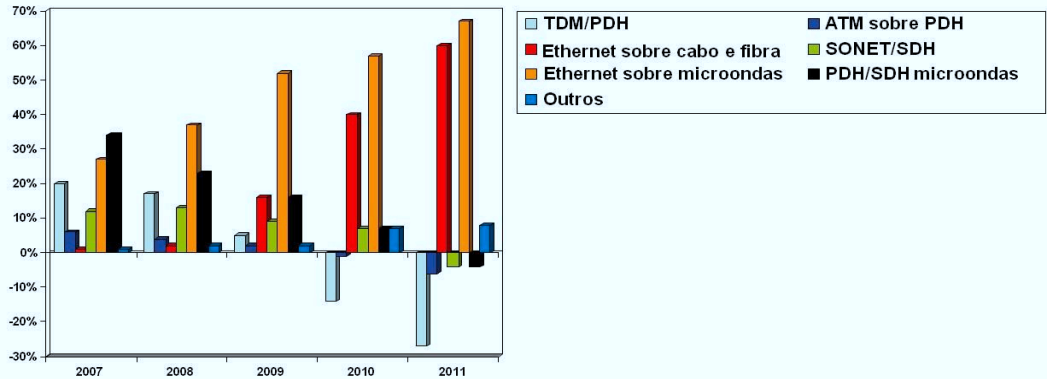

Figura 2.22 – Tecnologias de *backhaul* utilizadas no mundo, extraído de [39].

2.7.1 ELEMENTOS DA REDE DE ACESSO

Os principais elementos de uma rede de acesso de rádio móvel são as BTSs e as BSCs. A BTS é o equipamento que provê comunicação entre o equipamento do usuário e a rede móvel. A BSC tem como principal função controlar as várias BTSs. A BSC é responsável também pelo controle dos *handoffs* que ocorrem devido à movimentação do usuário entre células. A tabela 2.6 apresenta de forma resumida as principais diferenças e convenções utilizadas nas principais tecnologias e suas gerações [40].

Tabela 2.6 – Principais características das tecnologias móveis.

Gerações	Tecnologia	Componentes da RAN	Principais funções
2G	GSM	BTS	Comunicação entre a interface aérea e a BSC
		BSC	Controlar múltiplas BSs
		MSC	Tratar as chamadas de voz e SMS
2.5G	GPRS	BTS	Comunicação entre a interface aérea e a BSC
		SGSN	Provê comunicação entre o backbone e a rede de acesso
		GGSN	Conexão para outra rede
		BSC + PCU	Controlar múltiplas BSs
3G	UTRAN	NodeB	Funções similares a BTS
		RNC	Funções similares a BSC
		PDSN	Conexão para outra rede externa
4G	LTE	eNodeB	Funções semelhantes a BTS
		SGW	Encaminhamento e roteamento dos dados dos usuários
		MME	Gerenciamento do handoff
		PDN	Conexão para outra rede externa
	WiMax	BS	DHCP, QoS e classificação do tráfego
		ASN GW	Agregação de tráfego
		CSN GW	Conectividade para a internet, rede pública ou privada

2.7.2 *BACKAHAUL* MÓVEL

O *backhaul* pode ser considerado uma parte da rede que conecta a estação base (BTS) à BSC e ao núcleo de rede móvel. O *backhaul* pode constituir um grupo de BSs, concentrando o tráfego em uma BSC, como mostra a figura 2.23. Essa figura apresenta uma BS conectada à BSC através de um *backhaul* móvel; essa BSC poderia estar concentrando outros tráfegos de outras BSs [40].

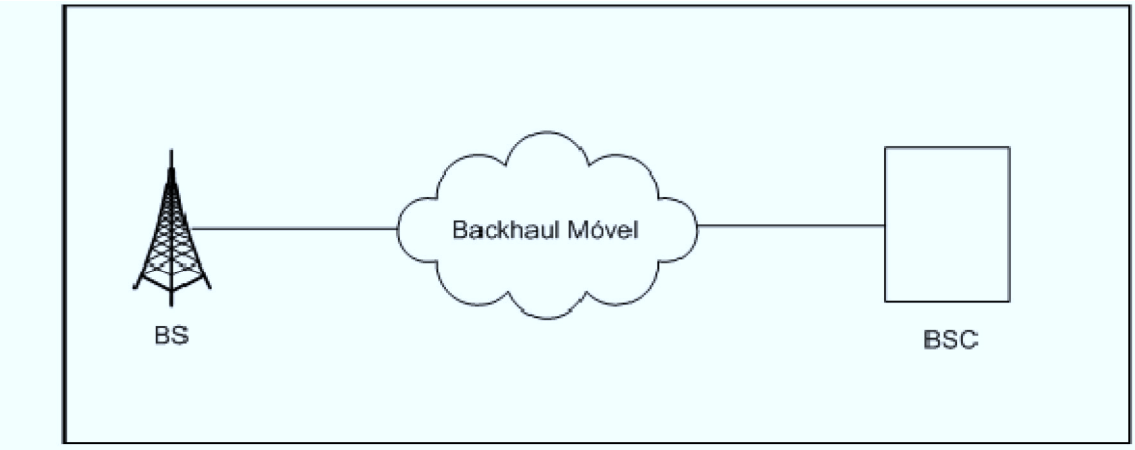

Figura 2.23 – Modelo geral de *backhaul*.

As novas tecnologias para o *backhaul* móvel levam em consideração a agregação do tráfego das BSs que podem estar conectadas através de uma VPN MPLS à BSC. Os novos *backhauls* devem suportar a integração das diferentes formas de acessos das gerações atuais e passadas, como 2G, 2.5G e 3G (*Rel* 99), que eram basicamente formadas de interfaces TDM e ATM nas estações base.

As gerações 2G e 2.5 G, que representavam as tecnologias GPRS, TDMA e CDMA, utilizavam basicamente interfaces E1 nas BSs e transportavam esse tráfego sobre uma rede de transporte SDH ou PDH até a BSC. Essa solução apresentava vários problemas técnicos e comerciais. Os problemas técnicos estão relacionados principalmente com a quantidade de portas nas BSCs necessárias para agregar todos os tráfegos das BSs, e o comercial é o custo dos enlaces dedicados que apresentam alto valor mensal, inviabilizando muitas vezes a instalação de novas BSs.

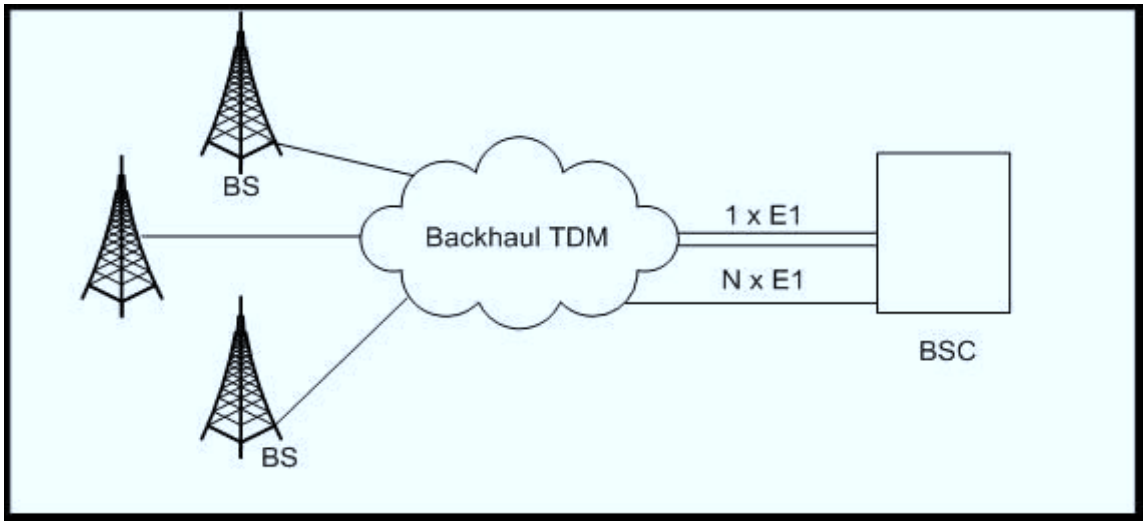

Figura 2.24 – Modelo de *backhaul* baseado em TDM.

As gerações 3G (*Rel* 99), que representam a tecnologia UMTS, já evoluíram em relação à interface física na BS, pois permitem a conexão através do protocolo ATM. Isso torna possível a conexão de várias interfaces das BSs até a BSC através de vários CVPs, permitindo uma grande economia de interfaces nas BSCs. No entanto, essa alternativa de *backhaul* não teve grande aceitação devido aos grandes custos das interfaces ATM e dos preços comerciais dos acessos ATM cobrados pelas operadoras, o que tornava inviável esse tipo de conexão para a formação de *backhaul*. Além do custo, a falta de granularidade das interfaces ATM prejudica a sua utilização, ou seja, uma situação comum entre uma BS e uma BSC são aproximadamente 12 x E1, obrigando a operadora móvel a contratar uma porta ATM de 34 Mbps.

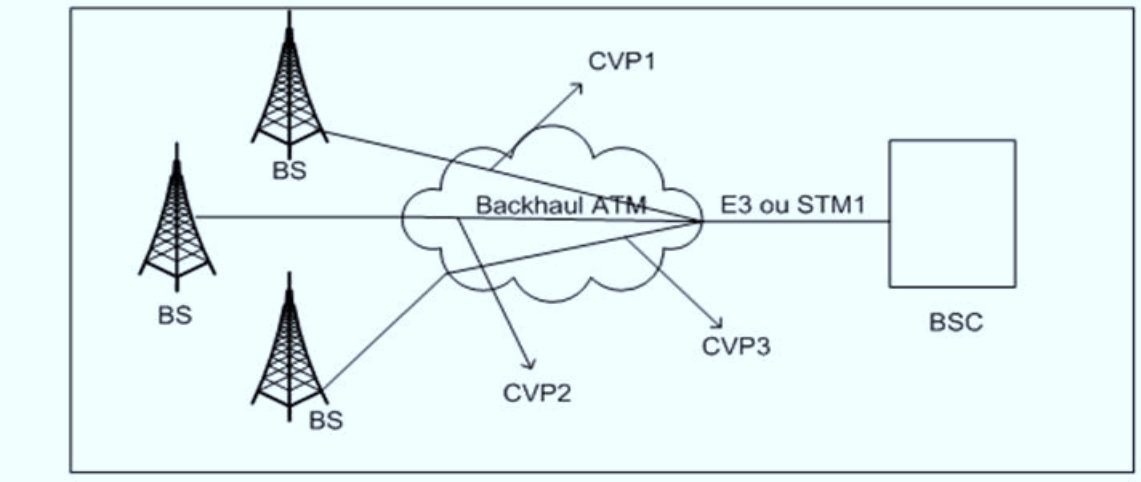

Figura 2.25 – Modelo de *backhaul* baseado em ATM.

As gerações 3G/4G, como EVDO, UMTS (*Rel5*), *WiMax* e LTE, já possuem interfaces IP. Portanto, é possível fazer um novo modelo de transporte baseado em MPLS criando uma VPN MPLS, o que é apresentado a seguir. A tabela 2.7 apresenta de forma resumida as principais características que são suportadas pelas BSs em um sistema móvel.

Tabela 2.7 – Principais características das BSs, extraído de [40].

Geração	Tecnologia	Suporte de interface na BS	Modelo de *backhaul*
2G e 2.5G	GPRS/TDMA/CDMA	Canalização TDM	PDH/SDH
3G (Rel99)	UMTS	ATM	ATM
3G/4G	EVDO, UMTS (Rel5), *WiMax* e LTE	IP	MPLS

As novas arquiteturas de *backhaul* devem suportar várias interfaces na BS para permitir a integração e a preservação dos investimentos realizados nas gerações 2G, 2.5G, 3G e nos novos avanços que surgirão.

Os principais motivos para a implementação do MPLS no núcleo das redes móveis são [41]:

- ✓ Necessidade de baixo valor do atraso (*delay*)

Dependendo do modelo de tráfego que será transportado sobre a rede, é preciso garantir o tempo necessário para que a aplicação tenha o seu desempenho adequado.

- ✓ Necessidade de baixo custo

É esperada, pelas operadoras de telecomunicações, uma redução do custo pelo compartilhamento da rede. No próximo capítulo, é mostrado que, diferentemente das soluções baseadas em núcleo TDM, *frame relay* e ATM, onde o custo varia com n^2, nas soluções baseadas na tecnologia IP MPLS o custo varia com n. A figura 2.26 apresenta uma comparação entre as tecnologias baseadas em TDM e IP MPLS para atender às demandas de tráfego em dois períodos distintos. O primeiro período apresenta a época em que as redes transportavam

somente o tráfego de voz; nesse caso, a rentabilidade da operadora é positiva em ambas as tecnologias. No segundo período, é observado que as redes necessitam transportar dados multimídia; nessa situação, as redes convencionais baseadas em tecnologias TDM continuam tendo um custo exponencial maior que as receitas dos serviços, apresentando rentabilidade negativa, enquanto as redes baseadas em MPLS têm um custo constante com o aumento exponencial de tráfego, portanto, a margem de lucratividade será positiva e cresce à medida que o tráfego aumenta na rede.

(a) Tecnologia TDM (b) Tecnologia IP MPLS

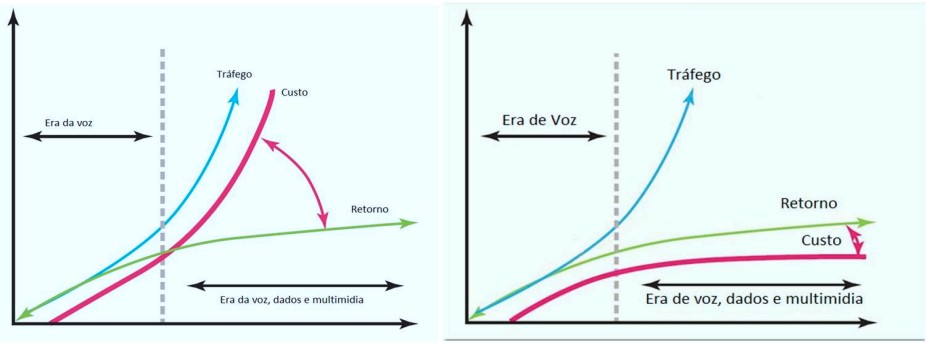

Figura 2. 26 – Comparação do tráfego, custo e retorno para as operadoras, adaptado de [41].

✓ Redução na quantidade e complexidade dos equipamentos

Com a implementação de MPLS no núcleo da rede com acesso *metroethernet* é possível uma grande simplificação nas interfaces dos equipamentos para agregação do tráfego, principalmente aquele entre as BSs e as BSCs, e entre as BSCs e os outros equipamentos do núcleo da rede.

2.7.2.1 Requisitos de um *backhaul* IP MPLS

Qualquer modelo de *backhaul* sugerido tem que ser capaz de tratar de forma diferenciada no mínimo quatro tipos de tráfegos, que são o de gerenciamento, o de sincronização, o de sinalização e o do usuário. Esses tráfegos precisam ser priorizados de acordo com as aplicações para o funcionamento correto do serviço. A estratégia proposta e avaliada no Capítulo 4 é baseada no campo DSCP da arquitetura *DiffServ* e no campo EXP do MPLS. Nessa estratégia, os

pacotes IP devem ser classificados a partir das BSs de acordo com os requisitos necessários e priorizados no *backhaul* MPLS.

O *backhaul* deve estar habilitado a suportar os principais tipos de tráfegos e prover uma baixa taxa de perda de pacotes, baixo *jitter e delay*. O Capítulo 5 avalia esses parâmetros da QoS.

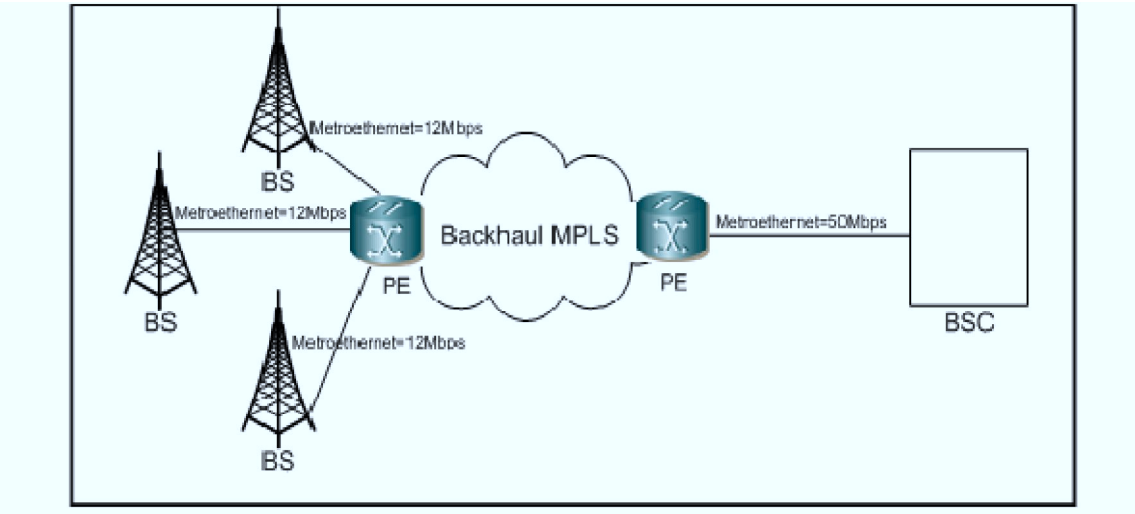

Figura 2. 27 – *Backhaul* MPLS.

A solução de *backhaul* com MPLS oferece às operadoras todos os benefícios dessa tecnologia. A complexidade é reduzida significativamente devido às características do MPLS e à simplicidade de implementação de interface IP nas BSs com grande granularidade de velocidades. Além da simplicidade e custo, as soluções de *backhaul* baseadas em MPLS permitem que as aplicações sejam classificadas de acordo com o grau de exigência. Por exemplo, é possível definir que uma classe chamada de *handoff* seja priorizada em relação às outras classes de serviços.

Este Capítulo mostrou como as tecnologias de banda larga podem ser utilizadas para desenvolver novas aplicações que vão além da *internet*, sendo apresentadas as principais tecnologias de acesso de banda larga que podem ser utilizadas para a formação das VPNs fixo-móveis, que representam a convergência/integração das redes. O capítulo faz uma comparação

da eficiência de banda para utilização das tecnologias de banda larga DSL em relação a *frame relay* para o transporte de voz, mostrando que, mesmo sendo uma tendência a utilização das tecnologias de banda larga para as redes de nova geração, elas apresentam pouca eficiência de banda em relação às tecnologias tradicionais, como *frame relay*. No entanto, como os custos das tecnologias banda larga são infinitamente inferiores aos das tecnologias tradicionais, as operadoras de telecomunicações têm optado por banda larga no acesso e MPLS no núcleo da rede. Essa tendência se refletirá, principalmente, nos *backhauls* móveis do futuro, que representarão uma grande diminuição da complexidade das redes móveis, com ênfase nas conexões entre BSs e BSC. De forma geral, a contribuição do capítulo é o uso das tecnologias de banda larga para as novas aplicações de VPNs fixo-móveis convergentes, dadas várias contribuições nas formas de construir novas arquiteturas de VPNs com banda larga. O próximo capítulo irá abordar as tecnologias de núcleo das VPNs com maior ênfase em MPLS.

Capítulo 3

Redes Virtuais Privadas Fixo-Móveis

Neste capítulo, analisam-se inicialmente os conceitos mais importantes dentro do ambiente das VPNs (*Virtual Private Network* - Redes Virtuais Privadas) fixas e as MVPNs (*Mobile Virtual Private Network* - Redes Virtuais Privadas Móveis), que em conjunto caracterizam o ambiente de convergência. São avaliados os requisitos mais fundamentais das aplicações para o transporte sobre a MVPN e as principais tecnologias de *core* de rede utilizadas para construir VPNs. O capítulo inicia apresentando as leis básicas responsáveis pelo sucesso da formação das tecnologias de comunicação digital e adaptar as mesmas leis com a necessidade de convergência das VPNs móveis – fixa.

3.1 **As leis básicas responsáveis pelo sucesso da convergência das redes**

Conforme Viterbi [8], é possível demonstrar que a implementação e o sucesso comercial e técnico das VPNs móveis (MVPN) e fixa dependem de quatro leis básicas, apresentadas a seguir [42]:

- ✓ Maxwell
- ✓ Shannon

- ✓ Moore
- ✓ Metcafe

As leis de Maxwell permitem o entendimento das propagações das ondas eletromagnéticas dos acessos sem fio entre os equipamentos dos usuários (CE) e os equipamentos de borda (PE) das redes dos provedores de serviços para a formação das VPNs. Shannon permite o entendimento e a melhor utilização da eficiência espectral e das novas tecnologias, possibilitando a otimização da capacidade máxima do canal. Gordon Moore, fundador da Intel Corporation, observou o número de componentes por unidade de área que podem ser encapsulados em um circuito integrado de silício e verificou que essa quantidade dobra a cada um ano e meio. A equação abaixo expressa esse crescimento [42].

$$V(T) = v(To)2^{(T-To)/1.5}$$

Onde V(T) é a quantidade de componentes em um tempo T>To.

Esse crescimento exponencial faz com que a indústria dos semicondutores coloque no mercado equipamentos de comunicações com melhor desempenho e preços mais acessíveis para seus usuários. Nas redes convergentes, esse fato está mais presente nos equipamentos dos usuários e nos equipamentos do núcleo da rede do provedor do serviço. De forma geral, Moore possibilitou a implementação das contribuições teóricas apresentadas por Shannon, tanto em relação à codificação de fonte quanto no que se refere à codificação de canal. A lei de *Metcalfe* é uma lei socioeconômica. Conforme *Metcalfe*, o custo de uma rede fixa ou móvel de comunicações cresce de acordo com o número de usuário ao quadrado. Mais precisamente, é possível escrever que:

$$Custo\_MVPN = N(N-1)/2 \qquad (3)$$

Onde "N" é o número de usuários da MVPN.

A consideração de *Metcalfe* é válida para Redes Virtuais Privadas (VPNs) que eram implementadas baseadas nos conceitos convencionais, como *frame relay* e ATM. Para essas tecnologias, o preço final da solução é função da quantidade de CVP (circuitos virtuais privados) e do degrau de cada CVP (distância entre os *sites*). Como para estabelecer a conexão completa entre todos os *sites* é necessário n(n-1) /2 conexões, o preço final é também proporcional a n^2. Uma das contribuições desta tese é utilizar o MPLS no núcleo das redes convergentes de nova geração, o que traz como grande benefício econômico para o usuário o preço final da solução, que deixa de ser função de n^2 e passa a ser função de n somente, onde n é número de *sites* da VPN. Outro benefício econômico é o preço do serviço, que passa a ser por acesso, e não mais por degrau (distância).

3.2 **Introdução às VPNs**

VPN é chamada de Rede Virtual Privada em função de três principais motivos [43]:

- ✓ Primeiro, porque é uma rede e oferece conectividade entre os *sites* localizados em ambientes distintos;
- ✓ Segundo, é virtual porque o provedor do serviço pode usar os mesmos recursos da rede para atender vários clientes e prover vários serviços sobre a mesma plataforma;
- ✓ Terceiro, é privada porque, desde que configurada corretamente, apresenta o mesmo nível de *segurança* que uma rede privativa (dedicada).

A solução fim a fim das VPNs basicamente dividem-se em rede de acesso e rede do núcleo, conforme mostra a figura 3.1. As VPNs também são classificadas em VPNs fixo - móveis e móveis. O que diferencia uma VPN móvel (MVPN) de uma VPN fixa é o tipo de tecnologia utilizada no acesso. As MVPNs mais comuns são aquelas que utilizam no acesso as tecnologias

GPRS e 3G, mas é fundamental para o sucesso comercial que as soluções oferecidas pelas operadoras das MVPNs suportem outras tecnologias de acesso e estejam preparadas para integração com as futuras formas de acesso, como 4G e *metroethernet*. O núcleo (*core*) da rede pode utilizar duas tecnologias: ATM ou MPLS. Atualmente, todas as operadoras de telecomunicações estão preparando seus planos de negócios e suas arquiteturas de rede para suportar uma variedade de tipos de acessos às MVPNs e a integração das MVPNs com as VPNs fixas.

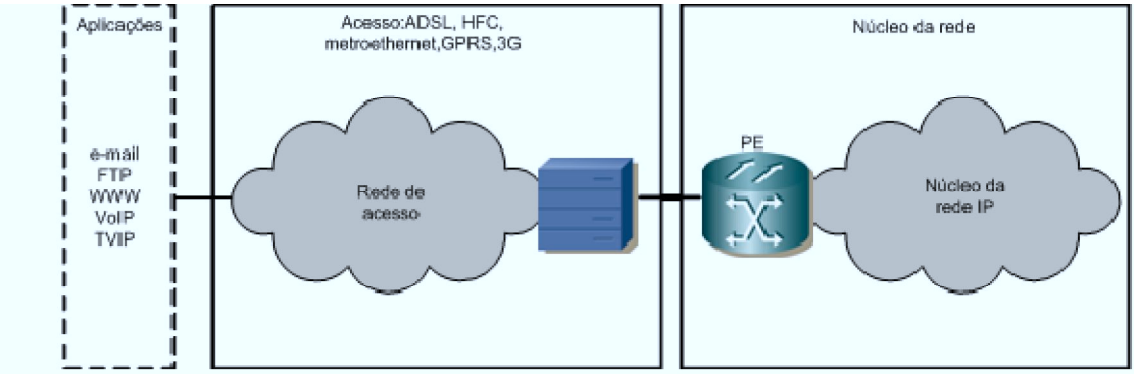

Figura 3.1 – Topologia de VPN fixo - móvel.

É fundamental conhecer as principais tecnologias das redes de acesso e de *core* (núcleo) para o entendimento completo das VPNs fixo - móveis. A rede de acesso refere-se à tecnologia utilizada para conectar o equipamento do usuário (CE ou CPE) ao equipamento do provedor de serviço. Em MVPN, essas tecnologias de acesso são constituídas de redes sem fios, que foram abordadas no capítulo anterior. O *core* (núcleo) de rede é definido como o protocolo utilizado pelas redes das operadoras para interagir com as estações ou equipamento do usuário para oferecer gerenciamento, suporte à mobilidade, configuração das MVPNs, qualidade de serviço e segurança no núcleo da rede. A seguir, são apresentadas as deficiências e os principais problemas que as tecnologias de *core* (núcleo) de rede baseado em ATM/*frame relay* oferecem, para, em seguida, apresentar uma solução baseada no protocolo de núcleo chamado MPLS. O MPLS, como toda solução tecnológica, apresenta novos problemas, que são avaliados nos capítulos 4, 5 e 6, onde também são propostas alternativas para solucioná-los.

3.3 **Requisitos das principais aplicações das VPNs fixo - móveis**

Muitos aplicativos de rede têm requisitos de qualidade de serviços diferentes. Esses requisitos devem ser atendidos pelas VPNs fixo - móveis de acordo com as suas respectivas especificações.

A tabela 3.1 apresenta os principais aplicativos que normalmente são encontrados no ambiente do usuário e que geram tráfego sobre as MVPNs: VoIP (*Voice over IP*), *e-mail*, FTP (protocolos de transferência de arquivos) e videoconferência.

Tabela 3.1 – Principais aplicações e seus requisitos de qualidade de serviço.

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

Para um bom desempenho de VoIP (Voz sobre IP), não é necessário que a MVPN disponibilize grandes bandas de transmissão, mas a latência e *jitter* são críticos, pois o ser humano necessita escutar o que ele próprio falou (eco) em um tempo menor que 100 ms. As amostras precisam ser transmitidas e recuperadas em intervalos regulares. Em relação às perdas, as aplicações de áudio não apresentam requisitos críticos.

As aplicações que envolvem a transmissão de imagens, paradas ou em movimento, são algumas das que mais demandam vazão das VPNs. As aplicações de vídeo são quase invariavelmente transmitidas na forma "comprimida". As técnicas de compressão tradicionais geram um tráfego a taxa constante, enquanto técnicas mais modernas, como o MPEG, geram tráfego variável. Pode-se atingir relações de compressão da ordem de 100:1 ou melhores. Para aplicações científicas, que exigem alta definição (HDTV), podem ser necessárias várias centenas de *megabits* por segundo para cada transmissão de vídeo ou até mesmo taxas de *gigabits*/segundo. Para aplicações como videoconferência, os requisitos podem ser reduzidos a alguns *megabits*/ segundo.

Em aplicações de dados, a VPN fixo - móvel tem que fornecer como principal requisito, a baixa perda. Isso requer que sejam empregadas infraestruturas de rede de alta confiabilidade e sejam implementados mecanismos de detecção e correção de erros. Outros requisitos menos críticos estão relacionados à banda de transmissão e ao atraso.

3.4 VPNs com núcleo (*Core*) ATM/*Frame Rela*y e suas deficiências

As VPNs com acesso *frame relay* [44] e núcleo ATM foram o método mais seguro e econômico de construir VPN na década de 1990 e início de 2000. Era a técnica mais comum para prover serviços de VPNs que exigiam requisitos de segurança e QoS (*Quality of Service*). Nesse modelo, cada *site* de acesso do ambiente do usuário tem um roteador, que é conectado, através de enlaces ponto a ponto, até o outro roteador remoto do usuário. O ambiente do usuário pode ter um ou mais roteadores, que são conectados a todos os outros *sites* ou a um subconjunto destes. A rede formada por esses enlaces ponto a ponto e os roteadores instalados formam um "*Backbone Virtual*". É nesse *backbone* virtual que os provedores de serviços de telecomunicações formavam as VPNs para interligar as redes dos *sites* dos usuários (Figura 3.2).

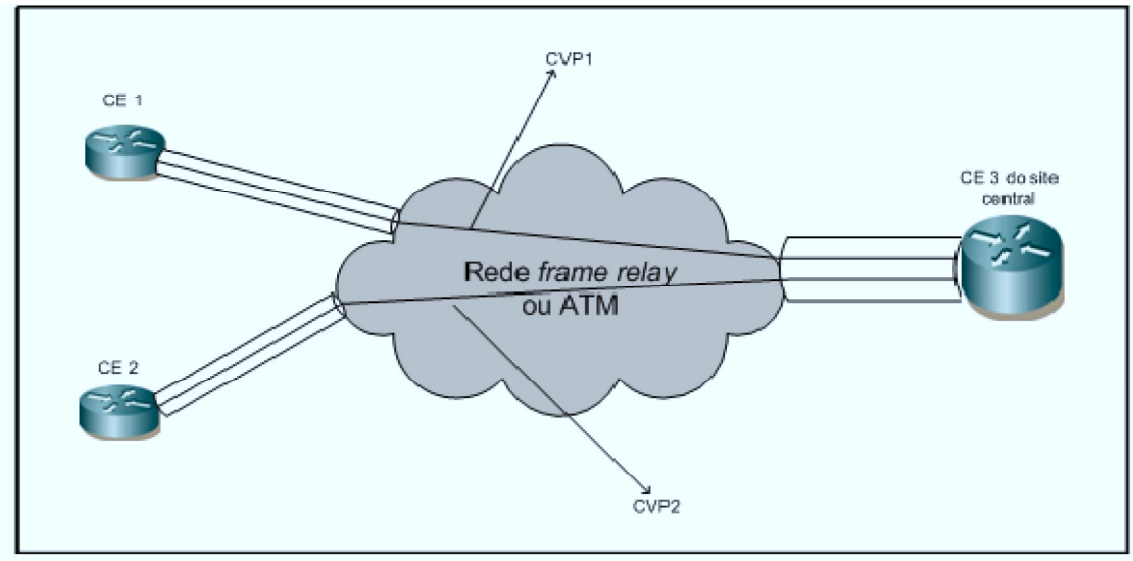

Figura 3.2 – VPN *frame relay*/ATM.

As soluções das VPNs baseadas em *core*/núcleo ATM/ *frame relay* eram as predominantes no mercado mundial. Porém, esse tipo de solução apresenta vários problemas que limitam o desenvolvimento em larga escala do serviço de VPN.

- ✓ Primeiro Problema

O primeiro problema surge da obrigatoriedade que o usuário tem em operar e administrar sua própria VPN. Nesse caso, é necessário um conhecimento sobre protocolos de roteamento IP, o que dificulta a implementação das VPNs, pois os usuários são orientados normalmente na administração de seus negócios, e não em VPNs. Como resultado, muitas empresas não utilizavam o serviço de VPN, pois requeriam um alto investimento na administração e operação de suas próprias VPNs [44].

Com o objetivo de resolver esses problemas, provedores de serviços começaram a oferecer o que é conhecido como "CPE gerenciável", em que o provedor instala, opera e gerencia as VPNs dos usuários. Portanto, enquanto se resolve um problema, cria-se outro, pois isso requer que o provedor de serviço opere uma VPN para cada usuário. Essa necessidade faz com que o provedor encontre dificuldade em oferecer serviços para um grande número de usuários.

- ✓ Segundo Problema

O segundo problema vem dos clientes que têm um grande número de *sites* e precisam conectividade completa com todos os *sites* (configuração *full mesh*) [44]. Nesse caso, para uma VPN com *n sites*, cada roteador precisará de (n-1) *sites* para trocar tráfego (*peering*). Esse problema é o mesmo encontrado na interconexão baseada no modelo *overlay*[13] de redes IP sobre ATM (*Asynchronous Transfer Mode*). Ou seja, em uma VPN *frame relay* de *n sites*, a quantidade necessária de conexões é a combinação de *n* dois a dois. A combinação de *n* dois a dois, à medida que *n* tende a grandes valores, aproxima-se de $n^2 - n$. Com esse resultado, é possível concluir que a complexidade de uma rede *frame relay* varia com n^2.

$$CVP = \frac{n!}{(n-2)!2!}$$

$$CVP = \frac{n(n-1)(n-2)!}{(n-2)!2!}$$

$$CVP = \frac{n(n-1)}{2}$$

$$n \to \infty$$

$$CVP \cong (\mathrm{n}^2)/2 \qquad (4)$$

Onde a variável "CVP" representa a quantidade de conexões para a formação de uma VPN *full mesh* de *n sites*.

[13] No modelo *overlay* cada roteador localizado nos sites da VPN estabelece conectividade ponto a ponto com pelo menos um outro roteador de outra localidade.

A figura 3.3 representa a quantidade de conexões necessárias para a formação de uma VPN usando o modelo tradicional e o novo modelo proposto, que é baseado em MPLS, apresentado nos próximos itens.

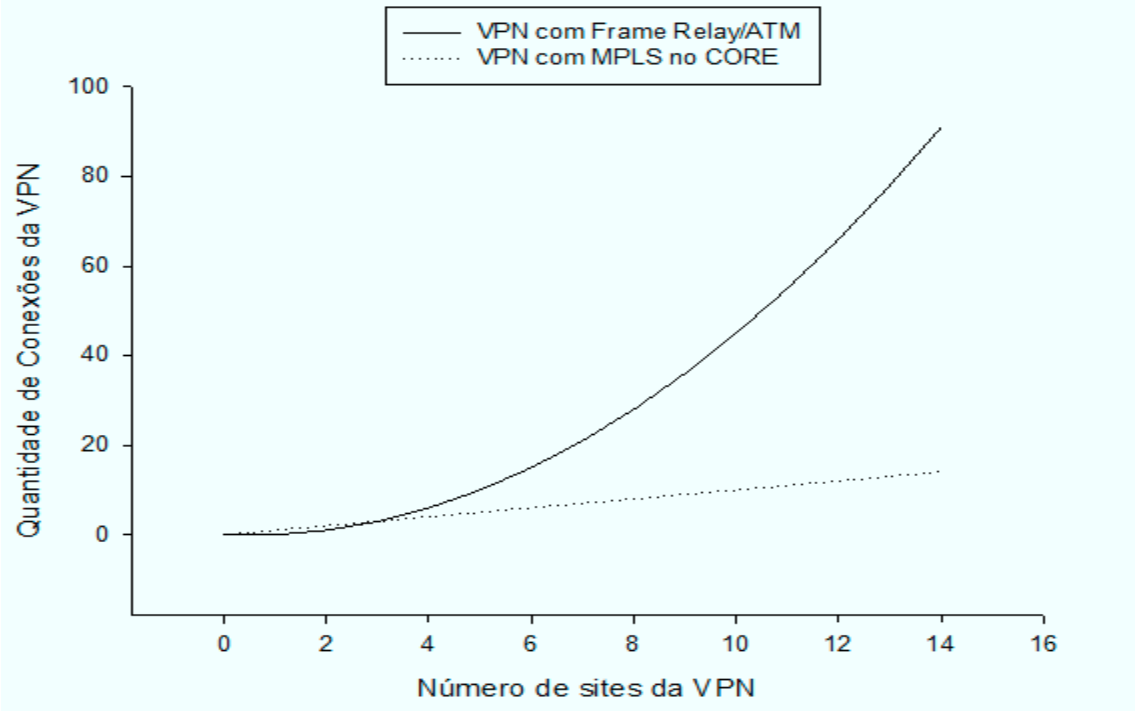

Figura 3.3 – Comparação das VPNs *frame relay* /ATM x VPN MPLS.

Esse problema aumenta ainda mais quando o usuário tem a necessidade de rodar a aplicação de VoIP entre seus *sites*. Isso requer várias configurações de CVP (Circuito Virtual Permanente) somente para VoIP. Por exemplo, uma empresa que tem 100 *sites* precisaria de 5.000 CVPs, de acordo com a equação 4, para oferecer comunicação completa de voz (VoIP).

- ✓ Terceiro Problema

O terceiro problema das VPNs *frame relay* é a quantidade de configurações necessárias para inclusão de um novo *site* em uma VPN existente. Para uma VPN que requer conectividade

completa (*full mesh*) entre todos os *sites*, cada um desses *sites* necessita de uma conexão e roteamento *site* a *site* com todos os outros da VPN [44].

- ✓ Quarto Problema

Os problemas anteriores estão diretamente relacionados com o *core* da rede, mas o quarto problema das VPN fixas vem do alto custo do acesso e da falta de capilaridade das redes fixas, o que torna os projetos às vezes inviáveis economicamente.

