Uma Arquitetura Baseada em Políticas para Gerência de VPNs de Camada 1

Neumar Malheiros[1], Edmundo Madeira[1], Fábio Verdi[2], Maurício Magalhães[2]

[1]Instituto de Computação – Universidade Estadual de Campinas (UNICAMP)
Caixa Postal 6176 – 13.083-852 – Campinas – SP

[2]Faculdade de Engenharia Elétrica e de Computação – UNICAMP
Caixa Postal 6101 – 13.083-970 – Campinas – SP

{ncm,edmundo}@ic.unicamp.br, {verdi,mauricio}@dca.fee.unicamp.br

Resumo. *Um plano de controle distribuído permite o aprovisionamento dinâmico de conexões em redes de transporte de camada 1, como redes ópticas ou redes TDM (Time Division Multiplexing). Dessa forma, essas redes podem oferecer serviços mais sofisticados, como serviços VPN de camada 1 (Layer 1 Virtual Private Network). Neste trabalho, propomos uma arquitetura baseada em políticas para a gerência de serviços VPN de camada 1 em redes com um plano de controle baseado na arquitetura GMPLS (Generalized Multi-Protocol Label Switching). Apresentamos também um protótipo implementado para validar a arquitetura proposta, assim como resultados de simulações.*

Abstract. *A distributed control plane provides dynamic connection control on layer 1 transport networks as optical and TDM networks. In this way, those networks can provide advanced connectivity services like VPNs. Such services are called Layer 1 VPN (L1VPN) services. In this work, we propose a policy-based architecture for L1VPN service management on GMPLS enabled transport networks. We also present a prototype implemented to validate the proposed architecture, as well as simulation results.*

1. Introdução

Em geral, as redes de transporte atuais apenas oferecem serviços estáticos de conexão ponto-a-ponto. O controle de tais conexões é realizado por sistemas de gerência centralizados e proprietários. Dessa forma, o aprovisionamento de serviços é lento e apresenta alto custo. Além disso, a operação dessas redes tem se tornado mais complexa, por causa de vários fatores como: o desenvolvimento de aplicações avançadas com severos requisitos de qualidade de serviço; o aumento da demanda por capacidade de transmissão; e a necessidade de funções avançadas de admissão de conexões, agregação de tráfego e gerência de falhas.

Para lidar com esses problemas, foi proposta a idéia de um plano de controle com uma arquitetura distribuída. As principais funções do plano de controle consistem no suporte ao aprovisionamento dinâmico de conexões, descoberta automática de recursos e suporte a mecanismos para recuperação de conexões afetadas por falhas. Uma proposta neste sentido é a arquitetura GMPLS (*Generalized Multi-Protocol Label Switching*) [Mannie 2004], desenvolvida pela *Internet Engineering Task Force* (IETF).

Esta arquitetura define mecanismos de sinalização e roteamento para o controle automatizado de conexões, considerando várias tecnologias de comutação. Esses mecanismos são baseados principalmente em extensões de protocolos utilizados em redes IP, como OSPF (*Open Shortest Path First*) e RSVP (*Resource Reservation Protocol*).

Assim, com um plano de controle GMPLS, redes de transporte de camada 1, como redes ópticas ou redes TDM (*Time Division Multiplexing*), podem oferecer serviços avançados de "conectividade", como serviços VPN (*Virtual Private Networks*). Estes serviços VPN são então denominados VPN de camada 1 (L1VPN – *Layer 1 VPN*) [Takeda et al. 2004a].

Entidades internacionais de padronização têm dispensado esforços na especificação desse serviço. A *International Telecommunications Union* (ITU) definiu conceitos e especificou cenários, requisitos de alto-nível e um modelo de referência para L1VPNs [ITU 2003], assim como funções e arquiteturas para o suporte a serviços L1VPN [ITU 2004]. No mesmo sentido, a IETF recentemente criou um grupo de trabalho cujo objetivo é especificar mecanismos para o aprovisionamento de serviços L1VPN em redes de transporte com um plano de controle GMPLS. As primeiras atividades deste grupo consistem em definir os requisitos e um *framework* para serviços L1VPN [Takeda et al. 2006a] e em analisar a aplicação de mecanismos e protocolos GMPLS no aprovisionamento desses serviços [Takeda et al. 2006b].

Serviços L1VPN possibilitam que a rede de transporte de um provedor seja compartilhada entre vários clientes. Esse serviço compreende um conjunto de funcionalidades que permitem um cliente "interconectar" suas redes, através do estabelecimento dinâmico de conexões de camada 1 na rede do provedor. O provedor deve oferecer a cada cliente certo nível de controle e gerência sobre seu serviço L1VPN. A questão é que a gerência sobre a operação de cada VPN deve ser independente das demais.

Entendemos que a abordagem de Gerência Baseada em Políticas (PBM - *Policy Based Management*) [Verma 2002] é uma solução adequada para atender esses requisitos. Neste artigo, propomos uma arquitetura baseada em políticas para a gerência de configuração de serviços L1VPN em redes com um plano de controle GMPLS. A arquitetura define, sob a perspectiva do provedor, como cada cliente pode criar políticas para configurar seu serviço L1VPN.

O artigo está organizado da seguinte maneira. Primeiro, apresentamos conceitos básicos sobre L1VPN e na seção seguinte, discutimos trabalhos relacionados. Na Seção 4, apresentamos uma adaptação do *framework* de políticas da IETF considerando a gerência de serviços L1VPN e também definimos classes de políticas pertinentes. A arquitetura proposta é então detalhada na seção 5, com a descrição de cenário de uso, módulos funcionais e implementação. Por fim, na Seção 6, são apresentados conclusões e trabalhos futuros.

2. Conceitos Básicos

Com um plano de controle distribuído, um provedor pode usufruir do controle automatizado de conexões de camada 1 para oferecer serviços de "conectividade" sob demanda para redes clientes. Neste contexto, o serviço L1VPN representa uma solução estruturada e flexível para uma organização compartilhar sua rede de transporte entre vários clientes ou entre vários de seus departamentos, que ofereçam diferentes serviços de rede.

Através do serviço L1VPN, um cliente pode alocar recursos da rede do provedor a fim de estabelecer conexões para interconectar as suas diversas redes locais, de acordo com uma topologia desejada. O cliente pode alocar os recursos de acordo com sua demanda de tráfego e o trabalho de operação e manutenção da rede de transporte fica a cargo do provedor.

