Universidade Federal de Pernambuco - UFPE

Centro de Informática - CIn

Pós-Graduação em Tecnologias da Informação

Ambiente Integrado para Gerenciamento da Rede Interna da Secretaria da Receita da Paraíba (SER-PB)

Pedro Gustavo de Farias Paiva

Recife, Março de 2010

Universidade Federal de Pernambuco - UFPE
Centro de Informática - CIN
Especialização em Tecnologias da Informação

Ambiente Integrado para Gerenciamento da Rede Interna da Secretaria da Receita da Paraíba

Pedro Gustavo de Farias Paiva

Monografia apresentada à Coordenação da Pós-Graduação do Centro de Informática da Universidade Federal de Pernambuco, como parte dos requisitos para conclusão da pós-graduação *lato sensu* em Tecnologias da Informação.

Orientador: Dr. Paulo André da S. Gonçalves

Recife

2010

Agradecimentos

Aos meus pais, Álvaro e Verônica, pela confiança e apoio as minhas atitudes e em todos os momentos que precisei.

Aos meus irmãos Paulo Vinícius e Bruno Fábio, que estão trilhando seus caminhos na área de computação. Boa sorte pessoal.

Ao professor Doutor Paulo André, pela paciência e prontidão durante o processo de orientação.

Ao pessoal do CIN, Marcos Nascimento e Professor Doutor Fernando Fonseca.

A Juliana, que me deu força e apoio para a conclusão deste trabalho em sua reta final.

A todo o pessoal da Sub-Gerência de Suporte e Produção, pela amizade e companheirismo de sempre.

Aos colegas do setor de Infra-estrutura de Redes André, Antônio, Adrivagner, Eraldo, Francisco Neto, Morgana por todo o conhecimento que me passaram e por terem me ajudado sempre que solicitados.

Ao pessoal da Politec.

Aos amigos Fábio Mariz, Fábio Chacon e Rodrigo Monteiro por toda a ajuda que me deram no decorrer do curso além das conversas durante as viagens intermináveis até Recife.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

A.C – Antes de Cristo

APD – Avalanche Photodiode

ATM – Asynchronous Transfer Mode

BER – Bit Error Rate

BGP – Border Gateway Protocol

CDM – Code Division Multiplexing

CIRs – Commited Information Rates

DLC – Digital Loop Carrier

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

DWDM – Dense Wavelenght Division Multiplexing

EDFA – Erbium Doped Fiber Amplifier

FDDI – Fiber Distributed Data Interface

FDM – Frequency Division Multiplexing

FEC – Forwarding Equivalence Class

FTTC – Fiber To The Curb

FTTB – Fiber To The Building

FTTH – Fiber To The Home

GMPLS – Generalized Multiprotocol Label Switching

GPL – General Public License

GTI – Gerência de Tecnologia da Informação

HDSL – High-Bit-Rate digital Subscriber Line

HLAN – Helical LAN

HTML – Hypertext Markup Language

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISDN – Integrated Services Digital Network

ISP – Internet Service Provider

IS-IS – Intermediate System-to-Intermediate System Protocol

ITU – International Telecommunications Union

LAN – Local Area Network

LDP – Label Distribution Protocol

LED – Light Emiting Diode

LLC – Logical Link Control

LMDS – Local Multipoint Distribution System

L2TP – Layer 2 Tunneling Protocol

LSPs – Label Switched Paths

LSRs – Label Switch Routers

MAN – Metropolitan Area Network

MBGP – Multiprotocol BGP

MMF – Multimode Optical Fiber

MPLS – Multiprotocol Label Switching

MIB – Management Information Base

MRTG – Multi Router Traffic Grapher

NMS – Network Management System

NIC – Network Interface Card

OC – Optical Carrier

OCDM – Optical Code Division Multiplexing

OID – Object Identifier

OTs – Optical Terminals

OTDM – Optical Time Division Multiplexing

OSPF – Open Shortest Path First

OXC – Optical Cross Connect

PIN – Positive-Intrisic-Negative

PPTPP – Point-to-Point Tunneling Protocol

POTS – Plain Old Telephone Service

QoS – Quality of Service

RD – Route Destinguer

RFC – Request for Comment

RNP – Rede Nacional de Ensino e Pesquisa

ROI – Return On Investment

RTT – Round Trip Time

SER-PB – Secretaria do Estado da Receita da Paraíba

SDH – Synchronous Digital Hierarchy

SLA – Service Level Agreement

SMF – Single-mode Optical Fiber

SNMP – Simple Network Management Protocol

SONET – Synchronous Optical Network

TCP – Transmission Control Protocol

TDM – Time Division Multiplexing

TE – Traffic Engineering

TONs – Transparent Optical Networks

TTL – Time To Live

UDP – User Datagram Protocol

UONs – Ultra-High Optical Networks

VHDSL – Very High-Bit-Rate digital Subscriber Line

VPN – Virtual Private Network

WAN – Wide Area Network

WDM – Wavelength Division Multiplexing

Resumo

A Secretaria da Receita do Estado da Paraíba (SER-PB), adotou o MPLS como protocolo de encaminhamento para o núcleo da sua rede interna, provida pela empresa Oi. Com a adoção desse protocolo foram resolvidos os problemas de falta de capacidade dos enlaces, falta de redundância de enlaces e balanceamento de carga, mas, problemas com o gerenciamento da rede interna surgiram. O gerenciamento do tráfego de rede é de grande importância para que a SER-PB possa se planejar futuras expansões e, além disso, possa ser capaz de realizar um dimensionamento correto para que novas aplicações e serviços sejam oferecidos sem que recursos sejam desperdiçados.

Este trabalho propõe um ambiente de gerenciamento composto pela integração de um analisador de tráfego, que coletará e classificará os dados da rede, um sistema de gerenciamento de rede, que terá o papel de monitorar o ambiente de rede gerando relatórios, gráficos, alertas a partir das informações coletadas e um sistema de gerenciamento de banco de dados para que as informações levantadas possam ser armazenadas de forma organizada e uma base histórica mantida.

Palavras-chave: gerenciamento de redes, MPLS, redes ópticas, análise de tráfego

Abstract

Secretaria da Receita do Estado da Paraíba (SER-PB) adopted the Multipath Label Switching(MPLS) protocol as main way to route all your data trough an Internet Service Provider core as a network service. With this solution, some deals like lack of links capacity, lack of links redundancy and load balancing were solved, but, network management troubles appeared. The network traffic management is a very important strategy where the network growth can be measured without waste of network resources.

A management environment to SER-PB local area network will be proposed in this study. This environment is composed by integration of two network tools and a database management system. Each environment component has one specific functionality. The network traffic analyzer will capture the network traffic and identify it by protocol load sending these information to be treated and presented by the network management system (NMS). The network management system will plot graphics and maps, make reports, make system alerts showing the results as a user interface, this component will do the environment presentation for your users. The database management system will store all the information generated from the proposed network environment keeping them for future queries.

***Keywords**: network management, MPLS, optical networks, traffic identification*

Capítulo 1 - Introdução

A evolução das redes ópticas possibilitou que grandes taxas de transmissão fossem alcançadas num curto espaço de tempo e a grande utilização de aplicações multimídia (voz e vídeo) sob demanda ou em tempo real, na Internet, exigem muita capacidade de banda para que possam ser executadas. Esses tipos de aplicações modelam a carga que a maioria dos usuários depositam nas redes. Assim, muitas aplicações coorporativas deixam de funcionar adequadamente por conta de congestionamentos que poderiam ser evitados. Observando esse panorama é possível perceber a necessidade de se gerenciar uma rede de forma adequada, pois só assim, os administradores saberão quantificar e qualificar os recursos da rede.

1.1 Motivação

A SER-PB é a entidade governamental responsável por gerir os recursos financeiros arrecadados pelo estado da Paraíba através dos seus pontos de coleta fiscais. Nela existe uma gerência responsável por todo seu parque tecnológico, a Gerência de Tecnologia da Informação (GTI). O parque tecnológico da SER-PB contempla todos os recursos computacionais da entidade, como, computadores, dispositivos de suas sub-redes, além de contratos com prestadores de serviços, operadoras de telefonia, provedores de serviços de rede e de pessoal. O ambiente de rede da GTI é composto por várias sub-redes onde se destaca a sub-rede Intranet, que após um processo de migração passou a utilizar em sua estrutura o protocolo MPLS (*Multipath Label Switching*) provido através de um serviço de prestado pela empresa Oi.

A empresa Oi é uma das maiores empresas de telecomunicações do país e oferecem serviços de telefonia fixa, móvel, voz sobre IP e de acesso, doméstico ou empresarial, à Internet. Através do modelo de negócio *Outsourcing,* a Oi fornece infra-estrutura de rede para empresas que necessitam de ligação entre várias localidades distintas, caracterizando-se como um ISP (*Internet Service Provider*). O cliente, por sua vez, escolhe o serviço desejado e paga uma taxa fixa por ele. A SER-PB possui um contrato de prestação de serviços, com a Oi, por meio de um acordo entre a empresa e o Governo do Estado da Paraíba, responsável por todas as Secretarias de Estado, onde, a prestadora de serviços deve fornecer acesso à Internet e infra-estrutura para as redes de longa distância para todas elas. Desta forma, a GTI não pode recusar o recurso oferecido pelo Governo, nem solicitar mudanças no projeto de implantação do serviço de rede.

O MPLS é um protocolo de roteamento que visa a comutação de pacotes IP rotulados de acordo com a aplicação que os geraram possibilitando otimização da rede, plano de controle de tráfego e menor processamento de pacotes, pois, os cabeçalhos da camada de rede não são analisados a cada salto dos pacotes. Alguns fatores contribuíram para a adoção deste protocolo por parte da SER-PB e o principal deles foi a renovação da infra-estrutura do núcleo da rede óptica da Oi. Outro fator observado foi a sobrecarga devido a criação de novos módulos para o principal sistema da SER-PB além da criação novas aplicações coorporativas, que contribuíram para que a rede se tornasse cada vez mais congestionada. O problema de congestionamento se dava também pela má utilização, por parte dos usuários, da banda disponível. Que despejavam grande quantidade de dados derivados de aplicações P2P, *streaming* de vídeo, rádios *on-line,* o que demandou a identificação e priorização do tráfego para que as aplicações coorporativas tivessem maior prioridade na rede.

Com a adoção do MPLS, grande parte dos problemas da rede interna da SER-PB foram solucionados e as melhorias na velocidade dos enlaces e na utilização de enlaces redundantes para as localidades críticas ficaram evidentes, porém, outros problemas foram observados. Problemas de gerenciamento da rede devido ao modelo de negócio e arquitetura de rede adotada pela provedora de serviços. Visando total controle da rede, a provedora não permite que seus roteadores de borda sejam acessados por seus clientes, dessa maneira o cliente, em tese, não precisa se preocupar com o gerenciamento da rede, o que é ideal para empresas que não possuem setores de tecnologia da informação. Uma rede sem gerenciamento interno não é adequada para a GTI, por esse motivo uma forma de gerenciamento se faz necessária para que seus serviços sejam devidamente monitorados, informações sobre o tráfego sejam coletadas, que o tráfego seja priorizado corretamente e que, operações e modificações da rede interna possam ser efetuadas de forma proativa.