Uma nova proposta para as VPNs fixas com *core* ATM ou *frame relay* são as VPNs fixo – móveis [42] que integram os acessos banda larga sem fio com os acessos banda larga com fio. Com esse modelo, o provedor do serviço resolve as três primeiras deficiências implementando o protocolo MPLS no núcleo da rede para desenvolver roteadores que são capazes de atuar como VR (roteadores virtuais) ou VRF (*VPN Routing and Forwarding*). Nesse caso, um único roteador (PE) atua como uma coleção de vários roteadores virtuais ou VRF. Um roteador virtual tem o funcionamento equivalente a um roteador convencional, exceto pelo fato de que compartilha CPU (*Central Processing Unit)*, largura de banda e recursos de memória com outros roteadores virtuais. A VRF é uma tabela de encaminhamento e roteamento para cada VPN dentro dos roteadores de borda (PE) da rede do provedor do serviço. A implementação de MPLS no *core* da rede torna simples a implementação de VPNs fixo - móveis pelas operadoras. Agora, adicionar ou retirar um *site* de uma MVPN é mais simples com MPLS no *core*, pois requer somente uma configuração entre o PE e o CE. As VRFs garantem que as informações de roteamento de diferentes usuários das redes virtuais privadas móveis (MVPN) e fixas sejam separadas e isoladas. A figura 3.4 apresenta os conceitos de VRFs e encaminhamento dos *labels* (rótulos) no núcleo da rede.

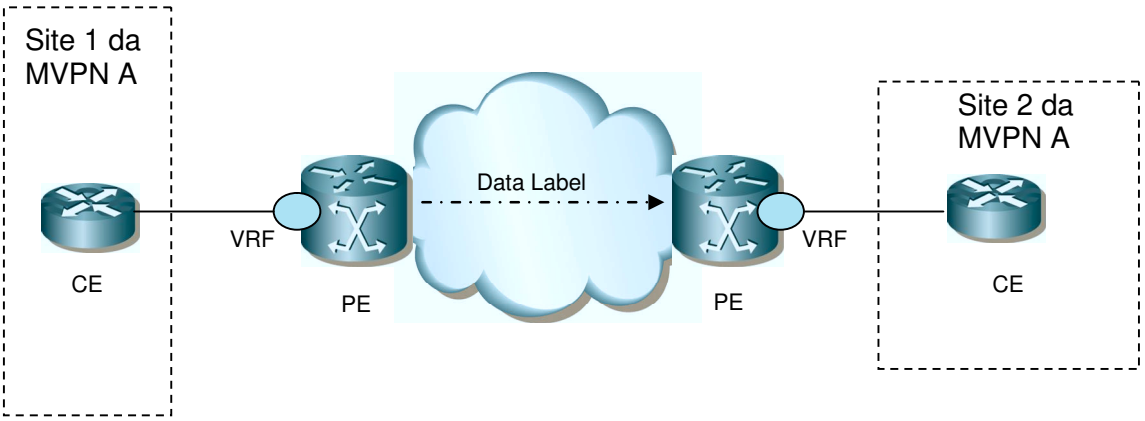

Figura 3.4 – Conceitos de VRF aplicada às MVPN MPLS.

Para adicionar um novo *site* à VPN A (por exemplo, um *site3*), o provedor necessita realizar somente uma configuração entre o CE do novo *site* com o PE da sua rede. Com isso, elimina-se toda a complexidade das redes *frame relay*, em que era necessário criar vários circuitos virtuais permanentes e configurar uma grande quantidade de DLCIs. Esse é o grande benefício para o provedor de serviço de VPN Móvel (MVPN) com MPLS implementado no núcleo (*core*) da rede. Existem outros benefícios da implementação de MPLS no núcleo da rede pelo operador para o fornecimento de serviços de MVPN, mas também temos duas desvantagens, uma para o usuário e outra para o provedor:

- ✓ O protocolo de roteamento entre o usuário (CE) e o provedor de serviço (PE) não é mais transparente a protocolo, ou seja, o usuário deverá configurar o protocolo de roteamento de acordo com a disponibilidade oferecida pela operadora.
- ✓ O equipamento de borda da rede do provedor (PE) deve ser um equipamento com grande capacidade de processamento, alta disponibilidade e segurança, pois ele será o responsável no suporte das múltiplas VRFs dos equipamentos dos usuários (CE) conectados a ele.

A primeira característica mencionada anteromente é uma desvantagem, pois o usuário terá que trocar rotas diretamente com o provedor; as alterações em sua rede deverão provocar alteração também no PE do provedor. A segunda desvantagem está relacionada diretamente

com os custos dos PEs. O provedor de serviço é responsável pela escalabilidade e pela convergência de roteamento de seus usuários que estão conectados aos PEs; esses PEs devem estar habilitados para transportar todas as rotas de seus usuários, bem como para atender a um futuro crescimento das VRFs. O capítulo 6 avalia a questão de escalabilidade do PE da rede MPLS e propõe algumas alternativas para minimizar esse problema.

Para resolver a quarta deficiência apresentada pelas VPNs fixas tradicionais, as operadoras têm investido em soluções com acesso banda larga, como GPRS, ADSL, UMTS, HSPDA e *metroethernet*.

As VPNs fixo - móveis com núcleo MPLS resolvem os problemas já apresentados pelas VPNs fixas tradicionais, mas acrescentam novos problemas que precisam ser investigados:

- ✓ Necessidade de garantir o isolamento das VRFs dos usuários das VPNs diferentes;
- ✓ Garantia da qualidade de serviço;
- ✓ Garantia da conectividade das VRFs de usuários da mesma MVPN;
- ✓ A escalabilidade do equipamento do roteador de borda (PE) para grandes números de VRFs diferentes;
- ✓ Erros de configuração das VPNs cometidos pela operadora.

A qualidade de serviço é avaliada no capítulo 4, enquanto o isolamento e conectividade das MVPNs são avaliados no capítulo 5, e escalabilidade do PE é avaliada no capítulo 6.

3.5 **Conceito de MVPN**

As MVPNs requerem o uso de tecnologias compartilhadas disponíveis pelo provedor dos serviços das VPNs fixo - móveis que permitem criar MVPNs (Redes Virtuais Privadas

Móveis) para conectar os equipamentos (CE) dos seus clientes ao equipamento mais próximo do provedor. Essas tecnologias são baseadas no encapsulamento dos pacotes de dados do usuário a partir do CE dentro de outros pacotes que trafegam sobre uma rede compartilhada. Essas tecnologias de encapsulamento devem permitir que seus usuários utilizem os mesmos planos de endereços sem ser conflitantes dentro do núcleo da rede. O termo *encapsulamento* ou *tunelamento*, no contexto de VPN fixo - móvel, é normalmente designado para transmissão de dados seguros sobre uma rede compartilhada, mas as novas propostas de encapsulamento sobre uma rede compartilhada, como a tecnologia MPLS, permitem, além da entrega de dados com segurança, o suporte à qualidade de serviço, a engenharia de tráfego e facilidades do controle de endereçamentos dos seus usuários. Antes de tratar em detalhe o tunelamento MPLS que é sugerido nesta tese para construir as VPNs fixo-móveis, são apresentados os principais protocolos de tunelamento utilizados pelas operadoras de telecomunicações no Brasil e no mundo para implementar suas VPNs fixo - móveis [45]. Ao final do capítulo, apresentam-se as possíveis arquiteturas convergentes – atual e do futuro.

3.5.1 PROTOCOLO DE TUNELAMENTO L2TP

O protocolo de tunelamento de nível 2 (L2TP) é definido na RFC2661 para prover um padrão de tunelamento PPP (Protocolo ponto a ponto) sobre IP. Esse protocolo de tunelamento pode ser transportado sobre qualquer célula, quadro ou rede de pacotes. Esse protocolo foi a primeira alternativa utilizada para formar VPN fixo - móvel pelas operadoras de Telecom no momento inicial.

Esse protocolo foi criado pela IETF (*Internet Engennering Task Force*) para resolver falhas presentes no PPTP e do L2F. Ele utiliza os mesmos conceitos do L2F e, assim como este, foi desenvolvido para transportar pacotes por diferentes meios, como X.25, *frame relay* e ATM. O L2TP também é capaz de tratar outros pacotes diferentes de IP, como o IPX e o *NetBEUI* (protocolo baseado na camada 2 do modelo OSI). O L2TP é, porém, um modelo de tunelamento "compulsório", ou seja, criado pelo provedor de acesso, não permitindo ao usuário qualquer

participação na formação do túnel (o tunelamento é iniciado pelo provedor de acesso). Nesse modelo, o usuário disca para o provedor de acesso à rede e, de acordo com o perfil configurado para o usuário e, ainda, em caso de autenticação positiva, um túnel L2TP é estabelecido dinamicamente para um ponto predeterminado, onde a conexão PPP é encerrada [46].

O L2TP define duas entidades de rede e com duas funções distintas que devem ser pares desse protocolo:

- ✓ O concentrador de acesso L2TP (LAC) é instalado no ponto de terminação da rede de acesso e deve estabelecer túneis L2TP adequados com os servidores da rede de acesso (LNSs),
- ✓ O LNS termina os túneis dos LACs, que também oferecem serviços de acesso à rede, tais como a autenticação do usuário e a atribuição de endereços.

Uma estação cliente estabelece uma conexão até o LAC, e o LAC estabelece um túnel até o LNS. O túnel L2TP estabelecido entre o LAC e o LNS é um túnel independente da tecnologia da rede de acesso e de transporte. A figura 3.5 apresenta o funcionamento básico do protocolo L2TP[45].

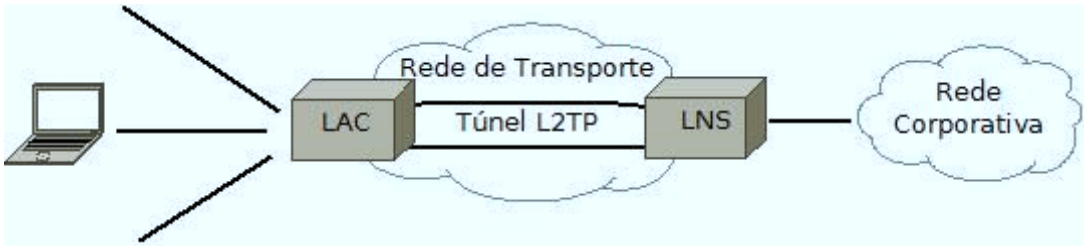

Figura 3.5 – Topologia para o protocolo L2TP

A figura 3.6 apresenta uma ilustração do funcionamento completo de um tunelamento de nível 2 (L2TP) para formação de uma VPN. O L2TP é suportado pelo Windows e Cisco e provê

autenticação entre os dois extremos do túnel. Ele não provê mecanismo de criptografia, mas pode ser combinado com o IPSec, que é abordado a seguir.

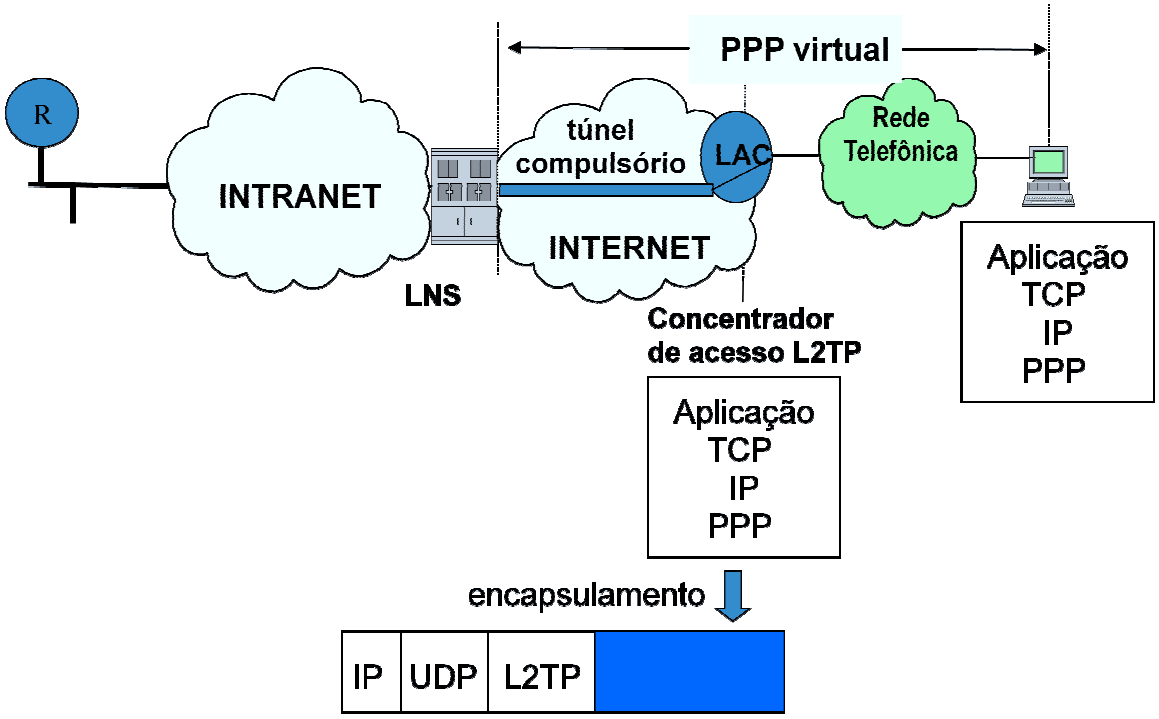

Figura 3.6 – Topologia fim a fim para o protocolo L2TP.

O L2TP não exige nenhum suporte no usuário, mas sim no provedor. O Servidor L2TP(LNS) passa a ter o controle total sobre a conexão do usuário.

3.5.2 TUNELAMENTO IPSEC

A arquitetura IPSec define as componentes necessárias para prover comunicação segura entre entidades pares do protocolo IP. O IPSec amplia o protocolo IP com dois cabeçalhos:

- ✓ O cabeçalho ESP (*Encapsulating Security Payload*), que é definido na RFC 2406;
- ✓ O AH (*Authentication Header*), que é definido na RFC 2402.

O ESP é usado para prover confidencialidade, integridade e autenticação das informações úteis. O AH é utilizado para oferecer integridade aos dados úteis e garantir a integridade dos campos não-alteráveis do cabeçalho IP. Ambos os cabeçalhos podem ser usados para encapsular um pacote IP em outro pacote IP (modo de túnel IPSec) ou apenas para encapsular os dados úteis de um pacote IP (IPSec modo de transporte). A figura 3.7 mostra

como o campo AH e o campo ESP podem ser utilizados para prover um modo de transporte IPSec. Também existe a possibilidade de uma combinação de ambos [45].

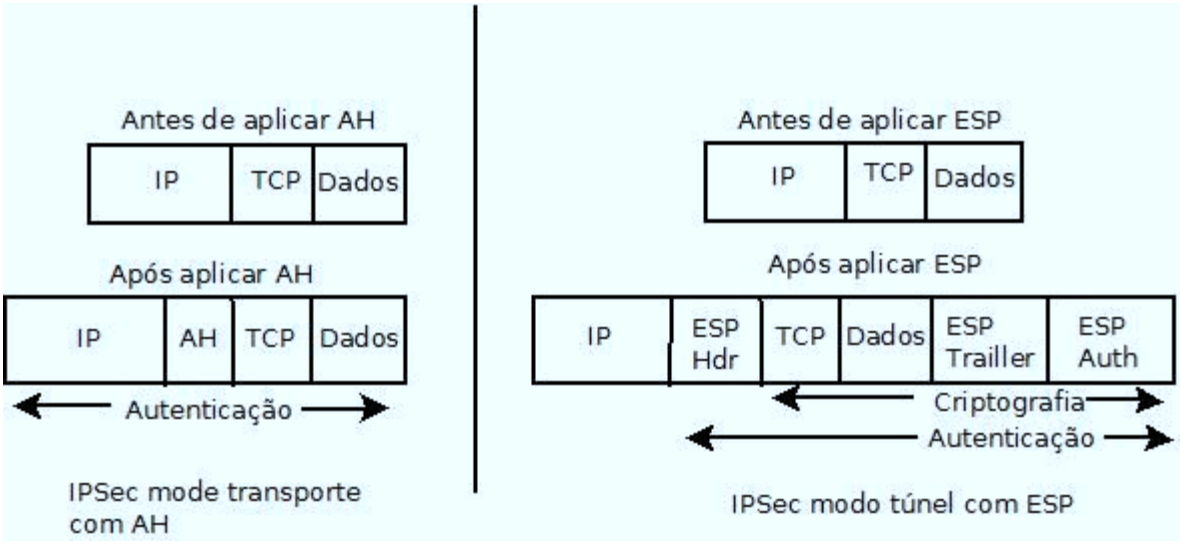

Figura 3.7 – Modo de túnel e transporte IPSec com ESP e AH, extraído de [45].

Nos pacotes criados no modo transporte, são adicionados cabeçalhos IPSec entre o cabeçalho IP original e os dados. Esse modo é muito utilizado para computadores em diferentes redes, comunicando-se diretamente entre si, que desejam proteger o seu tráfego IP por encapsulamento, autenticação ou ambos. Cada pacote IP é assinado digitalmente pelo *gateway*, que assegura a integridade do pacote, incluindo seu cabeçalho, autenticando cada pacote enviado, isto é, assegura que o emissor do pacote é e continua a ser aquele que ele diz ser. A figura 3.8 mostra o que foi apresentado acima.

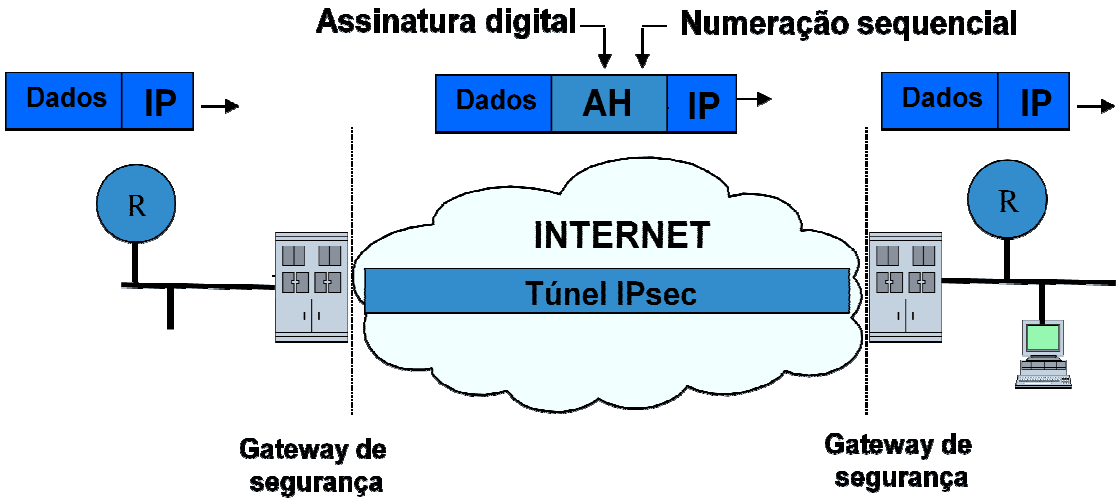

Figura 3.8 – Modo de transporte *IPSec* com AH.

O modo túnel é comumente utilizado na comunicação entre *gateways*, pois fornece maior segurança aos dados originais encriptados dentro do novo pacote. Cada pacote IP é criptografado pelo *gateway*, que assegura a confidencialidade do pacote. O *gateway* também pode assinar o pacote, garantindo a autenticação/integridade do conteúdo (mas não do cabeçalho IP). A figura 3.9 mostra esse funcionamento.

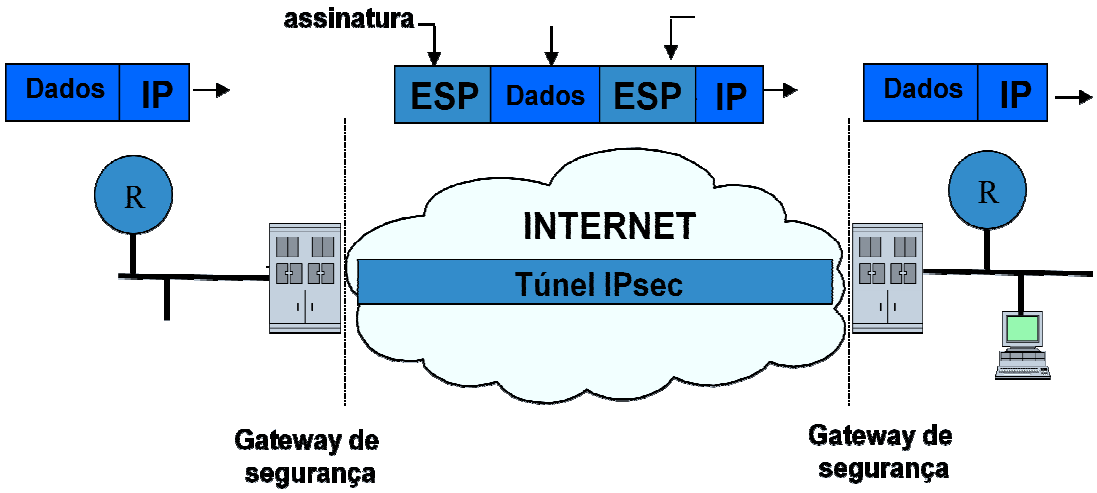

Figura 3.9 – Modo de túnel IPSec.

3.5.3 PROTOCOLO DE TUNELAMENTO GPRS

O GTP (protocolo de tunelamento GPRS) foi originalmente definido em [3GPP TS 29.060] e [GSM TS 09.60]. GTP é um protocolo utilizado para suportar as transmissões de dados que utilizam GPRS e UMTS como tecnologias de acesso das VPNs Móveis. Ou seja, todo tráfego de dados entre os equipamentos GGSN e SGSN é encapsulado através de túneis GTP. O protocolo GTP não possui suporte pela estação móvel; é um protocolo usado somente dentro do *backbone* e em interconexão com outras redes [45].

Há duas versões do protocolo GTP: a versão 0, descrita em [GSM TS 09.60], que é usada nos sistemas que trabalham com a tecnologia GSM; e a versão 1, descrita em [3GPP TS.29.060], que foi ampliada para sistemas que trabalham com as tecnologias GSM e UMTS como interface de rádio. O 3GPP decidiu criar uma nova versão do protocolo GTP não usando a versão anterior do GTP. O 3GPP queria criar um protocolo de tunelamento que separasse o plano do usuário (GTP-U) do plano de controle (GTP-C). O motivo para essa nova versão foi a necessidade dos sistemas 3G (UMTS) ao suporte de tunelamento feito a partir das estações móveis dos usuários. Outra grande diferença do GTPv1 do GTPv0 é o suporte a vários níveis de QoS por endereços IP definidos pela estação móvel. O GTPv0 podia ser transportado sobre TCP ou UDP. O TCP foi proposto no início para o transporte de dados confiáveis de usuários que trabalham com o protocolo X.25, mas, como esse protocolo deixou de ser utilizado pelo mercado de comunicação de dados, a partir de R'99 UMTS, o GTP passou a ser transportado somente sobre UDP. O número da porta UDP para o GTPv0 é 3386, para o GTPv1 é 2023 e para o GTP-U é 2052 [45].

O GTP-C inclui as seguintes mensagens [45]:

- ✓ Túnel de mensagens de gerenciamento que são usadas para detectar falhas e perda de conectividade;

- ✓ Mensagens de gerenciamento de sessão que são usadas para configurar túneis entre GGSNs e SGSNs. Essas mensagens também são utilizadas para atualizar parâmetros de qualidade de serviço (QoS);
- ✓ Gerenciamento da mobilidade usada para transferir a estação móvel nas condições de *handoff.*

O GTP-U é utilizado simplesmente para encapsular os pacotes de dados do usuário, mas também pode monitorar falhas no caminho da transmissão usando mensagens de gerenciamento de túneis. Elas são utilizadas entre SGSNs, entre GGSNs e SGSNs e entre as SGSN UMTS e as UMTS RNC [45].

3.5.4 IMPLEMENTANDO TÚNEIS ATRAVÉS DA TECNOLOGIA MPLS

MPLS (*Multiprotocol Label Switching*) é uma tecnologia desenvolvida no âmbito do IETF (*Internet Engineering Task Force*), inicialmente com o objetivo de tornar eficientes o encaminhamento e a comutação de fluxos de tráfegos através da rede. O MPLS é uma tecnologia utilizada no núcleo da rede e tem o objetivo de solucionar problemas atuais de redes de computadores, como velocidade, escalabilidade, gerenciamento de qualidade de serviço (QoS) e a necessidade de TE (engenharia de tráfego) [47].

A figura 3.10 apresenta o cabeçalho do protocolo MPLS. O cabeçalho é formado por 32 *bits*, sendo que esses 32 *bits* se dividem em quatro campos, que são: O *label* (rótulo), EXP, S e TTL.

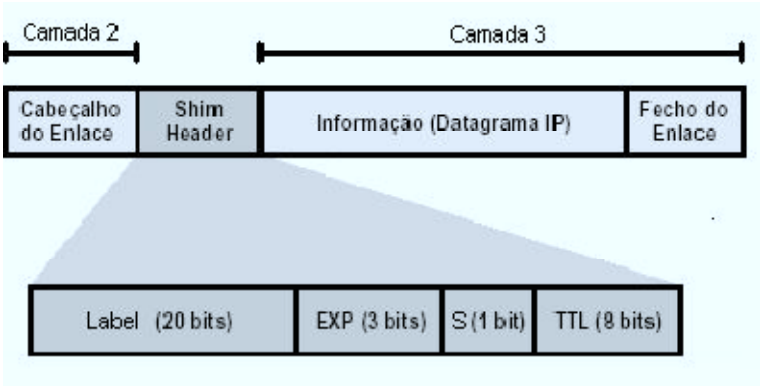

Figura 3.10 – Cabeçalho MPLS.

Todo pacote, ao entrar numa rede MPLS, recebe um *label.* O campo chamado *label* é formado por 20 *bits* e contém o número do *label* MPLS que é usado para comutar no núcleo da rede e é inserido no pacote entre os cabeçalhos dos níveis 2 e 3.

O campo EXP (*EXPerimental*) é reservado para uso experimental; é formado por 3 *bits* e é utilizado para implementar qualidade de serviço no núcleo da rede. Nos testes realizados no capítulo 4, foi utilizado esse campo para implementar a QoS para as devidas aplicações.

O campo S possui 1 *bit* de tamanho, e sua função é suportar uma hierarquia de pilhas de *label*. Finalmente, o campo TTL (*Time to live*) é decrementado a cada *hop* para evitar que *loops* de roteamento sejam criados na rede MPLS. O TTL conta por quantos roteadores o pacote passou. Caso o pacote viaje por mais de 255 roteadores, ele é descartado, sendo formado por 8 *bits*.

Uma rede que utiliza o protocolo MPLS consiste de equipamentos de comutação habilitados para MPLS. Esses equipamentos são denominados *roteadores de comutação por rótulos*, ou LSR (*Label Switch Router*). Um LSR localizado na periferia da rede MPLS denomina-se LSR de Borda (*Edge LSR - LERs*) ou PE (*Provider Edge*) na arquitetura das VPNs MPLS. Um LSR localizado no núcleo da rede denomina-se simplesmente de LSR núcleo (*core* LSR) ou P (*provider*) na arquitetura das VPNs MPLS. O conjunto dos LSRs forma uma rede MPLS [45,48].

Um túnel MPLS unidirecional, conhecido como *caminhos comutados por rótulos*, ou LSP (*Path Label Switching*), é construído entre os LERs com o objetivo de fazer com que o pacote que está entrando no primeiro LER de ingresso ou PE possa ser transportado de forma adequada para o LER de egresso ou PE. Quando os pacotes entram na rede, o roteador PE de ingresso determina a qual FEC os pacotes pertencem. Os pacotes que são encaminhados para o mesmo ponto de egresso da rede ao longo do mesmo caminho e que têm o mesmo tratamento são ditos pertencerem à mesma FEC. Pacotes que pertencem à mesma FEC serão encaminhados com o mesmo rótulo MPLS. Os roteadores que fazem parte do caminho do LSP têm sua decisão de encaminhamento baseada no cabeçalho do MPLS, que é de comprimento fixo. Portanto, MPLS não precisa armazenar as rotas IP para análise de roteamento. Essa característica é uma importante vantagem das redes MPLS sobre as redes tradicionais IP, pois estas analisam até o cabeçalho IP para executar o roteamento em cada roteador [45,48].

Em MPLS, caminhos comutados são estabelecidos segundo orientação por topologia e denominados *caminhos comutados por rótulos*, ou LSP (*Label Switch Path*). LSPs são estabelecidos por ação de protocolos do plano de controle ou por ação de gerência de rede. Os LSRs dispõem, em seu plano de controle, de um protocolo para o estabelecimento de LSPs. A rota estabelecida para um LSP pode ser determinada com o auxílio de protocolos de roteamento convencional, por exemplo, OSPF e BGP. Nesse caso, datagramas encaminhados através do LSP seguem a mesma rota dos datagramas encaminhados segundo o roteamento convencional. Um LSP pode ser estabelecido também segundo roteamento com restrições, por exemplo, roteamento na origem ou roteamento com qualidade de serviço. O roteamento com restrições, ou CR (*Constraint-based Routing*), é fundamental para a engenharia de tráfego. Os LSPs são unidirecionais, isto é, suportam encaminhamento de datagramas em um único sentido. Assim sendo, um LSP pode ser definido como uma sequência ordenada de LSRs, sendo que o primeiro LSR denomina-se LSR de ingresso (*Ingress LSR*) e o último, LSR de egresso (*Egress LSR*) [48]. A figura 3.11 apresenta os principais elementos da arquitetura MPLS.

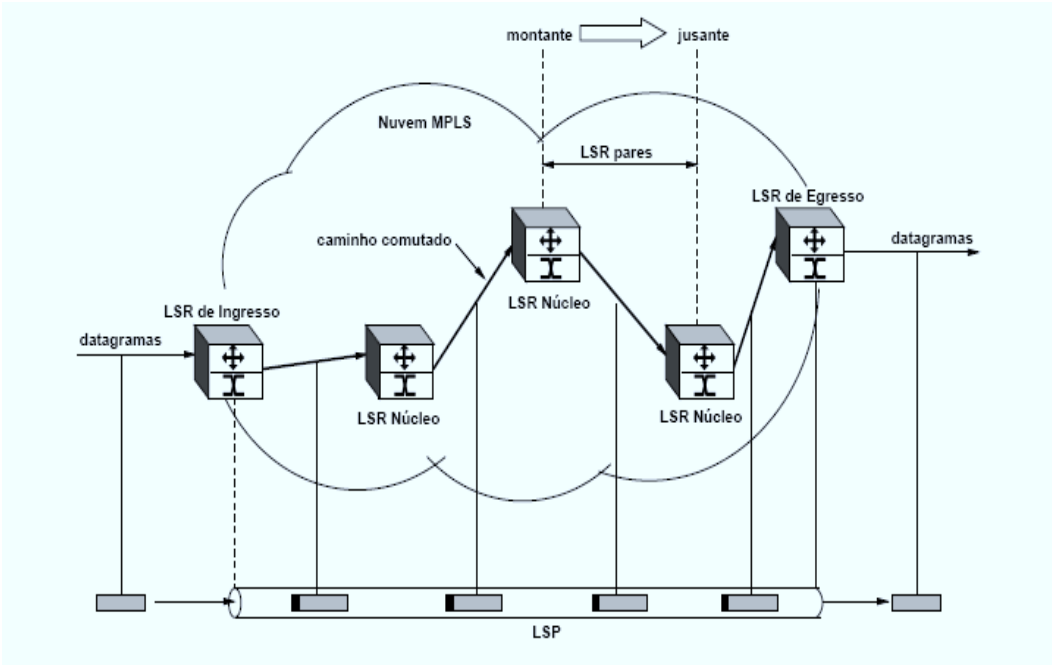

Figura 3.11 – Elementos da arquitetura MPLS

Uma das propriedades fundamentais da arquitetura das redes MPLS é que elas podem ser utilizadas para vários modelos de túneis de tráfego através do núcleo da rede.

O tunelamento é uma ferramenta fundamental para construir novos serviços sobre uma rede MPLS. Os túneis MPLS têm as seguintes características [43]:

- ✓ O tráfego pode ser roteado explicitamente, dependendo do protocolo de sinalização utilizado.
- ✓ Existe proteção contra a falsificação de dados (*spoofing*). O único local onde os dados podem ser injetados dentro dos túneis MPLS é em seu cabeçalho, mas dados podem ser inseridos em um túnel MPLS, desde que tenha conectividade com a rede MPLS.
- ✓ O comprimento do cabeçalho para encapsular os dados é relativamente baixo, sendo de 4 *bytes* por cabeçalho MPLS.

O MPLS (*Multi-protocol Label Switching*) tem se mostrado como a solução que melhor atende aos requisitos de implementação de túneis para as VPNs, com alta qualidade de serviço e segurança. Porém, os túneis implementados nas VPNs MPLS que são baseados em *labels* apresentam algumas diferenças em relação aos túneis convencionais, já apresentados nas seções anteriores. Nos tunelamentos convencionais, os pacotes são transportados a partir do primeiro roteador de entrada da rede IP até o último roteador de saída, ou seja, o tunelamento depende somente do endereço fonte e do endereço destino [45]. A figura 3.12 apresenta o tunelamento convencional.

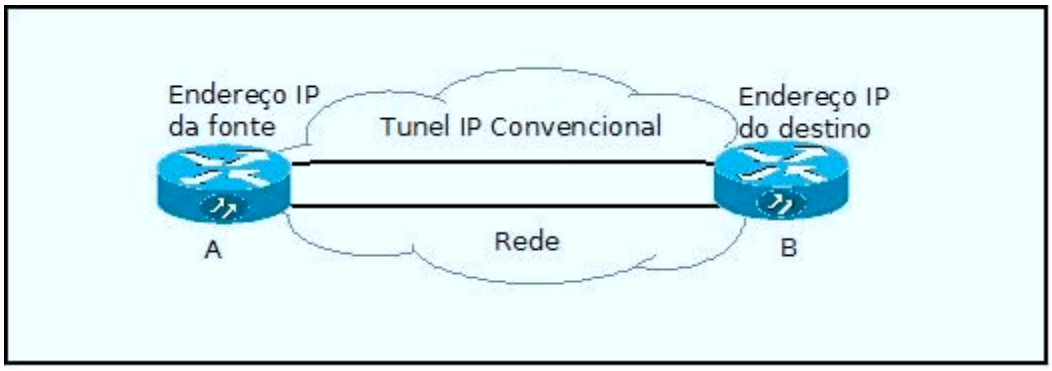

Figura 3.12 – Túnel IP convencional, extraído de [45].

No tunelamento baseado em *label* usando a tecnologia MPLS, os pacotes são transportados através de caminho comutado de *labels* (LSPs) do ponto de ingresso na rede até o ponto de egresso, mas, entre o ponto de ingresso e egresso, os pacotes são comutados com base em *labels* em cada roteador, ou seja, a comutação é feita conforme a tabela de rótulos armazenados em cada roteador, e não no endereço IP [45]. A figura 3.13 apresenta a topologia básica para a formação do LSP.

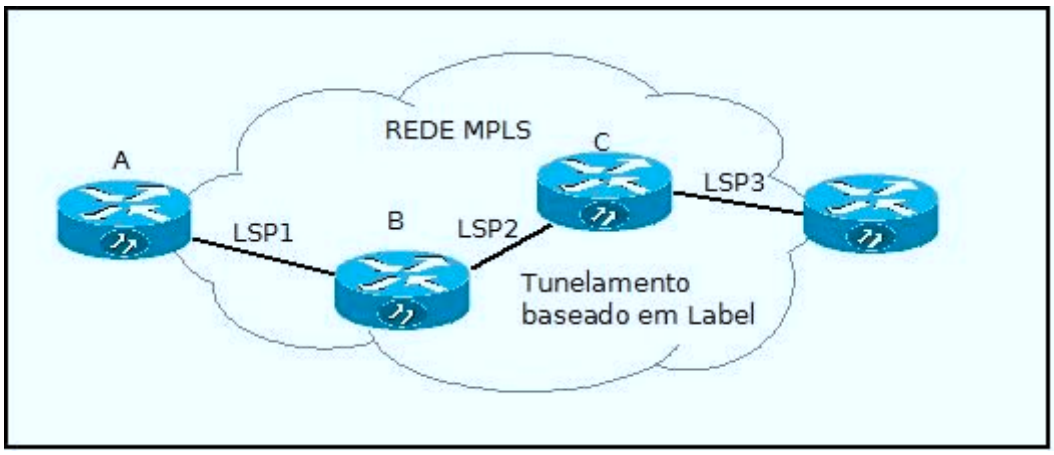

Figura 3.13 – Tunelamento baseado em LSP.

Cada LSP está associado a uma classe equivalente de encaminhamento, ou FEC (*Forwarding Equivalent Class*). Uma FEC determina quais *datagramas* serão encaminhados pelo LSP. O LSR de ingresso, ao receber um *datagrama*, verifica se este pertence a uma FEC. Em caso afirmativo, o *datagrama* é encaminhado através do LSP associado à FEC. Caso contrário, o *datagrama* recebe o encaminhamento IP padrão (*hop-by-hop*). Uma FEC é composta de Elementos FEC (*FEC Elements*). Elementos FEC podem ser entendidos como condições que determinam se um dado *datagrama* pertence ou não à FEC [48].

3.5.4.1 VPNs MPLS – RFC 4364

As VPNs MPLS (Redes virtuais privadas MPLS) na RFC - 4364, antiga RFC 2574, são definidas como 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 *sites* que compartilham informações de roteamento e cuja conectividade é controlada por um conjunto de regras. A RFC - 4364 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. A figura 3.14 apresenta os componentes principais da arquitetura das VPNs MPLS, que são CE, PE, P e VRF [49].