A Figura 1 demonstra um modelo de referência para o serviço L1VPN, conforme apresentado em [Takeda et al. 2004a]. Um *Customer Edge device* (CE) é um nó da rede do cliente que está conectado à rede do provedor. Um *Provider Edge device* (PE) é um nó da rede do provedor ao qual pelo menos um CE está conectado. O PE provê serviços L1VPN para o CE. Um *Provider device* (P) é um nó do núcleo da rede do provedor que não está conectado a nós das redes clientes, mas somente a nós da rede do provedor. Neste exemplo a rede de transporte do provedor é compartilhada por dois clientes, A e B. A parte superior da figura mostra uma possível topologia para "interconectar" as redes do cliente A. As conexões da VPN estão representadas pelas linhas tracejadas entre os CEs.

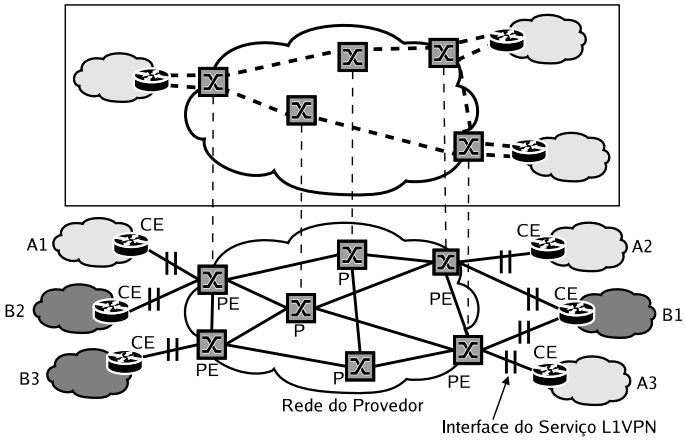


Figura 1. Modelo de referência para serviço L1VPN.

Um importante requisito do serviço L1VPN é que o cliente tenha certo nível de controle e gerência sobre sua VPN, incluindo a capacidade de reconfigurar sua topologia. Outro requisito é que a conectividade seja restrita aos membros de uma mesma VPN (*VPN membership*). Portanto, um CE que pertence a um cliente não pode estabelecer uma conexão com um CE que pertence a outro cliente.

O modelo funcional do serviço L1VPN é apresentado em [Takeda et al. 2004a]. São discutidas quatro categorias principais de funções: controle de informações sobre os membros da VPN; controle de informações de roteamento e cálculo de rotas; controle de conexões; e funções de gerência. É importante observar que apenas as funções relacionadas com a primeira categoria são específicas para serviços L1VPN. No entanto, as funções de roteamento, controle de conexões e gerência já presentes na rede do provedor precisam ser estendidas para suportar tais serviços.

Existem dois modelos de alocação de recursos para serviços L1VPN: compartilhado e dedicado. No modelo dedicado, recursos da rede do provedor são reservados exclusivamente para uma L1VPN. Esses recursos não podem ser alocados para nenhuma outra L1VPN. Por outro lado, no modelo compartilhado, os recursos são compartilhados no tempo e podem ser alocados por qualquer L1VPN.

Além disso, foram definidos três modelos de serviço L1VPN de acordo as características da interface do serviço [Takeda et al. 2006a]. No modelo baseado em gerência, as redes clientes acessam o serviço através de uma interface de gerência. Neste caso, não há transferência de mensagens de controle entre o cliente e o provedor. No modelo baseado em sinalização, existe uma interface no plano de controle entre o cliente e o provedor, mas as mensagens trocadas se restringem a mecanismos de sinalização. Por fim, no modelo baseado em sinalização e roteamento, a interface no plano de controle também provê funções de roteamento. Neste caso, um CE pode obter, via plano de controle, informações das redes clientes remotas que pertencem à mesma VPN ou até mesmo informações (resumidas) sobre a topologia da rede do provedor.

3. Trabalhos Relacionados

O trabalho apresentado em [Takeda et al. 2005] discute como os mecanismos da arquitetura GMPLS podem ser utilizados para implementar as funcionalidades do serviço L1VPN. Este trabalho primeiro descreve motivação e conceitos básicos do serviço L1VPN e então analisa a aplicação de mecanismos GMPLS no suporte a serviços L1VPN, considerando, principalmente, aspectos relacionados com endereçamento, descoberta automática de membros e sinalização de conexões. Além disso, são identificadas áreas de trabalho que exigem estudo adicional, como gerência de serviços L1VPN.

Mecanismos para aprovisionamento de serviços VPN em redes GMPLS são propostos em [Ould-Brahim 2005]. Este trabalho descreve o serviço denominado *Generalized VPN* (GVPN). O serviço GVPN utiliza o protocolo BGP (*Border Gateway Protocol*) para automatizar a descoberta de informações de membros de uma VPN (*VPN reachability auto-discovery*) e utiliza protocolos GMPLS para sinalização quando do estabelecimento de conexões.

O trabalho apresentado em [Swallow et al. 2005] descreve extensões a mecanismos de sinalização da arquitetura GMPLS para suporte a um cenário *overlay*, no qual as redes do cliente e do provedor executam diferentes instâncias do plano de controle e existe, portanto, uma interface para troca de mensagens de controle entre essas redes. As extensões propostas consideram o suporte a serviços VPN. Neste caso, as conexões VPN solicitadas pelos nós de borda da rede cliente podem ser estabelecidas através de um mecanismo de hierarquia de conexões [Kompella e Rekhter 2005]. A conexão VPN é "tunelada" através de uma conexão na rede do provedor, que é previamente estabelecida ou criada em função da própria requisição de conexão VPN.

Além de requisitos e modelo funcional, são apresentados três tipos de arquiteturas para serviços L1VPN em [Takeda et al. 2004a]. Na arquitetura centralizada, as funções de controle são implementadas em uma entidade de gerência centralizada. Na arquitetura distribuída, essas funções são distribuídas nos nós da rede (CEs, PEs e Ps). A arquitetura híbrida é caracterizada por uma combinação das duas anteriores, onde algumas funções são centralizadas e outras distribuídas. Em geral, as funções específicas para L1VPNs, como gerência de informações de membros de VPNs, são centralizadas, enquanto que funções comuns, como controle de conexões e roteamento, são distribuídas.

Uma arquitetura para serviços L1VPN é proposta em [Takeda et al. 2004b]. Este trabalho considera o modelo baseado em gerência como o mais adequado para os passos iniciais no desenvolvimento de serviços L1VPN, uma vez que os modelos baseados em

sinalização e roteamento exigem extensões aos protocolos do plano de controle. Então são avaliadas as abordagens centralizada e híbrida para definição da arquitetura do serviço L1VPN baseado em gerência. Por fim o trabalho propõe uma arquitetura híbrida com funções de controle e gerência para serviço L1VPN, devido às vantagens da arquitetura híbrida sobre a centralizada.