A GTI possui um ambiente de gerenciamento composto por vários sistemas de gerenciamento de rede (*Network Management Systems*) o que torna desorganizada e descentralizada a busca pelas informações desejadas. Alguns sistemas utilizados são sistemas já consolidados, de código aberto e sob licença GPL (*General Public License*) porém sem suporte aos requisitos da rede MPLS adotada, já outras ferramentas utilizadas pela GTI não possuem interface gráfica para o usuário, o que facilitaria sua utilização, nem oferecem suporte à integração de alguns serviços básicos, como por exemplo, armazenamento de informações em bancos de dados.

1.2 Objetivos

Este trabalho tem como objetivo geral propor melhorias no ambiente de gerenciamento da rede interna da SER-PB. Será proposto um ambiente de gerenciamento de rede composto pela integração de um sistema de coleta e análise de protocolos, um sistema de gerenciamento de rede e um sistema de gerenciamento de banco de dados (SGBD). Cada integrante desse ambiente terá uma finalidade específica que contribuirá para que o ambiente proposto seja centralizado, de fácil utilização, sendo capaz também de gerar relatórios automaticamente, informar o estado atual da rede através de gráficos e mapas, além de armazenar dados históricos para planejamento de crescimento da rede ou implantação de novos serviços.

Para alcançar o objetivo geral, os seguintes objetivos específicos são definidos:

- Propor um novo ambiente para facilitar o gerenciamento da rede;
- Analisar as ferramentas de gerenciamento de rede utilizadas pelas equipes de Infra-estrutura e Monitoramento da GTI;
- Fazer o estado da arte das redes ópticas;
- Estudar o ambiente de rede da Secretaria da Receita da Paraíba;
- Identificar pontos de melhoria no gerenciamento da rede interna da SER-PB, para que medidas proativas sejam tomadas.

1.3 Organização do Trabalho

O restante desta monografia se encontra organizada da seguinte forma. No Capítulo **Erro! Fonte de referência não encontrada.** são descritos os principais conceitos relacionados às redes ópticas, técnicas de multiplexação, tipos e arquiteturas de redes ópticas, bem como uma perspectiva histórica das comunicações ópticas.

O Capítulo 3 mostra uma visão geral sobre gerenciamento de redes, onde serão apresentados protocolos e ferramentas para gerenciamento de redes além de suas características e aplicações.

No Capítulo 4 são descritos os conceitos sobre redes MPLS, Qualidade de Serviço, Engenharia de Tráfego e Segurança em redes MPLS com a utilização de redes privadas virtuais (VPNs).

Seguindo para o Capítulo 5, são apresentados o ambiente de rede da Secretaria da Receita do Estado da Paraíba bem como seus problemas encontrados após a implantação de uma rede MPLS.

O capítulo 6 apresenta uma proposta de ambiente de gerenciamento que poderá ser adotada pela SER-PB. Finalmente, as conclusões, são apresentadas no Capítulo 7.

Capítulo 2 – Redes Ópticas

Neste capítulo serão discutidos conceitos básicos a cerca das redes ópticas, apresentando seus conceitos básicos, seus tipos e suas arquiteturas, técnicas de multiplexação e uma perspectiva histórica.

2.1 Conceitos Básicos

As redes ópticas podem ser definidas como redes de telecomunicações de alta capacidade baseadas em tecnologias ópticas [3,4]. A utilização das fibras ópticas trazem muitas vantagens, pois são capazes de oferecer larguras de banda muito altas, a baixo custo e sem perda de informação. Outros pontos importantes como, estabilidade e grande escalabilidade garantem as fibras como um excelente meio físico [2].

2.1.1 Fibras Ópticas

A fibra óptica é o meio por onde são transmitidos pulsos luminosos, sendo capaz de trafegar mais informação do que os cabos convencionais. Além disso, podem ser usadas tanto em redes locais quanto nas transmissões de longa distância, apesar de sua conexão ser mais complexa que a conexão de uma rede *Ethernet* [1,2,8].

O tipo de fibra que possui a propriedade de propagar sinais luminosos com diferentes comprimentos de onda, são chamados de fibras multimodo ou MMF (*Multimode Optical Fiber)*. Se o diâmetro da fibra for reduzido, o meio se comportará como um guia de onda, pois o sinal luminoso será transmitido em linha reta. As fibras com essa característica são conhecidas como fibras monomodo ou SMF (*Single-mode Optical Fiber*). As fibras monomodo são mais caras e utilizadas em distâncias mais longas podendo transmitir dados a 50 Gbps (*Gigabits per second*) por 100 Km sem amplificação. Taxas de dados mais altas foram obtidas em laboratório, para distâncias mais curtas [3].

Os cabos de fibra óptica são semelhantes aos cabos coaxiais, exceto por não terem a malha metálica. No centro do cabo encontra-se o núcleo de vidro, através do qual se propaga a luz [2]. Nas fibras multimodo o núcleo possui aproximadamente 50 mícrons de diâmetro, o que é equivalente à espessura de um fio de cabelo humano, já as fibras monomodo possuem entre 8 e 10 mícrons [3,4]. O núcleo é envolvido por uma malha de vidro com índice de refração inferior ao seu, para que o raio luminoso permaneça dentro do núcleo. Envolvendo a malha de vidro, existe uma cobertura de plástico fino que serve de proteção para o revestimento interno.

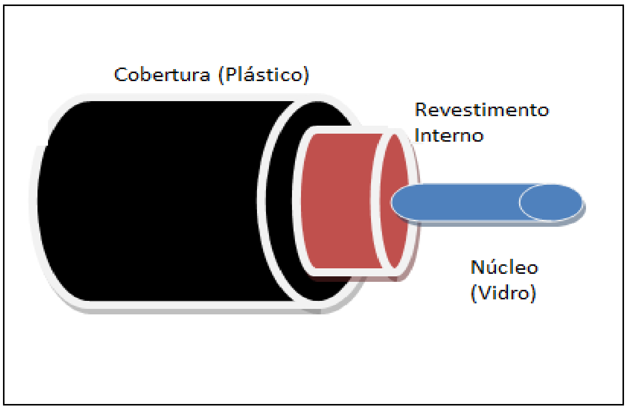


Figura 1: Fibra Óptica simples (Cabo Monofibra) [2,3]

Existem estruturas criadas para proteger e facilitar o manuseio das fibras ópticas [6]. O cabo óptico, representado na Figura 1, é utilizado para 3 tipos de ambientes:

- Ambientes Internos – quando protegem o meio físico para *backbones*;
- Ambientes Externos – quando são utilizados para proteger a fibra em dutos submersos e instalações aéreas;
- Ambientes Temporários – quando destinados à operações de manobras, ligações temporárias e manutenção entre fibras e painéis de distribuição.

O revestimento óptico tem como finalidade a proteção das fibras contra adversidades mecânicas ou ambientais durante sua instalação ou operação de manutenção [6]. Esse revestimento deve ser resistente para evitar que as fibras se partam com tensões causadas por sua movimentação durante a instalação e deve possuir também a rigidez necessária afim de suportar curvaturas excessivas nas fibras [3,6]. Os cabos submarinos transoceânicos devem suportar a pressão que a água exerce sobre eles devido à profundidade. Já os cabos aéreos devem garantir o funcionamento adequado das fibras em casos de temperaturas extremas entre -20ºC a + 65ºC [6].

O desempenho do cabo óptico pode diminuir ao longo do tempo por alguns fatores, conforme descrito a seguir. A fadiga estática é um exemplo de quando uma fibra se parte devido à um longo período de uso. Pode ocorrer também o envelhecimento térmico da estrutura do cabo que faz com que a atenuação aumente. E ainda, pode ocorrer a atenuação devido a presença de hidrogênio, originado pela corrosão metálica da estrutura de suporte físico pela ação da água ou pela decomposição do material plástico de proteção [3,4,6].

Um revestimento simples, às vezes é o mecanismo de proteção suficiente para utilização da fibra numa estrutura de cabeamento óptico. Entretanto, na maioria das aplicações, a fibra é envolvida de acordo com um procedimento conhecido como *"buffering"*. O processo de *buffering* se caracteriza pela junção de várias fibras em um único feixe (*Loose Buffers*) que posteriormente será agrupado a outros feixes de fibra para formar o cabo óptico, mostrado na Figura 2. Os tipos de cabos ópticos utilizados são: tipo Solta (*Loose*), tipo Compacta (*Tight*), Groove (tipo "V"), tipo Fita (*Ribbon*) [3,6].

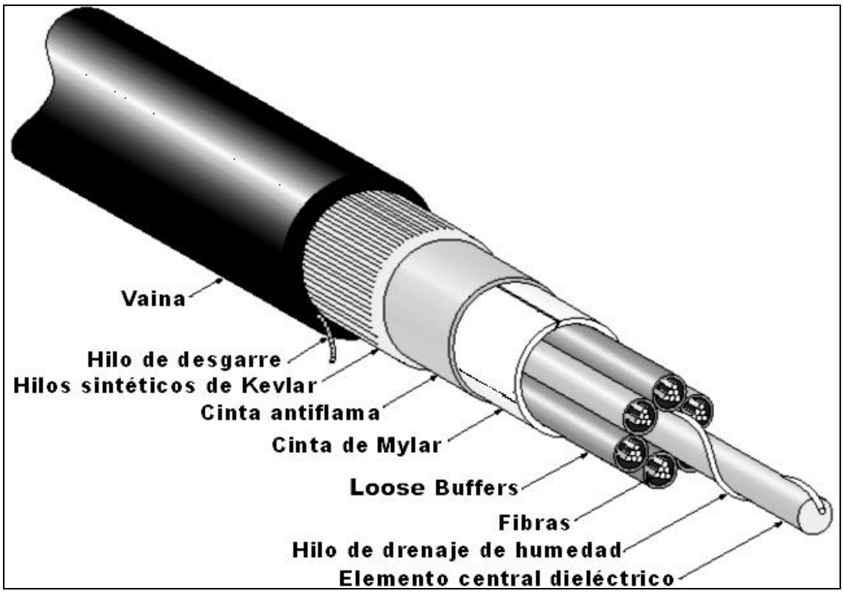


Figura 2: Exemplo de cabo óptico [3]

2.1.2 Princípios da comunicação óptica

Um sistema de transmissão óptico é composto pelo sistema transmissor, meio de propagação e o detector óptico. O circuito emissor possui a função de transformar o sinal elétrico em óptico. O meio de transmissão é uma fibra de vidro ultrafina e o detector óptico é o responsável pela detecção do sinal óptico e conversão desse sinal óptico para sinal elétrico [3,6].