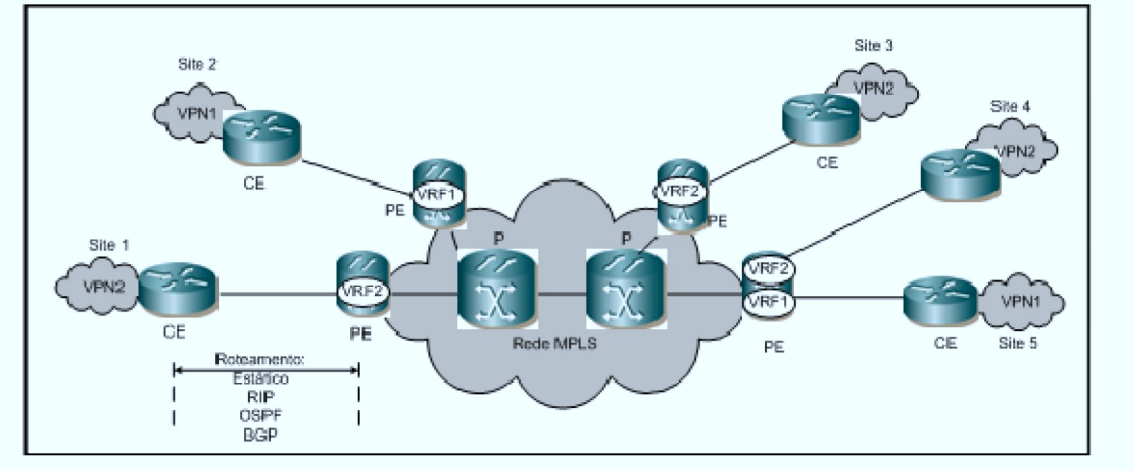

Figura 3.14 – Componentes básicos da arquitetura das VPNs MPLS.

- ✓ CE (*Customer Edge*) – o CE é o equipamento que fica no ambiente do usuário. Um 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 a VRF do roteador PE e aprende as rotas remotas da VPN [22,49].
- ✓ PE (*Provider Edge*) – o PE é o equipamento que fica no ambiente do provedor do serviço e borda da rede. Os roteadores PEs trocam informação de roteamento com os roteadores CEs através de roteamento estático, RIPv2, OSPF ou BGP. Esse modelo de VPN realça a escalabilidade porque elimina a necessidade de os roteadores PEs manterem rotas VPNs com todos os PEs do provedor de serviço. Cada roteador PE mantém uma VRF para cada *site* conectado diretamente. Observa-se que múltiplas interfaces do roteador PE podem ser associadas com uma única VRF se todos os *sites* 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. Quando se utiliza 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 [22,49].

- ✓ P(*Provider*) – o roteador P é instalado no ambiente das operadoras e conecta os PEs entre si. Um Roteador 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. 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 [22].
- ✓ VRF (*Virtual Routing Forwarding*) – um conceito chave na arquitetura VPN MPLS é o elemento chamado de *tabela de Encaminhamento e Roteamento dos roteadores PE*. 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 *sites* 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 daqueles *sites* serão roteados e encaminhados com base unicamente na informação encontrada na VRF correspondente [22].

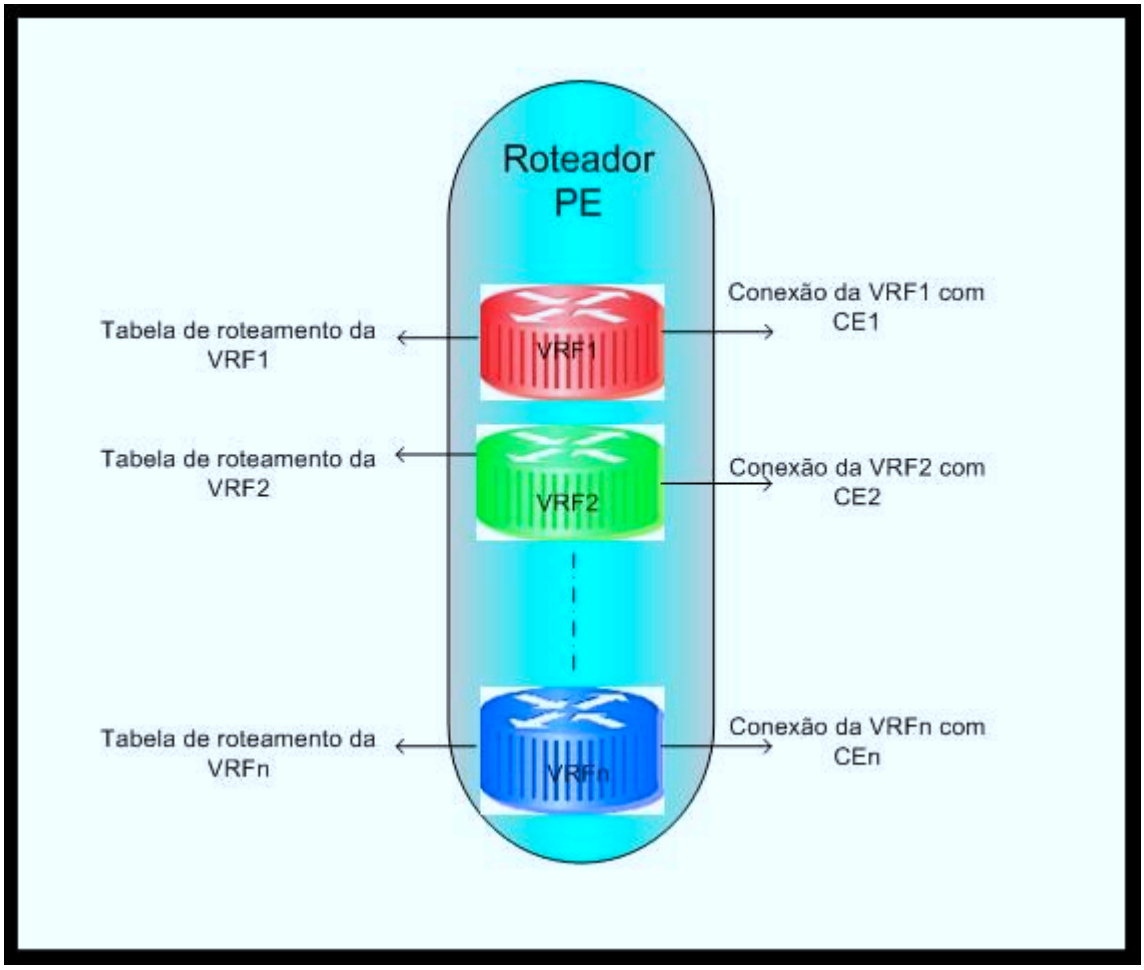

Figura 3.15 – PE com várias VRFs.

A conexão entre os roteadores CE e PE pode ser uma conexão remota através de *frame relay*, ADSL, *WiMax*, satélite, 3G ou *ethernet*. Os protocolos de roteamento entre os CEs e PEs podem ser: Rotas estáticas, RIP, OSPF ou BGP [47].

Quando o roteador PE recebe a rota atualizada, é criada uma tabela de roteamento (VRF) e as informações de alcançabilidade são encaminhadas para todas as VRFs da mesma VPN conectadas ao PE.

Os roteadores PEs estabelecem sessões para trocar rotas das VPNs dos clientes. O tráfego da rede do provedor passa através do LSP (*Label Switched Path*) preestabelecido através dos

protocolos de sinalização LDP (*Label Distribution Protocol*). O roteador PE adiciona dois rótulos como prefixos para cada pacote do tráfego IP do cliente.

3.5.4.2 Modelo operacional das VPNs MPLS

Dois fluxos fundamentais de tráfegos ocorrem em uma VPN MPLS: o fluxo de controle, que é responsável pela distribuição de rotas das VPNs e estabelecimento do LSP (*Label Switched Path*), e o fluxo de dados, que é utilizado pelos usuários para encaminharem seus dados gerados por suas aplicações. A figura 3.16 apresenta uma topologia de quatro *sites* que pertencem a duas VPNs MPLS em que o provedor de serviço oferece soluções de VPN MPLS. Dois *sites* estão conectados à VPN1 e dois *sites* à VPN2 [49,50].

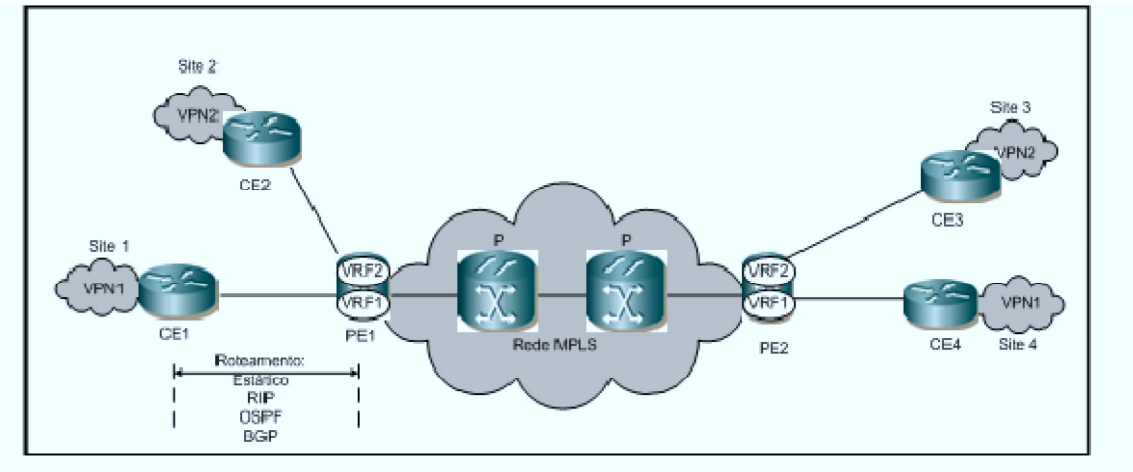

Figura 3.16 – VRFs x VPNs.

- ✓ Fluxo de Controle

Em uma VPN MPLS, o fluxo de controle é dividido em dois subfluxos. O primeiro é responsável pela troca de informação de roteamento entre os roteadores CE – PE e entre os roteadores PEs dentro do núcleo da operadora. O segundo subfluxo é responsável pelo estabelecimento dos LSPs entre os roteadores PEs do provedor de serviço [49,50].

Na figura 3.16, é configurada uma VRF1 nos PEs para os *sites* 1 e 4 que pertencem à VPN1, enquanto que, para os *sites* 2 e 3, é configurada a VRF2 para a VPN2. O CE1 anuncia as

suas rotas para o PE1, que as habilita na VRF1. O PE1 anuncia as rotas da VRF1 para a VRF1 do PE2, que as transmite para o CE4 do *site* 4. As VPNs MPLS permitem que a VPN1 e a VPN2 utilizem o mesmo endereço através do uso de rotas distintas (RD). Quando o PE2 recebe as rotas do PE1, a decisão de instalar as rotas dentro da VRF1 e não na VRF2 é baseada nos atributos RD e RT [49,50].

O primeiro passo no projeto de um serviço de VPN baseado na arquitetura MPLS é definir e configurar a VRF. Nesse caso, significa configurar uma VRF para as VPN1 e VPN2. Cada roteador PE deve ser conectado ao roteador CE do usuário que deseja receber rotas de uma VPN específica. As configurações das VRFs devem existir em todos os roteadores PEs [49].

Os PEs suportam múltiplos VRFs dentro de um único sistema. Isso permite ao provedor de serviço configurar múltiplos roteadores separados dentro de um único equipamento.

O CE conectado no roteador PE vê uma interface de roteador. O 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 de que há múltipla instância de roteadores [50].

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. O protocolo de roteamento do PE provê todo o suporte para BGP-4, OSPF, rotas estáticas e RIP. Esses protocolos podem ser habilitados ou desabilitados para cada instância de um roteador no PE. Esses protocolos são tratados em detalhe [51,52].

Entre os roteadores PEs, o BGP é o protocolo usado para distribuir rotas das VPNs entre os roteadores PEs. Antes de apresentar como as rotas são distribuídas entre os PEs, deve-se analisar como as VPNs BGP/MPLS facilitam o roteamento original dos usuários. Foi mencionado que as rotas das VPN1 e VPN2 são independentes e que elas são isoladas de outras VPNs. Além disso, as rotas das VPNs são separadas pelo provedor de serviço no núcleo, sendo possível mais de uma VPN usar o mesmo plano de endereço. 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 [51,52].

Sempre foi o objetivo das operadoras de telecomunicações oferecer serviços de VPNs e fazer com que estas sejam tratadas de forma única no núcleo da rede, e as VPNs MPLS atendem a esse objetivo de possibilitar um endereço único para cada VPN. As rotas dos *sites* devem ser tratadas em diferentes caminhos, dependendo da VPN a que elas pertencem. O multiprotocolo BGP extensão permite ao BGP transportar rotas de múltiplas "famílias de endereços". Uma VPN-IPv4 é composta de 12 *bytes*, iniciando com 8 *bytes*, que correspondem ao RD, e terminando com 4 *bytes*, que se referem ao endereçamento IPv4 [51,52].

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, bem como a semântica do campo administrador [51].

O principal requisito da arquitetura VPN MPLS é que todas as rotas das VPNs sejam únicas dentro do núcleo e que não se restrinja o uso de endereçamento privado do usuário. O BGP seleciona um único caminho entre todos os possíveis, descrevendo uma rota para um dado destino. Entretanto, o BGP, por si só, não pode operar corretamente se as VPNs utilizam os mesmos planos de endereços. Isso significa que é necessário utilizar o mecanismo de identificador de rotas (RD). A figura 3.17 apresenta o campo RD e o IP convencional.

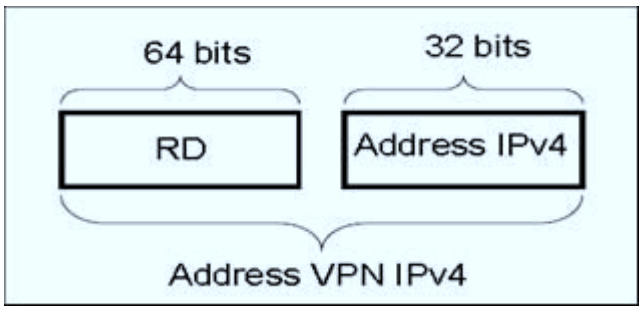

Figura 3.17 – VRFs x VPNs.

Esse mecanismo consiste de uma sequência de 64 *bits* na frente do endereço IPv4, que está contido no MP-BGP. Essa sequência de *bits* é conhecida como RD e é diferente para cada VPN, sendo única dentro do núcleo MPLS/VPN.

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

Pelo mecanismo do RD, é possível aos *sites* das VPNs o uso dos mesmos endereços privados. Isso não resolve o problema de múltiplos *sites* dentro da mesma VPN usarem o mesmo endereçamento entre suas redes.

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

as VRFs que constituem as VPNs usam os mesmos identificadores de rotas, independentemente do *site* específico da VPN à qual a VRF pertence [51,52].

Quando certas topologias (Ex: *extranet*) são criadas, pode ser necessário estender os identificadores de rotas por VRF 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 ASN (número do sistema autônomo), que é atribuído pela IANA (*Internet Assigned Numbers Authority*) 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, poderá ser único por VPN [50]. A tabela 3.2 mostra os valores para cada VPN da figura 3.16.

Tabela 3.2 – Valores de RD para as VPNs.

VPN	ASN	Valor único	RD
VPN1	200	20	200:20
VPN2	200	30	200:30

O parâmetro RD é utilizado para identificar a VPN dentro do núcleo da rede MPLS, mas é necessário conhecer como as VRFs das VPNs importam e exportam as rotas de suas VRFs. Para realizar isso, as VRFs trabalham com o atributo RT (*Rotas targets*). O atributo RT identifica uma coleção de VRFs pela qual um roteador PE distribui as rotas. Um roteador PE usa esse atributo para restringir a importação e exportação de rotas para as VRFs [49].

Cada VRF tem uma política de configuração para importação e exportação das rotas. O roteamento que é distribuído para outros PEs é marcado como atributo RT de exportação. As rotas recebidas pelo outro roteador PE são checadas, de modo a verificar se seu atributo RT de importação aceita inserir a rota na 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*" [51,52].

Os roteadores PEs estabelecem sessões 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 por Rótulo) preestabelecido através dos protocolos de sinalização LDP. Para usar o MPLS para o encaminhamento do tráfego da VPN por meio do núcleo do provedor, Um LSP deve ser estabelecido entre o roteador PE que aprende a rota e o roteador PE que anuncia a rota [49,50]. A figura 3.18 ilustra esse conceito.

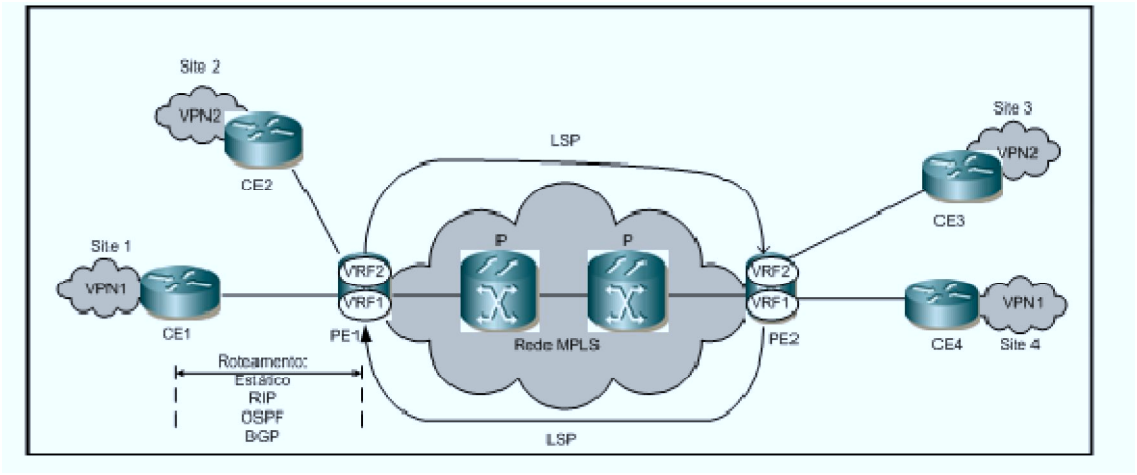

Figura 3.18 – Formação de LSPs entre PEs.

- ✓ Fluxos de dados

Será considerado para análise do fluxo de dados que o *site* 4 deseja encaminhar pacotes de informações para o *site* 1 da VPN 1. Os pacotes são encaminhados do *site* 4 através do CE4 em direção ao PE2. Quando chegam ao PE2, eles são inseridos na VRF1 que possuem as informações de encaminhamentos, ou seja, a VRF1 informará a rota com a inserção de um *label*, o *next hop* (próximo salto) e a interface de saída do PE2 para a formação do LSP entre PE2 e PE1.

Conforme o tráfego dos usuários, são encaminhados 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. 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 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 é encaminhado para o PE1 [48,49].

Quando o PE1 recebe o pacote, ele retira o rótulo, criando o pacote nativo IPv4. Finalmente, o PE1 encaminha o pacote IPv4 nativo para CE1, que encaminha os pacotes para o *site* 1 [49,50]. A figura 3.19 mostra esse fluxo de dados.

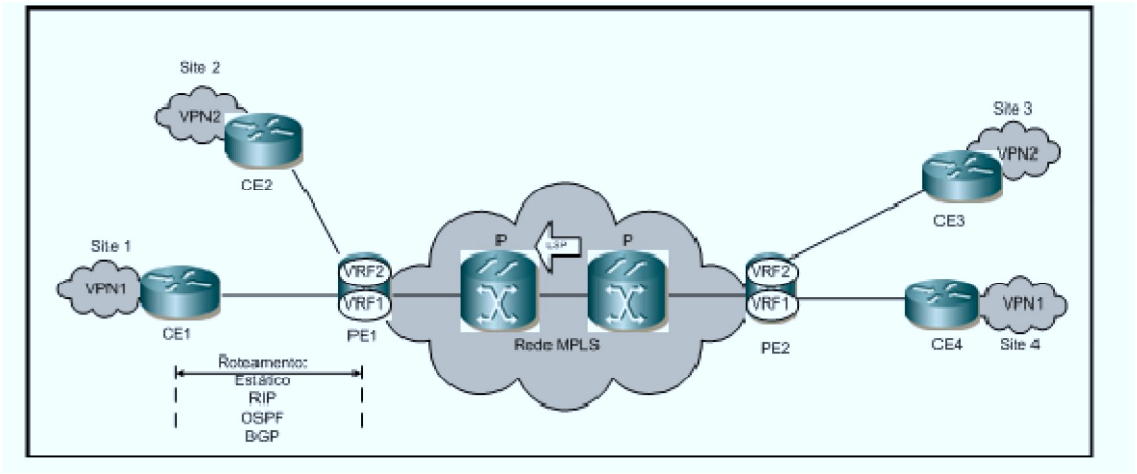

Figura 3.19 – Fluxo de dados do *site* 4 para o *site* 1.

3.6 Integração/convergência da rede móvel com a fixa

A necessidade de interoperabilidade entre os acessos das redes móveis e os acessos da rede fixa é chamada de convergência ou integração de fixo – móvel.

A integração entre as redes fixa e móvel consiste na utilização de acessos móveis basicamente para a formação de redes virtuais privadas móveis (MVPN). Essa integração entre a rede fixa e móvel também é chamada de convergência de redes. Na perspectiva do usuário, a

convergência consiste na possibilidade de conectar seu celular ou outro equipamento sem fio a qualquer outro *site* fixo ou móvel em alta velocidade e com baixo custo.

A topologia apresentada na figura 3.20 mostra uma arquitetura geral de rede para o serviço de integração entre as redes fixa e móvel. Nessa figura, são apresentadas as possíveis formas de realizar a convergências através de diversas tecnologias. Algumas operadoras iniciaram a convergência de suas redes integrando as redes tradicionais como *internet, frame relay e* DSL com a rede móvel. No momento em que as operadoras implementarem o MPLS em suas estruturas de núcleo e *backhaul*, a convergência será natural, pois o MPLS permite todas as formas de acesso fixo e móvel, mas, como o protocolo MPLS ainda está em processo de implementação no núcleo e no *backhaul* das operadoras móveis, a figura 3.20 mostra como as operadoras podem oferecer a convergência para seus clientes utilizando as tecnologias convencionais.

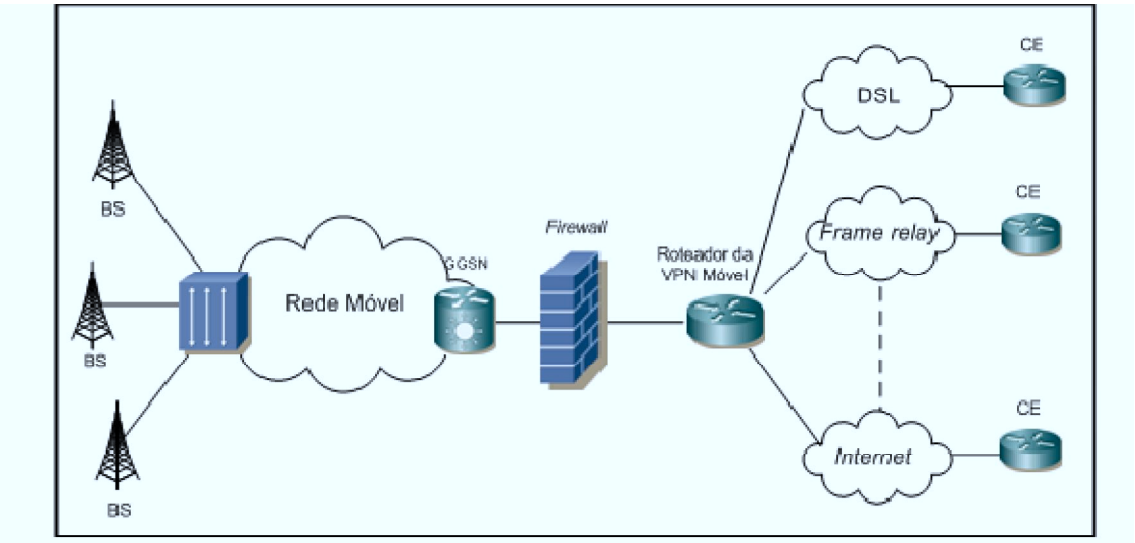

Figura 3.20 – Topologias para convergências.

A convergência das redes permite disponibilizar os serviços de VPN fixo-móvel através das seguintes modalidades:

- ✓ VPN fixo-móvel integrada com VPN Fixa ADSL (*layer* 2 VPN): nessa modalidade, o serviço VPN fixo-móvel complementa o serviço de VPN existente na rede fixa,

oferecendo acesso móvel ao serviço ADSL. A VPN móvel poderá ser integrada à VPN ADSL.

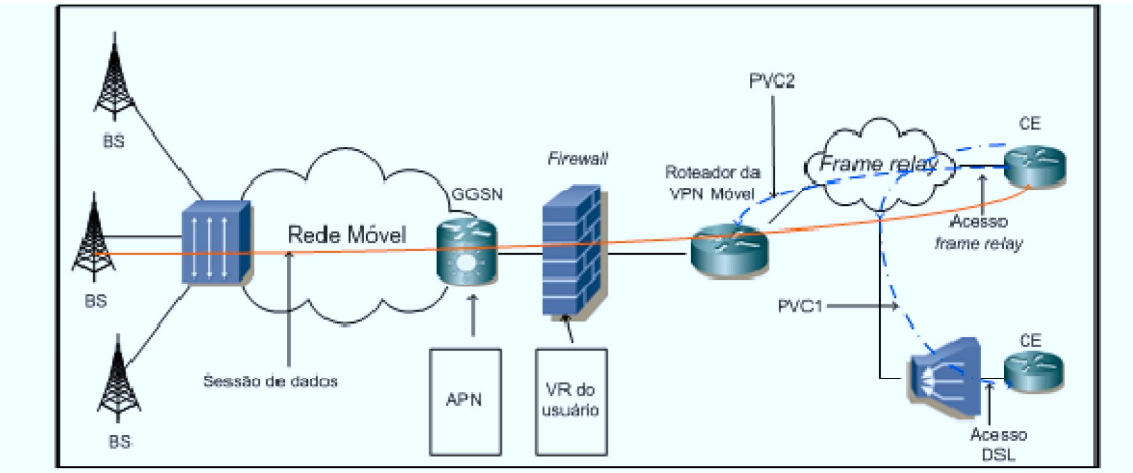

Figura 3.21 – Topologias para convergências fixo-móveis com acesso DSL.

- ✓ VPN fixo-móvel integrada com produto *frame relay*: nessa modalidade, o serviço VPN fixo-móvel complementa o serviço *frame relay* existente na rede fixa, oferecendo acesso móvel ao serviço *frame relay*.

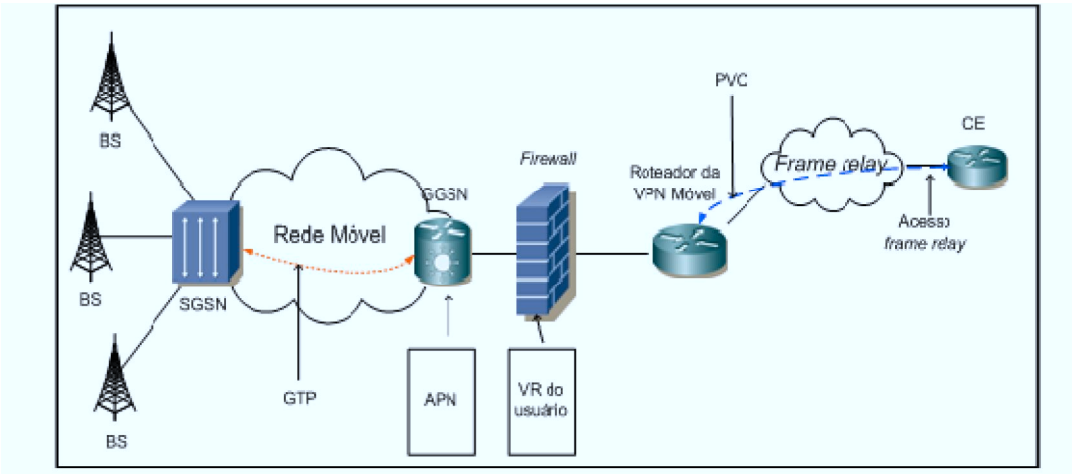

Figura 3.22 – Topologias para convergências fixo-móveis com acesso *frame relay*.

- ✓ VPN fixo-móvel com L2TP: nessa modalidade, a conectividade com o *site* principal da VPN é realizada através da *internet* pública, com uso de túnel L2TP entre o *gateway* da rede móvel (GGSN) e o equipamento terminador de túneis L2TP (LNS) localizado no ambiente do usuário.

Nessa modalidade, o cliente corporativo possui um acesso à *internet* e deseja oferecer acesso fixo-móvel à sua *intranet* corporativa. O elemento GGSN da rede GPRS, em função da APN (*Access Point Name*) definida para o cliente do serviço VPN fixo-móvel, abre um túnel L2TP até o VPN *gateway* (terminador de túneis L2TP) localizado no *site* do cliente, estabelecendo, assim, a conectividade entre o terminal fixo-móvel e a *intranet* corporativa, conforme a figura 3.23 abaixo.

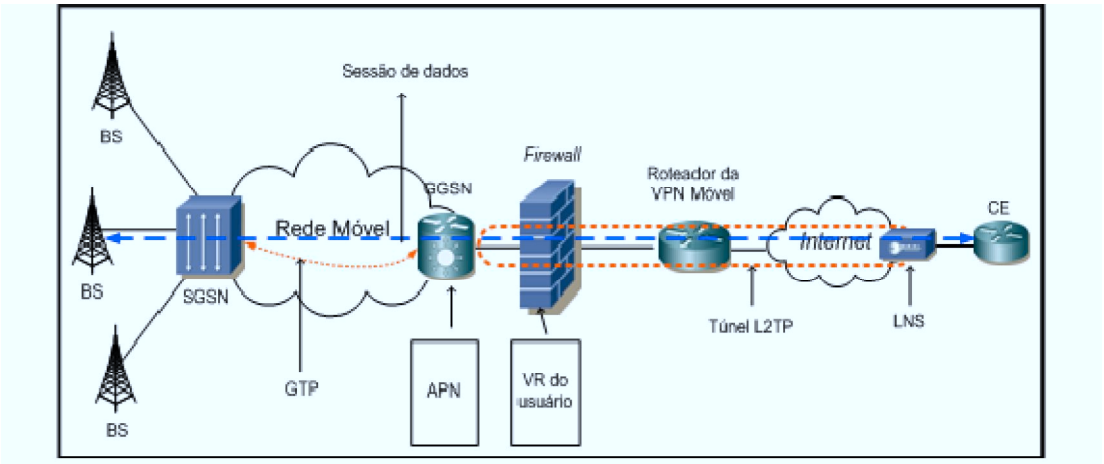

Figura 3.23 – Topologias para convergências fixo-móveis através de L2TP.

- ✓ VPN fixo-móvel com IPSec: nessa modalidade, a conectividade com o *site* principal da VPN é realizada através da *internet* pública, com uso de túnel IPSec entre o *firewall* da rede móvel ou a partir do elemento GGSN e o do equipamento terminador de túneis IPSec localizado no ambiente do usuário.

Nessa modalidade, o cliente corporativo possui um acesso à *internet* e deseja oferecer acesso fixo-móvel seguro à sua *intranet* corporativa. O *firewall* da rede GPRS abre um túnel IPSec até o VPN *gateway* (terminador de túneis IPSec) localizado no *site* do cliente, estabelecendo, assim, a conectividade segura entre o terminal fixo-móvel e a *intranet* corporativa, conforme figura 3.24.

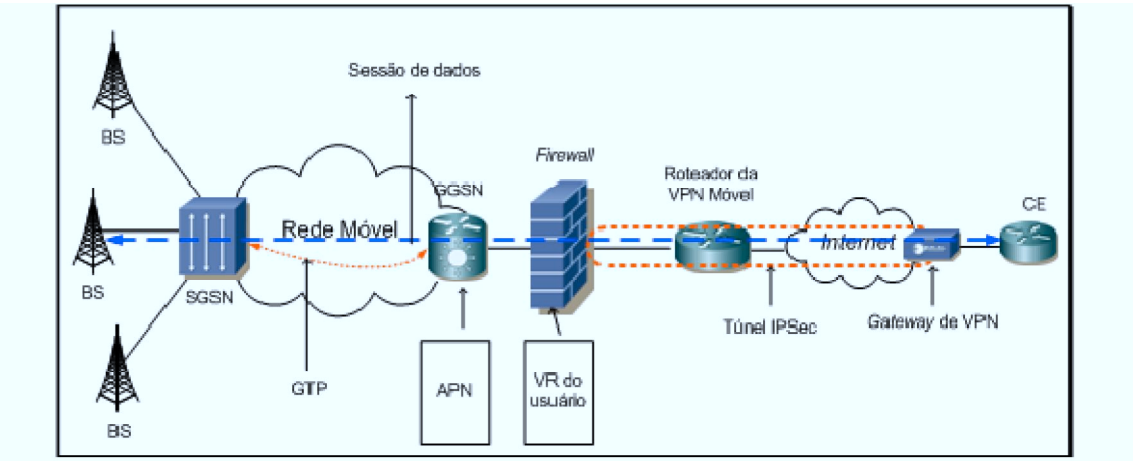

Figura 3.24 – Topologias para convergências fixo-móveis com IPSec

A seguir, é apresentada uma proposta que pode ser considerada a ideal para operadora que ainda não tem o MPLS na rede móvel, mas tem o MPLS já implementado na rede fixa. Nessa proposta, a conectividade entre a rede móvel GGSN e PE é realizada através de um PVC. As tecnologias tradicionais, como *frame relay*, DSL e TDM, passam a ser unicamente acesso da rede MPLS.

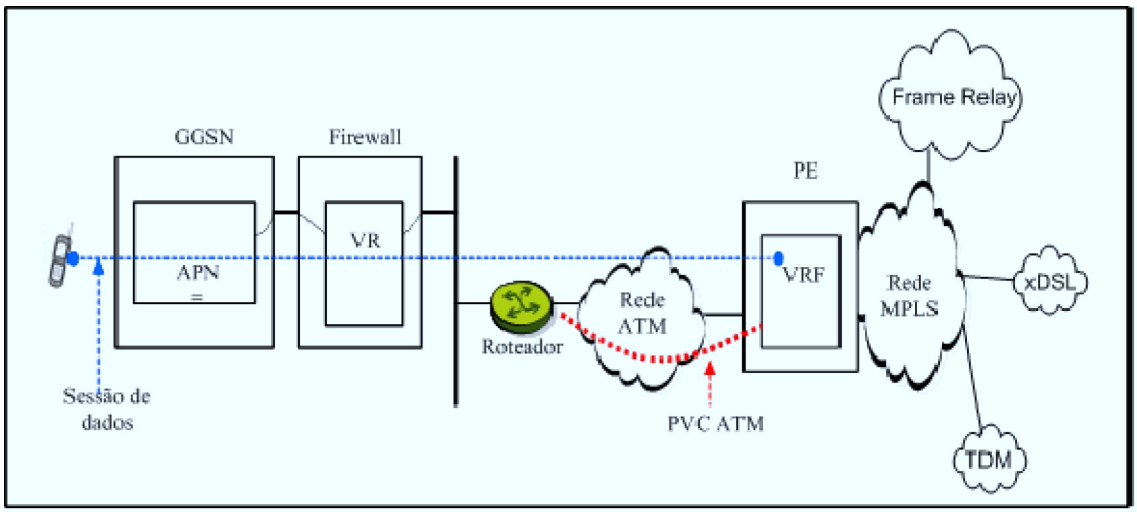

Figura 3.25 – Topologias para convergências fixo-móveis com MPLS.

Este capítulo mostra claramente a diminuição da complexidade de uma rede baseada em MPLS em relação às redes baseadas nas tecnologias convencionais, como *frame relay* e ATM. Mostrou-se matematicamente que a complexidade, que nas redes convencionais varia com n^2,

onde *n* é o número de *sites*, passa a variar somente com *n* em uma rede MPLS. Essa diminuição de complexidade e outras facilidades que foram apresentadas levam à conclusão e ao consenso de que as redes MPLS são as mais indicadas para formar o núcleo das redes de nova geração convergentes. No entanto, o preço dessa simplificação é o compartilhamento das estruturas de redes, o que está diretamente relacionado com a qualidade de serviço, a segurança e a escalabilidade do equipamento de borda da rede (PE). A qualidade de serviço será avaliada no próximo capítulo; a segurança, avaliada no capítulo 5; e a escalabilidade, que é avaliada no capítulo 6.

Capítulo 4

Qualidade de Serviço (QoS) em VPN Fixo-Móvel

A arquitetura das redes convergentes fixa e móvel proposta pode ser dividida em dois principais componentes: o núcleo de rede e a rede de acesso. O núcleo de rede é responsável por prover o transporte dos diversos tráfegos e conectar as VPNs fixo-móvel e móveis. A rede de acesso pode ser com fio (*ADSL, frame relay, ATM e metroethernet*) ou sem fio (*GPRS, UMTS, WiMax e 3G*). Neste capítulo, avalia-se a qualidade de serviço das VPNs no núcleo da rede. Para isso, foi montado um ambiente de teste real que é formado de quatro etapas para as aplicações de dados, dados com prioridades, voz e multimídia. Após a avaliação do desempenho das classes de serviços, foi feito o mapeamento destas em classes correspondentes ao *WiMax* e 3G para oferecer qualidade de serviço para as VPNs fixo-móveis.

A infraestrutura de comunicações móveis e fixas está evoluindo para oferecer suporte a aplicações de usuários das VPNs fixo-móveis e móveis com soluções fim a fim baseadas no protocolo IP que sejam capazes de prover QoS (*Quality of Service)* aos seus usuários, com

conectividade e segurança. Mais velocidades estão sendo proporcionadas às VPNs fixo-móveis , com aumento da largura de banda no enlace de rádio e a utilização de comutação por pacotes no núcleo de rede. No entanto, somente o aumento de velocidade no acesso e a implementação do IP no núcleo da rede não são suficientes para oferecer a qualidade de serviço, a segurança e a conectividade às VPNs fixo-móveis. Este capítulo aborda a qualidade de serviço (QoS) no núcleo da rede para atender aos requisitos das aplicações e aspectos de relacionados à QoS. A segurança, a conectividade e a escalabilidade das VPNs são avaliadas nos próximos capítulos.