Os primeiros trabalhos, apresentados em [Takeda et al. 2005, Ould-Brahim 2005, Swallow et al. 2005], discutem problemas relacionados com mecanismos e protocolos do plano de controle. Diferentemente, o presente trabalho envolve questões relacionadas com a gerência de configuração de serviços L1VPN. A arquitetura aqui proposta considera o modelo funcional e a abordagem de arquitetura híbrida apresentados em [Takeda et al. 2004a] e a arquitetura de serviço L1VPN apresentada em [Takeda et al. 2004b]. A principal contribuição da arquitetura proposta é o suporte à gerência baseada em políticas.

4. *Framework* de Políticas

A abordagem de Gerência Baseada em Políticas tem sido utilizada com sucesso na gerência de serviços de rede, incluindo VPNs de camadas 3 e 2. Nesta abordagem, um administrador define um conjunto de políticas que controlam a utilização de recursos e o funcionamento da rede em vários aspectos como a operação de protocolos, serviços ou elementos da rede. Uma política consiste em um conjunto de regras que são formadas por condições e ações. Mediante uma requisição ou ocorrência de determinados eventos, as condições são avaliadas. Se as condições são satisfeitas, as ações são então executadas.

Como discutido em [Verma 2002], essa abordagem de certa forma automatiza o processo de gerência. Isso porque o administrador, por si mesmo, não precisa mais observar o estado da rede e decidir sobre ações de configuração. Uma vez que ele define as políticas, o sistema deve ser capaz de decidir as ações de configuração correspondentes, em função das políticas e do estado da rede. Outro ponto é que as políticas são regras de alto nível de abstração que determinam o comportamento do sistema como um todo. Isso libera o administrador de conhecer detalhes específicos de tecnologias. O sistema deve ser capaz de traduzir políticas que governam a operação da rede para dados de configuração específicos para cada entidade gerenciada. Por esses e outros motivos, a abordagem baseada em políticas simplifica o processo de gerência.

4.1. *Framework*

A seguir, é apresentada uma proposta de adaptação do *framework* de políticas da IETF, considerando a gerência de serviços L1VPN (Figura 2). Os administradores das redes do cliente e do provedor elaboram políticas para a gerência de serviços L1VPN através de uma ferramenta de *Gerência de Políticas*. Essas políticas são baseadas nos objetivos administrativos, no modelo de serviço L1VPN oferecido e nas características da infraestrutura da rede do provedor. Além disso, as políticas devem ser modeladas segundo um Modelo de Informação de Políticas padronizado, principalmente por questões de "interoperabilidade". O resultado desse processo é um conjunto de *Políticas de Configuração* de alto nível, que controlam e determinam a configuração e a operação dos serviços L1VPN.

Um Ponto de Decisão de Políticas (PDP – *Policy Decision Point*) é responsável por avaliar as políticas e gerar decisões de configuração na forma de *Dados de Configuração*

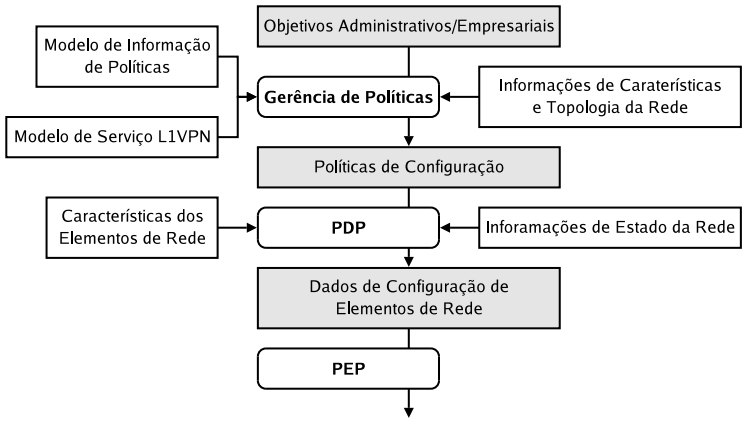


Figura 2. *Framework* baseado em políticas para gerência de Serviços L1VPN.

para os elementos de rede. Essas decisões podem ser requisitadas ou podem ser efetuadas em resposta à ocorrência de determinados eventos. O processo de decisão de políticas deve considerar o estado da rede e as características dos elementos de rede. Neste processo, as políticas de alto nível de abstração são traduzidas para dados de configuração específicos para as entidades gerenciadas.

Um Ponto de Aplicação de Políticas (PEP – *Policy Enforcement Point*) é responsável por efetivamente executar as ações correspondentes às decisões de gerência definidas por um PDP. Outra função do PEP é reportar informações de estado e características das entidades gerenciadas para o PDP.

4.2. Classes de Políticas

A seguir são propostas três classes de políticas para gerência de serviços L1VPN: políticas de configuração, admissão de controle e roteamento. As **Políticas de Configuração** são utilizadas para definir parâmetros de configuração que controlam a operação de serviços L1VPN. Elas podem ser definidas segundo um contrato de nível de serviço entre cliente e provedor. A seguir são discutidos alguns aspectos de serviços VPN que podem ser controlados por meio de políticas de configuração:

- A infra-estrutura de rede do provedor pode suportar ambos os modelos de alocação de recursos: compartilhado e dedicado. Políticas de configuração podem ser definidas para determinar o modelo de alocação usado em cada VPN. Ou ainda, para determinar regras para alterar o modelo usado em uma VPN em função das condições da rede.
- O provedor pode suportar diversos mecanismos de recuperação (*recovery schemes*), os quais são utilizados para o restabelecimento de conexões afetadas por falhas em enlaces ou nós da rede. A arquitetura GMPLS contempla duas abordagens de mecanismos de recuperação [Mannie e Papadimitriou 2006]: proteção (conexões secundárias previamente estabelecidas ficam disponíveis para substituir conexões ativas afetadas) e restauração (novas conexões são estabelecidas mediante a ocorrência de falha). As políticas de configuração podem ser especializadas para tratamento de falhas [Carvalho et al. 2005]. Elas permitem determinar o mecanismo de recuperação utilizado em cada VPN, assim como diferenciar os mecanismos utilizados para as conexões de cada membro da VPN.