Por convenção, um pulso luminoso indica o *bit* 1 e a ausência de luz representa o *bit* zero. A luz é inserida em determinando ângulo na fibra através de uma de suas extremidades. O princípio da reflexão total da luz Para que essa luz seja propagada na fibra óptica se baseia no princípio da reflexão total da luz, onde a luz é sempre mantida no meio físico devido a diferença entre os índices de refração.

No sistema de comunicação óptica digital representado na Figura 3, o sinal elétrico, de entrada, se apresenta na forma de pulsos digitais do bloco transmissor. Esses pulsos elétricos modulam a intensidade de luz a partir do diodo laser ou LED (*Light Emiting Diode*)e os converte em pulsos ópticos. No bloco receptor, o detector óptico converte os pulsos ópticos em pulsos elétricos. Um demodulador converte os pulsos ópticos no sinal elétrico original [3].

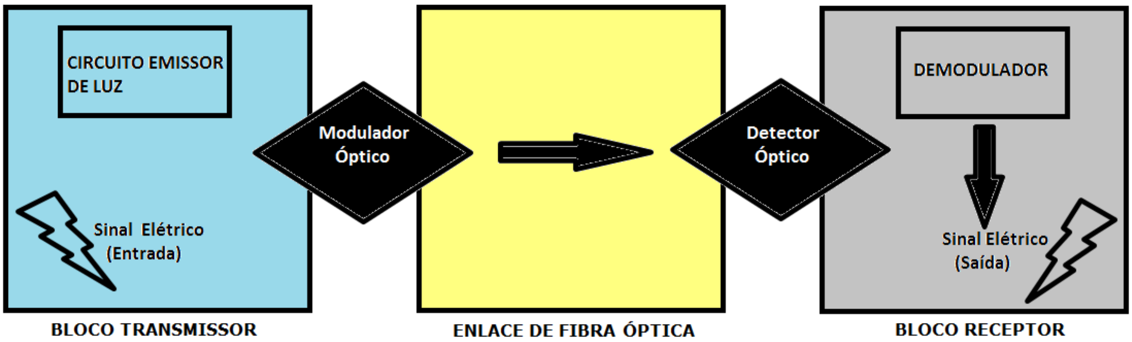


Figura 3: Sistema básico de comunicação óptica

Os componentes ópticos utilizados são os agentes que fazem com que um sistema de comunicação óptica funcione. Alguns deles serão descritos abaixo:

Detectores Ópticos – semicondutores baseados em fotodiodos são utilizados como detectores ópticos. São pequenos, possuem alta sensibilidade e resposta rápida. Como exemplos de detectores ópticos existem os fotodiodos PIN (*Positive-intrisic-negative*) e os fotodiodos APD (*Avalanche Photodiode*) [2,4].

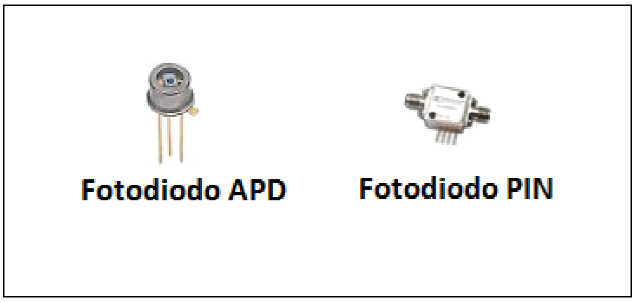


Figura 4: Exemplos de fotodiodos [4]

Amplificadores Ópticos ou Repetidores – em sistemas ópticos de longa distância, os repetidores ópticos são posicionados a cada 100 Km e são utilizados para amplificar sinais transmitidos para a sua intensidade original e depois passados para fibra principal [2,4,8].

Figura 5: Amplificador Óptico [4]

Acoplador de Fibra – é um dispositivo que distribui luz a partir de uma fibra principal para uma ou mais ramos de fibras. Existem basicamente dois tipos de acopladores: Os acopladores de interação com o núcleo e acopladores do tipo interação com a superfície [6,8].

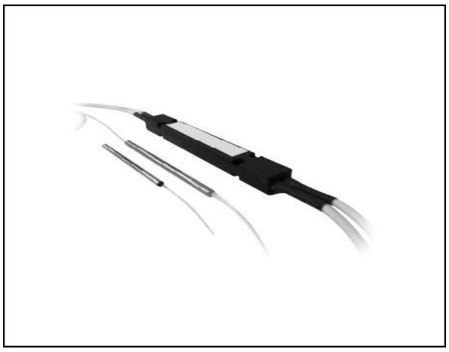


Figura 6: Exemplos de acopladores [6]

Conectores de Fibra – antes de conectar uma fibra com outra num enlace de comunicação óptica, deve-se decidir se a junção será permanente ou se poderá ser desmontável. O conector é utilizado para prover interface à junção de enlaces de fibra que podem ser desmontados [6,8].

2.1.3 Vantagens e desvantagens da fibra óptica

Nos últimos anos a fibra-óptica se tornou o meio de transmissão mais utilizado por prover grande capacidade de banda, baixa atenuação e baixa taxa de erro (*Bit Error Rate* – BER). As características das fibras sugerem grandes vantagens em relação aos antigos suportes físicos de transmissão, tais como os pares metálicos e cabos coaxiais. Seguem abaixo algumas propriedades que tornam a utilização de fibras vantajosas [2,8].

- Baixa perda de transmissão: a utilização de fibras de sílica de baixíssima perda, lubrificadas com Érbio, possibilita a transmissão quase perfeita, com pouquíssima perda ou atenuação. Pesquisas com novos materiais prometem fibras ópticas com atenuações menores, na ordem de centésimos e até mesmo, milésimos de decibéis por quilômetro. Atualmente nos sistemas de telecomunicações ópticos, as fibras possuem perdas de até 0,002 dB/km. Assim, sistemas de transmissão de longa distância podem ser estruturados com um espaçamento muito grande entre cada repetidor. Isso reduz custos e a complexidade de todo o sistema já que a quantidade de repetidores é reduzida [1,4,6].

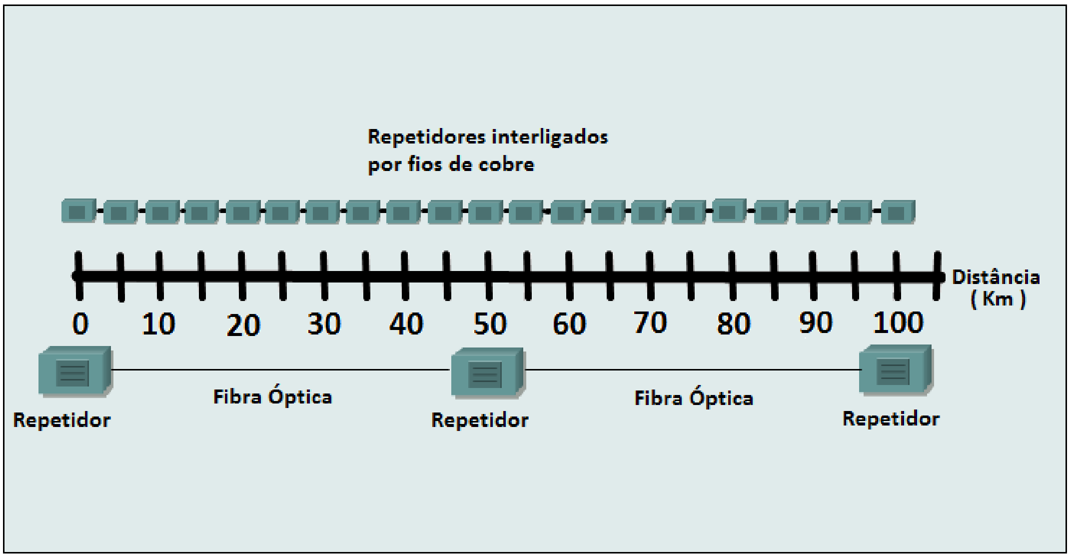


Figura 7: Comparação entre o número de repetidores de fibras e o número de repetidores para cabeamento metálico

- Guia de onda dielétrico: as fibras ópticas são feitas a partir da sílica que é um isolador elétrico. Portanto, elas não são afetadas por nenhum tipo de interferência eletromagnética e por picos de voltagem [4,6].

- Segurança do sinal: o sinal transmitido através da fibra não é irradiado, como acontece nas transmissões via rádio. Desta forma, qualquer tentativa de captura de mensagens ao longo de uma fibra é facilmente detectada, pois, exige o desvio de uma porção considerável da potência luminosa. Assim, a segurança total do sinal transmitido é garantida [8].
- Pouco peso e tamanho: os cabos de fibra óptica possuem raio pequeno, são flexíveis, compactos e leves. Além disso, podem ser dobrados ou retorcidos sem serem danificados. Essa propriedade facilita sua instalação em localidades onde os dutos estão com pouco espaço para a adição de uma nova fibra [8].

Uma desvantagem que deve ser observada, é que os cabos de fibras podem ser danificados, caso a fibra seja rompida por tratores, britadeiras ou até mesmo por ação de roedores. Outra grande limitação das redes ópticas é o gargalo eletro-óptico. Esse gargalo é causado pelo fato de que transferências de informação envolvem o tempo utilizado para o processo de conversão do sinal elétrico para sinal óptico e vice-versa. O tráfego de dados transferido através das fibras deve ser processado nas taxas compatíveis com os equipamentos do núcleo da rede. Caso a rede seja composta por circuitos eletrônicos, o tráfego não passará da ordem de *Gigabits* por segundo, o que mostra uma limitação na vazão para este tipo de rede [6,8].

2.1.4 Onde são usadas as redes ópticas

Os sistemas de comunicação ópticos podem interligar diferentes tipos de redes. Nas redes locais ou LANs (*Local Area Networks*), servem para interligar *hosts* geralmente localizados em um mesmo domicílio [4].

Hoje em dia, as redes ópticas de acesso são utilizadas predominantemente por grandes assinantes, empresas operadoras de telecomunicações, empresas e órgãos públicos que necessitam de conexões de alta velocidade. No caso das instituições de ensino e pesquisa, existe uma rede de alta velocidade mantida pela Rede Nacional de Ensino e Pesquisa (RNP). Alguns países oferecem esse tipo de rede de acesso para assinantes domésticos que necessitam de banda ultra-larga.

Nas redes Metropolitanas ou MANs (*Metropolitan Area Networks*), as fibras ópticas são utilizadas para suportar todo o tráfego de dados, voz e imagem existentes. São redes gerenciadas por *Tiers*, provedores de grande capacidade, onde trafegam os maiores volumes de tráfego da Internet [2,3].

2.2 Técnicas Multiplexação em Redes Ópticas

Multiplexar o meio físico em uma rede óptica, nada mais é, do que utilizar várias freqüências e comprimentos de ondas com o objetivo de trafegar a maior quantidade de sinais ópticos numa mesma fibra. Para compartilhar a banda, foram criadas várias técnicas de multiplexação. Essas técnicas incluem a Multiplexação por Comprimento de Onda ou WDM (*Wavelenght Division Multiplexing*), a Multiplexação Óptica por Divisão de Tempo ou OTDM (*Optical Time Domain Multiplexing*), a Multiplexação por Divisão de Códigos Ópticos ou OCDM (*Optical Code Division Multiplexing*) além das técnicas híbridas WDM/OTDM e WDM/OCDM [3,12].