4.1 **Introdução**

Existem percepções diferentes do provedor e dos usuários em relação aos níveis de serviços de comunicações. Os três principais componentes que são utilizados para caracterizar os níveis de serviços de comunicações são: CoS (*Class of Service*), QoS (*Quality of Service*) e SLA (*Service Level Agreement)*. O primeiro passo do provedor é identificar as necessidades de serviço dos usuários e mapeá-las em parâmetros de acordo com a classe de serviço oferecida pela operadora. Esses parâmetros devem ser facilmente entendidos, percebidos e medidos, tanto pelo usuário quanto pela operadora. Do ponto de vista do usuário, a qualidade de serviço é mais óbvia. Para garantir que o provedor entregue ao usuário o que ele contratou, é feito um contrato de SLA (*Service Level Agreement*) entre o usuário e o provedor [1].

As classes de serviços são agrupamentos de negócios baseados em aplicativos comuns com requisitos similares. Elas são utilizadas pelas operadoras para diferenciar os serviços oferecidos aos seus clientes, com o preço em função da classe adquirida. Por exemplo, considere-se uma operadora que ofereça o serviço com quatro classes de serviços, designadas de dados, voz, vídeo e dados com prioridades. Um determinado usuário que tem a necessidade de trafegar VoIP e TVIP deverá contratar a classe de voz e vídeo, enquanto um outro usuário, que tenha necessidade diferente e queira trafegar somente dados, deverá contratar somente a classe de dados.

Em uma rede baseada em MPLS, diferentes classes de serviços orientadas aos negócios dos clientes podem ser estabelecidas. Diferentemente da *internet*, onde todo o tráfego é tratado de forma igual, uma rede baseada em MPLS oferece a possibilidade de criar várias classes de serviços, conforme a aplicação e negócio dos usuários. Com o advento de tráfego sensível ao *delay* e *jitter*, por exemplo, algumas aplicações, como VoIP, TVIP e outras, precisam ser tratadas e priorizadas de forma diferente das convencionais. Para a análise feita neste capítulo, são consideradas quatro classes:

- ✓ A classe 4 será o tráfego com mais alto nível de prioridade: o tráfego de voz;
- ✓ A classe 3 será o tráfego com o segundo nível de prioridade: o tráfego de multimídia;
- ✓ A classe 2 será o tráfego com o terceiro nível de prioridade: o tráfego de dados prioritários;
- ✓ A classe 1 será o tráfego sem nenhuma priorização: o tráfego de dados comum.

A qualidade de serviço é definida na recomendação E.800 do ITU-T (*International Telecommunications Union – Telecommunication Standardization Sector*) como sendo o efeito conjunto do desempenho do serviço que determina o grau de satisfação do usuário de um serviço [53].

A QoS (*Quality of Service*) pode ser definida com parâmetros específicos necessários para uma determinada aplicação do usuário. Esses parâmetros de serviço podem ser definidos em termos de largura de banda, latência, *jitter* e perdas de pacotes, de forma que a aplicação possa obter uma melhor qualidade ao longo da rede. Assim, podemos definir QoS como: "a capacidade da rede de fornecer tratamento especial a certos tipos de tráfego de forma previsível" [54].

A aplicação IPTV, por exemplo, é muito sensível a esses parâmetros de QoS: largura de banda, *jitter*, latência e perdas de pacotes.

A qualidade de serviço é fundamental para as novas redes convergentes, que precisam tratar de forma diferenciada os aplicativos de voz, vídeo e dados de missão crítica. Isso porque cada um desses aplicativos tem requisitos diferentes de QoS para o seu perfeito desempenho e a rede convergente tem que fornecer a devida QoS, de acordo com a aplicação. A seguir, são definidas e apresentadas as principais características dos quatro principais parâmetros de QoS que determinam o bom desempenho dos aplicativos.

4.2 Principais parâmetros de qualidade de serviço

- ✓ *Jitter*

O *jitter* é importante para as aplicações executadas em rede cuja operação adequada depende, de alguma forma, da garantia de que as informações (pacotes IPTV) sejam processadas em períodos de tempo bem definidos. Do ponto de vista de uma rede IP, o *jitter* pode ser entendido como a variação no tempo e na sequência de entrega das informações (ex.: pacotes) devido à variação na latência (atrasos) da rede. Uma possibilidade para eliminá-lo é *buferizar* alguns pacotes antes de produzir o som, para que pacotes atrasados possam chegar, gerando assim mais atraso [54].

De acordo com a RFC 3550, o *jitter* é definido como uma estimativa da variação estatística do tempo entre chegadas dos pacotes RTP (*Real-time transport protocol*) [55].

As principais causas do *jitter* são as variações dos tempos de fila nos roteadores, ou seja, variação no atraso no enfileiramento, devido às mudanças dinâmicas do tráfego de rede. Algumas aplicações interativas, tais como voz e vídeo, são incapazes de lidar com o *jitter*, pois este resulta em *trancos* ou em uma qualidade irregular para o som ou a imagem. A solução está no provisionamento adequado pela rede de mecanismo, tais como os mecanismos de priorização, que condicione o *jitter* a níveis adequados [53].

- ✓ Latência e atraso

A latência e o atraso são parâmetros importantes para a qualidade de serviço das aplicações IPTV. Ambos os termos podem ser utilizados na especificação de QoS, embora o termo "latência" seja convencionalmente mais utilizado para equipamentos, e o termo "atraso" seja mais utilizado quando se consideram as transmissões de dados (ex.: atrasos de transmissão, atrasos de propagação) [54].

De maneira geral, a latência da rede pode ser entendida como o somatório dos atrasos impostos pela rede e pelos equipamentos utilizados na comunicação. Do ponto de vista da aplicação, a latência (atrasos) resulta em um tempo de resposta (tempo de entrega da informação, ou pacotes) para a aplicação. Os principais fatores que influenciam a latência de uma rede são os seguintes: (1) atraso de propagação (*Propagation delay*), (2) velocidade de transmissão e (3) processamento nos equipamentos [54].

O atraso de propagação corresponde ao tempo necessário para a propagação do sinal elétrico ou propagação do sinal óptico no meio utilizado (fibras ópticas, satélite, coaxial e outros). Esse é um parâmetro imutável, e o gerente de rede não tem nenhuma influência sobre ele. O intervalo de tempo em que um pacote sai da origem e chega ao seu destino, quando elevado, pode causar perda de sincronização. Para uma boa qualidade em comunicação de voz, a latência deve possuir um valor menor que 150 ms [54].

- ✓ Perda de Pacotes

As perdas de pacotes são normalmente ocasionadas por três fatores: o enlace físico, que pode não permitir a transmissão dos pacotes; congestionamento; e ruído, que pode corromper os pacotes. Os enlaces físicos dificilmente oferecem problemas, pois possuem um elevado índice de disponibilidade. Portanto, a causa principal das perdas de pacotes em rede é o congestionamento. Essa situação é avaliada nos testes realizados e analisados.

A perda de pacotes tem influência na qualidade de serviço e pode causar o estouro de *buffers* em roteadores e *switchs*. Por utilizar protocolos UDP e RTP, esses pacotes não podem ser retransmitidos, e a própria retransmissão não é tolerável em aplicações IPTV [54].

A figura 4.1 apresenta a relação entre o atraso e a perda de pacotes com a qualidade de serviço na rede. Quatro níveis de qualidade de serviços são definidos: *Toll quality* (desejável), *Good quality* (boa), *Potentially useful quality* (útil) e *Poor quality* (inaceitável) [53].

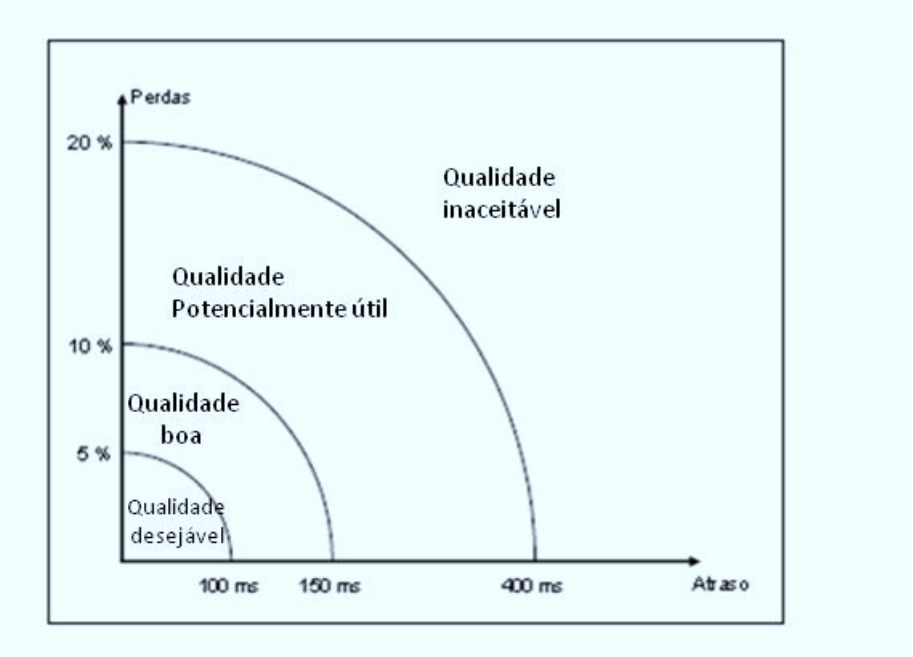

Figura 4.1: Atraso x perdas de pacotes x qualidade

- ✓ Vazão

A vazão (banda) é o parâmetro mais básico de QoS e é necessária para a operação adequada de qualquer aplicação. Em termos práticos, as aplicações geram vazões que devem ser atendidas pela rede [54].

Abaixo, seguem os valores recomendados do WT-126 da latência, atraso, *jitter* e perdas de pacotes para o tráfego IPTV que uma rede de comunicação deve atender fim a fim [54].

Tabela 4.1: Valores recomendados para compactação MPEG-2 em qualidade SDTV, extraída de [54].

Fluxo de Vídeo (Mbit/s)	Latência (ms)	*Jitter (ms)*	Perdas de Pacotes (%)	Taxa média de perda de pacote IP
3.0	<200	<50	1	1,9E-9
3.75	<200	<50	1	1,6E-06
5.0	<200	<50	1	1,2E-06

Tabela 4.2: Valores recomendados para compactação MPEG-4 em qualidade SDTV, extraída de [54].

Fluxo de Vídeo (Mbit/s)	Latência (ms)	*Jitter (ms)*	Perdas de Pacotes (%)	Taxa média de perda de pacote IP
1.75	<200	<50	1	3,3E-06
2.0	<200	<50	1	2,9E-06
2.5	<200	<50	1	2,3E-06
3.0	<200	<50	1	1,9E-06

Tabela 4.3: Valores recomendados para compactação MPEG-2 em qualidade HDTV, extraída de [54].

Fluxo de Vídeo (Mbit/s)	Latência (ms)	*Jitter (ms)*	Perdas de Pacotes (%)	Taxa média de perda de pacote IP
8	<200	<50	1	9,14E-08
10	<200	<50	1	7,31E-08
12	<200	<50	1	6,09-08

Outra aplicação muito utilizada é VoIP (*Voice over IP*). A tabela abaixo apresenta os requisitos de QoS necessários, conforme recomendação G.114 da ITU-T.

Tabela 4.4: QoS para a aplicação de VoIP.

Atraso	Qualidade
Atraso <150 ms	Alta Qualidade
150 ms <Atraso<400 ms	Aceitável
Atraso>400 ms	Qualidade inaceitável

Para Voz Sobre IP (VoIP), também são recomendados os seguintes parâmetros de QoS:

- ✓ Perdas de pacotes menores que 1%;
- ✓ Média do *jitter* menor que 30 ms.

4.3 A evolução das arquiteturas de qualidade de serviço em redes IP

A entrega de serviços IP por parte das operadoras de telecomunicações com qualidade de serviço deu-se basicamente a partir do ano de 1995 em alguns países e em 2002 no Brasil. Em função da explosão dos serviços baseados em IP, as indústrias de telecomunicações começaram a desenvolver seus produtos com foco nesse protocolo. A necessidade de oferecer serviços como VoIP (*Voice over IP*), dados e negócios de missão crítica com classes diferenciadas de serviços fez surgir duas principais propostas para oferecer QoS em redes IP: *IntServ* e *DiffServ*. Apresentam-se, a seguir, alguns conceitos da arquitetura *IntServ*, para depois enfatizar a arquitetura *DiffServ*, que trabalhará em conjunto com o MPLS para a formação de túneis IP MPLS das respectivas VPNs [47].

4.3.1 SERVIÇOS INTEGRADOS (*INTSERV*)

As redes IP públicas, tradicionalmente, sempre ofereceram um único serviço, baseado no modelo de melhor esforço (*Best Effort-BE*), que apresenta um desempenho aceitável para aplicações como correio eletrônico e transferências de arquivos. Com o desenvolvimento de novas aplicações, como VoIP, videoconferência e telemedicina, que são aplicações em tempo

real, o IETF trabalhou no desenvolvimento do *IntServ* para tornar viável uma rede de serviços integrados [56].

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*[47].

4.3.2 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, onde o tráfego e a quantidade de fluxos são maiores devido à agregação dos tráfegos originários de vários roteadores de borda. A figura 4.2 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 [47].

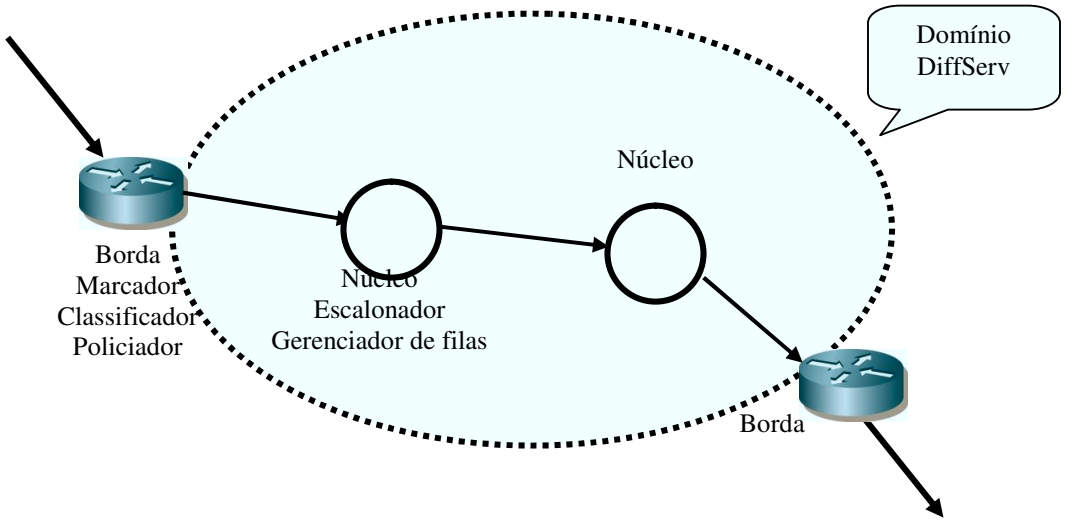

Figura 4.2: Arquitetura *DiffServ*.

4.3.2.1 Serviços diferenciados (*DiffServ)*

A diferenciação de serviços (*DiffServ*) [57] 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.

A identificação da classe de serviço é feita pela marcação no campo DS – Serviço 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 [47].

4.3.3 QUALIDADE DE SERVIÇO E MPLS

Qualidade de serviço em uma rede MPLS pode ser obtida de duas formas. A primeira é usando o campo EXP da pilha de rótulos (*labels*), que permite a diferenciação de até oito classes de tráfego dentro de um único LSP. A segunda opção é baseada simplesmente na associação de um PHB em outro rótulo (*label)* MPLS. Este modelo é conhecido como L-LSP (*label-only-inferred packet-scheduling class* LSP) [58].

O modelo da qualidade de serviço (QoS) adotado para análise do desempenho da VPN MPLS no núcleo da rede está baseado em *DiffServ*/MPLS. A classificação e marcação de DSCP dos pacotes IP será realizada pelos CEs, e a marcação de EXP dos pacotes MPLS será feita pelos PEs envolvidos. A partir dessas marcações, serão realizadas as classificações em filas em cada roteador da rede. Cada fila está associada a uma classe de serviço (CoS), onde serão definidas características de prioridade para transmissão (WFQ, WRR), tamanho da fila (*buffer*) e políticas de controle de fluxo (WRED). A tabela 4.1, abaixo, apresenta os mecanismos da QoS para cada um dos elementos de rede MPLS envolvidos na análise de desempenho utilizada.

Tabela 4.5 – Classificação e Marcação no CE e PE

	CE	PE
Classificação	TCP/UDP/IP	DSCP (IP)
Marcação	ACL → DSCP	DSCP → EXP
Fila de Voz	LLQ	LLQ
Fila de Serviços	CWFQ	CWFQ

É importante observar que voz foi classificada em filas de baixa latência do tipo LLQ, enquanto aplicações como dados podem ser classificadas em filas do tipo CWFQ.

4.3.4 TESTE DA QUALIDADE DE SERVIÇO DO NÚCLEO DA REDE

O objetivo do teste é avaliar os principais parâmetros de QoS no núcleo da rede para quatro classes de serviços (CoS) quando o PE for submetido a várias condições, de acordo com as etapas abaixo, na presença de uma demanda de tráfego superior à banda nominal disponível no acesso. A topologia para o teste está apresentada na figura 4.3.

4.3.5 TOPOLOGIA PARA O TESTE

A topologia apresentada abaixo é um ambiente real que foi desenvolvido para avaliar a qualidade de serviço no núcleo da rede de nova geração. Será gerado tráfego entre 256 kbits/s a 512 kbit/s (*site* A) no acesso de 512 kbits/s e medido no receptor (*site* B). Ponto de congestionamento a ser considerado será a conexão entre o roteador de borda (PE) do provedor da rede MPLS e o acesso de 256 Kbps. O computador gerador de tráfego está em uma localidade situada a uma distância euclidiana de 1.600 km do receptor. A medição dos parâmetros de qualidade de serviço (QoS) será feita através da utilização do programa Iperf para os parâmetros de *Jitter*, Vazão e Perda de Pacotes. O atraso (*delay*) será medido através do comando *ping* na fila classe de serviço de voz. O atraso a ser considerado será o tempo que o pacote leva para ir ao receptor e retornar ao transmissor, normalmente chamado de RTT.

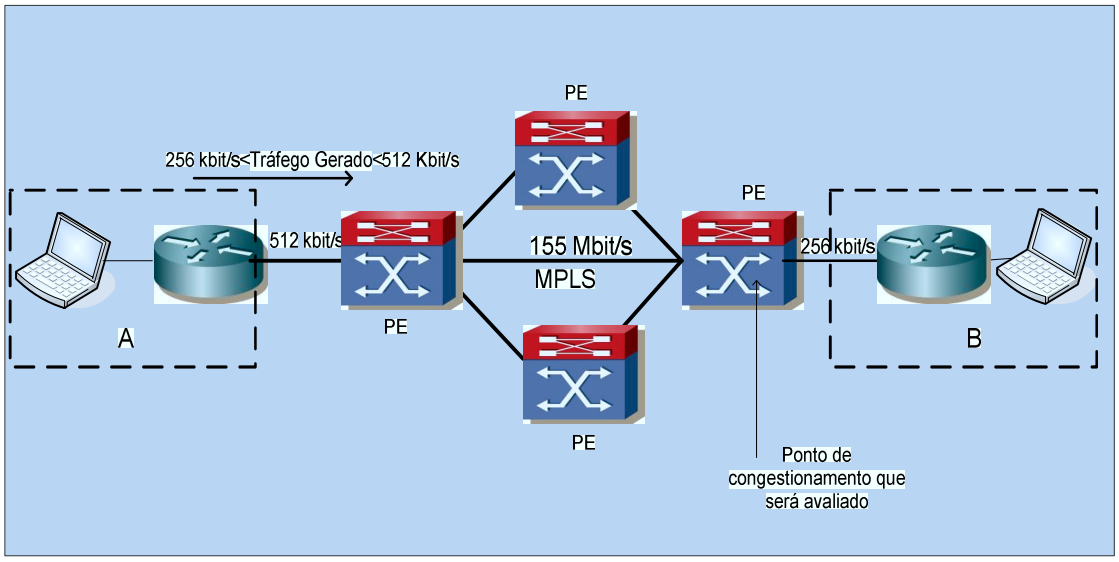

Figura 4.3 – Topologia para o teste da QoS

O Iperf é um gerador de tráfego que mede a vazão, as perdas e a variação do atraso na entrega de rajadas de pacotes [59]. Para realizar os testes, foi considerado que o emissor de tráfego no *site* A atua como o servidor, e o *site* B atua como cliente. Assim, a leitura dos dados rodavam no computador do *site* A. A velocidade dos acessos em cada *site* é mantida constante, sendo que no *site* A temos a velocidade de 512 Kbit/s e no *site* B a velocidade de 256 Kbit/s. Nos testes, a taxa de tráfego gerada de cada classe foi variada, conforme as etapas abaixo:

4.3.5.1 Etapa 1:

Nesse estágio, é avaliada a capacidade do PE em priorizar o tráfego de voz em relação a dados em uma situação sem congestionamento. Ou seja, a situação sem congestionamento é aquela em que o tráfego gerado pela classe de voz, mais a classe de dados, é menor que a velocidade do acesso de 256 kbit/s. A capacidade de priorizar os pacotes de voz nesse estágio é avaliada fazendo-se o tamanho do pacote assumir os valores de 500 *bytes* e 1.200 *bytes*. Após essa variação do tamanho do pacote, são medidos as perdas de pacotes, a banda consumida, a variação do atraso (*jitter*) e o atraso (*delay*). Conforme a tabela 4.6, configura-se para a classe voz o tamanho do pacote de 60 *bytes* para todos os estágios. A banda configurada para a classe dados nesse estágio é de 345 kbit/s, e o tráfego gerado para a mesma classe é de 150 kbits/s. O tráfego gerado pela classe voz foi de 30 Kbit/s. Com essas configurações, são medidos os parâmetros de perda de pacotes, variação do atraso (*jitter*), vazão (*bandwidth)* e atraso. As classes multimídia e dados com prioridades não serão consideradas nessa etapa.

4.3.5.2 Etapa 2:

Esse estágio avalia o desempenho do núcleo da rede na situação de congestionamento, ou seja, será avaliada a capacidade do PE em priorizar o tráfego quando a soma do tráfego gerado pelas classes for maior que a velocidade de acesso de 256 Kbits. Nesse estágio, a classe de voz gerou 36 kbit/s, enquanto a classe de dados gerou 300 kbit/s. A banda configurada para a classe de voz foi de 36 k bit/s, e para a de dados foi de 345 kbit/s. Como a soma das bandas das classes de voz e dados (330 kbit/s) é superior à velocidade do acesso (256 Kbit/s), haverá congestionamento no PE. Além da situação de congestionamento, serão avaliados os parâmetros

quando mudamos os tamanhos dos pacotes de 500 *bytes* para 1.200 *bytes*. Os parâmetros a serem registrados serão variação do atraso (*jitter*), atraso (*delay*), perda de pacotes e vazão. Nessa etapa, as classes a serem avaliadas são somente *dados* e *voz*.

4.3.5.3 Etapa 3:

Esse estágio avalia o desempenho do PE em priorizar os pacotes para quatro classes na situação sem congestionamento quando o tamanho dos pacotes de dados prioritários, multimídia e dados é variado e voz mantém o seu tamanho do pacote constante. A situação sem congestionamento é aquela onde a somatória do tráfego gerado pelas quatro classes é inferior à velocidade do acesso (256 Kbit/s). Nesse cenário, a somatória das quatro classes representa 192 kbit/s, enquanto no acesso temos a velocidade de 256 kbit/s. Os valores de pacotes para as classes dados, dados com prioridades e multimídia assumirão os valores de 500 *bytes* e 1.200 *bytes*, enquanto o pacote de voz permanecerá constante. A ideia é avaliar o efeito da variação do tamanho dos pacotes das classes dados, dados com prioridade e multimídia sobre o pacote de voz, que permanece constante. Serão medidos os principais parâmetros (variação do atraso, atraso, perda de pacotes e vazão) que caracterizam a qualidade de serviço para posterior análise. A medição dos principais parâmetros será para cada classe de serviço.

4.3.5.4 Etapa 4:

Nesse estágio, além de se avaliar a capacidade de PE em priorizar os pacotes para cada classe quando os pacotes de dados, dados com prioridades e multimídia tem seus tamanhos variados de 500 *bytes* para 1200 *bytes*, também é avaliada a situação de congestionamento; ou seja, quando a somatória das velocidades do tráfego gerado por cada classe é maior que a velocidade do acesso, caracteriza-se a situação de congestionamento. Os principais parâmetros de qualidade de serviço que serão avaliados são a perda de pacotes, variação do atraso (*jitter*), atraso (*delay*) e vazão. O total de tráfego gerado para esse estágio foi de 410 kbit/s, o que caracteriza a situação de congestionamento, pois a velocidade do acesso é de 256 kbit/s.

Tabela 4.6 – Etapas de teste das classes de serviços.

Etapas	Classes	Tamanho do Pacote (*bytes*)	Largura de banda configurada (kbit/s)	Tráfego Gerado (Kbit/s)	DSCP	EXP
1	Classe de serviços 1	500 1200	345	150	BE=000000	000
	Classe de serviços 2	-	-	-	AF21=010010	010
	Classe de serviços 3	-	-	-	AF41=100010	100
	Classe de serviços 4	60	36	30	EF=101110	101
2	Classe de serviços 1	500 1200	345	300	BE=000000	000
	Classe de serviços 2	-	-	-	AF21=010010	010
	Classe de serviços 3	-	-	-	AF41=100010	100
	Classe de serviços 4	60	36	30	EF=101110	101
3	Classe de serviços 1	500 1200	192	82	BE=000000	000
	Classe de serviços 2	500 1200	80	40	AF21=010010	010
	Classe de	500	80	40	AF41=100010	100

	serviços 3	1200				
	Classe de serviços 4	60	36	30	EF=101110	101
4	Classe de serviços 1	500		300	BE=000000	000
		1200				
	Classe de serviços 2	500	80	40	AF21=010010	010
		1200				
	Classe de serviços 3	500	80	40	AF41=100010	100
		1200				
	Classe de serviços 4	60	34	30	EF=101110	101

Na tabela acima, a classe 1 equivale às aplicações de dados sem nenhum nível de prioridade, ou seja, é a classe menos prioritária. A classe 2 representa os dados com prioridade superior aos da classe 1 de dados. A classe 3 tem maior prioridade que as classes 2 e 1, sendo que normalmente se encontram dentro dessa classe a aplicação de multimídia. A classe 4 é a classe com maior nível de prioridade e normalmente representa o tráfego de voz.

4.3.6 ANÁLISE DOS RESULTADOS DOS TESTES

Os testes utilizando o Iperf como ferramenta de captura de dados geraram resultados importantes para avaliação dos parâmetros de Qualidade de Serviço (QoS) que serão apresentados e analisados a seguir.

4.3.6.1 Análise dos resultados da Etapa 1

A figura 4.4 apresenta os resultados para o *Jitter* na situação sem congestionamento para as classes 1 e 4 (voz e dados), conforme a etapa 1.

- ✓ *Jitter*, Atraso e Perdas de Pacotes

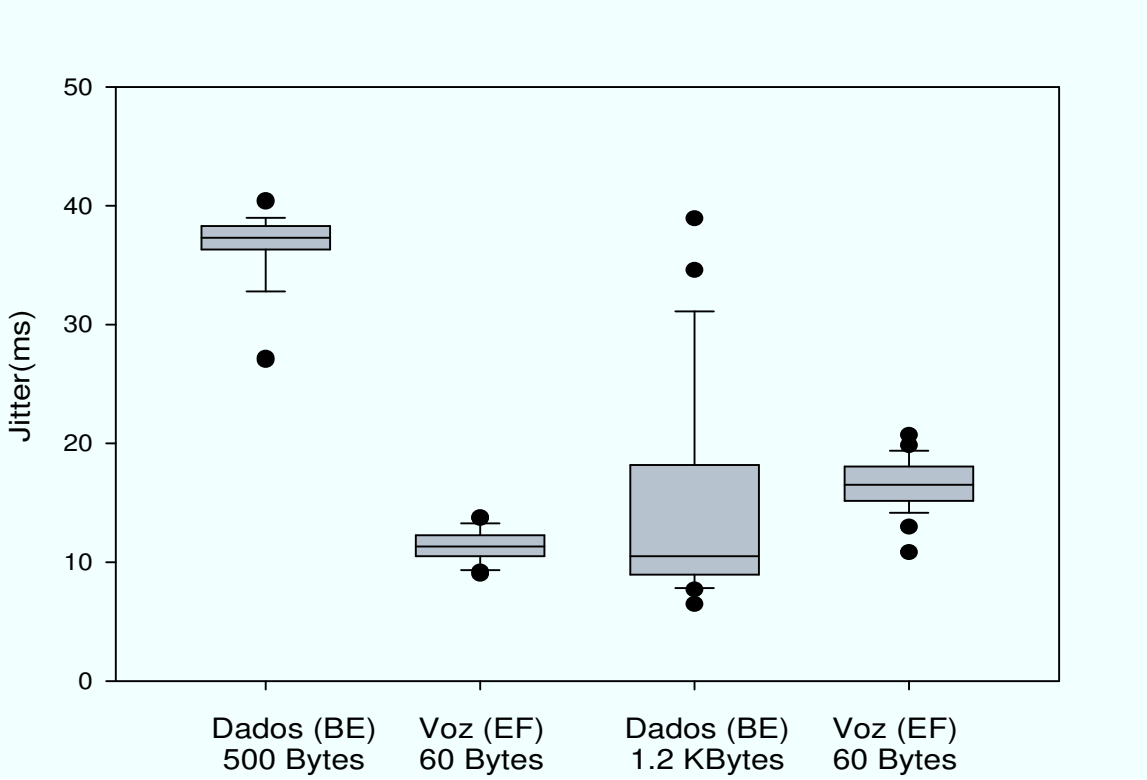

Figura 4.4 – Avaliação do *jitter* para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 bytes para a etapa sem congestionamento.

A figura 4.4 apresenta a variação do *jitter* para as classes de dados e voz quando o tamanho do pacote de dados é variado de 500 *bytes* e 1.200 *bytes*. As aplicações de dados não são sensíveis ao *jitter*, mas as aplicações de voz são. O resultado anterior mostra que a prioridade dada aos pacotes de voz (EF) sobre os pacotes de dados (BE) funcionou adequadamente, pois EF tem maior prioridade que BE. A classe dados para o tamanho de pacote de 500 *bytes* apresentou um *jitter* entre 32 e 38 ms, praticamente 100% das medidas realizadas. A classe voz para o tamanho de pacote de dados 500 *bytes* e voz de 60 *bytes* apresentou um *jitter* variando de 9 ms a 12 ms para 100% das medidas, e, quando o tamanho do pacote de dados foi alterado para 1.200

bytes, o *jitter* manteve-se com valores aceitáveis entre 12 e 17 ms para cem porcento das medidas, justificando a sua priorização em relação a dados. Fazendo uma comparação com os requisitos recomendados de *jitter* da IPTV e VoIP, que são, respectivamente, de 50 ms e 25 ms, observamos que os resultados estão de acordo as necessidades de Qualidade de Serviço (QoS) dessas aplicações. Não houve perdas de pacotes para essa etapa sem congestionamento.

O atraso medido de ida e volta (RTT) para essa etapa foi de 173 ms, o que atende totalmente aos requisitos de transmissão de IPTV e VoIP.

4.3.6.2 Análise dos resultados da etapa 2

A figura 4.5 apresenta os resultados para o *jitter* na situação com congestionamento para as classes voz e dados, conforme a etapa 2, ou seja, será gerado um tráfego de 330 Kbit/s, que é superior à velocidade do acesso do ponto receptor, que é 256 Kbit/s, caracterizando a situação de congestionamento. Nessa etapa, também serão avaliadas somente as classes dados e voz em situação de congestionamento e variando o tamanho do pacote de dados de 500 *bytes* para 1.200 *bytes*, mantendo-se fixo o tamanho do pacote de voz em 60 *bytes*.

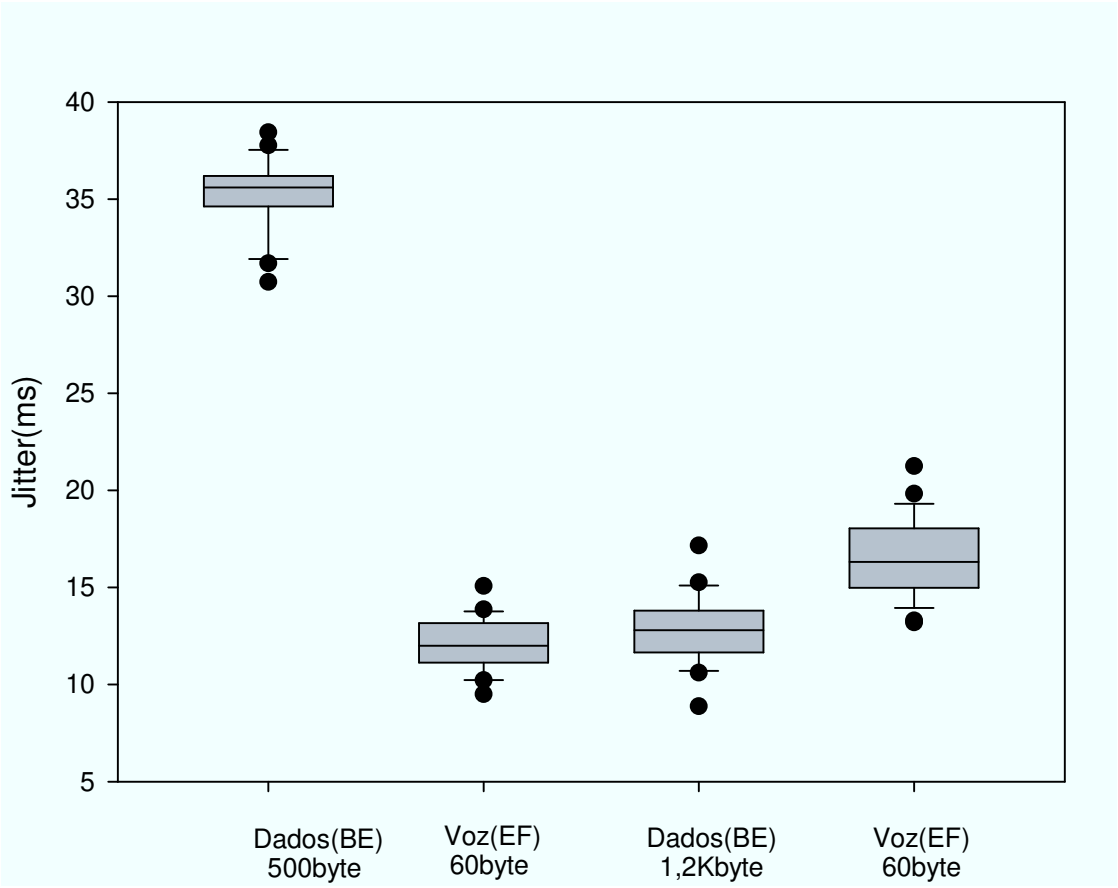

Figura 4.5 – Avaliação do *jitter* para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 *bytes* em situação de congestionamento.

O resultado da figura 4.5 anterior mostra que a prioridade dada aos pacotes de voz (EF) sobre os pacotes de dados (BE) funcionou adequadamente mesmo em situação de congestionamento, pois EF tem maior prioridade que BE. As classes dados e voz para o tamanho de pacote de dados 500 *bytes* e voz de 60 *bytes* não apresentaram grandes alterações em relação ao estágio anterior. Quando o tamanho do pacote de dados foi alterado para 1.200 *bytes*, o *jitter* manteve-se com valores aceitáveis entre 12 e 17 ms para cem porcento das medidas, justificando a sua priorização em relação a dados e mostrando sua eficiência na situação de congestionamento. Os resultados continuam ainda satisfazendo as recomendações para o transporte das principais aplicações sensíveis a *jitter*, como TVIP e VoIP. Contudo, como observado na figura 4.4, o aumento do tamanho do pacote provoca um aumento do *jitter* para a classe voz. Isso já sugere que seja utilizada a fragmentação de pacotes de dados para aumentar a qualidade de transmissão de voz.