- Se o provedor suporta diferentes classes de serviço L1VPN, políticas de configuração podem ser utilizadas para definir a classe para cada VPN. Políticas permitem inclusive a configuração dos mecanismos implementados para atender aos diferentes requisitos de qualidade de cada classe de serviço, mas isso está fora do escopo deste trabalho.
- Políticas de configuração também permitem determinar parâmetros relacionados com os procedimentos de roteamento em cada serviço VPN, uma vez que as instâncias de processo de roteamento são separados por VPN. As políticas podem definir algoritmos de cálculo de rotas, pesos de enlaces, hierarquia, parâmetros de protocolos de roteamento, entre outros.

As **Políticas de Controle de Admissão** permitem definir regras adicionais para controlar o processo de admissão de conexões, que considera também informações sobre membros da VPN e disponibilidade de recursos. Essas políticas permitem definir condições e regras para a admissão das conexões requisitadas, como descrito a seguir:

- Políticas de controle de admissão permitem controlar a utilização de recursos pelos clientes. Por exemplo, elas podem ser usadas para limitar o número de conexões por VPN ou por membro da VPN.
- Conexões são permitidas apenas entre membros da mesma VPN. Políticas de admissão possibilitam definir restrições de conectividade mais elaboradas, incluindo restrições entre membros da mesma VPN.
- Os elementos de borda possivelmente executam mecanismos para agregação de tráfego das redes clientes e instalação desses fluxos em conexões previamente estabelecidas na rede do provedor. Políticas de controle de admissão permitem controlar mecanismos de agregação ou otimizar a seleção das conexões pré-estabelecidas. Em um trabalho anterior, foi proposto uma arquitetura baseada em políticas para agregação dinâmica de tráfego em redes ópticas [Verdi et al. 2005].

As **Políticas de Roteamento** são utilizadas para controlar o cálculo ou a seleção de rotas. Elas permitem definir métricas e restrições para o cálculo de rotas, assim como otimizar a seleção de uma rota para uma conexão quando existem várias rotas disponíveis. Além disso, essas políticas podem ser usadas na gerência de recursos. A seguir, são apresentados os principais casos onde políticas de roteamento são adequadas:

- Suporte a Roteamento Baseado em Restrições (*Constraint-Based Routing*), principalmente em mecanismos de engenharia de tráfego [Banerjee et al. 2001]. Neste caso, o algoritmo de cálculo de rotas considera um conjunto de restrições relacionadas com aspectos administrativos e com requisitos de qualidade de serviço. As políticas de roteamento permitem definir essas restrições que condicionam o cálculo de rotas para as conexões requisitadas. Essas políticas podem restringir por quais domínios, ou nós, uma rota pode passar; estabelecer critérios para mecanismos de balanceamento de carga; critérios de segurança; entre outros. Em particular, mecanismos de recuperação de falhas podem utilizar essas políticas como restrições para o cálculo de caminhos disjuntos.
- As políticas de roteamento podem ser usadas na gerência de recursos no suporte aos modelos de alocação compartilhado e dedicado, principalmente, quando o cálculo de rotas é realizado por uma entidade centralizada. Neste caso, as políticas controlam quais recursos podem ser utilizados no cálculo da rota quando uma conexão é solicitada.

5. Arquitetura Proposta

A arquitetura proposta considera o modelo baseado em gerência para serviços L1VPN. Também consideramos que a rede do provedor implementa um plano de controle GMPLS, enquanto que a rede do cliente não precisa, necessariamente, implementar os protocolos GMPLS. O cenário considerado está ilustrado na Figura 3. Para criar uma conexão VPN entre dois CEs, o cliente envia uma requisição de conexão a um sistema de gerência de serviços L1VPN. Este sistema então se encarrega de requisitar ao PE de ingresso uma conexão entre os PEs correspondentes.

Assumimos que o estabelecimento da conexão no núcleo da rede do provedor é efetuado pelo mecanismo de sinalização do plano de controle, por exemplo, por meio do protocolo RSVP. Tal conexão, iniciada por um sistema de gerência e estabelecida pelo plano de controle, é denominada *soft permanent connection* (SPC). Dessa forma, os CEs estabelecem uma adjacência de roteamento utilizando a conexão estabelecida entre os respectivos PEs. Este cenário caracteriza um modelo *overlay*.

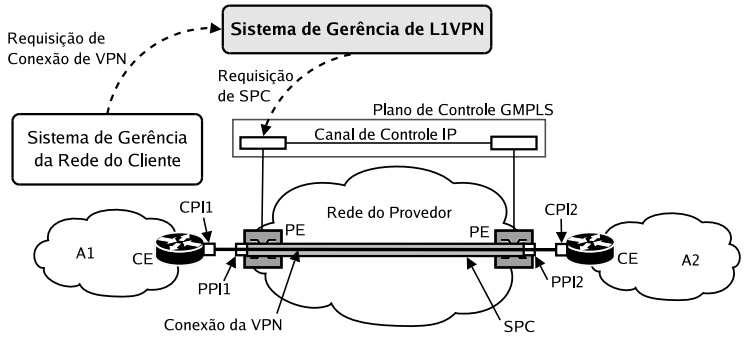


Figura 3. Cenário de aplicação.

Um membro de uma VPN é designado por uma par de portas (lógicas) que representam os extremos de uma conexão estática entre um CE e um PE [Takeda et al. 2005]. Assim, esse par é formado por dois identificadores: o identificador de porta do cliente (CPI – *Customer Port Identifier*) e o identificador de porta do provedor (PPI – *Provider Port Identifier*). Portanto, um par CPI-PPI identifica um membro da VPN. Ainda considerando a Figura 3, os CEs das redes A1 e A2, de um cliente A, podem ser identificados como dois membros CPI1-PPI1 e CPI2-PPI2 da L1VPN A. Para estabelecer uma conexão VPN entre suas redes A1 e A2, o cliente requisita ao sistema de gerência uma conexão entre aqueles dois membros. O sistema de gerência então requisita ao plano de controle uma SPC entre os PEs correspondentes, identificados pelas portas PPI1 e PPI2. Dessa forma, o tráfego enviado pela porta CPI1 é transmitido até a porta CPI2 pela conexão estabelecida na rede do provedor.