2.2.1 Multiplexação por Comprimento de Onda – WDM

Numa rede que utiliza esse tipo de multiplexação, dois ou mais sinais ópticos, com diferentes comprimentos de onda, são transmitidos simultaneamente na mesma direção. Essa técnica de multiplexação pode suportar qualquer combinação de taxas, incluindo canais ópticos ou OC (*Optical Carrier*) síncronos e assíncronos - OC-3, OC-12, OC-48, ou OC-192, na mesma fibra e ao mesmo tempo. A tecnologia WDM já está num estágio avançado de desenvolvimento e é utilizada em componentes comerciais e sistemas[12].

2.2.2 Multiplexação Óptica por divisão de Tempo – OTDM

A multiplexação por divisão de tempo (TDM) é um esquema que combina vários sinais para transmiti-los numa única linha de comunicação ou canal. Cada linha de comunicação ou canal é dividido em vários segmentos de tempo, cada um tendo uma pequena duração. Um multiplexador na ponto inicial do enlace de comunicação aceita a entrada de cada usuário, divide cada sinal em segmentos e associa cada segmento a um número de sequência. A variação do número de sinais ao longo da fibra é a flexibilidade oferecida por essa técnica de multiplexação[12].

Na multiplexação óptica por divisão de tempo, muitos canais de baixa velocidade transmitem na forma de pulsos ópticos de pequena duração, na ordem de picosegundos (ps) ou femtonsegundos (fs). Esses pulsos são intercalados para gerar grandes streamings de dados, que serão transmitidos através da fibra.

2.2.3 Multiplexação por divisão de códigos Ópticos – OCDM

Inicialmente a multiplexação por divisão de códigos CDM (*Code Division Multiplexing*) foi estudada no contexto de microondas para comunicações sem fio. No CDM, os sinais são digitalizados e codificados, para então, ser transmitida através da banda disponível. Vários sinais são sobrepostos num único canal onde cada canal possui uma única assinatura de seqüência ou código óptico. A OCMD, foi desenvolvida para utilização em redes ópticas. Uma fonte óptica é conectada a um certo número de transmissores que transmitem, em broadcast através da rede, códigos e modulam o sinal óptico. Para que cada transmissão seja diferenciada, cada usuário é associado a um único código óptico. O receptor, que é ajustado para o código correto, é capaz de selecionar qual transmissão deseja receber [3].

Este protocolo é uma tecnologia independente capaz de transportar qualquer tipo de sinal digital porém só em ambientes broadcast. A OCMD oferece uma série de vantagens, quando comparada, com outras técnicas de multiplexação (WDM ou OTDM). Segue abaixo algumas delas:

- Os sistemas OCDM são mais eficientes que os WDM, pois o sinal é reconhecido pelos códigos únicos ao invés do comprimento de onda. Nos sistemas WDM uma parte da banda, entre cada canal, é reservada para prevenção de prováveis interferências causadas por freqüências espalhadas.
- Os sistemas OCDM são inerentemente assíncronos. Sistemas OTDM requerem um alto nível de sincronização entre o transmissor e o receptor. Um pequeno atraso poderá acarretar uma interferência entre os bits de slots adjacentes a um quadro OTDM ocasionado perda de dados.

Esse tipo de multiplexação pode ser implementado utilizando técnicas de detecção coerentes e técnicas de detecção não coerentes. Na detecção coerente, um receptor verifica tanto a amplitude quanto a fase do sinal, enquanto que no método de detecção não coerente observa apenas a amplitude do sinal. Geralmente sistemas que utilizam o método de detecção coerente são mais eficientes em compensação são mais difíceis de serem implementados. Portanto, os sistemas de multiplexação por divisão de códigos ópticos, utilizam técnicas não coerentes como espalhamento de tempo, salto de freqüência e o híbrido espalhamento de comprimento de onda e tempo.

2.2.4 Técnicas híbridas de multiplexação

A técnica de multiplexação WDM pode ser combinada com outras técnicas, como por exemplo a OTDM e a OCDM. O objetivo de se combinar técnicas de multiplexação é aumentar drasticamente o número de usuários que poderão ser alocados num único canal de comunicação. Essas combinações poderão ser bastante úteis para situações onde os recursos de comunicações possam ser limitados ainda que a demanda por banda ainda permaneça alta.

2.3 Redes Totalmente Ópticas

São redes baseadas exclusivamente em comunicação óptica para todas as suas interfaces, de uma rede para outra, de usuários para uma rede, do encaminhamento e roteamento de pacotes de uma rede. Dessa maneira, a informação é transmitida inteiramente no formato óptico, descartando transformações e conversões do sinal elétrico em óptico. A eliminação das conversões reduz atrasos, aumenta a capacidade e melhora a flexibilidade da rede [12].

2.3.1 Tipos de Redes Totalmente Ópticas

As redes totalmente ópticas podem ser classificadas em Rede Ópticas Passivas (*Passive Optical Networks* - PONs), Redes Ópticas Transparentes (*Transparent Optical Networks* - TONs) e Redes Ópticas de Alta velocidade (*Ultra-High Optical Networks* - UONs).

Redes Ópticas Passivas

São redes que se utilizam de equipamentos ópticos passivos, como fibra óptica, acopladores direcionais, acopladores em estrela, roteadores passivos e filtros para sua interconexão. Geralmente utilizadas para prover comunicação entre curtas distâncias, aproximadamente 50 quilômetros. Por serem redes de curta distância, geralmente não necessitam de amplificadores de sinal óptico além de não utilizarem ativos que necessitam de energia elétrica para funcionar [3,12].

Por oferecerem baixo custo, alta disponibilidade e grandes taxas de transmissão são consideradas as melhores soluções para redes locais (LANs) e redes metropolitanas (MANs). Essas redes podem ser configuradas utilizando as topologias em estrela, árvore, barramento e anel.

Elas podem ser utilizadas para diversas aplicações. Seguem abaixo alguns exemplos:

- *Fiber To The Node* (FTTN) – A fibra é terminada numa plataforma de conexão a uma distância maior do que 300 metros do usuário final [14].

- *Fiber To The Curb*(FTTC) – Esta aplicação está relacionada com a implantação e utilização de fibra óptica, que é trazida pelo provedor de acesso até uma plataforma de conexão, aproximadamente a 300 metros do cliente final. A partir dessa plataforma, os clientes são conectados pelos cabos metálicos. Com esse tipo de aplicação a provedor de serviços poderá servir banda larga e Internet de alta velocidade para seus clientes variando as taxas de conexão de acordo com a distância do cliente para a plataforma de conexão [12,14].
- *Fiber To The Building* (FTTB) – Nessa arquitetura a fibra alcança o prédio do cliente final [14].
- *Fiber To The Home* (FTTH) – é uma arquitetura que propicia acessos em banda larga para uma série de serviços, tais como Internet, telefonia e televisão. Com o FTTH, a rede de acesso é capaz de prover taxas de transmissão de 10 Mbps até 1 Gbps. A arquitetura FTTH pode ser utilizada ainda nos projetos das "residências inteligentes", na automação doméstica e nas atividades de entretenimento [12,14].

Além das aplicações citadas acima, as rede ópticas passivas, podem ser utilizadas para alimentar outras redes com sinal óptico, tanto numa comunicação ponto a ponto, quanto em comunicações multiponto. Nessas redes estão inclusas as *Digital Loop Carrier* (DLC), os sistemas de distribuição para redes de banda larga sem fio multiponto ou LMDS (*Local Multipoint Distribution System*), sistema de distribuição multicanal para redes sem fio multiponto ou MMDS(*Multichannel, Multipoint Distribution System*), o HDSL(*High-Bit-Rate Digital Subscriber Line*) e o VHDSL(*Very High-Bit-Rate Digital Subscriber Line*) [12].

A utilização de uma rede óptica passiva ocasiona redução de custos numa DLC, pois ela provê uma solução alimentadora de fibra óptica multiponto. Uma PON pode ser usada entre um Escritório Central, de um ISP e o terminal remoto DLC provendo uma solução um enlace local a baixo custo.

Redes de banda larga sem fio precisam de uma rede núcleo de alta velocidade, entre a Central do provedor e as estações base. As estações base podem ser conectadas e o tráfego que volta para a Central pode ser agregado se uma PON for utilizada. Pode-se observar que as redes ópticas passivas oferecem uma alternativa mais barata, de maior capacidade e multiponto, quando comparada as redes de microondas [12].

As PONs podem utilizar como técnica de multiplexação o WDM, OTDM ou qualquer combinação desses, para carregar dados de voz, vídeos e outros serviços, incluindo o antigo serviço de telefonia POTS (*Plain Old Telephone Service*) OC-3, OC-12, OC-48, e sinal de televisão (analógico e digital) [14].

Redes Ópticas Transparentes

Permitem que o sinal atravesse a rede independente da modulação do sinal, taxa de dados e outras características particulares. Podem ser montadas de várias maneiras, considerando-se que, flexibilidade, alto desempenho e a cobertura local para a cobertura global são os principais objetivos dessas redes [16].

Nas redes ópticas transparentes existem limitações de transmissão devido às diferenças de requisitos de desempenho fim a fim. Tipos diferentes de sinais possuem sensibilidades diferentes à degradação cumulativa a partir das fontes, como ruídos, não linearidade óptica, dispersão cromática e polarizada. Além disso, é muito difícil suportar a transmissão de sinais analógicos por conta de sua sensibilidade a reflexões ópticas e sua necessidade de linearidade. Desta forma, as redes ópticas transparentes podem não oferecer a transparência mais pura e para reduzir esse problema, existem formas de definir níveis de transparência nas TONs [14].

Redes Ópticas Ultra-Rápidas

Se utilizam das características de alta velocidade fornecidas por fenômenos ópticos para transmissão de pulsos ópticos, a 100GB/s ou mais, em de redes de longa distância. Algumas tecnologias chaves são necessárias para a implementação dessas redes incluindo, a geração de pulsos ópticos, multiplexação, recuperação de sincronismo e *buffers* ópticos. Esse tipo de rede utiliza OTDM como técnica de multiplexação.

Existem duas características físicas nas fibras ópticas que direcionam a estrutura de uma rede óptica. A primeira é a dispersão cromática, uma propriedade, de toda fibra óptica, que produz pulsos luminosos de diferentes freqüências que passam através da fibra com velocidades diferentes. A segunda propriedade é a pequena modificação causada no índice de refração da fibra que comprime o pulso quando a luz viaja através da fibra. Essa modificação é conhecida como efeito Kerr e é definida pela força e forma do pulso.

Na multiplexação óptica por divisão de tempo, a sincronização é essencial para se estimar o tempo que informação levará para chegar no receptor. Duas técnicas de sincronização foram propostas para as redes ópticas ultra-rápidas que usam OTDM.