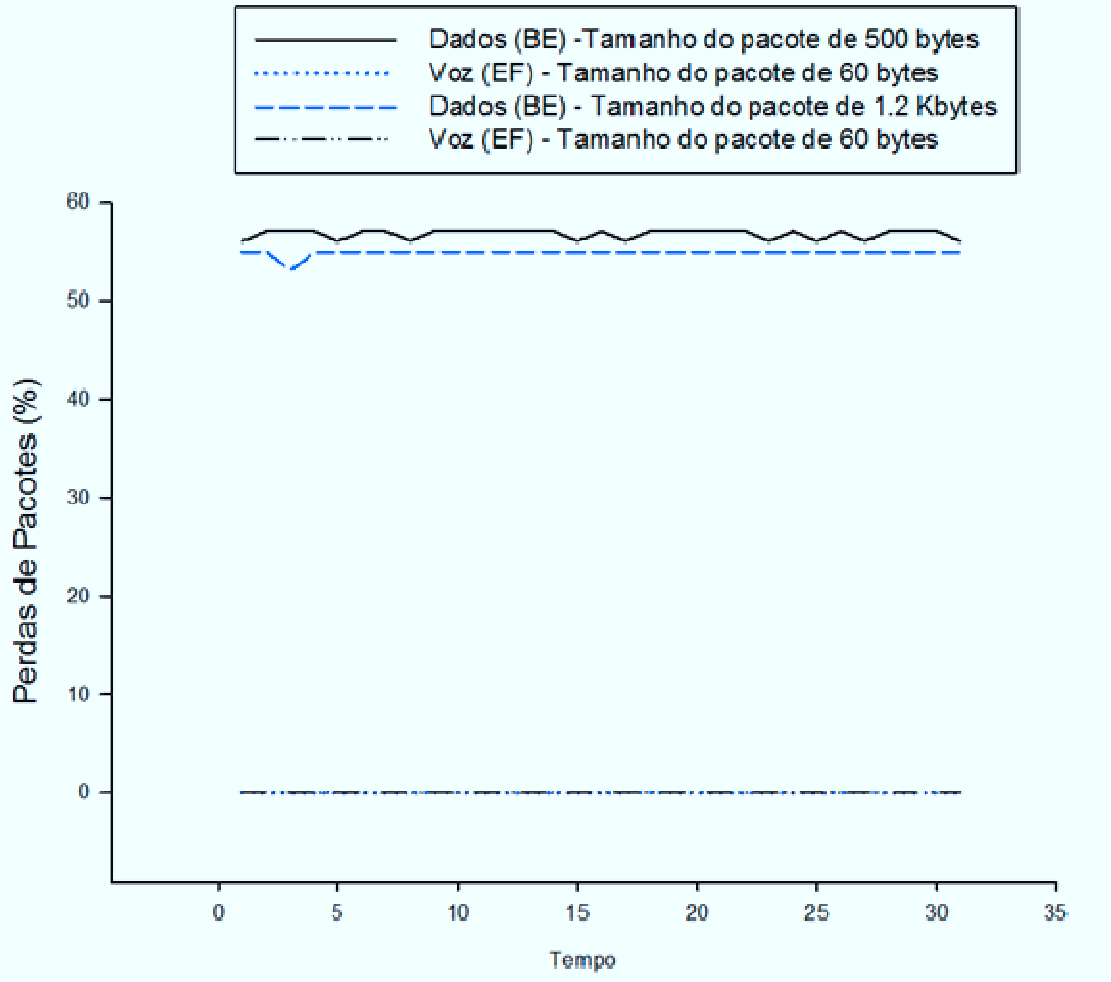

Figura 4.6 – Avaliação das perdas de pacotes para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 *bytes* em situação de congestionamento.

Como já foi avaliado na etapa 1, não houve nenhuma perda de pacotes naquela etapa. Porém, como é possível verificar na figura 4.6 da etapa 2, que representa as perdas de pacotes para está etapa na condição de congestionamento, perdas significativas ocorrem para as classes de dados (BE). Para a classe de voz (EF), observou-se que não ocorre nenhuma perda de pacotes, mostrando a eficácia da prioridade da classe de voz (EF) sobre a classe de dados (BE).

O atraso medido de ida e volta (RTT) para essa etapa foi de 340 ms, o que atende aos requisitos de transmissão de IPTV e VoIP.

4.3.6.3 Análise dos resultados da etapa 3

A figura 4.7 apresenta o *jitter* para a etapa 3 para as quatro classes: dados(BE), dados com prioridades(AF21), voz(EF) e multimídia(AF41). A etapa é sem congestionamento, pois o tráfego gerado pelas quatro classes foi de 192 Kbits/s, que é menor que a velocidade de 256 Kbit/s. A figura 4.7 mostra que, à medida que aumentamos o tamanho do pacote, os níveis desejáveis para as aplicações de voz (EF) e multimídia (AF41) mantêm o nível recomendado pelas aplicações, por exemplo, de VoIP e IPTV. Quando o tamanho do pacote de 500 *bytes* é alterado para 1.200 *bytes*, dados e dados prioritários sofrem grandes variações, mas voz e multimídia mantêm seus valores aceitáveis.

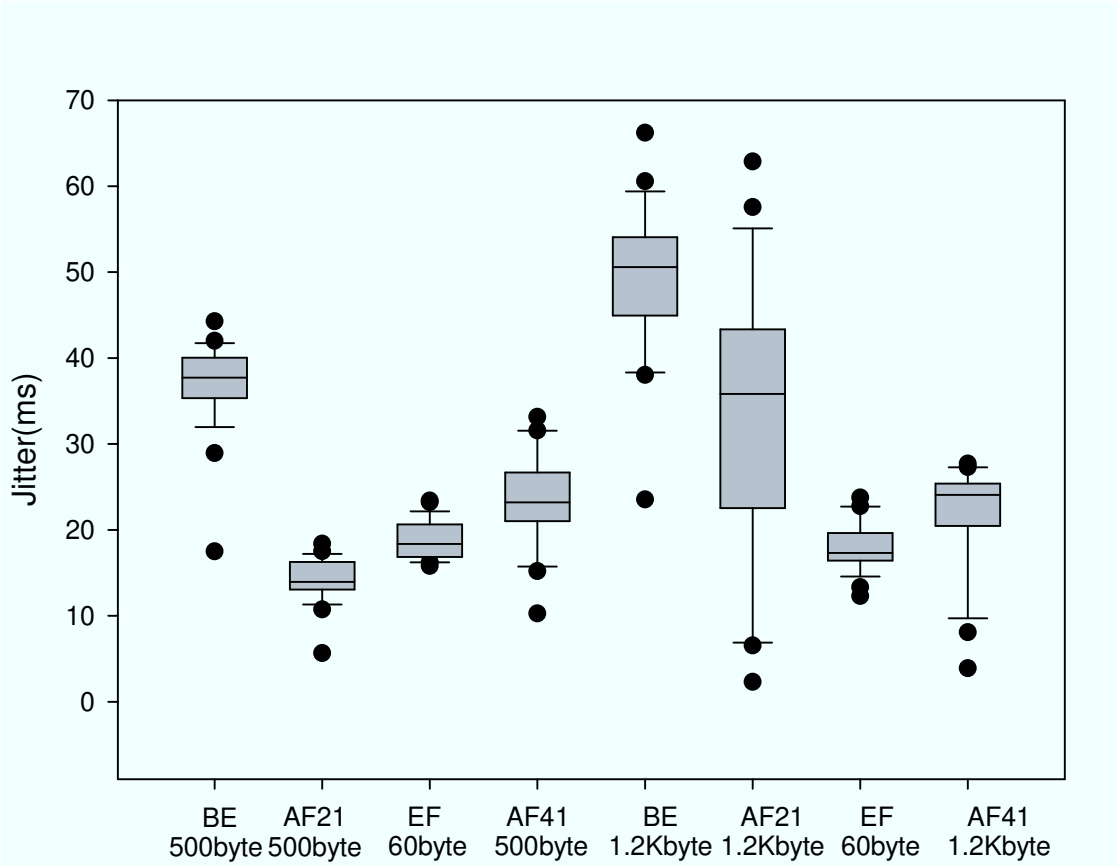

Figura 4.7 – Avaliação do *jitter* para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 *bytes* para a etapa sem congestionamento.

Foi observado que não ocorreu nenhuma perda de pacotes para essa etapa, o que já era esperado, pois não existe congestionamento.

O atraso medido de ida e volta (RTT) para essa etapa foi de 181 ms, o que atende aos requisitos de transmissão de IPTV e VoIP.

4.3.6.4 Análise dos resultados da etapa 4

A figura 4.8 mostra os resultados dos testes para a etapa com congestionamento para as quatro classes – dados, dados prioritários, voz e multimídia – na situação de congestionamento.

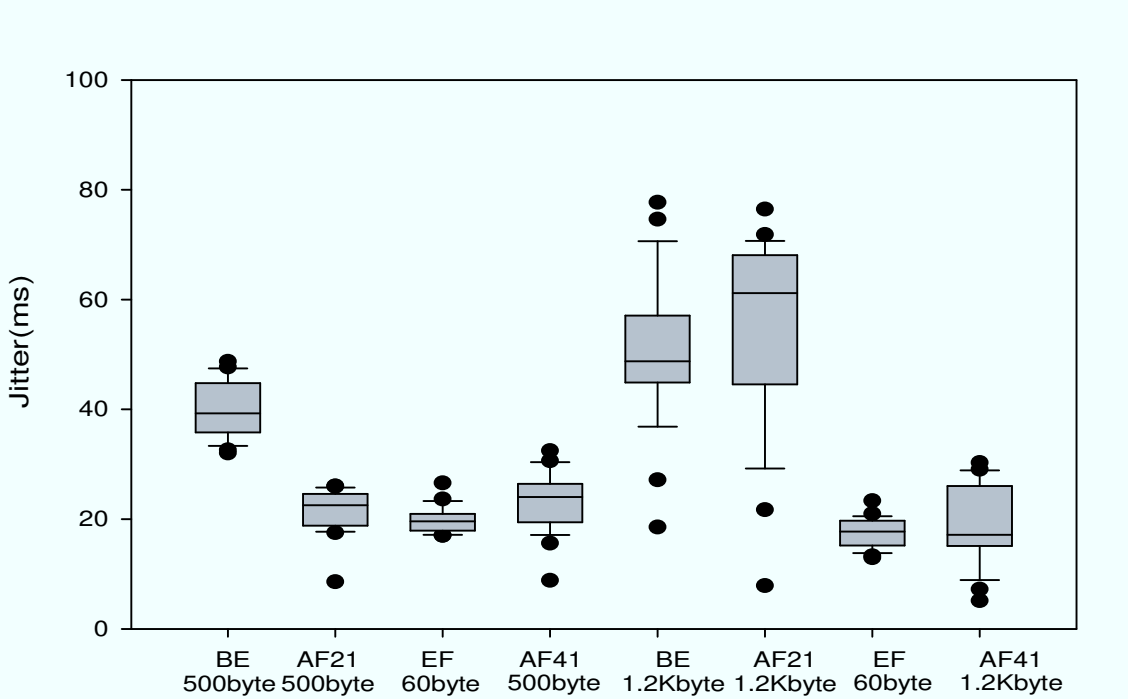

Figura 4.8 – Avaliação do *jitter* para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 *bytes* em situação de congestionamento.

Quando foi aumentado o tamanho dos pacotes de dados, dados com prioridades e multimídia de 500 *bytes* para 1.200 *bytes*, o *jitter* manteve-se com valores aceitáveis para as aplicações de voz e multimídia, justificando a técnica de prioridade adotada. Para voz (EF), o *jitter* apresentou valores em torno de 20 ms, enquanto que, para a classe AF41, apresentou *jitter* variando em torno de 20 a 30 ms.

A figura 4.9 apresenta os resultados das perdas de pacotes para as quatro classes de serviços quando o tamanho do pacote varia de 500 *bytes* para 1200 *bytes*.

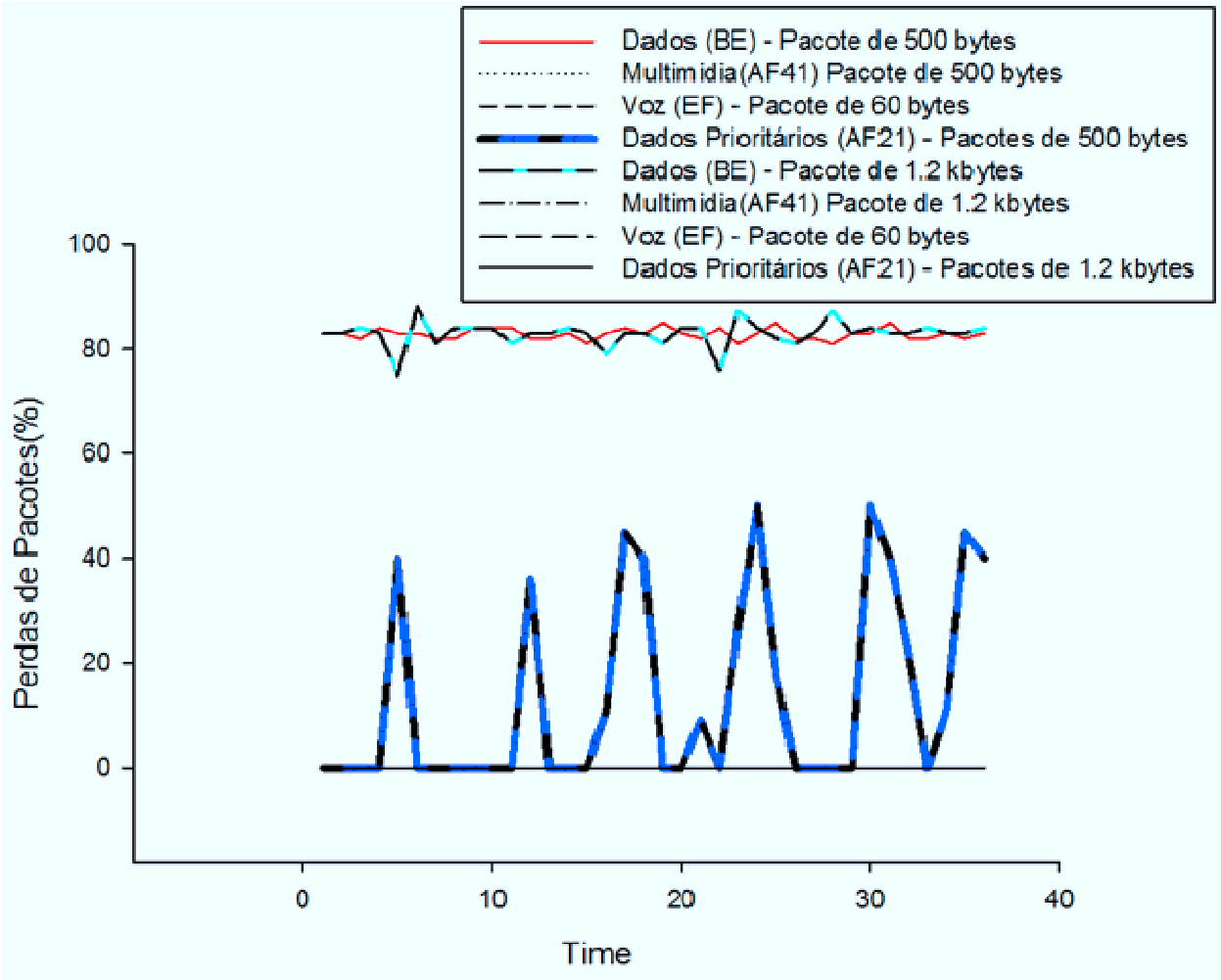

Figura 4.9 – Avaliação das perdas de pacotes para pacotes de dados de 500 e 1.200 *bytes* e voz de 60 *bytes* em situação de congestionamento.

Os resultados das perdas dos pacotes para situação com congestionamento mostram que os mecanismos de prioridade aplicados às classes mostraram sua eficácia, pois nenhuma perda de pacotes para as classes de voz e multimídia ocorreram, mesmo quando os pacotes de dados tiveram seus tamanhos alterados para 1.200 *bytes*.

4.4 Proposta para QoS em *WiMax* sobre MPLS

O padrão IEEE 802.16 especifica quatro categorias de serviço, que devem ser tratadas de forma diferenciada pelo mecanismo de escalonamento da camada MAC na rede de acesso e por algum outro mecanismo no núcleo da rede para oferecer a QoS fim a fim. O mecanismo sugerido nesta tese é MPLS com QoS no núcleo da rede. Será apresentado um mapeamento das quatro categorias de serviços do acesso *WiMax* em quatro classes do MPLS, apresentadas nos tópicos anteriores.

As quatro categorias de serviço do *WiMax* são:

- ✓ UGS (*Unsolicited Grant Service*): segundo Andrews, Ghosh e Muhamed [60], a categoria UGS é projetada para oferecer suporte aos fluxos de serviço de tempo real que geram pacotes de dados de tamanho fixo em intervalos periódicos, ou seja, tráfego (CBR). Essa categoria de serviço pode ser representada pelo tráfego gerado por emulação T1/E1 e por aplicações de voz sobre IP.
- ✓ rtPS (*real-time Polling Service*): essa categoria é utilizada para oferecer suporte aos fluxos de serviço em tempo real, como o *streaming* de vídeo.
- ✓ nrtPS: é projetada para oferecer suporte aos fluxos de serviço em tempo não-real que geram pacotes de tamanho variável em intervalos periódicos, como, por exemplo, uma transferência de arquivos via (FTP), (SMS), entre outros.
- ✓ *Best Effort*: o serviço de melhor esforço é tipicamente oferecido pela *Internet* para o tráfego gerado por navegação na Web e tráfego de *e-mails*.

4.4.1 MAPEANDO OS SERVIÇOS *WIMAX* EM CLASSES MPLS

Para oferecer o nível de QoS necessário pelas aplicações será proposto o mapeamento dos quatro serviços *WiMax* padronizados nas quatro classes do MPLS avaliadas anteriormente. A tabela 4.7 apresenta o mapeamento entre os serviços de acesso e o núcleo MPLS. A categoria de serviço *Best Effort* do acesso *WiMax* será mapeada na classe do MPLS de dados. Os pacotes do serviço nrtPS serão classificados como AF21 no núcleo MPLS. A categoria rtPS do *WiMax* será

classificada em AF41 no MPLS. Enfim, a categoria de serviços UGS, pelos seus fortes requisitos, será classificada como EF.

Tabela 4.7 – Classificação de *WiMax* em MPLS.

Categoria de serviços do *WiMax*	Classes de Serviços do MPLS
UGS	EF (Voz)
rtPS	AF41 (Multimídia)
nrtPS	AF21 (Dados com prioridades)
Best Effort	Dados (BE)

4.4.2 PROPOSTA DE QOS EM 3G SOBRE MPLS

As redes móveis, a partir da terceira geração, são baseadas no protocolo IP. Para a integração dessas redes móveis com as redes fixas para uma arquitetura de convergência fixa-móvel é necessário o suporte à qualidade de serviço no acesso e no núcleo da rede. A arquitetura para QoS das redes de 3G é uma evolução da arquitetura de QoS para o GPRS. Nessa arquitetura, são definidas as características e funcionalidades entre os pontos finais da comunicação com o objetivo de realizar um suporte consistente de QoS para serviços fim a fim. A arquitetura móvel é formada de três elementos básicos, que são a estação móvel, a rede de acesso e o núcleo da rede. A rede de rádio de acesso e o núcleo fazem parte dos serviços do UMTS (*Universal Mobile Telecommunications Systems*). No UMTS, os tipos de tráfegos suportados são divididos em quatro classes. Essa classificação é baseada nos requisitos de atraso, taxa de *bit*, taxa de erro e prioridade no tratamento do tráfego [61]:

- ✓ Classe conversacional: aplicações conversacionais de tempo real que têm restrições quanto ao atraso, como aplicações de videotelefonia.
- ✓ Classe *streaming*: para as aplicações enquadradas nessa classe, certa quantidade de variação no atraso é tolerável. Como exemplo dessa classe, pode-se citar vídeo de tempo real.

- ✓ Classe interativa: é aplicável a serviços que requerem uma vazão garantida. Alguns exemplos dessa classe incluem: comércio eletrônico e navegação Web interativa.
- ✓ Classe *background*: é utilizada para o tráfego *best-effort* tradicional, como transferência de arquivos e *e-mail*. Esse tráfego tem a menor prioridade dentre todas as classes.

Para prover QoS fim a fim, é proposto o mapeamento dessas quatro classes nas quatro classes avaliadas anteriormente, conforme a tabela apresentada a seguir:

Tabela 4.8 – Mapeamento de 3G em MPLS.

Categoria de serviços do *WiMax*	Classes de Serviços do MPLS
Classe conversacional	EF (Voz)
Classe *streaming*	AF41 (*Multimídia*)
Classe interativa	AF21 (Dados com prioridades)
Classe *background*	Dados (BE)

Este capítulo mostra o resultado de QoS *(Quality of service)* para quatro classes de serviços que foram avaliadas fim a fim. O resultado mostra que é possível tratar as aplicações de formas diferenciadas e de acordo com os requisitos necessários para o seu perfeito funcionamento. Os resultados apresentados mostram que o MPLS é capaz de oferecer *jitter*, *delay* e perdas de pacotes dentro dos valores aceitáveis. Com isso, é possível concluir que é viável a implementação de VPN fixo-móvel com qualidade de serviços através do mapeamento das classes de serviços das tecnologias sem fio, como *WiMax* e 3G, sobre MPLS. Como resultado dos testes, também é possível concluir que é fortemente recomendável a fragmentação dos pacotes de dados para oferecer a QoS adequada às aplicações. O próximo capítulo irá avaliar a conectividade, isolamento e segurança das redes MPLS em seu núcleo.

Capítulo 5

Segurança, Conectividade e Isolamento das VPNs fixo-móveis

Este capítulo aborda o nível de segurança no núcleo da rede que é proposto pelas novas arquiteturas de construção de redes virtuais privadas móveis e fixas. A interface aérea deverá manter o mesmo o nível de segurança da tecnologia de acesso utilizada para o acesso à rede virtual privada. As VPNs fixo-móveis, que permitirão a convergência das redes, devem utilizar no núcleo da rede o protocolo MPLS com o objetivo de garantir o isolamento e a conectividade entre as VPNs. O ambiente montado para o teste neste capítulo mostra a eficiência e valida a utilização das VPNs MPLS como um protocolo altamente seguro para as novas arquiteturas de redes convergentes.

5.1 **Introdução**

As NGNs (*Next Generation Networks*) para prover serviços de VPNs fixo-móveis com escalabilidade, segurança e qualidade de serviço estão estruturadas em três camadas: a camada

de transporte IP MPLS (*Internet Protocol Multi-Protocol Label Switching*), a camada de sessão multimídia IMS (*IP Multimedia Subsystem*) e a camada da infraestrutura de aplicações (*Java EE middleware*). A plataforma IP MPLS fornece papel fundamental na arquitetura NGN, pois apresenta suporte aos serviços de VPN (*Virtual Private Network*) fixo-móvel. Este capítulo aborda a camada IP MPLS, com ênfase na segurança das VPNs fixo-móveis, avaliando a capacidade de isolamento e conectividade das VRFs (*Virtual Routing and Forwarding*) das VPNs, aspectos esses fundamentais no ambiente de construção das novas redes NGNs. Este capítulo é baseado em um ambiente de teste que tem como objetivo avaliar a conectividade e isolamento das implementações das MVPNs seguras. Os testes realizados permitiram avaliar o desempenho em relação à conectividade e ao isolamento das VRFs. O capítulo inicia fazendo uma análise dos aspectos mais importantes de segurança das VPNs, para em seguida avaliar o desempenho da segurança das VPNs convergentes baseadas em um núcleo MPLS.

A segurança é um atributo chave para a convergência de serviços e rede dentro do contexto das redes de nova geração (NGN). Entre os principais requisitos das NGN para atender às necessidades das novas aplicações em relação à segurança, podemos destacar [62]:

- ✓ Separação de tráfego das VPNs fixo-móveis baseadas em MPLS

Um dos requisitos de segurança mais importantes das VPNs é que o tráfego dos *sites* pertencente a uma determinada VPN fique separado do tráfego das outras VPNs, ou seja, a solução de rede não deve permitir que o tráfego de um usuário de uma determinada VPN seja visto, nem que invada o tráfego da outra VPN. A avaliação de desempenho realizada mostra a eficiência das VPNs fixo-móveis baseadas em MPLS em relação a esse requisito. No final do capítulo, um dos testes realizados mostra esse resultado [62].

- ✓ Utilização do mesmo plano de endereços por diferentes VPNs fixo-móveis

Outro requisito importante para um provedor que pretende oferecer o serviço VPN é permitir que o plano de endereçamento de um usuário de uma VPN possa ser utilizado por outra VPN, sem afetar outras VPNs ou o núcleo da rede [62]. O ambiente de VPN MPLS

apresenta uma boa alternativa para esse requisito, que é avaliado em seguida. Em outras palavras, uma dada VPN deve ser completamente separada das outras VPNs ou do núcleo da rede em termos do tráfego ou plano de endereços. Neste capítulo propõe-se a avaliar a capacidade das VPNs MPLS em relação ao isolamento das VPNs, separação dos planos de endereços e conectividade.

Para tornar possível utilizar o mesmo endereço IP para vários clientes, as VPN MPLS utilizam o campo RD (*Route Distinguisher*) para distinguir as VPNs entre si. O objetivo do RD é permitir que os endereços IPv4 possam ser utilizados em diferentes contextos, como no caso das VPNs MPLS. Em um dado roteador, pode ser configurado um RD que define uma VRF em que os planos de endereços IPv4 possam ser usados em outra VRF, desde que esta seja configurada com RD distinto. Para as considerações de segurança, é importante entender que o RD faz com que as rotas das VPNs IPV4 sejam únicas no núcleo das VPNs MPLS. O RD é mais bem detalhado em IETF RFC 4364.

Os tráfegos das VPNs consistem do tráfego do plano de controle e de dados, como foi destacado no capítulo 3. Os requisitos dos usuários é que seus tráfegos não sejam misturados com outros tráfegos de outras VPNs. Mais precisamente, seus pacotes não devem ser transmitidos para outras VPNs, e as outras VPNs não devem transmitir pacotes para dentro de sua VPN.

5.2 Problemas das VPNs não orientada a conexão

O grande motivo pelo qual as VPNs baseadas em MPLS fazem sucesso comercial nos últimos anos é a sua facilidade em provisionar o serviço pela operadora e pelos seus clientes em relação às VPNs tradicionais que são baseadas em tecnologias *frame relay* e ATM. Essa facilidade de provisionar o serviço acaba refletindo-se no preço comercial das redes que trabalham com MPLS em relação ao das outras tecnologias disponíveis no mercado. Atualmente, os preços dos serviços com a tecnologia MPLS estão posicionados pelas operadoras de telecomunicações de

forma que para o usuário é mais econômico optar pelas soluções baseadas em MPLS do que pelas soluções baseadas em *frame relay* e ATM [63].

A principal razão que faz com que as VPNs MPLS sejam provisionadas de forma simples é o fato de que elas não são orientadas à conexão entre o CE e o PE. Diferentemente das outras VPNs, como *frame relay*, ATM e IPSec, que são orientadas à conexão, ou seja, cada CE precisar realizar uma conexão com todos os CEs da VPN para tornar viável a comunicação, nas VPNs baseadas em MPLS, o CE precisa somente de uma conexão até o PE mais próximo.

O preço pago pelo fácil provisionamento dos serviços das VPNs MPLS em relação às VPNs orientadas a conexões, como *frame relay* e ATM, é a questão da segurança, pois estas apresentam um alto nível de segurança de nível 2. Ou seja, a grande vantagem das VPNs baseadas nas tecnologias *frame relay* e ATM está na percepção dos usuários de que essas tecnologias são mais seguras que as VPNs MPLS, mas este capítulo mostra que as VPNs MPLS poderão ser tão seguras quanto as VPNs baseadas nas tecnologias *frame relay* e ATM se seguirem as recomendações aqui mencionadas [62,63].

Em uma VPN móvel-fixa baseada na tecnologia MPLS, o roteador do usuário encaminha os pacotes IP até o roteador da operadora mais próxima (PE), e este se responsabiliza por todo o encaminhamento dos pacotes até o CE de destino. Nesse modelo de VPN, o usuário não tem nenhuma visão dos encaminhamentos dos pacotes na rede, sendo o provedor o responsável total. Isso atende às necessidades dos provedores, que, além do fácil provisionamento dos serviços, conseguem a fidelização de seus clientes; por outro lado, seus clientes não precisam de nenhum conhecimento de rede, pois a operadora é responsável por toda a configuração das VPNs, inclusive as configurações relacionadas com os aspectos de segurança.

O aspecto de fidelização dos clientes através da tecnologia sempre foi um desejo das operadoras de telecomunicações, e a tecnologia das VPNs baseadas em MPLS tornou isso viável

tecnicamente. Com a solução VPN MPLS, o cliente depende totalmente da operadora, ou seja, para qualquer alteração em sua VPN, ele precisará de operadora. De uma forma mais objetiva, a operadora tem o controle da rede de seus clientes completamente, portanto, a segurança da rede do cliente é diretamente proporcional ao grau de confiança que ele tem na operadora que fornece o serviço de VPN MPLS.

Um dos problemas de segurança das VPNs MPLS diz respeito ao fato de o cliente não confiar no provedor do serviço MPLS devido à possibilidade de uma configuração não realizada corretamente em sua VPN. Normalmente, quando acontece esse problema, algum dos *sites* de determinada VPN A, por exemplo, são configurados indevidamente em outra VPN B. O capítulo 6 apresenta uma proposta para solucionar essa deficiência das VPNs MPLS, que é a utilização de IPSec sobre VPN MPLS para resolver prováveis erros de configurações realizados pelo provedor, apesar de o usuário do serviço, na maioria dos projetos de VPN MPLS, acabar confiando em seu provedor, não implementando IPSec em função dos motivos que são analisados no capítulo seguinte.

Outra questão fundamental relacionada à segurança das VPNs MPLS refere-se à possibilidade de um ataque a uma VPN afetar outras VPNs. Isso se deve principalmente ao fato de os usuários de diversas VPNs compartilharem o mesmo roteador PE. Portanto, se um ataque for realizado a partir de uma VPN a um determinado roteador PE, o atacante poderá derrubar o PE e deixar todos os usuários de diversas VPNs que estão conectados a esse roteador PE sem nenhum tipo de conexão. Normalmente, para evitar esse tipo de ataque, a operadora configura uma rota estática entre o roteador do cliente CE e o roteador de borda do provedor PE [62,63].

5.2.1 MODELOS DE SEGURANÇA PARA AS VPNS MPLS

Existem basicamente dois modelos de construção de VPNs MPLS, que são a *intranet* e a *extranet*. Dois *sites* podem somente ter conectividade IP através de uma rede se há no mínimo uma VPN que conecte ambos. A situação em que todos os *sites* que estão em uma VPN

pertençam a uma única empresa é chamada de *intranet*, e a situação em que pelo menos um *site* da VPN pertence a mais de uma empresa é chamada de *extranet* [22].

O *draft* que aborda segurança das VPNs MPLS é intitulado "*Security Framework for Provisioned VPNs*", utilizado como um modelo de referência para segurança das VPNs MPLS. Esse *draft* aborda as VPNs somente *intranet*, ou seja, o modelo considera que não há comunicação entre as VPNs para a formação de *extranet*.

5.2.1.1 Modelos de segurança para as VPNs MPLS *intranet*

É apresentada, na figura 5.1, uma implementação de uma *intranet* utilizando VPN MPLS. Essa *intranet* é formada de quatro *sites* que se comunicam entre si. A VPN ABCD é formada por quatro *sites* da mesma organização que se comunicam através da conectividade IP da VPN MPLS. Os elementos das VPNs MPLS e seu funcionamento básico já foram apresentados no capítulo 3. Agora, são avaliadas as questões de segurança em uma VPN MPLS.

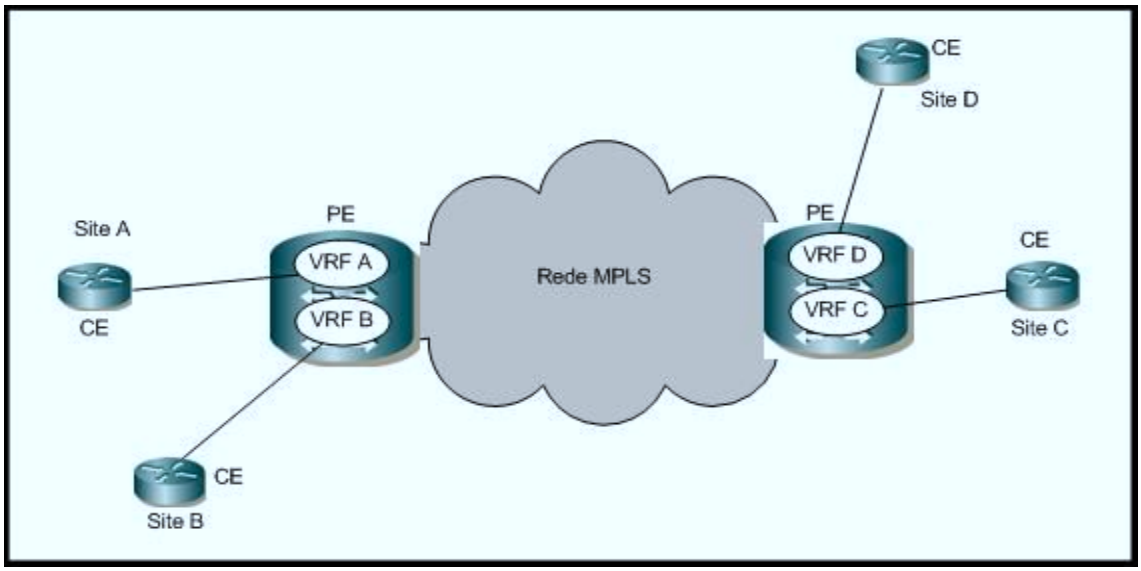

Figura 5.1 – Topologia *intranet.*

A implementação de *intranet* com a tecnologia MPLS através de VPN MPLS é realizada basicamente através dos parâmetros de RT (*Route Target*) e RD (*Route Distinguishers*).

Cada VRF no roteador PE necessita ter um identificador de rotas associado, que pode estar relacionado a um *site* ou a uma VPN. No caso mais comum, que é a formação de *intranet* em que os *sites* pertencem somente a uma VPN, é tecnicamente recomendável o uso de um único identificador de rotas RD para a VPN. Para uma topologia de um modelo de *intranet* simples, como o da topologia apresentada na figura 5.1, a tabela 5.1 mostra as configurações dos RDs e RTs – usa-se o mesmo identificador de rotas por VPN para reduzir o uso de memória do roteador PE. O atributo RT identifica uma coleção de VRFs pela 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 e 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 para verificar se seu atributo RT de importação aceita inserir a rota na VRF. Esse mecanismo flexível permite a construção de diferentes topologias de VPNs e modelos de negócios. Esse atributo é definido em BGP *Extended Communities Attribute* [51,52]. Erros de configurações do RT cometidos pela operadora de telecomunicações podem comprometer facilmente a segurança da VPN MPLS, pois o RT é responsável por controlar quais rotas devem ser inseridas nas VRFs.

Tabela 5.1 – RD e RT das VRFs.

VPN ABCD	RD	RT
VRF A	100	100
VRF B	100	100
VRF C	100	100
VRF D	100	100

Entretanto, se algum desses *sites* no futuro pretender ser membro de outra VPN para formar uma *extranet* – por exemplo, suponha-se que um identificador de rotas é utilizado pela VPN (*Voice over IP*), que esta tenha um servidor de VoIP e que este precise ser membro de múltiplas VPNs, não será possível determinar que identificador de rotas usar para esse servidor específico porque ele pertence a mais de uma VPN.

Quando certas topologias são criadas, pode ser necessário estender os identificadores de rotas por VRF/*Site* para um determinado modelo de projeto, mas somente para projetos especiais, pois a criação de identificadores de rotas RD por *site* não oferece escalabilidade para o provedor.

5.2.1.2 Modelos de segurança para as VPNs MPLS *extranet*

Há várias definições para *extranet*, mas genericamente é possível defini-la como uma solução que permite que várias VPNs sejam interconectadas entre si, compartilhando uma infraestrutura de rede. O controle da conectividade entre os *sites* é realizado através do parâmetro já definido das RTs (*Rotas Targets*) nas VRFs de cada PE da VPN. As rotas *targets* configuradas em cada VRF definirão como os *sites* da VPN trocam tráfego entre eles. O capítulo 6 apresenta uma proposta para o problema de formação de *extranet* segura com alta escalabilidade.

5.3 Teste de conectividade, isolamento e segurança das VPNs

5.3.1 OBJETIVO

O objetivo é investigar a capacidade das VPNs MPLS em conectar *sites* da mesma VPN, isolar *sites* de diferentes VPNs, garantindo que o usuário não tenha acesso ao núcleo da rede do provedor, e mostrar que, nas VPNs MPLS, os mesmos planos de endereços podem ser utilizados por diferentes usuários, desde que estejam em VPNs diferentes.

Para o teste, serão configurados três VPNs: a VPN azul do Banco X, a VPN verde do Banco Y e a VPN vermelha do Banco Z, de acordo com a topologia apresentada na figura 5.2. A VPN azul do Banco X é formada pelos seguintes *sites* e CEs: CE1, CE6, CE7 e CE10. A VPN verde do Banco Y é formada pelos *sites:* CE3, CE4 e CE8. A VPN vermelha do Banco Z possui os *sites* CE2, CE5 e CE9. O *software* utilizado para a avaliação de conectividade das VPNs será o comando *ping*, tratado brevemente a seguir.

5.3.2 MATERIAL UTILIZADO NO TESTE

Os materiais utilizados nos testes dividem-se em *software* e *hardware*. O *software* utilizado foi o comando *ping*, enquanto que o *hardware* foram roteadores, computadores, *link* de comunicações e uma infraestrutura de um núcleo de rede MPLS.