5.1. Descrição da Arquitetura

A Figura 4 apresenta a arquitetura proposta. São definidas duas interfaces a fim de aumentar o grau de flexibilidade e "interoperabilidade" da arquitetura. A interface denominada **Interface de Plano de Controle** (IPC) permite o acesso às funcionalidades do plano de controle. Através dessa interface, o sistema de gerência comunica com os mecanismos de roteamento e sinalização do plano de controle para controlar o estabelecimento de conexões, obter informações de roteamento, de disponibilidade de recursos, notificação de

ocorrência de falhas, entre outros. A arquitetura GMPLS suporta diferentes protocolos de sinalização e roteamento. Obviamente esta interface depende dos protocolos implementados na rede do provedor.

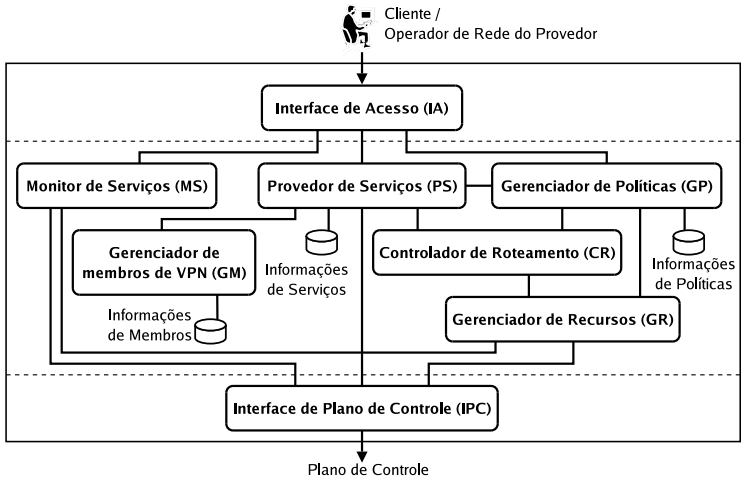


Figura 4. Arquitetura para gerência de serviços L1VPN.

A outra interface, denominada **Interface de Acesso** (IA), é a interface através da qual clientes e operadores da rede do provedor acessam as funcionalidades do serviço L1VPN. Ela também pode suportar mecanismos de controle de acesso e autenticação. Essa interface é responsável por processar as requisições e então invocar o módulo correspondente, entre os descritos a seguir:

- O módulo **Monitor de Serviços** é responsável por gerenciar informações sobre desempenho e ocorrência de falhas. Ele permite que cada cliente seja capaz de monitorar as informações relacionadas a seu serviço. Este módulo pode obter essas informações do plano de controle ou a partir da análise de informações sobre os recursos da rede, mantidas pelo próprio sistema de gerência.
- O módulo principal da arquitetura é o **Provedor de Serviços** (PS). Ele é responsável por "instanciar" e configurar serviços L1VPN. É também sua responsabilidade o controle de admissão sobre a requisição de conexões. Além disso, este módulo é responsável pelas funções de controle de conexões, como criar ou remover conexões entre membros da VPN.
- O módulo **Gerenciador de Políticas** (GP) permite aos clientes e operadores do provedor adicionar, remover ou editar políticas para a gerência de serviços L1VPN. Este módulo também pode executar as funções de um PDP, conforme descrito na seção anterior.

O **Gerenciador de Membros** (GM) é o módulo que gerencia as informações sobre quais membros pertencem a cada VPN. Essas informações podem ser fornecidas ao sistema de forma estática (configuração). No caso de uma arquitetura distribuída, as informações sobre membros de VPNs podem ser compartilhadas de forma automática, por meio de um mecanismo de *VPN Membership Auto-Discovery*, por exemplo, utilizando-se o protocolo BGP, como descrito em [Ould-Brahim et al. 2006, Takeda et al. 2005] ou o protocolo OSPF [Bryskin e Berger 2006].

O módulo **Gerenciador de Recursos** (GR) é responsável por gerenciar informações sobre o estado da rede, mantendo informações sobre a disponibilidade de recursos. Este módulo deve oferecer suporte aos dois modelos de alocação de recursos, compartilhado e dedicado. O **Controlador de Roteamento** (CR) é o módulo que calcula rotas para o estabelecimento de conexões. O cálculo de rotas é realizado a partir das informações fornecidas pelo gerenciador de recursos.

O suporte ao gerenciamento baseado em políticas é efetivamente implementado ao se condicionar a operação dos módulos Provedor de Serviços e Controlador de Roteamento às decisões de políticas realizadas pelo Gerenciador de Políticas. Dessa maneira o controle de conexões, bem como a admissão de conexões, realizados pelo Provedor de Serviço, estão sujeitos às regras determinadas pelas políticas. Da mesma forma, os procedimentos realizados pelo Controlador de Roteamento são governados pelas políticas definidas por clientes e administradores da rede do provedor.

Vejamos o exemplo da Figura 5. Ela apresenta um diagrama de seqüência que ilustra as interações entre os módulos para o estabelecimento de uma conexão. Após processar uma requisição de conexão enviada por um cliente, a Interface de Acesso encaminha a requisição ao Provedor de Serviço (1). Uma consulta é feita ao Gerenciador de Membros para verificar se os CEs de origem e destino da conexão pertencem à VPN do cliente (2). O Provedor de Serviços então requisita decisões de política relacionadas com a VPN em questão (3). Estas decisões configuram os processos de admissão e estabelecimento da conexão.

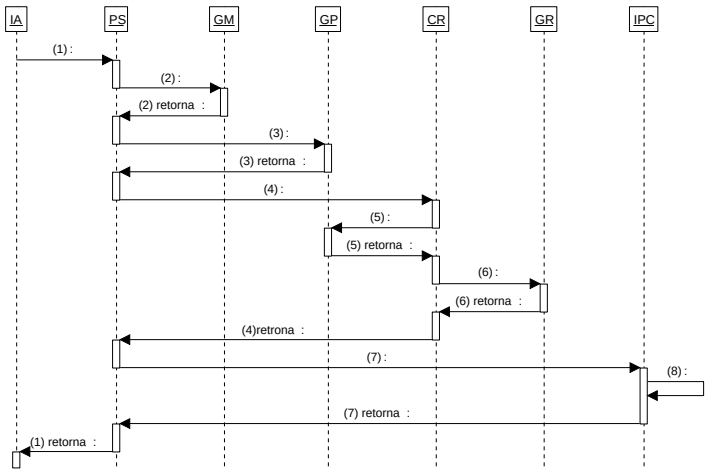


Figura 5. Interações entre os módulos para estabelecimento de conexão.