2.4 Arquiteturas de Rede Totalmente Ópticas

Nesta seção serão discutidas algumas arquiteturas baseadas nas técnicas de multiplexação WDM, OTDM, OCDM e suas aplicações.

2.4.1 Arquitetura baseada em WDM

A arquitetura, ilustrada na Figura 8, provê escalabilidade através da reutilização de comprimentos de onda e multiplexação por divisão de tempo (TDM), especificando 3 níveis hierárquicos de sub-redes independentes.

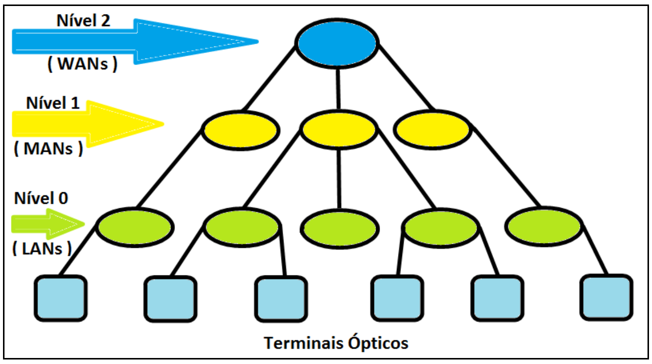


Figura 8: Arquitetura Baseada em WDM [14]

No nível mais baixo da hierarquia estão as sub-redes Nível 0, formada por uma coleção de redes locais (LANs) de alto desempenho. Os usuários acessam a rede através dos terminais ópticos (OTs) que são conectados a sub-rede de nível 0 através de um par de cabos de fibras [14]. Cada sub-rede compartilha recursos de rede com as outras sub-redes do mesmo nível. No nível 1, comumente conhecido como nível das redes metropolitanas (*Metropolitan Area Networks* - MANs), cada uma delas conecta um conjunto de sub-redes do nível 0 e compartilha recursos de rede entre elas. No nível mais alto da hierarquia pode-se observar a sub-rede nível 2, WAN (*Wide Aera Network*) que provê conexão para os níveis mais baixos através de nós interconectados por uma topologia em malha usando roteadores e conversores de comprimento de onda.

Cada sub-rede provê três tipos de serviços para sub-redes de nível mais baixo ou terminais ópticos, no caso do nível 0. Esses serviços podem ser classificados como serviços de Classe A, Classe B e Classe C. O serviço de Classe A provê meio físico óptico para comunicações ópticas ponto a ponto, ponto a multiponto e multiponto a multiponto. Os serviços de Classe B utilizam o TDM de forma transparente e são úteis para aplicações que necessitam de pouca banda. Um usuário consegue transmitir dados, de qualquer formato, através dos slots de tempo TDM. Os *slots* de tempo são especificados durante o início da conexão para garantir a recuperação do sinal apropriada na transmissão em caso de falha. A classe B suporta conexões ponto a ponto, ponto a multiponto, multiponto a multiponto. O serviço de Classe C não é transparente e serve como um enlace de comunicação comum entre todos os usuários da rede. Pode ser usado para configuração automática da rede, controle e gerenciamento da rede, operação e manutenção da rede.

Cada sub-rede possui um agente agendador que lida com várias funções, incluindo alocação de *slots* de tempo e comprimentos de onda para os pontos de acesso. Esses pontos de acesso são interfaces ópticas entre os terminais ópticos e a rede. O agente pode ser implementado em um ou mais terminais ópticos ou até mesmo em um nó específico de cada sub-rede. Um algoritmo distribuído é o responsável pela seleção do agente principal da sub-rede. Em caso de falha do agente selecionado este mesmo algoritmo é processado mais uma vez e um novo nó é escolhido.

Nessa arquitetura, quando um terminal óptico precisa estabelecer uma conexão, envia uma solicitação para o agente agendador do nível 0. A solicitação de conexão possui várias informações tais como, tipo do serviço solicitado, endereço do terminal solicitado, a vazão desejada e a prioridade. Assim que recebe a requisição o agente verifica se o terminal óptico está no mesmo nível de sub-rede. Se não estiver, verifica a disponibilidade dos recursos necessários para que a conexão seja estabelecida. Se os recursos estiverem disponíveis, então a conexão é estabelecida sem problemas.

No caso do destino estar localizado num nível acima, porém na mesma rede, o agendador do nível mais baixo solicita ao agente da rede superior que ele selecione um comprimento de onda para prover o caminho entre as sub-redes.

2.4.2 Arquitetura baseada em OTDM

Este tipo de arquitetura foi desenvolvida para lidar com comunicações de alta velocidade. Mesmo assim, algumas características relativas ao seu *design* tiveram que ser consideradas.

Primeiramente, a necessidade de uma arquitetura para prover, ao mesmo tempo, serviços que precisavam de banda garantida e acesso sob demanda. Em segundo plano, uma política para regulamentar o compartilhamento de banda de uma forma eficiente e justa para os usuários de aplicações sob demanda. E por último, algoritmos simples o bastante pra serem executados nas taxas requeridas pelas redes ópticas.

A HLAN (*Helical Local Area Network*) é uma arquitetura em quadros que utiliza barramento unidirecional e pode ser implementada numa estrutura linear, mais comum em redes metropolitanas. A HLAN foi projetada para operar a 100Gb/s.

2.4.3 Arquitetura baseada em OCDM

Nessa, arquitetura os nós da rede estão conectados a um acoplador passivo em estrela. O codificador OCDM de cada nó envolvido na transmissão representa um bit "1" para uma série de pulsos ópticos chamados de assinatura de sequência ou código óptico. O bit "0" não é codificado, sendo representado por uma sequência de zeros. Os sinais de cada nó são enviados separadamente para o acoplador e anunciados para os outros nós da rede via mensagens *broadcast*.

O objetivo principal de um sistema OCDM é fazer com que um nó seja capaz de trafegar informações na rede mesmo com a presença de pulsos ópticos de outros nós, utilizando para isso sua assinatura. Para que esse objetivo seja cumprido um sistema OCDM é desenvolvido baseado em três condições:

- Para qualquer correlação não deslocada no tempo, a auto-correlação será igual ao peso da assinatura e deve ser a maior possível para que o sinal recebido seja maior que o ruído do sistema.
- Para qualquer correlação deslocada no tempo, a auto-correlação será menor que o peso do código. Essa condição deve ser satisfeita para garantir que o sinal na saída do acoplador óptico seja menor quando não estiver sincronizado com o transmissor, isso permite que o sistema OCDM opere sem a necessidade de sincronização.
- A correlação deslocada para uma dada assinatura deve ser minimizada afim de permitir que o sistema OCDM opere sem a necessidade de sincronização.

Segundo Fábio Renan, sendo as condições acima satisfeitas o sistema operará de forma assíncrona e com baixa taxa de erros. Mesmo considerando que apenas uma fração de usuários utiliza a rede óptica simultaneamente, é preciso prover um número de assinaturas para todos os usuários da rede. O número máximo de códigos ópticos disponíveis numa rede óptica é dado pela cardinalidade. A cardinalidade representa o número máximo de usuários suportado por um conjunto de códigos OOC com o mesmo comprimento e peso que satisfazem as condições de correlação descritas acima. O desempenho de um sistema OCDM é medido por meio da taxa de erros de bits e considera o número de usuários que estão utilizando a rede simultaneamente.

2.5 Perspectiva Histórica

As redes de telecomunicações vem evoluindo durante um longo período de avanços tecnológicos e mudanças sociais. Redes que proviam apenas simples serviços de telefonia entre operadoras locais, hoje são capazes de transmitir milhões de dados para qualquer lugar do mundo, num curto espaço de tempo.

2.5.1 Surgimento da Comunicação Óptica

A utilização da luz para a transmissão de informação, de um lugar para outro é uma técnica muito antiga. Em 800 A.C., os Gregos usavam fogo e sinais de fumaça para mandar informações como vitórias em guerras, alertas contra inimigos, pedido de ajuda, etc. Durante o segundo século A.C., sinais ópticos foram codificados utilizando lâmpadas de sinalização e qualquer mensagem de sinalização podia ser enviada [1,2].

Até o final do século XVIII a comunicação óptica não evoluiu. Sua velocidade era limitada devido à exigência de caminhos lineares de transmissão, o olho humano como o receptor e o ar como um meio não confiável que sofria impactos como a chuva e geadas [1].

Em 1791, o francês Chappe desenvolveu o *Semaphore* para as telecomunicações na terra, mas que também possuía limitações quanto a transferência de informações. Considerado como o primeiro sistema de comunicações digitais de alta velocidade na história do homem, o *Semaphore* era baseado num dispositivo de braços mecânicos, o qual, instalado no alto de uma torre e operado manualmente, permitia a transmissão de sinais visuais à distância [1,3,4].

Em 1835, Sammuel Morse inventou o telégrafo e a era de comunicação elétrica foi iniciada pelo mundo. O telégrafo foi o principal sistema de comunicação a longa distância dos séculos XIX e começo do século XX, sendo utilizado por indústrias, governos, e forças armadas [4].

Alexander Graham Bell propôs, em 1872, o fotofone com diafragma, ilustrado na Figura 9, transmitindo um discurso falado por uma distância de 200m [1]. Quatro anos depois, em 1876, Graham Bell tinha mudado o *fotofone* para telefone utilizando a corrente elétrica para transmissão de sinais de voz e em 1878, o primeiro aparelho telefônico foi instalado em *New Haven, Connecticut*, pela *Bell Telephone Company*, criada por ele [1,2].

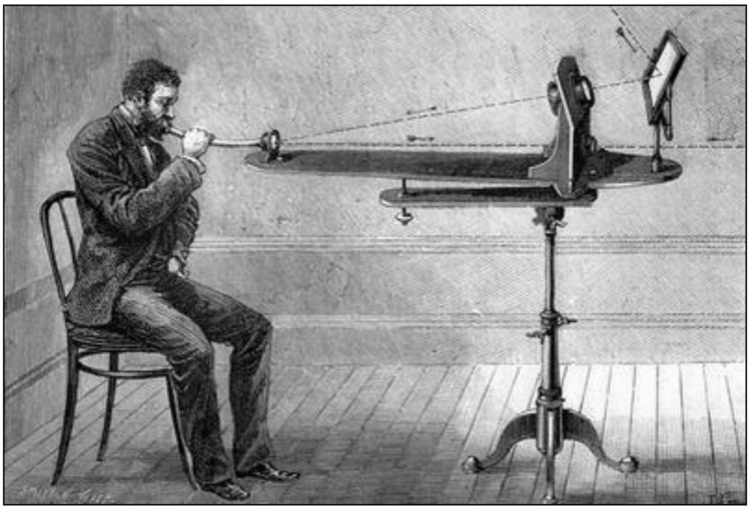


Figura 9: Fotofone inventado por Graham Bell [1]

As ondas de rádio foram descobertas por Hertz em 1887 e em 1895 Marconi demonstrou a comunicação de rádio sem a utilização de fios, utilizando técnicas de modulação de sinal [1,3].