5.3.2.1 Software

O comando *ping* está presente em grande parte dos sistemas operacionais e equipamentos de redes; nada mais é do que uma mensagem ICMP tipo *echo request*. O campo de dados do *echo request* pode trazer protocolos de camadas superiores e outras informações. O formato geral do comando *ping* em sistemas Microsoft é [64]:

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]
[[-j host-list] | [-k host-list]] [-w timeout] destination-list
```

Ping (*Packet Internet Groper*) é uma aplicação utilizada em redes de computadores que provê um teste básico de comunicação para verificar se determinado equipamento na rede está funcionando ou se está acessível. Seu funcionamento é similar ao de um sonar de submarino, em que ele envia sinais e ouve as respostas. O nome para essa aplicação vem do famoso jogo de pingue-pongue, no qual, fazendo-se uma analogia, o *ping* é o envio de pacotes, e a resposta ou seu eco seria o *pong*.

A aplicação *ping* envia pacote via ICMP (*echo request*) para o equipamento de destino e recebe a resposta ICMP (*echo reply*) contendo os seguintes dados:

- ✓ Atraso de ida e volta (em milissegundos);
- ✓ A quantidade de pacotes respondidos pelo destino;
- ✓ O tamanho dos pacotes enviados (*Bytes*);
- ✓ Uma estatística de comunicação média informando o menor e o maior tempo de resposta e, ainda, a média do tempo de resposta.

A ferramenta *ping* já vem instalada e configurada em qualquer ambiente Linux e Windows. Para testá-la, basta digitar o comando *ping*, seguido do endereço de destino.

Esse comando é utilizado para verificar o tempo de resposta do destino, permissão de acessibilidade e integridade na troca de pacotes. Dependendo das características da resposta, ele pode exibir diversas informações, auxiliando no diagnóstico de problemas no tráfego de dados entre um equipamento e outro. Outra ferramenta que utiliza o ICMP de maneira semelhante ao *ping* é o *traceroute*.

O ICMP (*Internet Control Message Protocol*) [Anexo B] apresenta como respostas que serão úteis na análise de conectividade das VPNs MPLS as seguintes mensagens de respostas:

- ✓ *Destination host unreachable*

Host Unreachable (Host Inalcançável) – Mensagem recebida de um roteador.

Causa: a rede destino foi alcançada, mas não foi possível entregar o pacote para o *host* destino, provavelmente por causa de uma submáscara configurada erroneamente ou porque o *host* destino não está acessível.

- ✓ *Request timed out*

O pacote foi enviado com sucesso ao destino, mas a resposta foi bloqueada ou perdida. Outra possibilidade para essa mensagem é que a resposta poderá ser bloqueada ou descartada em algum roteador que fica no caminho de retorno.

5.3.2.2 Hardware

Os equipamentos utilizados foram dez roteadores de acessos que funcionaram como CE, cinco roteadores de borda da rede MPLS que funcionaram como PE da arquitetura MPLS e mais três roteadores P da arquitetura MPLS. Os *links* de comunicação utilizados foram de 512 Kbit/s para a rede de acesso, ou seja, para a conexão do CE até o PE. As conexões entre os PEs e PEs com P foram implementadas através de conexões de 155 Mbit/s SDH, 622 Mbit/s SDH e 1 Gbit/s.

Também foram utilizados três computadores (C1, C2 e C3) para leituras dos dados gerados pelo comando PING.

5.3.3 PREPARAÇÃO DO AMBIENTE DE TESTE DE CONECTIVIDADE E ISOLAMENTO

A configuração da topologia do ambiente de teste é apresentada na figura 5.2.

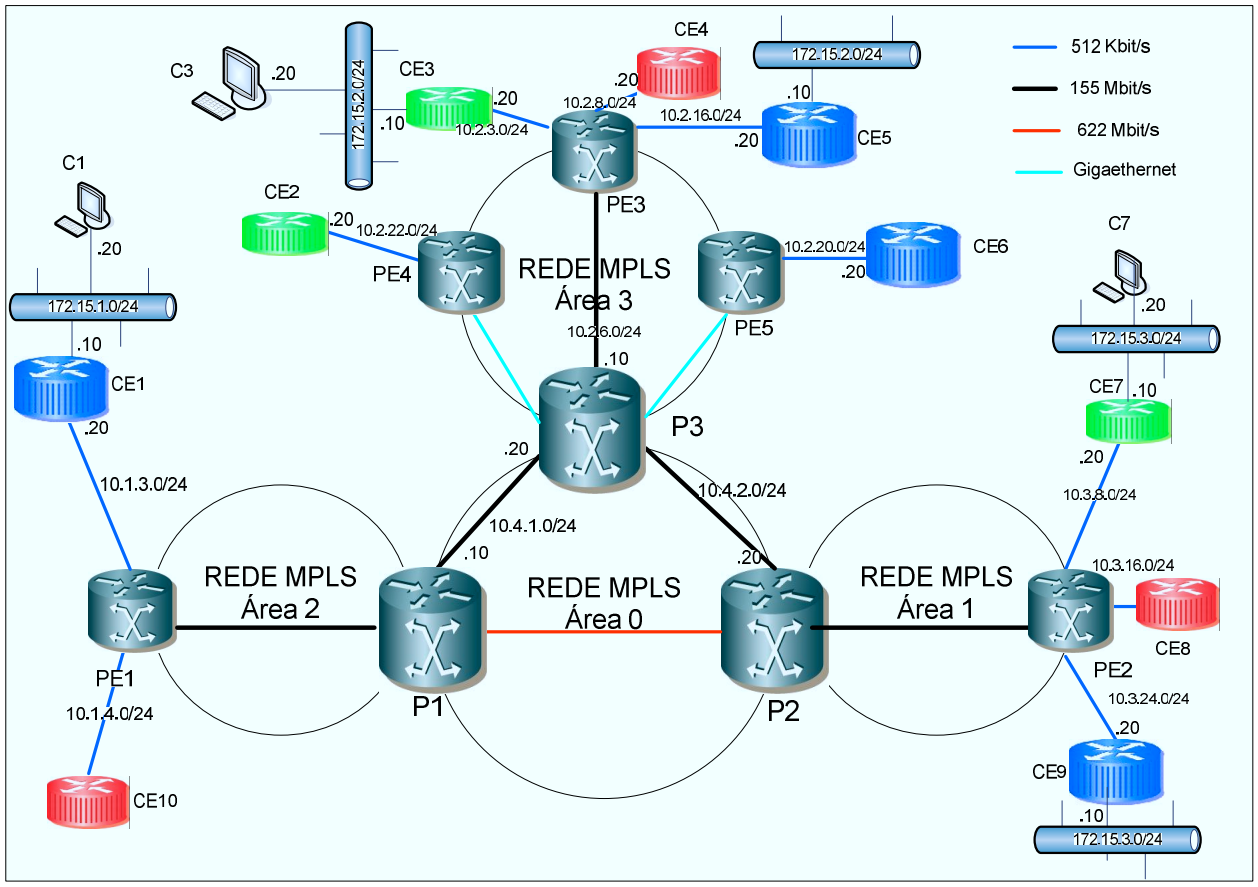

Figura 5.2 – Topologia para o teste de endereçamento, conectividade e isolamento.

5.3.4 TESTES REALIZADOS

- ✓ Do computador C1 da VPN Azul, que foi configurada para o Banco X, tentar conectar-se, através do comando *ping*, aos roteadores CE1, CE5, CE6 e CE9, que pertencem à mesma VPN Azul do Banco X. O objetivo do teste é avaliar a

capacidade de conectividade dos *sites* que pertencem à mesma VPN, no caso, a VPN Azul.

- ✓ Do computador C1 da VPN Azul, que foi configurada para o Banco X, tentar conectar-se ao computador C7 da rede 172.15.3.0/24, que possui o mesmo endereço da rede 172.15.3.0/24 do CE9, mas está em VPN diferente, ou seja, na VPN Verde do Banco Y. O propósito é testar a capacidade da solução em trabalhar com endereços idênticos, desde que eles estejam em VPNs diferentes. Sendo assim, é possível que o Banco X utilize os mesmos endereços do Banco Y se ambos trabalham em VPNs distintas, ou seja, apresentam diferentes RDs.
- ✓ Do computador C1 da VPN Azul do Banco X, tentar conectar-se, através do comando *ping*, aos roteadores CE2, CE3, CE7 e ao Computador C7, que pertencem à VPN Verde do Banco Y. O propósito é avaliar a capacidade de isolamento das VPNs do Banco X em relação ao Banco Y, mostrando que as VPNs ficam totalmente isoladas umas das outras. A avaliação será a partir do computador C1 até os roteadores (CE3, CE7) e o computador C3.
- ✓ Do computador C7 da VPN Verde do Banco Y, tentar conectar-se ao roteador CE1 da VPN Azul do Banco X. A ideia é avaliar a capacidade de isolamento a partir da VPN Verde em relação à VPN Azul.
- ✓ Do computador C7 da VPN Verde, tentar conectar-se ao roteador CE3 e ao computador C3 da VPN Verde. Esse teste avalia a capacidade de conectividade entre os *sites* da VPN Verde do Banco Y.
- ✓ Do computador C1 da VPN Azul, tentar conectar-se ao P1, P2 e PE3. O teste também avalia a capacidade de isolamento entre o computador C1 e o Núcleo da Rede formada por P1, P2 e P3.

5.3.5 RESULTADOS DOS TESTES

Os resultados dos testes realizados para posterior avaliação são apresentados neste tópico.

5.3.5.1 Do computador C1 que está na VPN Azul, testar a conectividade com CE1, CE5, CE6 e CE9

- ✓ CE1 – Computador C1 tenta conectar-se com o roteador CE1

d:\>ping 10.1.3.20

Pinging 10.1.3.20 with 32 *bytes* of data:

Reply from 10.1.3.20: bytes=32 time<10ms TTL=255

Reply from 10.1.3.20: bytes=32 time<10ms TTL=255

Reply from 10.1.3.20: bytes=32 time<10ms TTL=255

Reply from 10.1.3.20: bytes=32 time<10ms TTL=255

Ping statistics for 10.1.3.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ CE5 – Computador C1 tenta conectar-se ao roteador CE5

d:\>ping 10.2.16.20

Pinging 10.2.16.20 with 32 bytes of data:

Reply from 10.2.16.20: bytes=32 time=15ms TTL=250

Reply from 10.2.16.20: bytes=32 time=15ms TTL=250

Reply from 10.2.16.20: bytes=32 time=15ms TTL=250

Reply from 10.2.16.20: bytes=32 time<10ms TTL=250

Ping statistics for 10.2.16.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 15ms, Average = 11ms

- ✓ CE6 – Computador C1 tenta conectar-se ao roteador CE6

d:\>ping 10.2.20.20

Pinging 10.2.20.20 with 32 bytes of data:

Reply from 10.2.20.20: bytes=32 time=16ms TTL=250

Reply from 10.2.20.20: bytes=32 time<10ms TTL=250

Reply from 10.2.20.20: bytes=32 time=16ms TTL=250

Reply from 10.2.20.20: bytes=32 time<10ms TTL=250

Ping statistics for 10.2.20.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 16ms, Average = 8ms

- ✓ CE9 - Computador C1 tenta conectar-se ao roteador CE9

d:\>ping 10.3.24.20

Pinging 10.3.24.20 with 32 bytes of data:

Reply from 10.3.24.20: bytes=32 time<10ms TTL=250

Reply from 10.3.24.20: bytes=32 time<10ms TTL=250

Reply from 10.3.24.20: bytes=32 time=16ms TTL=250

Reply from 10.3.24.20: bytes=32 time=16ms TTL=250

Ping statistics for 10.3.24.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 16ms, Average = 8ms

5.3.5.2 O computador C1 tentará conectar-se ao computador C7

d:\>ping 172.15.3.20

Pinging 172.15.3.20 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.15.3.20:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

5.3.5.3 O Computador C1 tentará conectar-se aos roteadores CE2, CE3, CE7 e ao computador C7

- ✓ CE2 - Computador C1 tenta conectar-se ao roteador CE2

d:\>ping 10.2.22.20

Pinging 10.2.22.20 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.2.22.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ CE3 - Computador C1 tenta conectar-se ao roteador CE3

d:\>ping 10.2.3.20

Pinging 10.2.3.20 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.2.3.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ CE7 - Computador C1 tenta conectar-se ao roteador CE7

d:\>ping 10.3.8.20

Pinging 10.3.8.20 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.151.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.3.8.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ C7 - Computador C1 tenta conectar-se ao roteador computador C7

d:\>ping 172.15.3.20

Pinging 172.15.3.20 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.15.3.20:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

5.3.5.4 O computador C7 tentará conectar-se ao roteador CE1 da VPN Azul

d:\>ping 10.1.3.20

Pinging 10.1.3.20 with 32 bytes of data:

Reply from 172.15.3.10: Destination host unreachable.

Reply from 172.15.3.10: Destination host unreachable.

Reply from 172.15.3.10: Destination host unreachable.

Reply from 172.15.3.10: Destination host unreachable.

Ping statistics for 10.1.3.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

5.3.5.5 O computador C7 tentará conectar-se ao roteador CE3 e ao computador C3 da VPN Verde

- ✓ CE3 - Computador C7 tenta conectar-se ao roteador CE3

d:\>ping 10.2.3.20

Pinging 10.2.3.20 with 32 bytes of data:

Reply from 10.2.3.20: bytes=32 time<10ms TTL=250

Reply from 10.2.3.20: bytes=32 time<10ms TTL=250

Reply from 10.2.3.20: bytes=32 time<10ms TTL=250

Reply from 10.2.3.20: bytes=32 time<10ms TTL=250

Ping statistics for 10.2.3.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ C3 - Computador C7 tenta conectar-se ao computador C3

d:\>ping 172.15.2.20

Pinging 172.15.2.20 with 32 bytes of data:

Reply from 172.15.2.20: bytes=32 time<10ms TTL=122

Reply from 172.15.2.20: bytes=32 time<10ms TTL=122

Reply from 172.15.2.20: bytes=32 time<10ms TTL=122

Reply from 172.15.2.20: bytes=32 time<10ms TTL=122

Ping statistics for 172.15.2.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

5.3.5.6 Do computador C1, tentar conectividade com os roteadores de núcleo P1, P2 e P3

- ✓ P1 – O Computador C1 tenta conectar-se ao roteador do núcleo da rede P1

d:\>ping 10.4.1.10

Pinging 10.4.1.10 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.4.1.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ P2 – O Computador C1 tenta conectar-se ao roteador do núcleo da rede P2

d:\>ping 10.4.2.20

Pinging 10.4.2.20 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.4.2.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

- ✓ P3 – O computador C1 tenta conectar-se ao roteador do núcleo da rede P3

d:\>ping 10.2.6.10

Pinging 10.2.6.10 with 32 bytes of data:

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Reply from 172.15.1.10: Destination host unreachable.

Ping statistics for 10.2.6.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

5.3.6 ANÁLISE DOS RESULTADOS

Nesta seção, são avaliados os resultados alcançados nos itens 5.4.5.

O primeiro resultado dos testes do item "5.3. 5.1" mostrou a capacidade de conectividade entre os elementos que pertencem à VPN azul do Banco X. No primeiro teste, o C1 faz tentativa e obtém total sucesso ao conectar-se ao roteador CE1. Os quatro pacotes transmitidos foram todos recebidos, e nenhum foi perdido. O mesmo resultado foi alcançado para as tentativas do C1 quando este tentou conectar-se aos roteadores CE5, CE6 e CE9. Isso era previsto, pois todos esses roteadores CE1, CE5, CE6 e CE9, pertencem à mesma VPN azul.

O segundo resultado dos testes do item "5.3.5.2" refere-se à capacidade das VPNs MPLS para trabalhar com os mesmos endereços IPs, desde que estes sejam de VPNs diferentes. O endereço IP do computador C7 é 172.15.3.20, que é o mesmo endereço do roteador CE9, mas pertencente à VPN verde do Banco Y. Ao tentar conectar-se ao CE7 através do comando PING, a

resposta ao comando foi uma negação às tentativas de conexão. Para quatro pacotes transmitidos, nenhum foi recebido com sucesso. Esse resultado confirmou a capacidade das VPNs MPLS de vários clientes do provedor em utilizar os mesmos endereços IP, desde que sejam utilizados em VPNs diferentes.

O terceiro resultado dos testes de avaliação do item "5.3.5.3" mostrou a capacidade das VPNs MPLS em isolar o tráfego entre as VPNs. O computador C1, que pertence à VPN azul do Banco X, tentou conectar-se aos roteadores CE2, CE3, CE7 e ao computador C7 da VPN verde do Banco Y. Nenhuma das quatro tentativas de conectar-se à VPN verde obteve sucesso; a resposta apresentou destino desconhecido para essas tentativas.

O quarto resultado dos testes da avaliação do item "5.3.5.4" mostra a capacidade de isolamento entre as VPNs verde e azul. O computador C7 da VPN verde tenta conectar-se com o roteador CE1 da VPN azul e não obtém sucesso, pois estão em VPNs diferentes. A resposta foi "destino desconhecido".

O quinto teste do item "5.3.5.5" tem o objetivo de avaliar a conectividade entre os *sites* da VPN verde; para isso, o computador C7 da VPN verde tenta conectar-se ao roteador CE3 e ao computador C3. Os resultados mostram que o computador C7 obteve total sucesso em suas solicitações de conexões para o CE3 e o C3.

O último teste do item "5.3.5.6" tem o objetivo de avaliar o nível de segurança das VPNs MPLS quando um usuário mal-intencionado tenta invadir os roteadores P1, P2 e PE3 do núcleo das VPNs MPLS. Nenhuma das três tentativas obteve sucesso. Isso mostra que a única forma de um usuário acessar o núcleo da rede MPLS é se o provedor implementar alguma configuração específica.

Este capítulo avaliou a capacidade das VPNs MPLS fixo-móveis de oferecer isolamento e conectividade das VPNs. Os resultados mostraram que as VPNs MPLS são totalmente seguras, desde que configuradas devidamente pelo provedor de serviço de telecomunicações. Os testes avaliaram a conectividade entre as três VPNs (Azul, Verde e Vermelha) quando elas utilizam o mesmo plano de endereçamento IP, pois um dos pontos fundamentais em uma solução de VPN MPLS é que seja possível conectividade entre VPNs que utilizam inclusive os mesmos endereços. Os resultados do teste mostram que existe conectividade entre os CEs da mesma VPN, mesmo que existam outros endereços iguais, mas em outra VPN. Os testes também avaliaram a capacidade de isolamento entre as três VPNs. Nesse teste de VPN MPLS, foi mostrada 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 este estiver configurado devidamente para isso (exemplos são as configurações *extranet*). O próximo capítulo irá avaliar a escalabilidade das VPNs MPLS.

Capítulo 6

Escalabilidade das VPNs MPLS convergentes – Novas propostas

As VPNs MPLS são consideradas os principais elementos da arquitetura de convergências das redes de nova geração e estão se tornando cada vez mais acessíveis para todos os usuários, principalmente em função da alta escalabilidade oferecida e pela fácil implementação, que são características próprias do modelo das VPNs baseadas em MPLS. Entretanto, esse modelo trabalha diretamente sobre as VRFs (*Virtual Routing and Forwarding*) do PE, que cresce rapidamente à medida que aumenta a quantidade de *sites* das VPNs conectadas aos PEs. Esse crescimento pode trazer alguns problemas para a operadora de telecomunicações, os quais podem prejudicar a escalabilidade e, consequentemente, gerar dificuldades para prover novos serviços de VPNs MPLS. Esses problemas aumentam seus graus de importância principalmente quando existe a necessidade de usuários que não pertencem à mesma organização acessarem a VPN, ou seja, para a formação de *extranet*.

Este capítulo apresenta uma nova proposta, com base na criação de VPN MPLS para os grandes provedores de conteúdos e no acesso a essas VPNs através de importação e exportação

de rotas dos atributos de RT e RD para usuários que já possuem suas VPNs e ACL (lista de controle de acesso) para usuários sem VPN. O capítulo apresenta também uma contribuição para as questões de erros de configurações provocados pelos provedores de serviço no momento da configuração das VPNs MPLS de seus clientes; a proposta é através da implementação de IPSec sobre MPLS. O capítulo inicia fazendo uma análise dos principais componentes da arquitetura de VPN MPLS, que são o CE e o PE. Em seguida, é avaliada a escalabilidade das VPNs MPLS, para após ser proposto um modelo que atenda à necessidade de construir VPN MPLS *extranet* altamente escalável. O capítulo é finalizado com uma alternativa para resolver os problemas de erros de configurações com a utilização de IPSec sobre MPLS.

6.1 O problema da escalabilidade das VRFs nos PEs para VPNs *extranet*

Na arquitetura MPLS, como apresentado na Capítulo 3, o roteador PE pode atender até milhares de *sites* dos clientes do provedor de serviços das VPNs MPLS que estão conectados diretamente às interfaces dos PEs. A fim de manter a conectividade entre todos os *sites* que pertencem à mesma VPN, cada roteador PE deverá possuir todas as rotas para os *sites* pertencentes à VPN em uma tabela VRF. Portanto, a tabela de roteamento da VPN nos roteadores PEs cresce rapidamente com o aumento de *sites* da VPN e com a quantidade de VPNs que se conectam ao PE. Como consequência desse aumento de VRFs no PE, a capacidade de memória e do processador dos PEs tem se tornado um foco de estudo de várias pesquisas para resolver as questões relacionadas com a escalabilidade dos PEs com o aumento das VRFs.

Para as VPNs *intranet*, os problemas mencionados acima são minimizados, pois é possível as operadoras de telecomunicações implementarem para as VRFs da mesma VPN o mesmo RD, ou seja, é configurado um RD por cliente/VPN, e não um RD por *site*. Isso traz como benefício um menor consumo da memória e processamento dos roteadores nos PEs. Na figura 6.1, são apresentadas duas VPNs MPLS (VPN AB e VPN CD) com dois *sites* por VPN, sendo que o RD (identificador da VPN) é o único para cada VPN. Tanto a VPN AB quanto a VPN CD são *intranet*, pois somente existe comunicação entre *sites* de mesma VPN. A figura 6.1a representa a

VPN AB, e a figura 6.1b representa a VPN CD, enquanto que a figura 6.1c representa a implementação das VPNs MPLS AB e CD. É importante observar na figura que o RD para cada VRF da mesma VPN é o mesmo. Sendo assim, é necessário somente que o RT de todas as VRFs importe e exporte o mesmo RD.

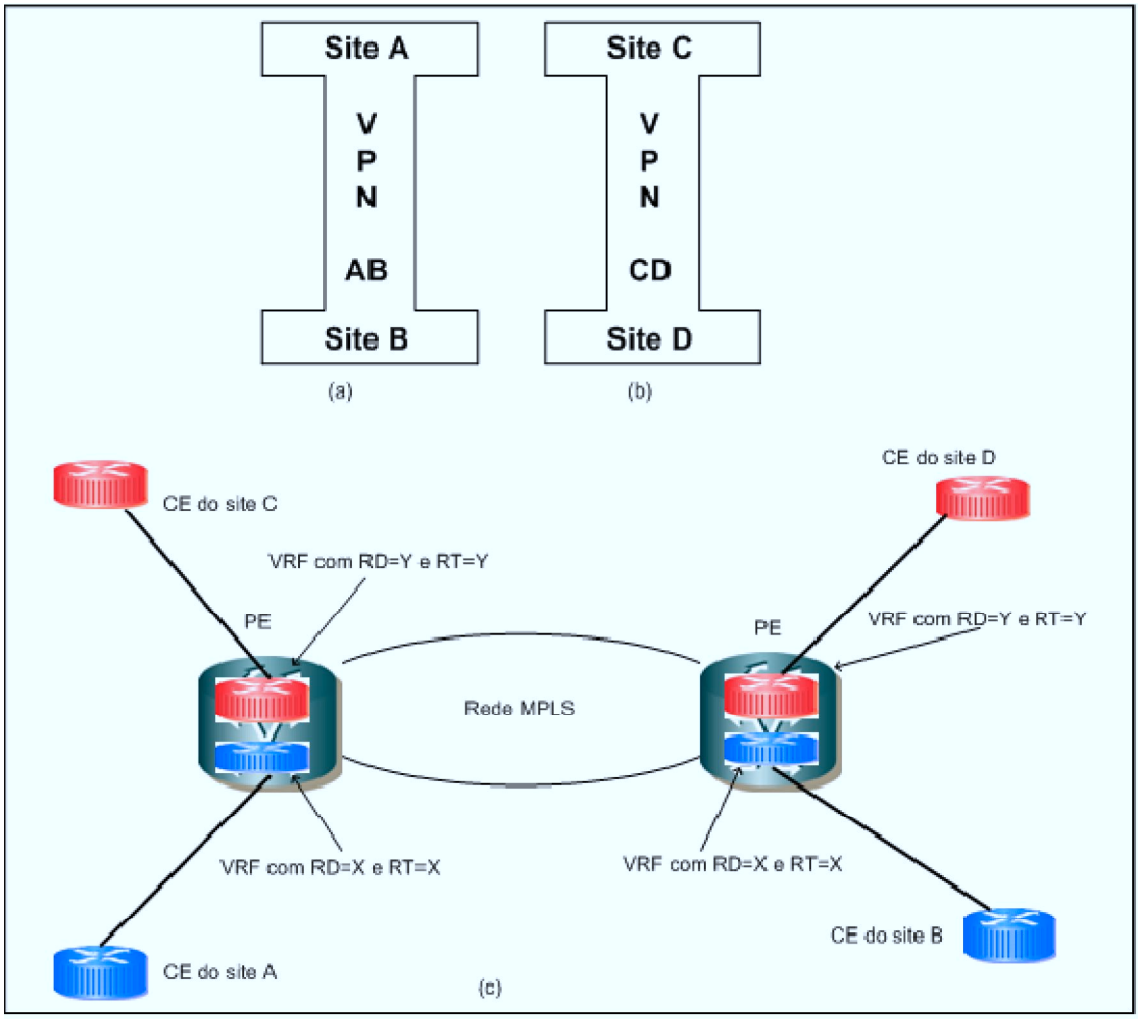

Figura 6.1 – Implementação de VPN *intranet*.

A decisão de criar RD por VPN e não por *site* tem o objetivo de melhorar a escalabilidade, mas o problema torna-se crítico quando é necessário formar uma *extranet*, por exemplo, onde um *site* precisa fazer parte de mais de uma VPN ao mesmo tempo, como mostra a figura 6.2. Nesse caso, temos dois *sites* que pertencem a duas VPNs simultaneamente, os *sites* B e C. Esses *sites* (B e C) formam o que é conhecido de *extranet*. Será considerado que o identificador da VPN AB (RD) seja X e que o identificador da VPN CD (RD) seja Y. Sendo que,

na VPN BC, somente o *site* B se conecta ao *site* C, caso seja configurado no *site* C o RT igual a X, não somente o *site* B se conectará ao *site* C, mas também o *site* A terá conectividade. Isso é devido ao fato de que está sendo configurado um RD por VPN, e não por *site*. Portanto, uma solução teoricamente viável seria configurar RD por *site*, e não por VPN, como mostra a figura 6.4.

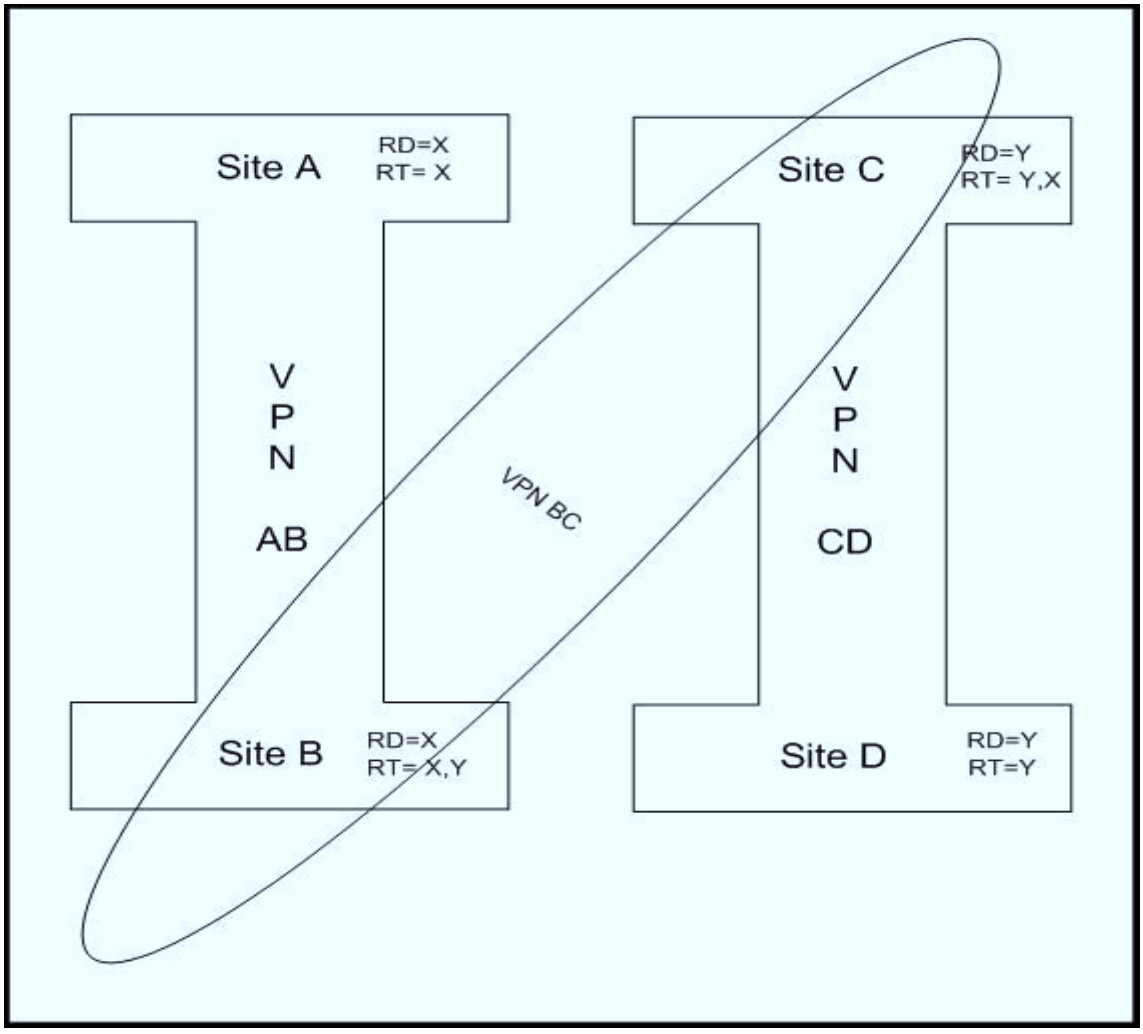

Figura 6.2 – Implementação de VPN *intranet* com RD por VPN.

Mesmo sendo a solução de RD por *site* uma alternativa teoricamente viável e um desejo de todos os usuários, pois, além dos aspectos de segurança, a criação de RD por *site* permite que o usuário utilize o mesmo endereço IP em todos os *sites*, desde que os RDs sejam diferentes. Essa solução não é a preferida pelas operadoras de telecomunicações em função de que a criação

de RD por *site* provocaria um consumo elevado de memória e processamento dos PEs, como mostra a figura 6.3.

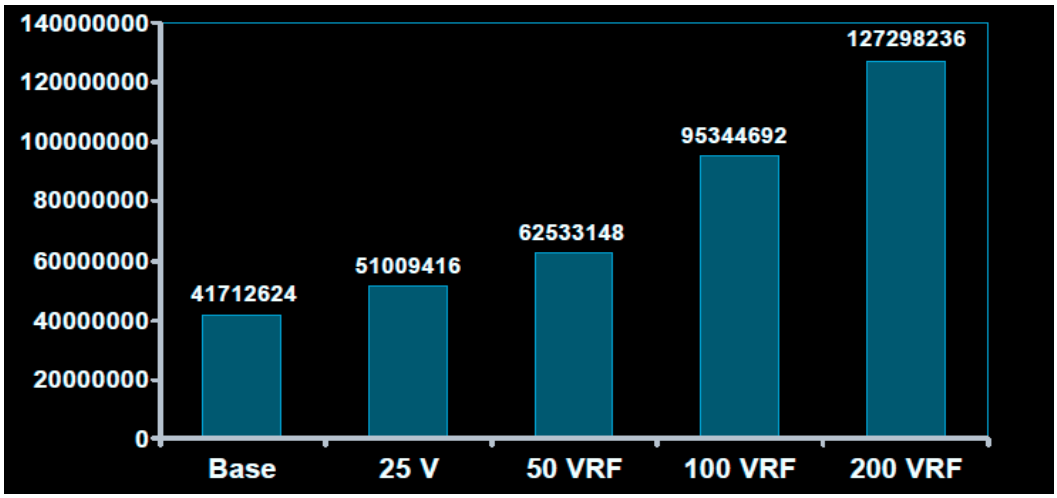

Figura 6.3 – Quantida de VRFs x Memória do PE, extraído de [35].

A figura 6.4 apresenta três VPNs (AB, CD e BC), sendo que o *site* B da VPN AB e o *site* C da VPN CD pertencem simultaneamente à VPN BC. A solução implementada tem que permitir que apenas o *site* A da VPN AB se conecte somente ao *site* B, que o *site* B se conecte ao *site* A e ao *site* C, que o *site* C se conecte ao B e ao D e que o *site* D se conecte somente ao C. Em função da não-recomendação para não utilizar RD por *site*, pois isso prejudica a escalabilidade das redes MPLS, o item 6.3 propõe uma alternativa para a questão de escalabilidade. Antes de apresentar a proposta de escalabilidade, são apresentadas, no item a seguir, algumas questões relacionadas aos protocolos de roteamento que são configurados entre o CE e o PE, pois a escolha de um determinado protocolo de roteamento poderá influenciar na escalabilidade do PE.

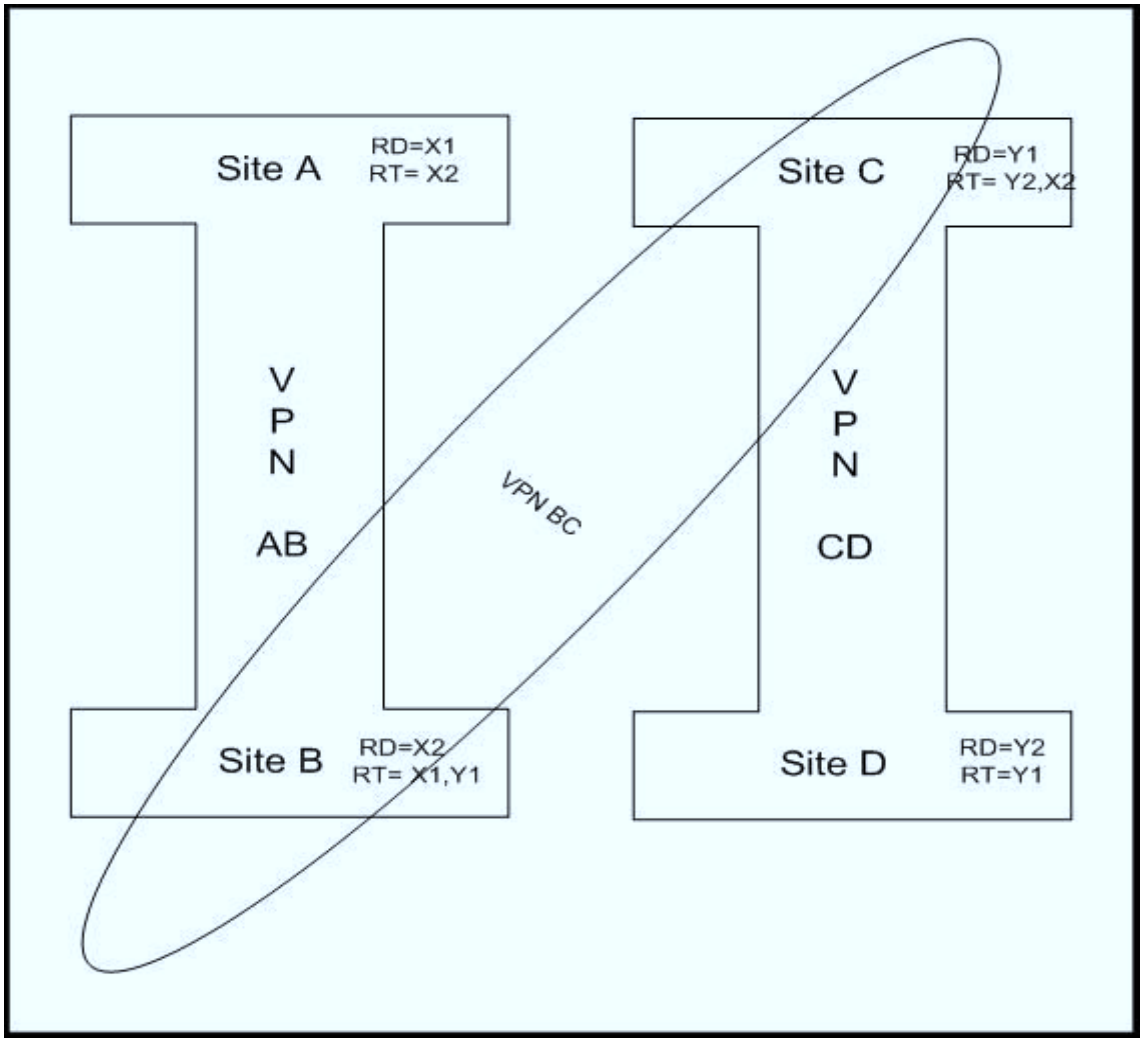

Figura 6.4 – Implementação de VPN *Intranet*.

6.2 **Avaliação do roteamento entre CE e PE**

Uma das questões fundamentais na arquitetura das VPNs MPLS é avaliar como as rotas dos *sites* das VPNs são encaminhadas e roteadas na rede MPLS através das VRFs (*VPN Routing and Forwarding)*. É importante conhecer o processo de criação e propagação das tabelas de roteamento nos roteadores PEs, pois, dependendo do protocolo de roteamento utilizado entre o CE e o PE, haverá um impacto maior ou menor no processamento dos roteadores PE e em sua memória, influenciando consideravelmente a escalabilidade das VPNs MPLS. São avaliados neste tópico os principais mecanismos utilizados pelas VRFs para aprender as rotas anunciadas pelos CEs dos usuários [63].

Os PEs aprendem quais são as rotas dos CEs que estão vinculadas às VRFs através dos protocolos de roteamento mais comuns, que são: Rotas Estáticas, RIPv2, OSPF e BGP. Esses protocolos de roteamento devem inserir as rotas aprendidas na VRF através de uma interface entre o CE, que é o equipamento do usuário, e o PE, que é o equipamento de borda da rede do provedor. Depois que foi definida a conexão do CE de cada *site* da VPN com uma VRF no PE, é necessário escolher qual protocolo de roteamento será utilizado para anunciar as rotas para a VRF do PE. A figura 6.5 apresenta uma topologia de duas VPNs (Vermelha e Azul) para dois *sites* de cada VPN, e podemos observar que outra vantagem das VPN MPLS é que não é necessário utilizar o mesmo protocolo de roteamento em todos os *sites* da VPN. Dependendo de algumas características dos usuários, é possível que, em alguns *sites*, exista rota estática e, em outros, BGP; portanto, a solução de VPN MPLS não é transparente a protocolos de roteamento. Sendo assim, a VPN pode ser formada por *sites* com diferentes protocolos de roteamento. Essa característica poderá ser muito útil quando a VPN está sendo projetada para determinado usuário que possui *sites* distribuídos em regiões de operadoras de telecomunicações distintas, por exemplo, um usuário que deseja integrar seus sistemas através de uma VPN que tem *sites* localizados em Porto Alegre, São Paulo e Miami. Essa VPN poderia utilizar o protocolo de roteamento estático em Porto Alegre, BGP em São Paulo e OSPF em Miami, ou seja, as VPNs MPLS permitem integração entre diferentes protocolos de roteamento, sendo que a escolha de qual protocolo utilizar será basicamente em função de alguns fatores, apresentados a seguir [63].

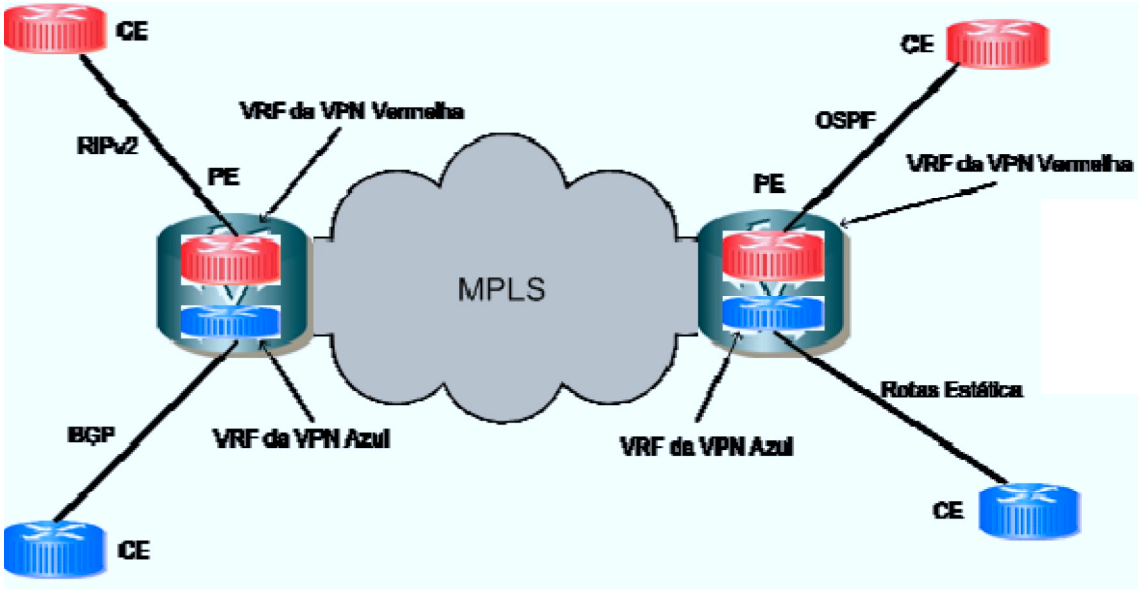

Figura 6.5 – Tipos de protocolos de roteamento.

Entre os principais fatores que influenciam a escolha do protocolo de roteamento, podemos citar [63,65,66]:

- ✓ Limitação do CE (Equipamento do usuário): é uma situação comum, principalmente no ambiente das pequenas e médias empresas – formação de VPNs MPLS com vários *sites* e CEs. Normalmente, para esse tipo de VPN MPLS, a necessidade do *site* remoto é somente uma rota estática para o servidor principal do *site* da matriz da empresa. Para tornar viável economicamente o projeto, a operadora de telecomunicação é obrigada a fazer os projetos com CEs com algumas limitações, e essas limitações refletem-se diretamente no protocolo de roteamento suportado pelo equipamento. Os CEs com pequeno custo e, por consequência, com configurações limitadas suportam, na maioria dos casos, somente os protocolos de roteamento com rota estática e RIP, não suportando BGP e OSPF. Essa necessidade de projetos com CEs de baixo custo para muitos projetos traz como consequência a utilização, na maioria dos *sites* das VPNs, o roteamento estático entre o CE e o PE.

- ✓ Segurança: quando existe um nível de confiança baixo entre o provedor e o usuário, então o provedor normalmente faz a opção pelo protocolo de roteamento estático para evitar interações dinâmicas de rotas com o usuário.
- ✓ Controle: entre os protocolos de roteamento dinâmicos, que são o BGP, OSPF e RIP, os provedores têm optado por disponibilizar ao usuário o BGP, pois este permite filtragem de rotas baseadas em políticas de roteamento. O uso do BGP permite ao provedor o controle sobre as rotas que devem ser aceitas do usuário. Em função dessa característica, é relativamente fácil para o provedor de telecomunicações proteger-se de um comportamento indevido de seus usuários das VPNs. Porém, o grande motivo que leva à escolha do BGP como protocolo de roteamento das VPNS MPLS está na necessidade em determinadas VPNs em que suas aplicações precisam de alta disponibilidade e utilizam o BGP para alcançar esse objetivo, pois o mesmo permite o balanceamento de tráfego. A figura 6.6 apresenta uma situação em que o *site* principal da VPN precisa de alta disponibilidade; em função desse requisito, são instalados dois acessos com protocolo de roteamento BGP, fazendo-se balanceamento entre eles. No *site* 1, existem dois acessos de 2 Mbit/s, sendo que eles trabalham com balanceamento de tráfego entre eles. Quando um dos acessos fica inoperante, o outro deve assumir todo o tráfego, e isso é possível porque o BGP é um protocolo de roteamento dinâmico, ou seja, o CE que está ativo aprende rapidamente as rotas do roteador que está inoperante. Os outros *sites* trabalham com rota estática.

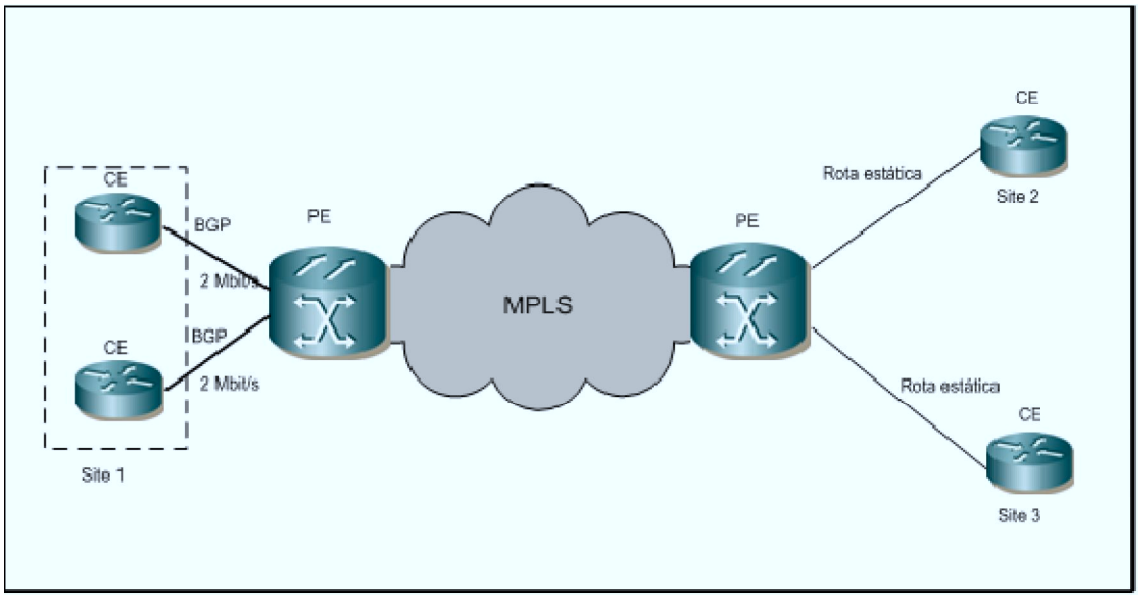

Figura 6.6 – Roteamento dinâmico com BGP.

6.3 **Análise da escalabilidade**

A escalabilidade é um aspecto fundamental de qualquer serviço de telecomunicações. Os serviços que são lançados no mercado sem escalabilidade acabam tornando-se vítimas do seu próprio sucesso comercial. À medida que aumenta o sucesso comercial de um determinado serviço de telecomunicações, existe uma tendência natural de aumentar a complexidade para atender novos usuários. Portanto, é necessário avaliar a capacidade das VPNs MPLS de atender os usuários atuais e os novos da rede MPLS [62,63].

Na análise da escalabilidade das VPNs MPLS, é necessário avaliar alguns aspectos fundamentais [62]:

- ✓ Existe algum limite para o número de VPNs por cliente e quantidade de *sites* por VPN?

- ✓ Caso exista algum limite de VPNs por cliente e de quantidade de *sites* por VPN, o serviço poderá ser bem dimensionado apenas acrescentando-se novos PEs e Ps[14] na rede MPLS?
- ✓ Os PEs e Ps serão impactados com o aumento dos usuários das VPNs e a quantidades de rotas?
- ✓ Como ficará o custo da rede com o aumento dos usuários e equipamentos?

6.3.1 POSSÍVEIS GARGALOS PARA A ESCALABILIDADE DAS VPNS MPLS

O crescimento das VPNs MPLS é afetado principalmente pelo aumento da quantidade de *sites* por VPN e pela quantidade de rotas por *site*. Portanto, é fundamental avaliar qual a influência na escalabilidade das VPNs MPLS quando são adicionados novos equipamentos CEs, o comportamento dos protocolos de roteamento e a largura de banda necessária para um aumento da quantidade das novas VPNs MPLS [62].

- ✓ Adicionando novas VPNs e novos *sites* (CEs)

Para adicionar novos *sites* a uma VPN MPLS, será necessária a instalação de um CE no *site* do usuário e a configuração de uma conexão do roteador CE até a interface da VRF no roteador PE em que o CE será conectado. Para a operadora de telecomunicações, não será necessário modificar as configurações dos outros PEs onde estão conectados os outros *sites* da VPN, pois os roteadores PEs aprendem automaticamente sobre as rotas do novo *site*. Em relação à questão de adicionar nova VPN MPLS, isso não requer nenhuma mudança nas configurações das VPNs MPLS existentes. No entanto, em princípio, quando se adiciona um novo PE na rede MPLS para prover o serviço de VPN MPLS, todos os PEs existentes devem ser reconfigurados para reconhecer o novo PE. No entanto, esse problema poderá ser solucionado caso seja adotado o protocolo de distribuição de *labels* (LDP) entre os PEs [62].

- ✓ Escalabilidade do protocolo de roteamento

[14] Ps são roteadores do núcleo da rede MPLS.

O roteador PE deve manter uma conexão para troca de rotas com todos os *sites* a ele conectados. Quando essa capacidade do protocolo de roteamento chegar ao seu limite, um novo roteador PE deverá ser instalado na rede [62].

- ✓ Informações que devem ser mantidas nos roteadores PEs e Ps

Os roteadores Ps não participam do roteamento da troca de tráfego das VPNs. O tráfego da VPN é encaminhado através de um túnel MPLS entre os roteadores PEs e PEs. Sendo assim, os roteadores Ps não conhecem qualquer alteração que seja realizada nos *sites* da VPN. A única implementação que é realizada sobre os equipamentos Ps que está diretamente relacionada com as VPNs é o túnel PE a PE [62].

Os roteadores PEs mantêm o estado da tabela de rotas das VPNs dos *sites* que estão conectados a eles.

- ✓ Largura de banda para o transporte do tráfego da VPN

À medida que cresce o número de usuários e *sites* das VPNs, é necessário um aumento de banda da estrutura de transmissão do núcleo da rede MPLS para transportar esse acréscimo de tráfego das VPNs ou de *sites* por VPN [62].

6.4 **Escalabilidade do PE**

As propriedades físicas dos roteadores de borda (PE) da rede MPLS, como a capacidade de processamento da CPU, o tamanho da memória e o tempo de convergência dos protocolos de roteamento, em conjunto, definem a potencialidade do roteador PE para trabalhar com várias VRFs simultaneamente. Neste tópico, mostra-se como é possível expressar essa potencialidade em termos das VPNs MPLS.

A quantidade de interfaces físicas e lógicas que um PE pode suportar é o primeiro fator importante para avaliar a escalabilidade de uma VPN MPLS, pois isso limita o número de VRFs

que um PE pode suportar. Pode existir situação em que a quantidade de VRFs seja menor que a quantidade de interfaces lógicas, o que leva os fornecedores de PE a especificarem duas características básicas, que são as quantidades de VRFs e as quantidades de rotas por VRF. A quantidade de rotas por VRF depende do protocolo de roteamento que está configurado entre o CE e o PE. A quantidade de rotas suportada por VRFs de um PE que está conectado ao CE através de RIP, por exemplo, é menor que a quantidade de rotas por VRFs se o protocolo de roteamento entre CE e PE for rota estática.

As propriedades da escalabilidade dos roteadores PEs em uma rede MPLS determinam o tráfego suportado por ela para o transporte dos serviços das VPNs MPLS. Esse tráfego é função da arquitetura de rede, mais precisamente, do número de PEs instalados. A questão fundamental para um provedor que deseja prestar um novo serviço de VPN MPLS, por exemplo, TVIP, é descobrir se os atuais PEs da rede MPLS suportarão os novos serviços [62].

Os fatores que mais influenciam a escalabilidade de um novo serviço são expressos em termos de [62]:

- ✓ Número de clientes: é o número total de VPNs oferecidas pelo provedor de serviço de VPNs MPLS para seus clientes;
- ✓ Número de acessos por VPN: é o número de acessos ou CEs da VPN MPLS que pertencem à mesma VPN;
- ✓ Número de rotas por equipamento CE: é o número de rotas injetadas pelos CEs na VPN.

Em relação ao projeto do núcleo de rede, existem dois parâmetros importantes [62]:

- ✓ O número de PE na rede: normalmente, o provedor inicia a oferta dos serviços de MPLS sobre uma rede com poucos PEs. A necessidade de expandir a rede com novos roteadores de bordas (PEs) cresce à medida que aumenta a demanda, a quantidade de clientes e os novos requisitos de SLAs. Quando a operadora possui

outras redes, como *frame relay*, que podem ser utilizadas como forma de acesso dos PEs, isso facilita a expansão do serviço de VPN MPLS para outras regiões, mesmo não possuindo PEs nessas regiões, pois é possível utilizar as redes tradicionais, como *frame relay*, para levar o serviço baseado em MPLS para seus clientes. Outra possibilidade natural é aumentar a quantidade de PEs na rede MPLS, levando para mais próximo dos usuários o protocolo MPLS. Normalmente, essa alternativa é escolhida somente quando a demanda justificar o investimento em novos PEs e as redes de acesso aos PEs mais próximos já estiverem saturadas, não apresentando alternativas senão a instalação de novos PEs. Normalmente, os PEs de grande processamento e memória são instalados nos grandes centros, que geram grande demanda de serviços, e os pequenos PEs são instalados nas pequenas localidades, onde existe baixa demanda por serviços.

- ✓ O número de interfaces em cada VRF é função principalmente da localização dos equipamentos de borda (PE) em relação à rede de acesso e da tecnologia utilizada na rede de acesso. O aumento do número de interfaces para as VRFs reduz o número total de VRFs requeridas através da rede.

A quantidade de interfaces das VRFs e roteadores de bordas (PEs) é o principal parâmetro que deve ser levado em consideração no momento de um projeto da rede MPLS em que o provedor pretende disponibilizar os serviços de VPN MPLS em grande escala.

O provedor, ao projetar sua arquitetura de rede MPLS para prover VPNs MPLS, deve primeiramente verificar onde está concentrado o maior potencial de futuros clientes da sua rede, para, a partir desse ponto, projetar onde instalar seus roteadores PEs. Muitos países têm a alta concentração econômica em um, dois ou três centros. Portanto, nesses centros, devem ser instalados os PEs em maior quantidade e com melhor capacidade de processamento e memória. No Brasil, podemos citar o caso da cidade de São Paulo, onde praticamente todo provedor de telecomunicação possui grande infraestrutura de PEs distribuídos pela cidade.

6.5 Proposta para a questão de escalabilidade

Neste tópico, são apresentadas duas propostas que têm como objetivo principal amenizar o problema de escalabilidade nas VRFs das VPNs MPLS configuradas nos roteadores PE. Para melhor compreensão da necessidade de escalabilidade do serviço de VPN MPLS, considere-se a necessidade de um determinado provedor de serviço de telecomunicação oferecer uma solução para três empresas de cartão de créditos e débitos que pretendem disponibilizar para os estabelecimentos comerciais transações financeiras. A figura 6.7 apresenta três clientes, sendo que dois deles já possuem VPN MPLS (VPN 1 e VPN 2) para uso corporativo e o outro ainda não possui VPN. Todos os clientes precisam ter acesso às VPNs das Bandeiras A, B e C. É importante observar que todos os *sites* conectados a cada VPN já possuem conectividade natural, pois estão na mesma VPN, como foi descrito e avaliado no capítulo anterior.

Também é possível verificar que os usuários dos estabelecimentos comerciais com um único *site* e que não têm VPN (por exemplo, as lojas com um único ponto comercial), mas precisam se conectar às Bandeiras de cartões. Esse cenário de um estabelecimento com um único *site* necessitando conectividade com vários provedores de conteúdo está se tornando uma situação comum. Esse caso deve ser avaliado com cuidado, pois impacta fortemente na escalabilidade. Como já mencionado anteriormente, a possibilidade de criar VPNs por *sites* está fora do escopo das operadoras de telecomunicações atualmente. Portanto, uma alternativa deve ser desenvolvida. As principais premissas utilizadas nas propostas apresentadas a seguir são:

- ✓ Usuários que já têm implementadas suas VPN corporativas (por exemplo, VPN 1 e VPN 2) e precisam conectar-se às Bandeiras de cartões. Hoje, basicamente todas as VPNs *intranet* têm a necessidade de conectar-se a grandes bases de conteúdos, como as empresas de cartões de créditos. Para essa situação, onde as empresas já possuem a VPN, ou seja, já possuem um RD identificando a sua VPN, a solução mais imediata é configurar as rotas de importação e exportação nas VPNs de conteúdos para esse RD.

- ✓ Usuários com um único *site* e sem VPN, mas que desejam conectar-se com as VPNs das Bandeiras de cartões;
- ✓ As operadoras do serviço de VPN MPLS fornecem o serviço de VPN MPLS, sendo que o identificador das rotas (RD) é por VPN, e não por acesso/*site*. Isso significa que é configurado um único RD por VPN.

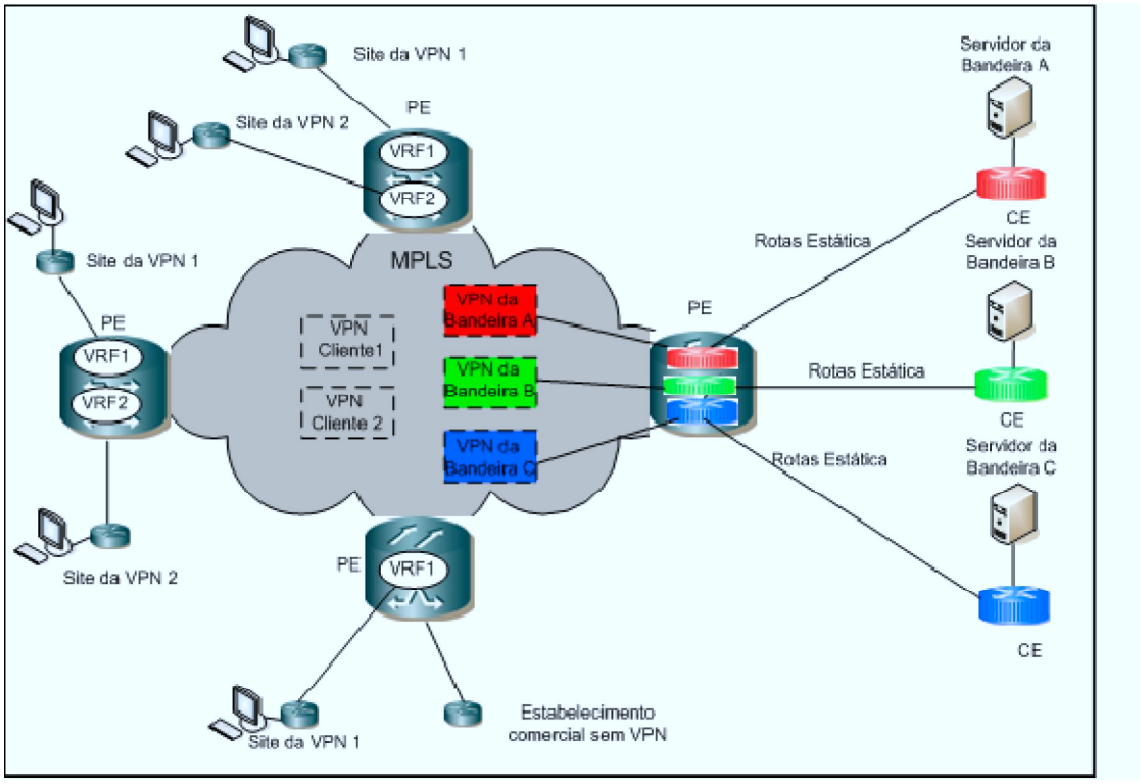

Figura 6.7 – Topologia para integração das VPNs.

A primeira proposta sugere a criação de um CVP (circuito virtual permanente) do estabelecimento comercial sem VPN até a VPN da Bandeira. Essa solução exige um CVP para cada Bandeira de cartão. Além da configuração do CVP para estabelecer a conectividade, é necessário configurar uma Lista de Controle de Acesso (ACL) para permitir que o acesso de um determinado estabelecimento possa ter conectividade somente com o servidor da Bandeira de cartão, impossibilitando a conectividade com outro estabelecimento indevidamente. Deve ser utilizado o protocolo de roteamento estático entre o CE e a VRF através de uma rota estática entre o endereço IP do CE e o IP do servidor da Bandeira.

Todos os estabelecimentos comerciais devem ser conectados na VRF da Bandeira, como mostra a figura 6.8. Como haverá vários acessos na mesma VRF de determinada bandeira e, conforme apresentado no capítulo anterior, na mesma VRF não é possível existir CE com os mesmos endereços IP, a solução proposta para resolver esse problema é a configuração da facilidade de NAT (*Network Address Translation*) no CE do estabelecimento.

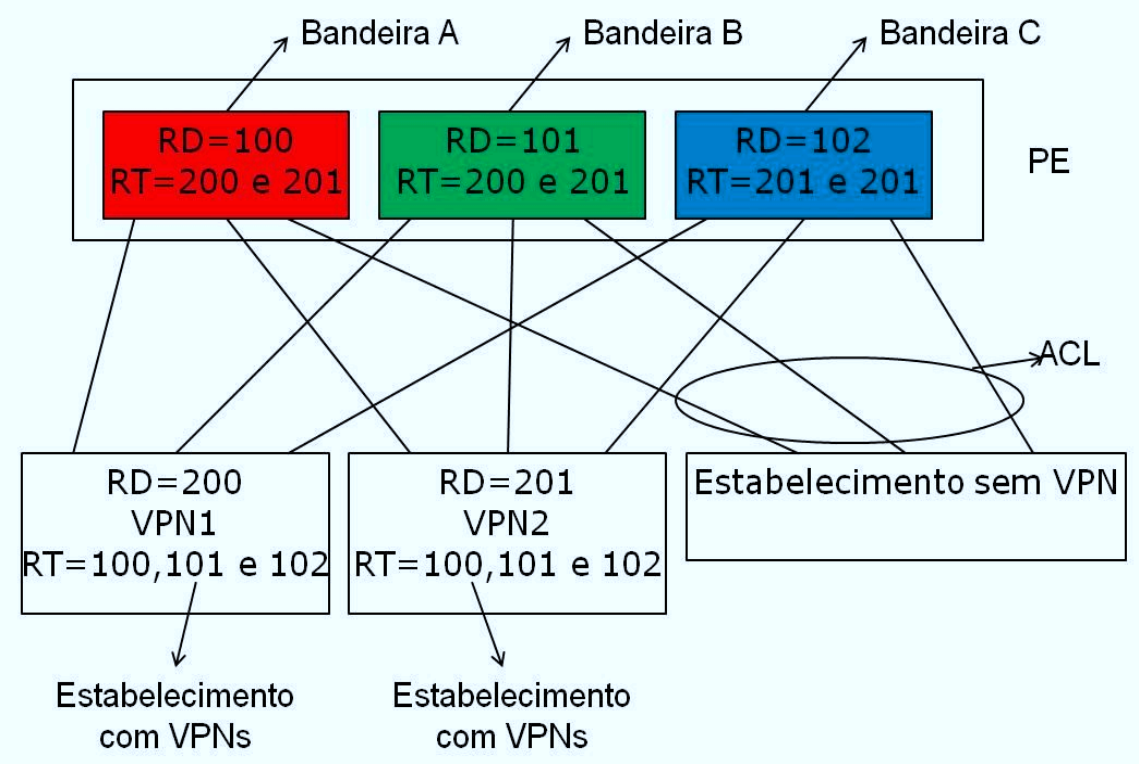

Figura 6.8 – Melhorando a escalabilidade através de ACL.

Para os estabelecimento que já possuem VPNs será configurado nas VPNs das Bandeiras apenas a importação e exportação de rotas, conforme mencionado no inicio do capítulo.

A figura 6.9 apresenta os pontos onde devem ser configurados os ACLs, os NATs e a implementação da figura 6.8.

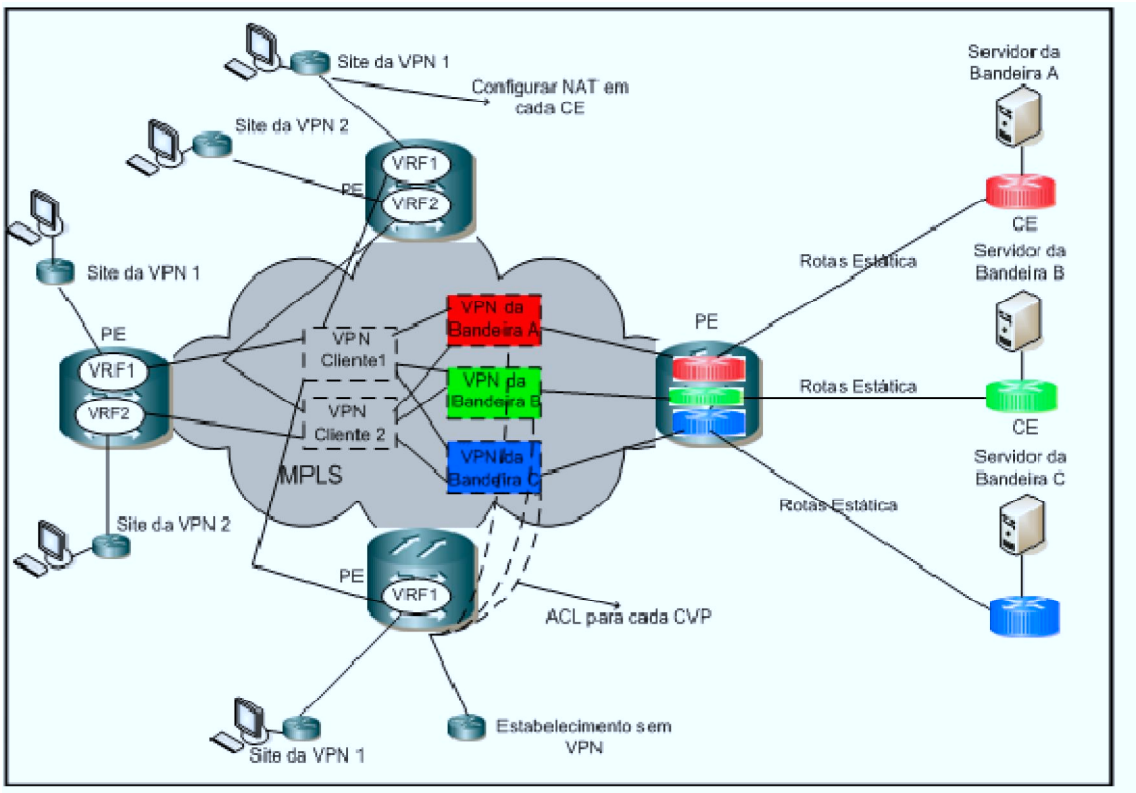

Figura 6.9 – Implementação a escalabilidade através de ACL.

A solução apresentada acima possui algumas limitações:

- ✓ O uso da funcionalidade de NAT minimiza a possibilidade de conflito de endereço IP, mas não consegue garantir absolutamente esse conflito em 100% dos casos, sobretudo quando existe uma grande quantidade de acessos às VRFs;
- ✓ A necessidade de habilitar um CVP e um ACL para cada bandeira com que o estabelecimento tenha interesse em conectar-se faz com que a solução perca um pouco da escalabilidade.

Em função das limitações apresentadas por essa alternativa, é sugerido o uso de um *firewall* externo, que é descrito a seguir. Deve ser implementada uma política de segurança no CE que restrinja o acesso apenas aos servidores de conteúdo.

Agora, com a nova proposta, cada VPN corporativa ou acesso sem VPN precisa somente de uma conexão ao *firewall*, que é conectado a todas as VPNs dos conteúdos. Esse procedimento

aumenta a escalabilidade, pois diminui consideravelmente a quantidade de configuração necessária. A nova proposta sugere a utilização da funcionalidade de *virtual context* ou *virtual systems*.

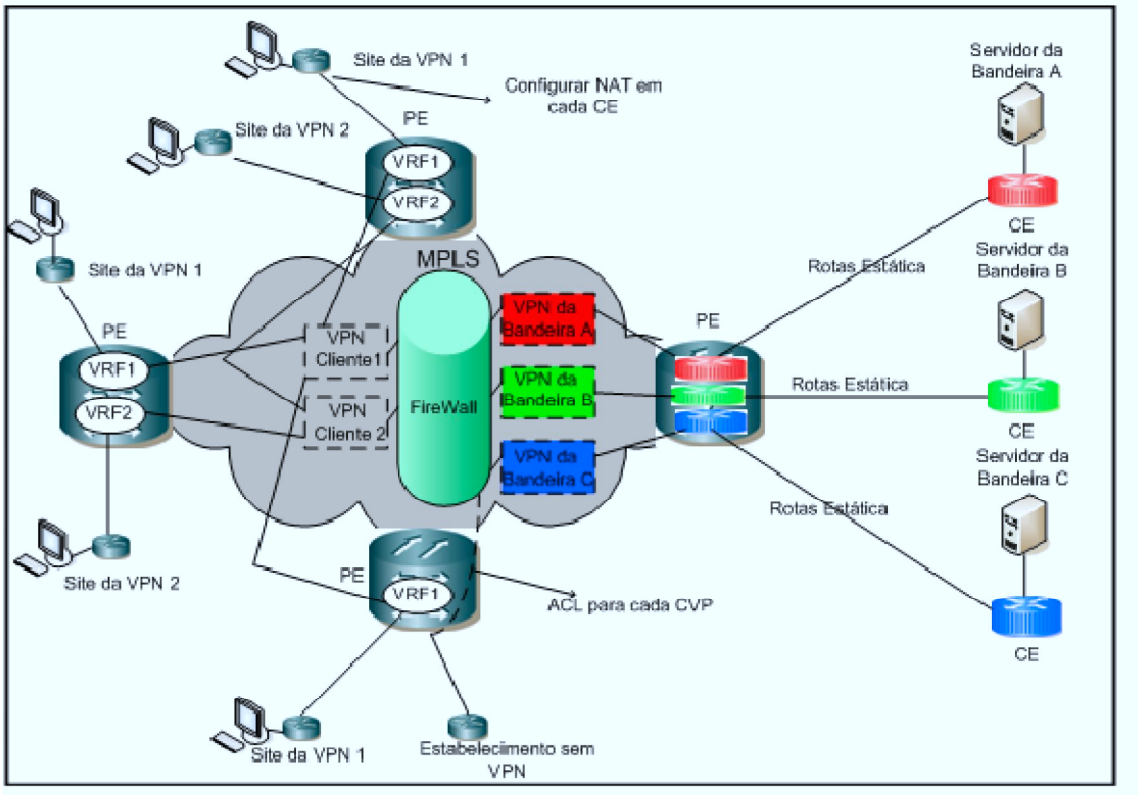

Figura 6.10 – Aumentando a escalabilidade com o uso de *firewall*.

6.6 Solução proposta para erros de configurações cometidos pela operadora

As VPNs MPLS oferecem alto nível de segurança, mas não permitem confidencialidade na rede. Quando existe, por parte do usuário do serviço, uma desconfiança do serviço oferecido pela operadora de telecomunicações, é sugerida a utilização do IPSec sobre MPLS.

A utilização de VPNs MPLS com IPSec é indicada para o usuário que, além de contar com a facilidade oferecida pelas VPNs MPLS, tem necessidade de certificar-se de que seus dados são inalterados dentro da rede da operadora quando esta comete algum erro de configuração

[63]. Por exemplo, no momento de ativar um novo *site* na VPN 100 de um cliente X, o técnico comete um erro de configuração e configura esse acesso na VPN 101 de cliente Y.

As possibilidades de implementação de IPSec sobre as VPNs MPLS são [63,65]:

- ✓ Implementação de IPSec somente no enlace entre o CE e PE;
- ✓ Implementação de IPSec somente entre os PE-PE;
- ✓ Implementação de IPSec fim a fim, ou seja, os dados são criptografados no primeiro CE e descriptografados no último CE.

A figura 6.11 apresenta as três formas de implementar IPSec sobre VPNs MPLS. Os conceitos básicos de IPSec já foram abordados no capítulo 3.

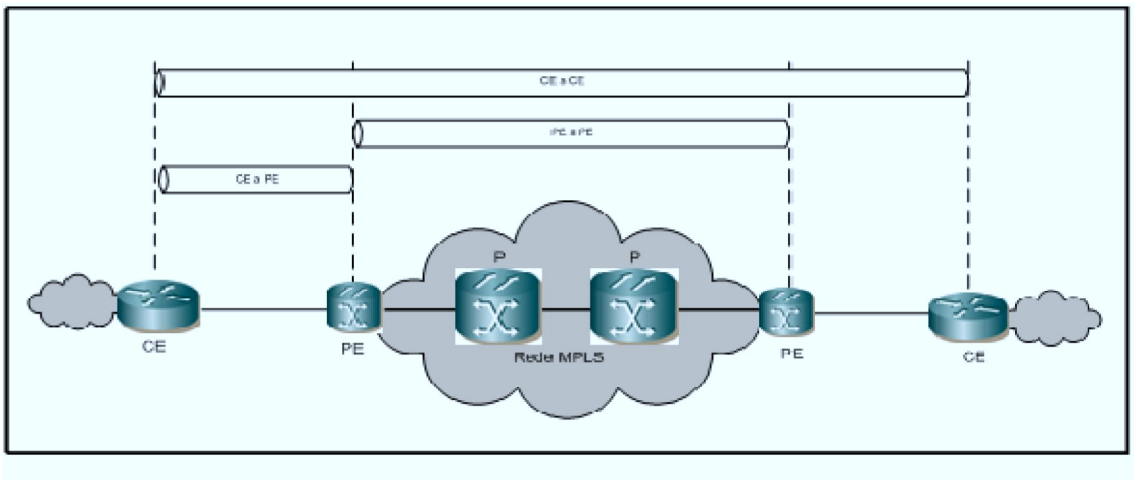

Figura 6.11 – Formas de implementar IPSec sobre MPLS, extraída de [63].

A escolha de um modelo em detrimento do outro normalmente está relacionada ao fato de a operadora de telecomunicações possuir o controle do CE ou não. Caso a operadora já possua o controle do CE, não tem sentido implementar IPSec sobre MPLS de CE a CE [63].

De modo geral, a implementação de IPSec sobre MPLS está vinculada às seguintes necessidades [63]:

- ✓ Autenticação dos roteadores CE fornece criptografias fim a fim entre os roteadores CE-CE da VPN, não sendo possível inserir outro CE, mesmo o núcleo da operadora sendo não seguro.

- ✓ Criptografias de partes ou de todo o tráfego que passará sobre a VPN MPLS. Se um atacante acessar o núcleo MPLS, ele não poderá ver os dados da VPN criptografados.
- ✓ A integridade dos dados não deve ser alterada quando em trânsito na rede.

6.6.1 IMPLEMENTANDO IPSEC NO ENLACE CE-PE

Essa solução implementa um túnel IPSec entre o roteador do ambiente do usuário (CE) e o roteador da borda da rede do provedor (PE). Em função de o túnel iniciar no CE e terminar no PE, a confidencialidade dos dados fica restrita a esse trecho. Esse tipo de implementação é muito comum em solução em que é necessário um *backup* para o roteador CE. Ou seja, é implementada no roteador CE uma conexão dedicada ao roteador PE e uma conexão discada (*dial*) *backup* para o PE. A figura 6.12 mostra o modelo de túnel entre o CE e PE [63].

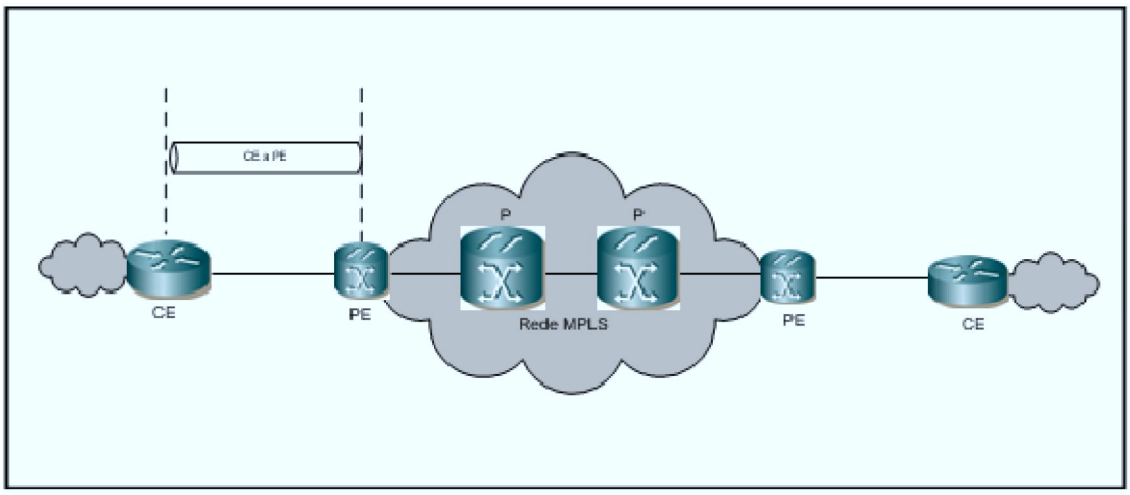

Figura 6.12 – Formas de implementar IPSec sobre CE e PE, extraída de [63].

Nas formas de acessos convencionais que utilizavam as tecnologias de acesso fixa, não havia muita preocupação do usuário com a segurança, pois a conexão entre o CE e PE era realizada com meios de comunicações exclusivos. Com as novas formas de VPNs móveis, esse trecho da VPN passa a merecer cuidados adicionais, pois o meio deixa de ser dedicado e passa a ser compartilhado.

6.6.2 IMPLEMENTAÇÃO DE IPSEC ENTRE PE-PE

Nesse modelo de implementação apresentado na figura 6.13, é realizado um túnel IPSec entre os roteadores PE-PE. Esse é um modelo de implementação transparente para o usuário, pois o túnel inicia no primeiro PE da rede e termina no último PE da rede.

Essa solução protege o núcleo da rede, dando uma falsa impressão de que a principal falha de segurança em uma solução de VPN MPLS ocorre no núcleo da rede, mas na prática isso não é verdade, pois é mais fácil um ataque ocorrer no acesso local a partir do CE do que no núcleo da rede, onde o provedor tem o total controle. Portanto, se o objetivo é construir VPN altamente segura, a utilização de túneis IPSec somente entre os PEs não é recomendada, pois o enlace entre CE e PE está sem nenhum tipo de segurança específica. A utilização de IPSec entre PEs oferece segurança adequada para as seguintes ameaças [63,65]:

- ✓ Ameaças oriundas da *internet* quando o provedor MPLS possui conectividade com a *internet*;
- ✓ Falhas nos roteadores Ps que poderão levar os pacotes a uma alteração ou encaminhamento para o PE errado no final do túnel.

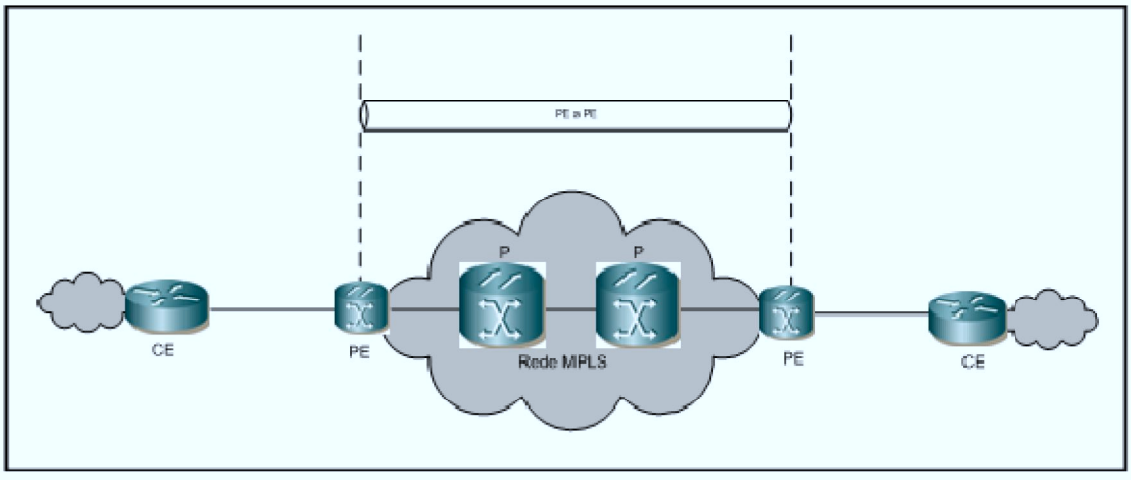

Figura 6.13 – Formas de implementar IPSec sobre PE a PE, extraído de [63].

Esse modelo de implementação não é comum em provedor de serviço de VPN MPLS. Em pesquisa junto aos provedores de serviços, não foi possível identificar algum provedor que

utilize somente IPSec entre PEs no Brasil. O IPSec entre PEs é uma boa alternativa quando operadoras distintas precisam realizar interconexão entre suas redes e pretendem garantir a segurança de seus PEs.

Nos Estados Unidos, os provedores têm usado interligação das redes MPLS para permitir que acessos de uma VPN de um determinado provedor possam conectar-se aos acessos da VPN de outra ILEC. Nesse caso, IPSec entre PEs garante segurança no núcleo da rede de cada operadora [63].

Na Europa, a utilização de IPSec entre PEs ficou restrita às redes governamentais, que, em função da necessidade dos governos de construir suas próprias redes MPLS e garantir segurança dos equipamentos PEs, implementaram IPSec entre eles. Nessas implementações de redes MPLS privadas, os PEs eram instalados nos próprios edifícios do governo. Nesse modelo de implementação, as conexões aos PEs da rede MPLS são realizadas somente por órgãos de governo, o que as diferencia de uma rede MPLS pública, em que as conexões aos PEs podem ser realizadas por qualquer usuário que contrate o serviço. No entanto, os Provedores de Serviços públicos de MPLS não implementam esse modelo em seu núcleo de rede, uma vez que ele não representa segurança fim a fim da VPN MPLS para seus clientes. Quando há a necessidade de segurança fim a fim (CE a CE), o modelo adotado é IPSec entre CEs sobre MPLS. Esse modelo é tratado a seguir [63,66].

6.6.3 IMPLEMENTAÇÃO DE IPSEC ENTRE CE-CE

Quando é utilizado o modelo de IPSec entre os roteadores CE, todo o caminho entre eles é protegido, ou seja, o acesso (conexão do CE com o PE), assim como todo o núcleo da rede, que é constituído de roteadores PEs e Ps. A solução de IPSec sobre MPLS de CE a CE é sugerida para casos em que a estrutura da rede de acesso e núcleo não é confiável. Os principais motivos que levam à utilização de IPSec sobre MPLS CE a CE são [63,66]:

- ✓ Quando o usuário exige que todo o tráfego seja protegido desde o seu CE até o outro CE de destino. Isso inclui as linhas de acesso que conectam o CE do usuário

até o PE da borda do núcleo da operadora e as linhas de transmissão do núcleo da rede MPLS que interliga os PEs e Ps.

- ✓ O usuário não confia no provedor de serviço da VPN MPLS. Como já mencionado na solução padrão de VPN MPLS, o usuário deverá confiar no provedor do serviço, pois todas as configurações relacionadas com a VPN são realizadas pelo provedor. O provedor pode fazer uma configuração errada de um *site* em uma VPN indevida, permitindo que esse *site* tenha acesso completo a uma VPN indevida.

Portanto, quando o usuário não confia no provedor de serviço, é sugerido que seja configurado IPSec de CE a CE com os dados criptografados. A figura 6.14 apresenta o modelo de implementação.

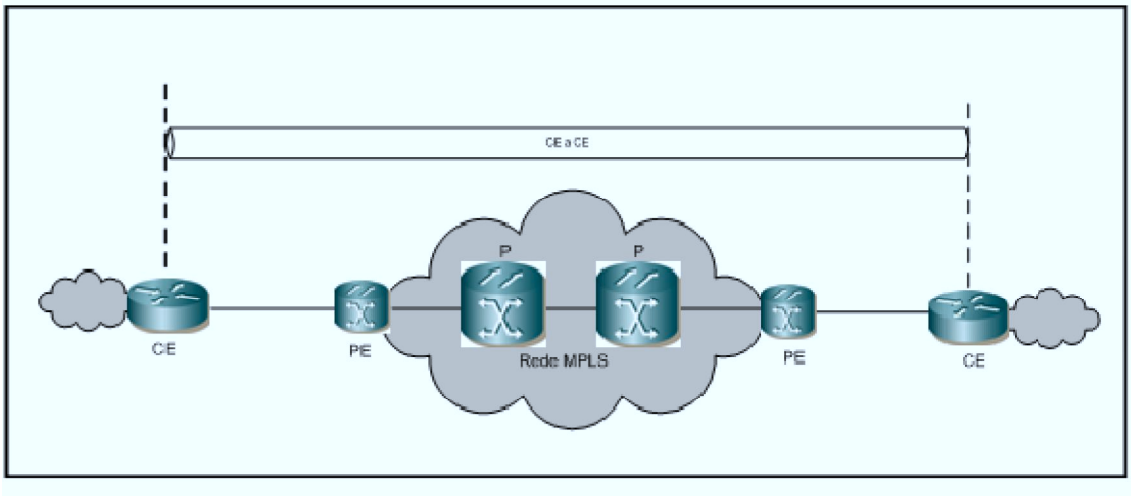

Figura 6.14 – Formas de implementar IPSec sobre CE e CE, extraído de [63].

Alguns cuidados devem ser levados em consideração na implementação do tunelamento IPSec clássico sobre uma rede MPLS que necessita qualidade de serviço (QoS), pois os roteadores dentro da rede MPLS (os PEs) têm visibilidade apenas do campo DSCP dos equipamentos que fazem as terminações dos túneis. Portanto, caso o usuário tenha interesse de

trafegar voz sobre a VPN MPLS, deverá ser realizada uma avaliação em conjunto com o provedor da VPN MPLS quanto ao modelo de segurança a ser adotado.