Uma vez admitida a conexão, uma requisição é feita ao Controlador de Roteamento, que retorna a rota calculada (4). Os procedimentos para cálculo da rota também estão sujeitos a decisões de políticas (5). A rota é calculada de acordo com informações de disponibilidade de recursos obtidas do Gerenciador de Recursos (6). Por fim, o Provedor de Serviço solicita ao plano de controle o estabelecimento de uma conexão (SPC) na rede do provedor (7). Esta solicitação consiste em uma requisição enviada ao PE de ingresso conforme a rota calculada. A conexão na rede do provedor é estabelecida através do mecanismo de sinalização do plano de controle, representado de forma simplificada pelo passo (8). O cliente é então notificado do resultado de sua requisição.

5.2. Implementação

Foi implementado um protótipo para validar a arquitetura proposta. Os módulos principais da arquitetura foram implementados como objetos remotos utilizando-se a tecnologia Java *Remote Method Invocation* (Java RMI). O módulo Monitor de Serviços ainda está sendo implementado. O módulo Provedor de Serviços possui dois sub-módulos responsáveis pelo controle de admissão e pelo controle de conexões. O módulo Controlador de Roteamento implementa o algoritmo de menor caminho de Dijkstra para o cálculo de rotas.

A interface de gerência definida pela Interface de Acesso foi implementada como um *Web Service*. A tecnologia *Web Services* suporta o desenvolvimento de sistemas distribuídos, facilitando a "interoperabilidade" na comunicação entre aplicações através do uso de protocolos da Internet e de especificações baseadas em XML (*Extensible Markup Language*).

Atualmente, as políticas são especificadas de forma estática (em tempo de compilação). Está sendo estudado o uso de XML para a representação de políticas, principalmente pela flexibilidade, "interoperabilidade" e disponibilidade de recursos para verificação de sintaxe. Para ilustrar as políticas XML, consideramos o modelo simplificado de informações de políticas apresentado na Figura 6.

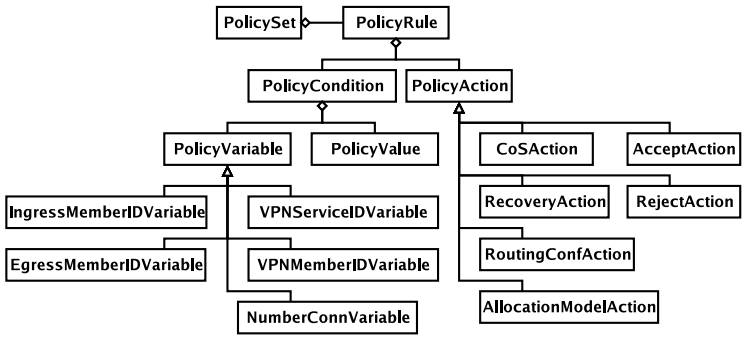


Figura 6. Modelo de Informação de Políticas simplificado.

Este modelo, baseado no *Policy Core Information Model* (PCIM) [Moore et al. 2001, Moore 2003], tem sido utilizado como referência na implementação. O modelo considera as classes de políticas definidas na seção anterior. Ele contempla as políticas de configuração e as políticas de admissão de controle relacionadas com restrição de conectividade e limitação de número de conexões. Neste modelo, as condições (*PolicyCondition*) das regras de políticas (*PolicyRule*) são formadas associando-se uma variável (*PolicyVariable*) a um valor (*PolicyValue*). O modelo define ações (*PolicyAction*) para aceitar ou rejeitar conexões e para configurar parâmetros de serviços L1VPN, conforme as políticas de configuração definidas na seção anterior.

A Figura 7 apresenta um exemplo de uma política em XML, considerando as propostas de classes e do modelo de informações de políticas. Essa política define duas regras, uma de configuração e outra de admissão de controle. A primeira regra define três parâmetros de configuração para a "VPN A", como está estabelecido na condição da regra (linhas 7 e 8). Ela define o modelo de alocação de recursos (como dedicado), a classe de serviço e um mecanismo de recuperação a ser utilizado (linhas 11 a 13, respectivamente).

A regra de admissão define um exemplo de restrição de conectividade. Neste caso, ela foi usada para impedir que dois membros específicos da VPN A possam estabelecer uma conexão entre si. A condição define quais são esses membros (linhas 21 e 23) e a ação determina que uma requisição entre esses membros deve ser rejeitada (linha 26).

```
1  <?xml version='1.0'?>
2  <!DOCTYPE Policy SYSTEM ''l1vpnPolicy.dtd''>
3  <Policy id=''001''>
4    <PolicySet>
5      <PolicyRule type=''configuration''>
6        <PolicyCondition>
7          <VPNServiceIDVariable/>
8          <PolicyValue>vpnA</PolicyValue>
9        </PolicyCondition>
10       <PolicyAction>
11         <ResourceAllocationAction allocationModel=''dedicated''/>
12         <CoSAction model=''basic'' class=''gold''/>
13         <RecoveryAction recoveryScheme=''protection:1+1''/>
14       </PolicyAction>
15     </PolicyRule>
16     <PolicyRule type=''admissionControl''>
17       <PolicyCondition>
18         <VPNServiceIDVariable/>
19         <PolicyValue>vpnA</PolicyValue>
20         <IngressMemberIDVariable/>
21         <PolicyValue>CPI1-PPI1</PolicyValue>
22         <EgressMemberIDVariable/>
23         <PolicyValue>CPI2-PPI2</PolicyValue>
24       </PolicyCondition>
25       <PolicyAction>
26         <RejecAction/>
27       </PolicyAction>
28     </PolicyRule>
29   </PolicySet>
30 </Policy>
```

Figura 7. Exemplo de política em XML.

Além disso, foi implementado um ambiente de simulação que integra o protótipo com uma rede de transporte óptica, cuja topologia está representada na Figura 8. Esse ambiente permite simular cenários com vários serviços L1VPN, onde os clientes requisitam conexões de forma concorrente. O estabelecimento de uma conexão na rede óptica consiste em determinar uma rota e alocar um comprimento de onda disponível em cada enlace do caminho, do nó origem até o destino. Um mecanismo de sinalização simplificado foi implementado através de um agente de controle que existe em cada nó. Esses agentes são responsáveis por alocar comprimentos de onda nos enlaces durante o estabelecimento de uma conexão.

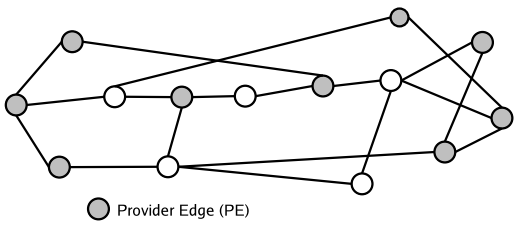


Figura 8. Topologia de rede simulada.