Em meados do século XX, percebeu-se que a utilização de sinais ópticos poderia ser aproveitada para transporte de informação. Com a invenção do laser em 1958 e sua primeira realização prática nos EUA em 1960, os esforços de pesquisa e desenvolvimento em comunicações ópticas tiveram um novo impulso. O laser constituía de uma fonte luminosa com potência e capacidade de transmissão que permitiu que, sistemas de comunicações ópticas de longo alcance com grande banda passante. Os avanços técnico-científicos na área resultaram, em 1962, na irradiação do primeiro laser semicondutor e do primeiro fotodiodo PIN de silício de alta velocidade [1,2,3].

2.5.2 Surgimento da fibra Óptica

No início da década de sessenta, os sistemas de transmissão óptica tinham como problema principal a falta de disponibilidade de um meio adequado para que a transmissão da luz a distância porque a atmosfera se mostrava como um meio adverso e limitado por sempre estar sujeita à modificações climáticas. O físico indiano Narinder Singh Kanpany inventou a fibra óptica em 1952 e em 1966, os cientistas Kao e Hockman defenderam a utilização de fibras de vidro em sistemas de transmissão a longa distância [1,4]. As fibras eram compostas por uma estrutura de núcleo e casca, utilizando a estrutura proposta anteriormente por Kanpany.

A atenuação no sinal representa a perda de potência óptica e é característica fundamental na determinação da distância máxima entre um transmissor e um receptor óptico. O trabalho defendido por Kao e Hockman, mostrava que a forte atenuação não era intrínseca ao material(vidro) utilizado, mas, principalmente, por conta das impurezas que ele continha. Com isso, chegaram a conclusão de que com a purificação do material básico das fibras era possível se chegar à atenuações inferiores a 20 dB/km, limite de viabilização, na época, para utilização de fibras em sistemas de telecomunicações. A partir daí, além da Inglaterra, outros países começaram a estudar formas de purificação do vidro e problemas de transmissão em fibras ópticas [4].

A década de setenta foi o período onde se consolidaram na prática as teorias sobre comunicações ópticas desenvolvidas anteriormente. A teoria simplificada sobre propagação em fibras ópticas apresentada por Gloge, em 1971, trouxe uma importante contribuição para o desenvolvimento de sistemas de transmissão com fibras ópticas. Segue abaixo uma lista de acontecimentos relevantes para consolidação da transmissão em fibras ópticas [2,4]:

- Em 1972, a Corning Glass Works anunciou a fabricação de fibra multimodo com perdas inferiores a 4 dB/km;
- Em 1973, o cientista Personik da *Bell Laboratories* analisou e apresentou o desempenho de receptores ópticos em sistemas de comunicações digitais;
- Em 1975, os ingleses Payne e Gambling identificam uma janela de dispersão mínima para fibras ópticas de sílica. A partir daí, estudos e desenvolvimento em fibras ópticas, foram concentrados nessa região espectral afim de se conseguir sistemas com grande capacidade de transmissão;
- Em 1976, surgiu a fibra monomodo, resultante de estudos sobre a purificação da sílica. Essa fibra possui atenuação inferior a0,46 dB/Km e o grau de purificação não interferia na perda de dados durante transmissões. Nesse ano também, foram testados os primeiros sistemas ópticos de transmissão. Surge em Hastings, Inglaterra, a primeira concessionária de serviços de rede com fibra. O sistema era composto por um enlace

de fibra de 1,4 km e provia o núcleo de rede para distribuição de sinais de televisão à cabo para aproximadamente 34 mil assinantes;

- Em abril de 1977 entrou em operação o primeiro enlace com fibra óptica no sistema telefônico dos Estados Unidos, na Califórnia.

2.5.3 Evolução das Redes Ópticas

A evolução das redes, que utilizam a fibra como meio, exige cada vez mais capacidade, velocidade e formas de conexão. É importante observar que num período de vinte anos, entre 1981 até 2001, a taxa de transmissão de dados para a comunicação geograficamente distribuída passou de 56 Kbps (ARPANET) para 1 Gbps. Do início deste século para os dias de hoje, ocorreu uma nova evolução com relação à capacidade dos enlaces da ordem de Gigabits por segundo (Gbps) passaram a operar na ordem de Terabits por segundo (Tbps).

A Bell Labs, parte da Alcatel-Lucent, já conseguiu transmitir 100 Petabits por segundo por quilômetro (Pbps/km), um recorde em transmissões via fibras ópticas. Esse tipo de avanço interessa aos fornecedores serviços de rede, por exemplo, provedores de redes de conteúdos, que necessitam de uma infra-estrutura capaz de suportar grandes taxas de transmissões e de aplicações sob-demanda, que desejam divulgar suas aplicações para a maior quantidade de usuários possível.

Um lado importante que deve ser observado é o fator economia. Segundo os gerentes de tecnologia da informação, a principal vantagem oferecida pela evolução das redes ópticas e aumento nas capacidades de transmissão é a queda do custo por bit ou dado trafegado.

Capítulo 3 - Gerenciamento e Monitoramento de redes

O gerenciamento de um ambiente de rede consiste na supervisão e controle do funcionamento da rede para que ele satisfaça os requisitos tanto dos seus usuários quanto do seus proprietários. O monitoramento da informação é uma função crítica numa rede coorporativa que pode trazer benefícios econômicos e um melhor aproveitamento dos recursos da rede. Neste capítulo serão abordadas questões sobre protocolos e ferramentas para gerenciamento de redes além de suas características e aplicações.

3.1 Gerenciamento de redes

O gerenciamento de redes se refere a atividades, métodos, procedimentos que devem verificar o funcionamento da rede sem que seu desempenho seja degradado, geralmente abrangendo as seguintes tarefas:

- Detecção de falhas de rede, gateways e servidores críticos;
- Formas de notificação, para os administradores, em caso de falhas da rede;
- Monitoramento geral para balanceamento de carga e planejamento de expansões;
- Documentação e visualização da rede;
- Administração de dispositivos de rede a partir de um ponto central.

As ferramentas para gerenciamento podem ser simples *softwares* ou *firmwares* embutidos, que integram *hardware* e uma camada de *software* de finalidade específica, conhecido como A*ppliance*. Para monitoramento de redes pode-se utilizar ferramentas bastante simples que enviam sinais para os dispositivos com a finalidade de verificar se estão respondendo às requisições, para analisar o tempo de resposta ou até mesmo identificar saltos entre os pontos da rede. As ferramentas mais utilizadas pelos administradores trazem informações mais detalhadas sobre o estado da rede sendo capazes de gerar relatórios sobre o comportamento da rede, coletar informações sobre o nível de utilização dos protocolos existentes, verificar quais as aplicações mais utilizadas na rede. Sempre gerando relatórios minuciosos e gráficos que resumem, de forma automática, as condições da rede em determinado instante.

3.1.1 Protocolos e ferramentas de gerenciamento de redes

Os protocolos de gerenciamento em redes padronizam as formas de análise e investigação de um ou uma rede de dispositivos, para observar suas configurações, seus estados de funcionamento, seu estado de conexões e carga de utilização dos recursos dos ambientes gerenciados. As ferramentas de gerenciamento são implementações do que foi padronizado pelos protocolos.

SNMP

O SNMP (*Simple Network Management Protocol*) é um protocolo muito utilizado na gerência de redes de computadores. Ele permite que os administradores sejam capazes de gerenciar recursos de servidores, tais quais, capacidade de armazenamento disponível, carga de processamento, gerenciar roteadores, verificando o número de pacotes enviados e recebidos, observando também o número de pacotes com erros, etc. Os dados SNMP são organizados segundo uma hierarquia padronizada que funciona de forma semelhante a um sistema de arquivos, porém, utiliza-se o ponto como caractere separador e cada objeto recebe um número de identificação. Esse número refere-se ao identificador do objeto ou OID (*Objetc Identifiers*) e serve para identificar as buscas por um objeto que contêm as informações de gerenciamento desejadas. Os OIDs são armazenados em uma base de dados conhecida como MIB (*Management Information Base*) que é acessada por agentes que procuram informações sobre um recurso específico de um dispositivo monitorado.

Por convenção, os objetos também recebem nomes textuais para facilidade de referência, sendo assim, uma conveniência de alto nível, e não um recurso da hierarquia definida. Essa convenção faz com que a identificação de um objeto SNMP ocorra de forma semelhante a identificação de um endereço IP (*Internet Protocol*) através do DNS (*Domain Name System*), onde um endereço IP é atrelado a um nome. Dessa forma, a busca por um *host* da rede pode ser feita através do nome escolhido, além da busca pelo IP. Segue abaixo um exemplo de utilização dessa convenção, onde pode-se observar o OID que se refere ao tempo de funcionamento do sistema e seu respectivo nome:

- *OID: 1.3.6.1.2.1.1.3.;*
- *Nome: iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.*

Num ambiente de gerenciamento existem entidades que possuem atribuições específicas definidas pelo protocolo SNMP. O gerente SNMP é a entidade responsável por coletar os dados de um dispositivo de rede que está sendo monitorado. Mesmo sendo denominado como gerente SNMP, essa entidade se caracteriza por ser uma aplicação cliente, quando implementada, pois recebe os dados fornecidos pelo agente SNMP. Um agente SNMP é a entidade responsável por coletar informações de um dispositivo monitorado e fornecê-las para o gerente SNMP que solicitou a informação, fazendo assim, o papel de um servidor de serviço.

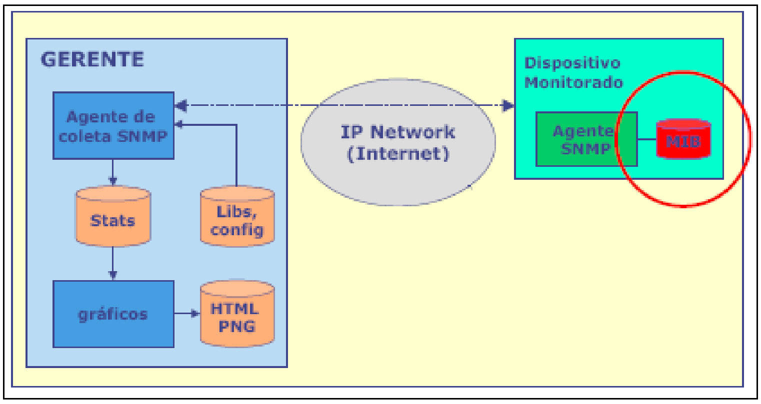


Figura 10: Ambiente de gerenciamento e suas entidades

A Figura 10 apresenta um ambiente de gerenciamento mostrando que uma rede gerenciada pelo protocolo SNMP é composta por 3 componentes básicos:

1. Dispositivos monitorado: objeto de análise;
2. Agentes: daemons para coleta de informações;
3. Sistemas de gerenciamento de rede (NMS).