As questões relacionadas à escalabilidade das VPNs MPLS foram avaliadas no capítulo 6, principalmente as relacionadas diretamente com o roteador PE. Devido aos limites de processamento e memória dos PEs, existe um limite da quantidade de VRFs que é possível implementar no mesmo equipamento. Em função da escalabilidade, é recomendável a utilização de um identificador por VPN, e não por *site*. Essa recomendação é viável quando a necessidade é somente a formação de *intranet*, pois não existe problema de um *site* conectar-se ao outro. Quando a necessidade é a formação de *extranet*, existe a solução de um RD por *site*, que, mesmo sendo possível tecnicamente, não é a indicada porque diminui a escalabilidade das VPNs MPLS. Devido a esse problema, foram propostas algumas alternativas para permitir a formação de *extranet* mantendo a alta escalabilidade das VPNs MPLS. Também foi proposta, no final do capítulo, a utilização de IPSec para aquelas VPNs MPLS em que o usuário não confia no provedor. Foi possível concluir, nesse capítulo, que as operadoras devem implementar arquiteturas de *firewalls* para a formação de *extranet* caso queiram manter a alta escalabilidade das redes MPLS.

Capítulo 7

Conclusão e trabalhos futuros

7.1 **Conclusão**

O trabalho mostrou a potencialidade das redes banda larga para a formação de redes virtuais privadas com escalabilidade, qualidade de serviço e segurança. Para alcançar esses objetivos, foi necessária a implementação de VPNs que utilizam várias tecnologias de acessos banda larga e o MPLS no núcleo da rede.

O maior problema que prejudica a escalabilidade das VPNs MPLS é a formação de *extranet*. Para resolver esse problema, foram propostas algumas implementações. A primeira implementação foi criar VRFs por *site*, e não por VPN. Essa primeira proposta não resolveu o problema de escalabilidade, então, foi sugerida uma segunda contribuição para resolvê-lo. A segunda proposta é uma combinação da criação de VRFs por VPNs em conjunto com a facilidade de ACL para os *sites* sem VPNs. Essa solução melhorou o item de escalabilidade, mas aumentou a probabilidade de conflitos de endereços IP. Para resolver esse novo problema, foi sugerida uma terceira proposta, que é a implementação de *firewall* baseada em contexto virtual.

Para a qualidade de serviço (QoS), foi implementado um mecanismo baseado em DiffServ/MPLS e posterior avaliação, com maior ênfase nos parâmetros *jitter* e perdas de pacotes. Os resultados dos testes mostraram que o mecanismo adotado funcionou adequadamente, de acordo com a priorização adotada para as classes de serviços.

O requisito segurança das VPNs MPLS foi avaliado, podendo-se concluir que os *sites* das VPNs MPLS são totalmente isolados entre VPNs distintas e totalmente conectáveis dentro da mesma VPNs. Essas considerações são válidas, desde que as operadoras façam as configurações devidas das VPNs. Para resolver essa dependência do usuário em relação à configuração correta pela operadora, propõe-se utilizar IPSec sobre MPLS. Porém, cuidados devem ser levados em consideração quando o tráfego for o de voz, pois, em princípio, IPSec sobre MPLS levará à perda de qualidade de serviço.

7.2 **Trabalhos futuros**

A tendência é a utilização das redes banda larga como forma de acesso para todos os serviços, assim como foi demonstrado com ADSL e *frame relay* no capítulo 2, onde foi avaliada a necessidade de banda para essas tecnologias para o transporte de voz. Um dos trabalhos para o futuro será a avaliação das necessidades de banda para o transporte dos vários aplicativos das tecnologias de acesso, como 3G, *metroethernet* e *WiMax*.

A tecnologia *metroethernet* está em processo de implementação no Brasil e em muitos países. As questões relacionadas diretamente com a qualidade de serviço sobre acesso *metroethernet* devem ser avaliadas com critérios bem específicos, de acordo com a aplicação do usuário.

Todas as operadoras de telecomunicações hoje colocam como pré-requisito que, no momento da contratação do serviço, o usuário contrate ao menos 25% da classe de dados sem

prioridade (*best effort*), ou seja, somente é garantido a QoS no máximo de 75% da banda contratada. Diante desse cenário, um trabalho para o futuro poderá ser analisar o porquê desse limite de no máximo de 75% da QoS.

Existe uma tendência natural de as empresas de telecomunicações interligarem suas redes MPLS que hoje ainda estão isoladas. Portanto, um importante estudo para o futuro será a avaliação da segurança e da qualidade de serviço entre redes MPLS de operadoras distintas.

A tendência no futuro é que os *backhauls* trabalhem com a tecnologia MPLS; assim, um grande ganho em relação à eficiência de transmissão entre as BSs e BSC será levar o protocolo MPLS até a estação BS.

Atualmente, as empresas têm trabalhado com sobredimensionamento de tráfego no núcleo da rede, mas, em função das novas aplicações que estão gerando novos modelos de tráfego, faz-se necessária a implementação de engenharia de tráfego no núcleo da rede, e essa é uma das facilidades do MPLS que podem ser explorada no futuro.

Tradicionalmente, o transporte de *broadcast* de TV entre estúdio/estúdio e estúdio/*head end* tem sido implementado através das tecnologias SDH, PDH ou ATM. Entretanto, há um grande interesse de migração para MPLS. *Broadcast* de TV sobre MPLS é uma das principais aplicações em tempo real e será uma tendência sobre as redes MPLS. Esse tipo de aplicação não pode ser confundido com *video streaming*, que normalmente envolve a transmissão de *streams* para o usuário final, sem nenhuma preocupação com a qualidade de serviço.

Referências Bibliográficas

[1] Joseph,Ghetie, " Fixed-Mobile Wireless Networks Convergence – Technologies, Solutions, Services" , Cambridge, University Press, 2008.

[2] Plano Geral para atualização da Regulamentação das Telecomunicações no Brasil, Brasília, 17 de junho de 2008. - http://www.anatel.gov.br/Portal/exibirPortalInternet.do, acessado em 05/05/2011.

[3] O desempenho do Setor de Telecomunicações no Brasil – Séries Temporais. – 2009. – Março de 2010. - http://www.telebrasil.org.br/, acessado em 05/05/2011.

[4] Estudo técnico para atualização da regulamentação das telecomunicações no Brasil, Brasília, abril de 2008. – http://www.anatel.gov.br, acessado em 05/05/2011.

[5] James F. Kurose e Keith W. Ross. – Redes de Computadores e a *Internet*., 5ª edição,2010.

[6] Barometro Cisco/IDC de Banda larga –Dezembro de 2008, OCDE, Booz & Company e ITU/2009.

[7] Cisco – Revista Veja – 16/09/2009.

[8] Nortel Networks, White Paper, Benefits Of Quality of Service in 3G wireless *internet*,2001.

[9] Viterbi, J. Andrew, "Wireless Communications", Prentice Hall Signal Processing Series, 1998.

[10] Davie, Bruce and Y.Rekhter "MPLS Technology and Applications" Morgan Kaufmann Publishers, 2000.

[11] Marcos A. de Siqueira, Marcel C. de Castro, Emílio T. Nakamura, Analysis of securit aspects of the VPNs MPLS,Unicamp,2003.

[12] Vasconcellos, Saulo Vaz; Provisionamento de Recursos e QoS em redes de Núcleo para sistemas de 3ª Geração, Tese – Universidade Federal do Rio de Janeiro,2002.

[13] Sabri M. Hanshi, Wajdi Al- Khateeb, “Enhancing QoS protection in MPLS networks”, 2010 Second International Conference on Network Applications, Protocols and Services, IEEE,2010.

[14] Hung-shih Chueh, Kuochen Wang, “An All-MPLS Approach for UMTS 3G Core Networks”, IEEE, 2003.

[15] Sasan Adibi, Shervin Erfani, “MOBILE-IPV6 MPLS OAM REQUIREMENTS”, IEEE, 2005.

[16] Tingzhou Yang, Dimitrios Makrakis, “Hierarchical Mobile MPLS: Supporting Delay Sensitive Applications Over Wireless *Internet*”, IEEE 2001.

[17] Ravi Bhagavathula, Nagaraja Thanthry, Dr. Ravi Pendse, “Mobile IP and Virtual Private Networks”, IEEE 2003.

[18] Rong Ren , Deng-Guo Feng, KE MA, “A DETAILED IMPLEMENT AND ANALYSIS OF MPLS VPN BASED ON IPSEC” , IEEE 2004.

[19] Cecilio, L. Edmundo, “Acesso residencial em banda larga”, Universidade Federal do Rio de Janeiro, Mestrado em informática,2000.

[20] A tecnologia xDSL, http://ensino.univates.br/~laschneiders/Rede/a_tecnologia_xdsl.html, acessado em 14/05/2011.

[21] Fernandes, A. Eduardo, “Estudo comporativo: DSL x Cable Modem, Universidade Federal do Rio Grande do Sul, Curso de bacharelado em ciência da computação, 1999.

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

[23] Wang, Xuepu, “ Seamless Mobile VPN data solution for *Wimax*”, GSG Technical Journal,2006.

[24] Figueiredo, L. Fabricio, “ Fundamentos da tecnologia *WiMax*”CPqD, Telecom & IT Solutions,2005.

[25] Nassif N Lilian, João Pinheiro. “*Internet* via Satélite: as expectativas da comunicação em banda larga e as implicações tecnológicas”,2001.

[26] MONTGOMERY, John. The Oriting Internet: Fiber in the Sky. BYTE Magazine,Nov. 1997.

[27] Rochol, Jurgen, Apostila de rede de computadores, grupo de rede de computadores da UFRGS, Porto Alegre,2001.

[28] Sauter, Martin, “Beyond 3G – Bringing Networks, Terminals and the Web Together”, John Wiley & Sons Ltda, first published,2009.

[29] Draft-Martini “*Frame Relay* Encapsulation over Pseudo-Wires”, http://tools.ietf.org/html/draft-martini-frame-encap-mpls-0, acessado em 15/05/2011.

[30] Zhuo (Frank) Xu/Alcatel –Lucent, Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services,2010.

[31] Promom, Business & Technology Review, “Gigabit Ethernet, o fim do gargalo nas redes de telecomunicações”, 2005

[32] IEEE 802.17 Resilient Packet Ring Working Group, http://www.ieee802.org/17/, acessado em 15/05/2011.

[33] Next Generation SDH, http://www.ng-sdh.com/, acessado em 15/05/2011.

[34] NG SDH Forum, http://www.ng-sdh.com/ng-sdh-forum/, acessado em 15/05/2011.

[35] Cisco, www.cisco.com, acessado em 10/05/2011.

[36] Calculadora Cisco – Voice Codec BandWidth Calculator, http://cisco.com/suport/vbc/do/codecCalc1.do

[37] Cisco Systems, “Cisco AVVID Network Infrastructure Enterprise Quality of Service Design”, 2002.

[38] White Paper “Converged IP/MPLS Backbone Networks for 2G and 3G voice services integration, Cisco Systems, 2006.

[39] Douglas Hunt, Luyuan Fang, “IP/MPLS in the Mobile Radio Access Network (RAN), An IP/MPLS Forum Sponsored Tutorial, 2009

[40] Juniper Networks “Mobile Backhaul Reference Architecture”, 2011.

[41] Strategic White Paper, “Deploying IP/MPLS in Mobile Networks”, Alcatel-Lucent, 2008.

[42] H. Vincent Poor, Gregory W. Wornell, “Wireless Communications”, Prentice Hall Signal Processing Series,1998.

[43] Ina Minei, Julian Lucek, MPLS-Enabled Applications, John Wiley & Sons Ltd, 2005

[44] Davie, Bruce and Y.Rekhter “MPLS Technology and Applications”, 2001

[45] Shneyderman, Alex;Casati, Alessio; Mobile VPN - Delivering Advanced Services in Next Generation Wireless Systems; Wiley Publishing, Inc; 2003.

[46] Abreu, H. Luiz, “Arquitetura MPLS para formação de VPN”, Uberlândia,2004.

[47] Boava. Adao; “Estratégia de Construção de VPN com qualidade de serviço”, Unicamp-Dissertação de mestrado, 2004.

[48] Magalhães, M. F.; Cardozo, Introdução à comutação IP por rótulos através de MPLS. Technical Report, UNICAMP/FEEC/DCA, Campinas, SP.2001

[49] RFC 4364 – “BGP/MPLS IP Virtual Private Networks”, http://www.ietf.org/rfc/rfc4364.txt

[50] Semeria, Chuck , “RFC 2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications, Juniper Networks,2000.

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

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

[53] Ruela, J. Carlos, “Algumas análises sobre mecanismos para prover qualidade de serviço em redes multimídia”, Dissertação de mestrado de 2006.

[54] Duarte H. Luciano; Menezes A. Amanda; Mendes Débora; Galdino S Juliano;Moura Shirley; “ Qualidade de Serviço e Experiência do Usuário”, www.teleco.com.br; acessado em 19/05/2010.

[55] RFC 3550, http://www.ietf.org/rfc/rfc3550.txt, acessado em 19/05/2010.

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

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

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

[59] http://sourceforge.net/projects/iperf/ developed by NLANR/DAST Luc De Ghein/Cisco Press, MPLS Fundamentals,2007

[60] Andrews, J.G;Ghosh, A; Muhamed,R. Fundamentals of *WiMax*; Understanding broadband wireless networking. Westford, 2007.

[61] Kelvin Lopes Dias & Dlamel Fauzi Hadj Sadok, “*Internet* Móvel: Tecnologias, Aplicações e QoS, UFPE,2003.

[62] Monique Morrow, Azhar Sayeed. “MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization”,2006.

[63] Michael H. Behringer, Monique J. Morrow. “MPLS VPN Security”, Cisco Press 2005.

[64] Apostila do laboratório de redes de computadores da USP, “Camada de rede TCP/IP”, Curso de especialização em telecomunicações – 2008.

[65] Yi Ji;Yaping Deng, “A scheme to enhance the security of BGP/MPLS VPN”. IEEE, 2006

[66] RFC - Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs) http://www.faqs.org/rfcs/rfc4381.html, /2010.

Apêndice A

IP Móvel

O IP móvel pode ser implementado através de vários mecanismos de tunelamentos, mas por si só não fornece um mecanismo específico. O IP móvel foi originalmente definido na RFC 2002, que mais tarde foi atualizada pela RFC 3220 para suportar mobilidade de *host* na camada de rede IP [60,61].

O IP móvel é uma proposta da IETF (*Internet Engineering Task Force*) como solução para prover mobilidade na camada de rede para os usuários móveis da *internet*. O IP Móvel permite que os usuários móveis continuem suas comunicações enquanto se locomovem de um ponto de acesso a outro na *internet* [61].

Assim como o L2TP (Tunelamento de nível dois), o IP Móvel provê um modelo de arquitetura que define as regras de diferentes entidades que podem ser envolvidas na operação do IP Móvel. O IP Móvel pode ser implementado através de três principais funções [60,61]:

- ✓ HA (*Home Agent*)
- ✓ FA (*Foreign Agent*)
- ✓ MN (*Mobile Node*)

O IP Móvel define duas entidades para prover o suporte à mobilidade: um HA (*Home Agent*) e um FA (*Foreign Agent*). O HA é atribuído estaticamente ao nó móvel (MN – *Mobile Node*) e baseia-se no endereço IP *home* permanente da estação móvel. O FA é atribuído ao nó móvel, baseando-se na localização atual da MN. O FA tem associado consigo um endereço IP chamado *Care-of-Address* (CA). Pacotes destinados para a MS são interceptados pelo HA, encapsulados e enviados para o FA usando o CA. O FA desencapsula os pacotes e encaminha-os diretamente para a MN. Portanto, o FA é a entidade IP mais próxima da MN [60,61].

A figura A.1 apresenta os elementos envolvidos na operação do IP Móvel, ilustrando o roteamento dos *datagramas* de um *host* IP, destinados a uma estação móvel que se moveu e não se encontra na sua HN (*Home Network*). Supõe-se que a estação móvel já tenha feito o registro com a FN (*Foreign Network*), obtido um CA (*Care-of Address*) e o tenha enviado para seu *home agent*. No passo 1, o *host* IP fixo envia o pacote da forma usual para a HN da estação móvel. O HA intercepta esse pacote e, sabendo que a estação móvel não está mais presente em sua HN, envia-o para o CA cedido à estação móvel pela FN (passo 2). No passo 3, o pacote é encaminhado para a estação móvel. Quando a estação móvel envia um pacote (passo 4), utiliza seu próprio endereço IP da HN no campo de fonte do cabeçalho IP e no campo de destino, o endereço do *host* IP. O roteador (no qual o FA está presente) age normalmente e encaminha o pacote da mesma forma que faria com qualquer outra estação pertencente à FN [60,61].

Apesar de não ter sido mostrado na figura A.1, após o passo 2, o HA pode informar ao host IP fixo como enviar pacotes diretamente para a estação móvel. Assim, caso o host IP fixo desejasse enviar mais pacotes, poderia enviá-los diretamente à estação móvel através do FA.

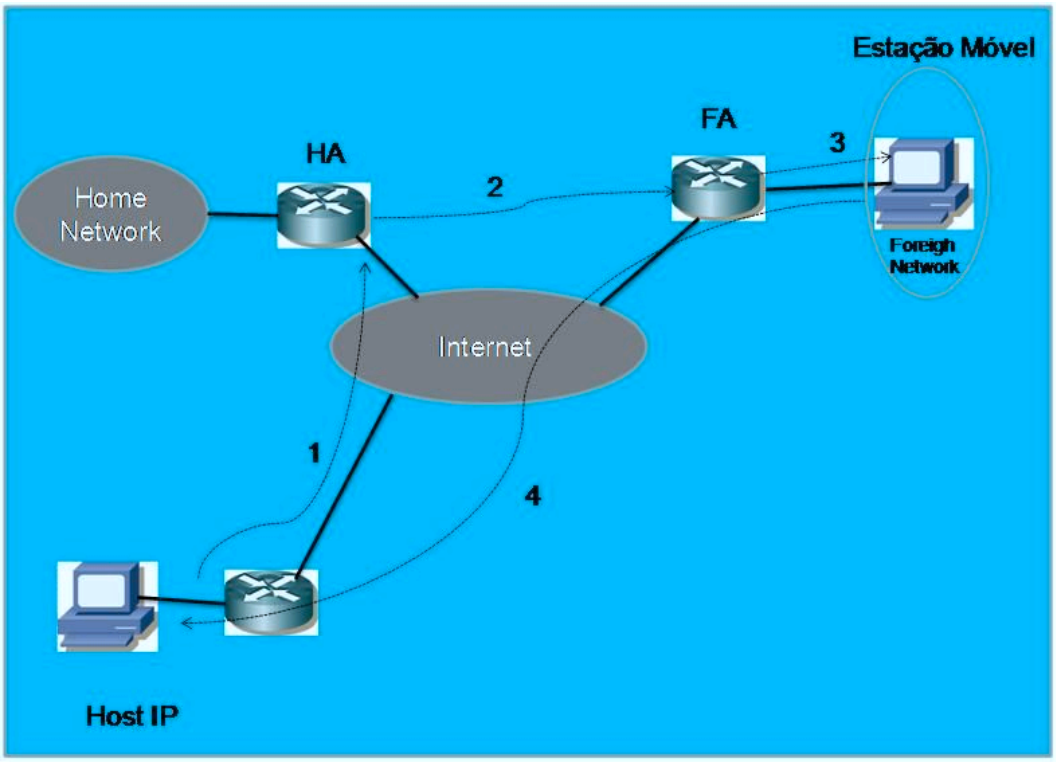

Figura A.1 – Roteamento do IP Móvel, extraído de [61].

Apêndice B

ICMPv4

O ICMP (*Internet Control Message Protocol*) é um protocolo obrigatório da camada de rede da arquitetura TCP/IP e serve para a transmissão de mensagens de erro, controle e obtenção de outras informações relacionadas à rede. Apesar de o ICMP ser um protocolo da camada de rede, ele utiliza os serviços do próprio IP para ser transmitido, sendo que, no campo Protocol do IPv4, o valor é 1, que é o número do ICMP. Se uma mensagem ICMP não pode ser enviada, não será gerada outra em seu lugar, evitando uma enchente de mensagens ICMP. Sua especificação encontra-se no RFC 792 – *Internet control message protocol* – DARPA *Internet program protocol specification* [64].

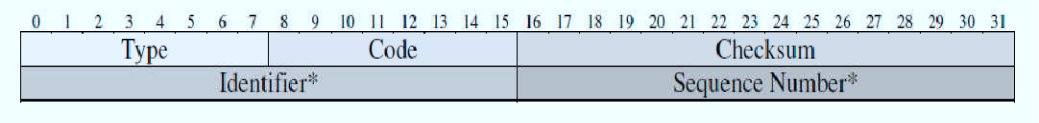

Figura B.1 – Especificação do ICMP (RFC – 792).

O formato do cabeçalho ICMPv4 é variável. Os campos marcados com "*" nem sempre estão presentes, e pode haver campos adicionais, para informar um *timestamp* ou o endereço de um *gateway*, por exemplo. Não serão apresentados aqui todos os formatos do ICMPv4.

Tabela B.1 – Tipo e código de mensagens ICMP, extraído de [64].

Tipo	Código	Significado
0	-	Echo Reply (Resposta a Eco) – Mensagem recebida de um *gateway* ou de um *host*. Um Echo Request foi recebido, e a mensagem de resposta deve conter os mesmos dados do Echo Request.
3	-	Destination Unreachable (Destino Inalcançável) – Mensagem recebida de um *gateway*. O endereço destino não pode ser alcançado por um dos motivos especificados pelo campo Code.
3	0	Network Unreachable (Rede Inalcançável) – Mensagem recebida de um roteador. Causa: o pacote foi descartado porque o roteador não conseguiu enviar o pacote para a rede destino, ou o roteador não possui uma rota para a rede destino, ou então o endereço de rede destino não existe.
3	1	Host Unreachable (Host Inalcançável) – Mensagem recebida de um roteador. Causa: a rede destino foi alcançada, mas não foi possível entregar o pacote para o *host* destino, provavelmente por causa de uma submáscara configurada erroneamente ou porque o *host* destino não está acessível.
3	2	Protocol Unreachable (Protocolo Inalcançável) – Mensagem recebida de um *host*. Causa: o *host* destino provavelmente não suporta o protocolo de camada superior especificado.
3	3	Port Unreachable (Porta Inalcançável) – Mensagem recebida de um *host*. Causa: o *socket* ou a porta TCP/UDP não estão disponíveis.
3	4	Fragmentation Needed and DF Set (Fragmentação Necessária e DF Setado) – Mensagem recebida de um *gateway*. Causa: o pacote possuía um tamanho maior que o MTU (Maximum Transmission Unit – Unidade Máxima de Transmissão) de alguma rede por onde ele tentou passar, necessitando então ser fragmentado, porém o *bit* Don't Fragment do IPv4 estava com

		valor igual a 1, indicando que o pacote não podia ser fragmentado. Como resultado, o pacote foi descartado.
3	5	Source Route Failed (Rota da Origem Falhou) – Mensagem recebida de um roteador. A rota especificada pela origem no campo Options do cabeçalho IP não pôde ser completada.
4	-	Source Quench (Estrangulamento da Origem) – Mensagem recebida de um *gateway* ou de um *host*. Quando um roteador ou um *host* está com seus *buffers* cheios e começa (ou está prestes) a descartar pacotes, essa mensagem é enviada para a origem, pedindo-lhe que pare de mandar mais pacotes. É um método de contenção de congestionamento. O roteador ou *host* continua mandando essa mensagem enquanto estiver com dificuldades em processar pacotes. A origem só volta a transmitir pacotes quando parar de receber essa mensagem.
5	-	Redirect (Redirecionar) – Mensagem recebida de um *gateway*. Nesse tipo de mensagem ICMP, há um campo extra, chamado Gateway *Internet* Address (Endereço *Internet* do Gateway), que especifica por qual *gateway* devem passar os datagramas para a rede destino do cabeçalho IP. Esse tipo de mensagem é recebido na situação a seguir: um *host*, H1, está diretamente conectado à rede de um *gateway*, G1. G1 recebe de H1 um datagrama, cujo destino é outro *host*, Hx, na rede X. Então, G1 consulta em sua tabela de roteamento e descobre que o próximo *gateway* na rota para a rede X é o *gateway* G2. Se G2 estiver na mesma rede que o *host* que originou o datagrama, G1 manda uma mensagem Redirect para o *host* H1, avisando-o que os próximos datagramas para a rede X devem ser encaminhados diretamente para G2. Se o *host* especificar uma rota para um determinado destino, mesmo que G1 conheça uma rota mais curta, a rota especificada será seguida e não será enviado um Redirect.

5	0	Redirect Datagrams for the Network (Redirecionar Datagramas para a Rede) – O *host* deve encaminhar os datagramas cujo destino é a rede X para um determinado *gateway*.
5	1	Redirect Datagrams for the Host (Redirecionar Datagramas para o Host) – O *host* deve encaminhar os datagramas cujo destino é o *host* Hx para um determinado *gateway*.
5	2	Redirect Datagrams for the Type of Service and Network (Redirecionar Datagramas para o Tipo de Serviço e Rede) – O *host* deve encaminhar os datagramas cujo destino é a rede X e que requerem o Tipo de Serviço T para um determinado *gateway*.
5	3	Redirect Datagrams for the Type of Service and Host (Redirecionar Datagramas para o Tipo de Serviço e Host) – O *host* deve encaminhar os datagramas cujo destino é o *host* Hx e que requerem o Tipo de Serviço T para um determinado *gateway*.
8	0	Echo Request (Pedido de Eco) – Mensagem recebida de um *gateway* ou de um *host*. O Echo Request é um datagrama enviado pelo comando *ping* (será explicado mais adiante) para testar se um destino é alcançável. Os dados enviados devem ser retransmitidos pelo destino para a origem.
11	-	Time Exceeded (Tempo Excedido) – O tempo de vida (TTL) de um pacote ou o tempo de remontagem de pacotes fragmentados foi excedido.
11	0	Time to Live Exceeded in Transit (Tempo de Vida Excedido em Trânsito) – Mensagem recebida de um *gateway*. Se o campo TTL de um datagrama chega a 0, ele deve ser descartado e o *host* que o originou deve ser notificado através de uma mensagem Time Exceeded tipo TTL Exceeded in Transit.
11	1	Fragment Reassemble Time Exceeded (Tempo de Remontagem do Pacote

		Excedido) – Mensagem recebida de um *host*. Se um *host* não receber todos os fragmentos necessários para a remontagem de um pacote dentro de um determinado tempo, os fragmentos são descartados e uma mensagem Fragment Reassemble Time Exceeded é enviada para o *host* de origem. Se o fragmento 0 não está presente, não é enviada a mensagem.
12	-	Parameter Problem (Problema de Parâmetro) – Mensagem pode ser recebida de um *host* ou de um *gateway*. Se um *gateway* não conseguir decodificar corretamente os campos de um datagrama e por causa disso ele precisar ser descartado, a origem é notificada através de uma mensagem Parameter Problem, indicando o campo com problema. Esse tipo de problema é mais frequente nos argumentos do campo Option do cabeçalho IP. Essa mensagem só é enviada caso o pacote precise ser descartado.
13	-	Timestamp (Marca de Tempo) – Possui um campo adicional de 32 *bits* informando o último momento (em ms contados a partir de meia-noite de Greenwich) no qual o 11 originador da mensagem mexeu nela. Se não houver sincronismo com o horário de Greenwich, ou se não for possível uma precisão com ordem de ms, o *bit* mais significativo desses 32 *bits* deve ser setado, indicando o uso de uma base de tempo diferente. O sincronismo pode ser feito com o NTP (Network Timestamp Protocol), RFC 1059 e RFC 1305.
14	-	Timestamp Reply (Resposta da Marca de Tempo) – Possui três campos adicionais de 32 *bits* informando o momento enviado pelo originador da mensagem, o instante no qual a mensagem foi recebida e o instante no qual ela foi enviada.
15	-	Information Request (Pedido de Informação) – Mensagem enviada por um *host*, com os campos origem e destino do cabeçalho IP iguais a 0 (significa "esta rede"). Esse é um modo de um *host* descobrir a qual rede ele

		pertence.
16	-	Information Reply (Resposta ao Pedido de Informação) – Mensagem enviada por um *host* ou um *gateway* quando eles recebem um Information Request. A mensagem Information Reply deve conter os endereços preenchidos corretamente. Os campos Identifier e Sequence Number são utilizados para associar corretamente uma Information Reply a uma Information Request.