5.3. Resultados de simulações

O ambiente de simulação implementado foi utilizado para avaliar os efeitos de políticas de configuração. Sob a perspectiva do cliente, consideramos a taxa de bloqueio de conexões. Uma requisição de conexão é bloqueada quando não há recursos (comprimentos de onda) disponíveis pra o estabelecimento da conexão. Sob o ponto de vista do provedor, foi analisada a taxa de utilização dos recursos da rede, em termos do número total de comprimentos de onda alocados para as conexões.

Nos cenários simulados, diversos clientes de serviços L1VPN requisitam conexões de forma concorrente. Consideramos que para cada cliente existe um CE conectado a cada PE (conforme a topologia da rede do provedor apresentada na Figura 8). Cada cliente solicita um total de 2500 conexões. Os pares origem e destino para as conexões são selecionados do conjunto de CEs membros de uma VPN, segundo uma distribuição aleatória uniforme. A taxa de requisição de conexões segue uma distribuição de Poisson, e é dada por número de requisições por segundo. O tempo de duração de uma conexão (até que os recursos sejam liberados) e o intervalo entre requisições seguem distribuições exponenciais. Os resultados são a média de 100 repetições das simulações.

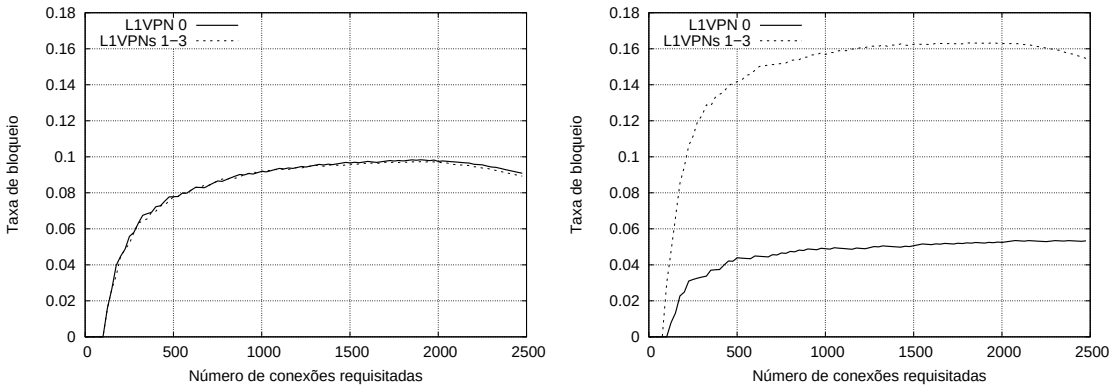
Em um primeiro cenário, consideramos 4 serviços (L1VPN 0-3) e 32 comprimentos de onda em cada enlace da rede. Neste cenário, é avaliado o efeito das seguintes políticas sobre a taxa de bloqueio de conexões:

1. Se a VPN é de alta prioridade, então: a alocação de recursos segue o modelo dedicado e um subconjunto dos recursos do provedor é dedicado para a VPN; no cálculo de rotas, devem ser considerados apenas os recursos dedicados para a VPN; o critério para determinar a rota é escolher os enlaces com maior número de comprimentos de onda disponíveis.
2. Se a VPN é de baixa prioridade, então: a alocação de recursos segue o modelo compartilhado e a VPN disputa com outras VPNs a alocação de recursos compartilhados; no cálculo de rotas, apenas os recursos compartilhados são considerados; o critério para determinar a rota é escolher o menor caminho (em número de *hops*).

Primeiro a simulação foi realizada sem considerar as políticas. A Figura 9(a) apresenta a taxa de bloqueio da L1VPN 0 e a média da taxa de bloqueio das outras L1VPNs. A Figura 9(b) mostra a alteração nesses valores quando as políticas são aplicadas.

Neste cenário, a L1VPN 0 é considerada como de alta prioridade, sendo reservados para ela 10 comprimentos de onda em cada enlace. Para implementar o cálculo de rotas priorizando os enlaces com mais comprimentos de onda disponíveis, assumimos que o custo do enlace é definido por $\frac{1}{w}$, onde w é o número de comprimentos de onda disponíveis (não alocados) no enlace. Por outro lado, quando o critério é o menor caminho, assumimos que o peso dos enlaces é igual a 1. Os resultados demonstram uma queda na taxa de bloqueio da L1VPN 0 e um aumento na média da taxa de bloqueio das outras L1VPNs.

Em um segundo cenário, consideramos 8 serviços L1VPN e 64 comprimentos de onda em cada enlace. Neste caso, foi avaliado o efeito da política de configuração do modelo de alocação de recursos sobre a taxa de utilização de recursos. Essa política define se o modelo de alocação é compartilhado ou dedicado. As simulações foram realizadas com diferentes taxas de requisição de conexões, primeiro com todas as VPNs utilizando

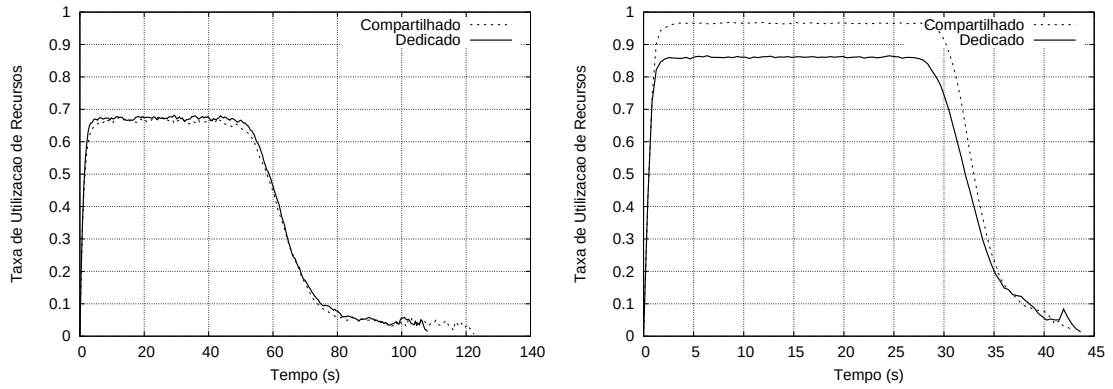


(a) Sem políticas (b) Com políticas

Figura 9. Taxa de bloqueio de conexões.

o modelo compartilhado e depois com todas utilizando o modelo dedicado. No caso do modelo dedicado, os recursos são divididos igualmente entre as L1VPNs.