Um dispositivo monitorado pode ser um *host* da rede que possui um agente SNMP instalado e se encontra em uma rede gerenciada. Esses dispositivos armazenam informações de gerenciamento em suas MIBs mantendo-as disponíveis para sistemas de gerenciamento. Um agente pode ser um *daemon* ou um *script*, geralmente um módulo de *software*, que fica armazenado no dispositivo monitorado coletando informações da MIB para o agente de coleta do gerente SNMP. A comunicação entre os gerentes e agentes se dá através da utilização do protocolo de transporte UDP (*User Datagram Protocol*), de maneira que as mensagens sejam trocadas de forma eficiente.

Um sistema de gerenciamento de rede é uma aplicação capaz de gerenciar vários agentes e a utilização de uma comunidade SNMP garante que esses agentes só respondam as solicitações dos gerentes que estão em sua comunidade. A comunidade SNMP é um *string* que define um grupo de agentes/gerente e funciona como forma de autenticação e controle de acesso às informações dos objetos.

O protocolo SNMP permite quatro operações básicas, *get, get-next, set* e *trap.* As operações *get* e *set* são operações básicas para leitura e gravação de dados em um objeto identificado por um OID específico. A operação *get-next* varre uma hierarquia MIB e podendo ler o conteúdo delas. A operação *trap* é uma notificação assíncrona e não solicitada do agente para o gerente que relata a ocorrência de um evento.

ICMP

O protocolo ICMP (*Internet Control Message Protocol*) permite o transporte de mensagens de controle e mensagens de teste utilizando como meio de transporte os protocolos TCP/IP. As mensagens enviadas pelo ICMP são encapsuladas em pacotes IP e transportadas pelo TCP. As mensagens trocadas podem ser classificadas como mensagens de erro e mensagens de solicitação (*Query*) e cada uma delas possui uma estrutura própria, onde o cabeçalho do pacote ICMP é fixo e a carga do pacote varia dependendo do tipo de mensagem ICMP. O cabeçalho do ICMP é formado por 3 campos, *Type, Code* e *Checksum*. O campo *Type* informa o tipo da mensagem ICMP e são identificados por um número. A Tabela 1, mostra o tipo de mensagem de acordo com o seu número.

Tipo	Mensagem ICMP
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
9	Router advertisement
10	Router solicitation

11	TTL excced
12	Parameter problem
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

Tabela 1: Tipos de mensagem ICMP

O campo *Code* indica alguma condição mais específica do tipo de mensagem ICMP e cada condição é identificada por um número. O campo *Checksum* recebe um código serve para verificação de consistência. Qualquer campo que não seja utilizado é reservado para extensões futuras. Os tipos de mensagens *Echo Request* e *Echo Reply* são utilizadas principalmente para fins de testes de conectividade entre dois *hosts* de uma rede, por exemplo.

PING

A ferramenta Ping testa se um determinado host está ativo numa rede IP. Ela funciona enviando uma requisição ICMP para um destino e escutando por respostas ICMP para respondê-las.

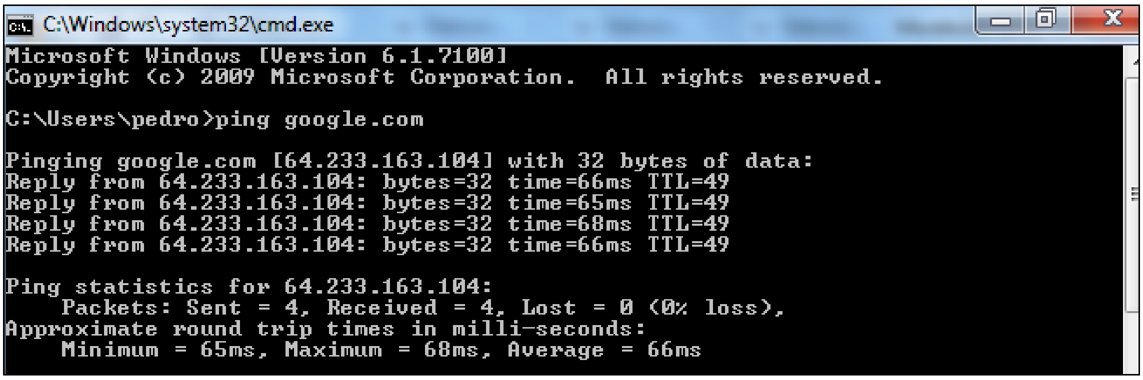


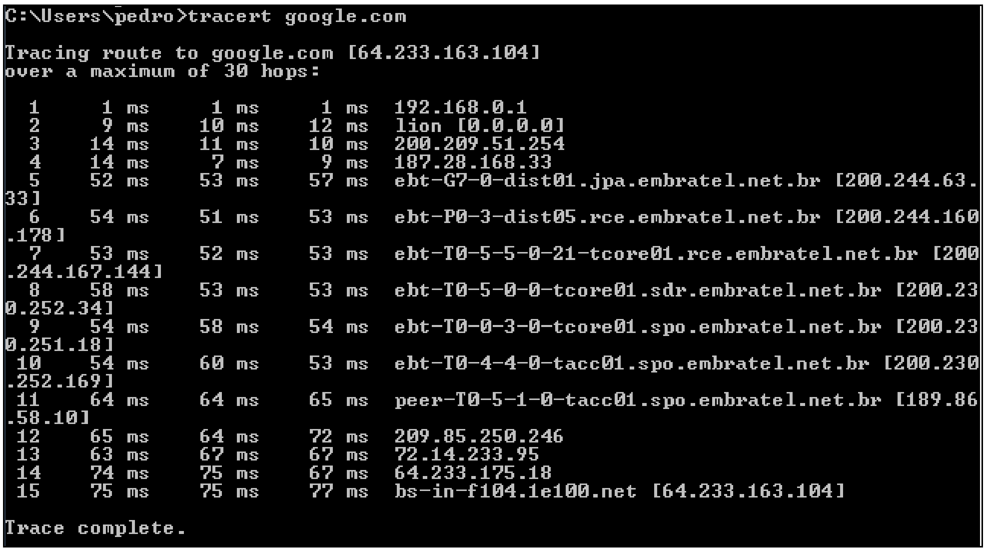
Figura 11: Saída padrão da ferramenta Ping

O Ping estima o RTT (*Round Trip Time*) em milisegundos, mostrando um relatório resumido com o percentual de pacotes perdidos e o tempo de resposta. A Figura 12 apresenta a saída básica do comando Ping quando utilizado sem a adição de parâmetros extras, além do *host* a ser testado. A resposta consiste no tamanho do pacote utilizado, no nome do *host* destino, no número de sequência do pacote ICMP, no tempo de vida e na latência, com todos os tempos dados em milisegundos.

Traceroute/Tracert

O traceroute é uma ferramenta que revela a sequência de gateways que um pacote IP percorre para alcançar seu destino utilizando mensagens ICMP. Existem implementações dessa ferramenta para os sistemas operacionais mais utilizados hoje em dia. O comando tracert utilizado pelo sistema *Microsoft Windows* e o comando traceroute utilizado pelos sistemas Linux.

O TTL (*Time To Live*) representa o tempo de vida de um pacote na rede e cada vez que um pacote passa por um roteador o TTL é decrementado em uma unidade. Um pacote pode entrar em *loop* devido a um defeito num roteador, ou até mesmo, a uma configuração mal feita. Para que isso não aconteça o TTL é decrementado até ser zerado e o pacote é descartado.


```
C:\Users\pedro>tracert google.com

Tracing route to google.com [64.233.163.104]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     9 ms    10 ms    12 ms  lion [0.0.0.0]
  3    14 ms    11 ms    10 ms  200.209.51.254
  4    14 ms     7 ms     9 ms  187.28.168.33
  5    52 ms    53 ms    57 ms  ebt-G7-0-dist01.jpa.embratel.net.br [200.244.63.
33]
  6    54 ms    51 ms    53 ms  ebt-P0-3-dist05.rce.embratel.net.br [200.244.160
.178]
  7    53 ms    52 ms    53 ms  ebt-T0-5-5-0-21-tcore01.rce.embratel.net.br [200
.244.167.144]
  8    58 ms    53 ms    53 ms  ebt-T0-5-0-0-tcore01.sdr.embratel.net.br [200.23
0.252.34]
  9    54 ms    58 ms    54 ms  ebt-T0-0-3-0-tcore01.spo.embratel.net.br [200.23
0.251.18]
 10    54 ms    60 ms    53 ms  ebt-T0-4-4-0-tacc01.spo.embratel.net.br [200.230
.252.169]
 11    64 ms    64 ms    65 ms  peer-T0-5-1-0-tacc01.spo.embratel.net.br [189.86
.58.10]
 12    65 ms    64 ms    72 ms  209.85.250.246
 13    63 ms    67 ms    67 ms  72.14.233.95
 14    74 ms    75 ms    67 ms  64.233.175.18
 15    75 ms    75 ms    77 ms  bs-in-f104.1e100.net [64.233.163.104]

Trace complete.
```

Figura 12: Saída padrão de Traceroute

O traceroute envia 3 pacotes com TTL igual a um. O primeiro salto (*hop*) responde que o pacote não pode ser transmitido porque o TTL expirou com a mensagem "*ICMP Time-To-Live Exceeded (Type 11)*". Então o segundo pacote é reenviado com TTL igual a dois e o segundo roteador responde que o TTL expirou. Esse processo continua até o *host* destino ser encontrado.

Com o traceroute obtemos apenas o caminho de ida dos pacotes até seu destino, pois, o caminho de retorno pode ser diferente, por questões de roteamento. A resposta do traceroute exibe três tempos, para cada salto, isso porque um roteador é testado três vezes.

A Figura 12 mostra um teste para descobrir quantos saltos são necessários para que um servidor, que responde pelo nome *google.com* na Internet, seja atingido.

Analisadores de Protocolos

Os analisadores de protocolos são ferramentas capazes de escutar o tráfego de uma rede, capturando os pacotes que atendam a certos critérios escolhidos pelo usuário que está fazendo a captura. Após a captura os dados coletados são analisados e utilizados para isolar os problemas descobertos.

A operação básica de uma analisador de protocolos consiste da utilização de uma interface de rede ou NIC (*Network Interface Card*) operando em modo promíscuo para capturar todos os pacotes que passam pela rede, com esses dados armazenados, o próximo passo é a filtragem e classificação dos protocolos coletados. Os resultados gerados e exibidos por esse tipo de ferramenta são capazes de classificar os protocolos, dessa maneira, os administradores da rede focarão seus esforços em examinar apenas os pacotes relevantes, de acordo com o critério adotado por eles.

Algumas características podem ser observadas nos analisadores de protocolos. A filtragem de pacotes é a forma de análise onde o analisador separa o tráfego coletado baseado no tráfego selecionado pelo administrador da rede. A estratégia de *Packet Slicing*, permite que o analisador guarde pedaços de pacotes capturados de acordo com a necessidade de quem está analisando a rede. O *Triggering* ocorre quando algum evento especial dispara a captura de pacotes. Outras características importantes são a geração de tráfego arbitrário a partir de tráfegos coletados, que podem ser usados para estudos sobre o comportamento de redes.