Para baixas taxas de requisição, não há diferenças significativas entre os modelos de alocação (Figura 10(a)). Por outro lado, para taxas mais altas, o modelo compartilhado garante melhor utilização dos recursos (Figura 10(b)). Neste cenário, assumimos uma taxa de requisição baseada em uma distribuição de Poisson com média igual a 100 (para cada cliente). As variações na taxa de requisições consistem em utilizar frações dessa média. Por exemplo, uma taxa igual a 0,4 significa considerar uma média de 40 requisições por segundo.



(a) Taxa de requisição = 0,4 (b) Taxa de requisição = 1,0

Figura 10. Taxa de utilização de recursos da rede do provedor.

Estes cenários representam um estudo de caso para demonstrar como as políticas podem ser aplicadas e seus diferentes efeitos. Foi demonstrado que políticas de configuração podem ser definidas para oferecer serviços com prioridades diferenciadas. Além disso, constatou-se que políticas que melhoram o desempenho de um serviço podem afetar o desempenho de outros serviços. Assim como, uma política que melhora o desempenho para um cliente, pode, por exemplo, afetar a taxa de utilização dos recursos da rede do provedor.

6. Conclusão

O controle automático de conexões, proporcionado por um plano de controle distribuído, possibilita o aprovisionamento de serviços VPN em redes de transporte de camada 1. Esse serviço permite que vários clientes compartilhem uma infra-estrutura de rede comum.

Muitos trabalhos têm discutido como prover serviços L1VPN considerando as implicações no plano de controle. Porém faltam propostas sobre como atender requisitos de gerência para esses serviços. Neste artigo, propomos uma arquitetura baseada em políticas para a gerência de serviços L1VPN em redes de transporte com um plano de controle GMPLS. A arquitetura permite que cada VPN, sobre a rede do mesmo provedor, seja gerenciada de maneira independente, através de políticas definidas pelos próprios clientes ou pela administração da rede do provedor. Além disso, foram propostos um *framework* e classes de políticas para gerência de serviços L1VPN.

A implementação de um protótipo demonstrou a viabilidade da arquitetura e está sendo usada para a avaliação de efeitos das políticas. A utilização de Web Services para interface de gerência contribuiu com um método padronizado e flexível para acesso ao sistema. Os trabalhos de implementação ressaltam a necessidade e importância de um modelo de informação de políticas padronizado, principalmente no caso de VPNs que abrangem vários domínios administrativos.

Trabalhos futuros incluem o aprovisionamento de serviços L1VPN considerando múltiplos domínios, estudos sobre algoritmos e mecanismos baseados em políticas para alocação de recursos e avaliações de outras políticas.

Agradecimentos

Os autores agradecem a CAPES, o CNPq, a FAPESP e o projeto AgroFlow pelo apoio financeiro.

Referências

Banerjee, A., Drake, J., Lang, J. P., Turner, B., Kompella, K., e Rekhter, Y. (2001). Generalized Multiprotocol Label Switching: an overview of routing and management enhancements. *Communications Magazine, IEEE*, 39(1):144–150.

Bryskin, I. e Berger, L. (2006). OSPF based L1VPN auto-discovery. IETF Internet-Draft, "work in progress".

Carvalho, C., Madeira, E., Verdi, F., e Magalhães, M. (2005). Policy-based fault management for integrating IP over optical networks. Em *Operations and Management in IP-Based Networks: 5th IEEE International Workshop on IP Operations and Management, IPOM 2005*, v. 3751 de *Lecture Notes in Computer Science*, p. 88–97, Barcelona, Espanha.

ITU (2003). Layer 1 Virtual Private Network generic requirements and architecture elements. ITU-T Recommendation Y.1312.

ITU (2004). Layer 1 Virtual Private Network service and network architectures. ITU-T Recommendation Y.1313.

Kompella, K. e Rekhter, Y. (2005). Label Switched Paths hierarchy with GMPLS traffic engineering. IETF RFC 4206.

Mannie, E. (2004). Generalized Multi-Protocol Label Switching (GMPLS) architecture. IETF RFC 3945.

Mannie, E. e Papadimitriou, D. (2006). Recovery (protection and restoration) terminology for GMPLS. IETF RFC 4427.

Moore, B. (2003). Policy Core Information Model (PCIM) extensions. IETF RFC 3460.

Moore, B., Ellesson, E., Strassner, J., e Westerinen, A. (2001). Policy Core Information Model – version 1 specification. IETF RFC 3060.

Ould-Brahim, H. (2005). GVPN services: Generalized VPN services using BGP and GMPLS toolkit. IETF Internet-Draft, "work in progress".

Ould-Brahim, H., Fedyk, D., e Rekhter, Y. (2006). BGP-based auto-discovery for L1VPNs. IETF Internet-Draft, "work in progress".

Swallow, G., Drake, J., Ishimatsu, H., e Rekhter, Y. (2005). GMPLS User-Network Interface: RSVP-TE support for the overlay model. IETF RFC 4208.

Takeda, T., Aubin, R., Carugi, M., Inoue, I., e Ould-Brahim, H. (2006a). Framework and requirements for Layer 1 Virtual Private Networks. IETF Internet-Draft, "work in progress".

Takeda, T., Brungard, D., Farrel, A., Ould-Brahim, H., e Papadimitriou, D. (2006b). Applicability analysis of GMPLS protocols to Layer 1 Virtual Private Networks. IETF Internet-Draft, "work in progress".

Takeda, T., Brungard, D., Papadimitriou, D., e Ould-Brahim, H. (2005). Layer 1 Virtual Private Networks: driving forces and realization by GMPLS. *Communications Magazine, IEEE*, 43(7):60–67.

Takeda, T., Inoue, I., Aubin, R., e Carugi, M. (2004a). Layer 1 Virtual Private Networks: service concepts, architecture requirements, and related advances in standardization. *Communications Magazine, IEEE*, 42(6):132–138.

Takeda, T., Kojima, H., e Inoue, I. (2004b). Layer 1 VPN architecture and its evaluation. Em *Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings. The 2004 Joint Conference of the 10th Asia-Pacific Conference on*, v. 2, p. 612–616.

Verdi, F., Carvalho, C., Magalhães, M., e Madeira, E. (2005). Policy-based grooming in optical networks. Em *4th Latin American Network Operations and Management Symposium, LANOMS 2005*, p. 125–136, Porto Alegre, Brasil.

Verma, D. C. (2002). Simplifying network administration using Policy-Based Management. *Network, IEEE*, 16(2):20–26.