3.2 Monitoramento de Rede

O monitoramento de uma rede pode ser feito através de vários softwares, através da combinação de *softwares* e um *hardware plug'n'play* específico ou até mesmo, com a aquisição de soluções *Appliance*. Qualquer tipo de rede pode ser monitorada, como por exemplo, redes sem fio, redes cabeadas, intranets, redes virtuais privadas (VPNs) ou uma até mesmo uma WAN (*Wide Area*

Network) provida por um ISP. Um ambiente de monitoramento bem estruturado poderá ajudar aos gerentes da rede a identificar atividades específicas e métricas de desempenho para a rede, coletando informações que direcionam os gestores da rede a atender as necessidades do negócio. Uma base de dados com informações críticas sobre a rede pode ser construída a partir de um sistema de monitoramento de rede que utilizará informações contidas nessa base para o planejamento de expansões. Algumas atribuições são pertinentes aos sistemas de monitoramento:

- Minimizar custos destacando pontos redundantes;
- Analisar a produtividade de funcionários de uma empresa;
- Apontar pontos de gargalo ou equipamentos sobrecarregados;
- Verificar latência e atraso na transferência de dados;
- Identificar tráfego anômalo ou desconhecido;
- Identificar quais são os usuários mais pesados e o que eles trafegam na rede;
- Levantar estatísticas e relatórios sobre o comportamento da rede.

As razões para se investir tempo, recursos humanos e financeiros num ambiente de monitoramento são a manutenção da segurança da rede em alto nível, a garantia da disponibilidade da rede e o principal, aumento no desempenho da rede.

3.3 Ferramentas utilizadas pela GTI

As ferramentas de gerenciamento de rede deixam o administrador a par do que está ocorrendo na rede no instante em que a informação foi coletada. Muitos problemas podem ser isolados com a utilização de ferramentas para gerenciamento da rede. Os problemas detectados podem estar relacionados ao mal uso dos recursos da rede, a falta de planejamento adequado no projeto de rede, mal dimensionamento da rede e falta de equipamentos, etc. A utilização de ferramentas auxilia o administrador de rede a identificar e isolar alguns desses problemas.

3.3.1 REPING

O Reping é um conjunto de ferramentas desenvolvidas pelos analistas de sistemas do setor de Infra-Estrutura de redes da GTI para monitorar a rede SER, servidores e os outros equipamentos interconectados (impressoras de rede, câmeras, etc), cujos dados são acessíveis via linha de comando Unix. O servidor do Reping é ativado a cada reinicialização através de um s*hell script* chamado ativa_reping.sh.

Com essa ferramenta podemos gerar relatórios a partir de um histórico sobre o comportamento dos enlaces além de monitorar os enlaces em tempo real e observar quando os mesmos estiveram inativos.

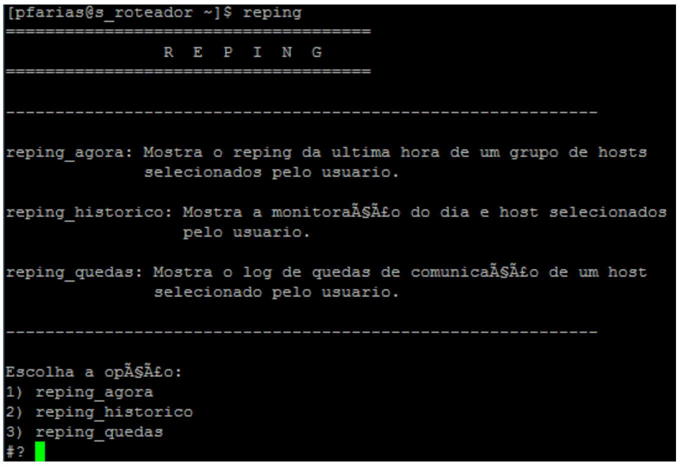


Figura 13: Tela Inicial do reping

Outro *shell script* chamado reping_host.sh cria, para o *host* monitorado, um arquivo contendo os dados da monitoração daquele *host* para cada dia, sendo este arquivo atualizado pela inserção de um caractere por minuto. Esse caractere indica o número de pacotes que foram perdidos em uma sequência de 10 pacotes de *ping*, usando-se a seguinte convenção:

- O caractere ponto (.) indica que não houve perda;
- Caracteres de um a nove (1 a 9) indicam o número de pacotes perdidos;
- Caractere til (~) indica perda de todos os pacotes;

Cada vez que a hora muda, esses caracteres passam a ser gravados em uma nova linha, precedidos pela identificação da hora. Assim, cada linha conterá aproximadamente 60 desses caracteres. Esse número não pode ser garantido pela possibilidade de congestionamentos e atrasos na rede. Na Figura 14, está o exemplo de um arquivo onde o enlace não possui congestionamentos nem perdas de pacotes.

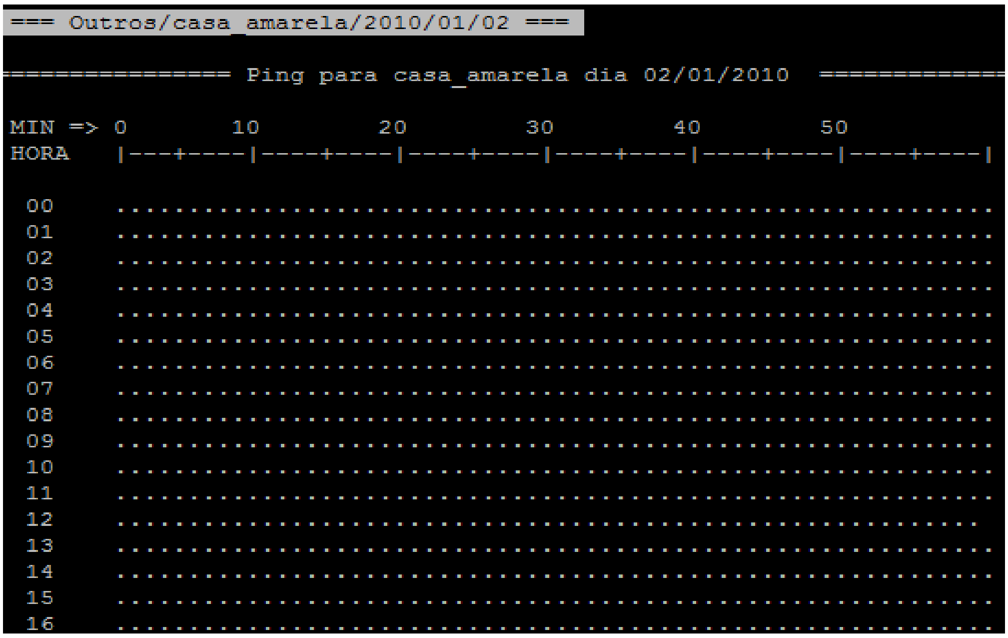


Figura 14: Exemplo de um arquivo de monitoração de um enlace sem problemas

É possível observar que o arquivo inicia-se por um cabeçalho que identifica o *host* e o dia e uma régua numerada onde os minutos são representados. Apesar de não ser rigorosamente exato, fornece valores aproximados.

3.3.2 MRTG

O MRTG (*Multi Router Traffic Grapher*) é uma ferramenta que utiliza o protocolo SNMP para a obtenção de informações de tráfego dos mais variados objetos presentes em um ambiente de rede. Apesar de ser uma ferramenta usada basicamente para análise de tráfego, quaisquer dados obtidos através do protocolo SNMP podem ser monitorados por essa ferramenta. O MRTG gera gráficos a partir de dados coletados de outros *softwares* que também suportam o protocolo SNMP. Os gráficos gerados pelo MRTG podem ser visualizados em formato HTML(*HyperText Markup Language*). Temos como características marcantes no MRTG:

- Geração de gráficos para medição de tráfego;
- Leitura de dados via protocolo SNMP ou através de scripts que retorne um formato padrão;
- Facilidade de instalação devido a presença de ferramentas web para instalação;

- O MRTG é um software livre. Distribuído de acordo com os termos da licença GPL(*General Public License*).

Capítulo 4 – Redes MPLS

Nesse capítulo serão discutidos tópicos relacionados a qualidade de serviço, segurança e engenharia de tráfego, todos relacionados as redes MPLS (*Multipath Label Switching)*.

4.1 Qualidade de Serviço (QoS)

A qualidade de serviço se baseia na capacidade de um dispositivo escolher o caminho para que o fluxo de tráfego tenha o nível de serviço aceitável criando as condições necessárias para o melhor uso dos recursos da rede. Estes níveis podem estipular nível de banda, atraso, perda, erros, prioridade para determinado tipo de tráfego dentre outras características relevantes ao bom desempenho da rede. É possível realizar *QoS* com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos de uma rede privada virtual ou VPN(*Virtual Private Network*) [26,28] . Os produtos que os provedores de serviços de redes utilizam ganham valor, pois passam a não oferecer apenas banda e sim um tráfego diferenciado com *QoS* provendo as seguintes classes de serviço:

- Priorização de Serviços de Multimídia: A qualidade de serviço poderá atuar priorizando o tráfego dos pacotes multimídia, como áudio, vídeo, vídeo sob-demanda, vídeo conferência;
- Priorização de Serviços de Voz: Nesse caso os pacotes de voz terão prioridade sob qualquer outro tipo de tráfego. Aplicações como telefonia IP, interligação de PABX;
- Priorização de tráfego de dados de aplicações críticas escolhidas pelos clientes;
- Dados: tráfego de dados sem priorização ou por melhor esforço.

Desta maneira a qualidade de serviço agrega inteligência e opções para a administração dos níveis de serviços de acordo com as políticas e necessidades do ambiente de rede.

Uma rede que possui o protocolo MPLS implementado tem a capacidade de rotear os pacotes com maior velocidade e menor carga de processamento nos roteadores da rede. Para que isso aconteça, rótulos são adicionados aos pacotes que serão roteados de acordo com sua aplicação geradora. Num domínio MPLS, o QoS no roteamento é feito de duas maneiras. A primeira forma de utilização da qualidade de serviço, o rótulo MPLS indica as informações sobre as Classes de

Serviço (*Class of Services* - CoS) e a partir dessas informações o tráfego é gerenciado e priorizado a medida que o tráfego segue na rede. A segunda forma de utilização é quando uma rede MPLS é capaz de estabelecer vários caminhos para os dispositivos de entrada e saída do domínio. Para cada parte da informação trafegada é estabelecido um nível de serviço apropriado, e o tráfego é direcionado para o caminho adequado quando entra na rede [28,29].

4.2 Conceitos Básicos

O MPLS (*Multiprotocol Label Switching*) é um protocolo que tem como objetivo, efetuar o encaminhamento de pacotes de forma mais eficiente através da troca de rótulos, onde cada rótulo representa um índice na tabela de roteamento do próximo roteador. A forma como os rótulos são agregados aumenta a eficiência no encaminhamento de dados, habilitando os provedores de serviços de redes a atenderem as demandas por QoS (*Quality of Service*) [24,28]. Membros do IETF (*Internet Engineering Task Force*) trabalharam extensivamente para elaborar um conjunto de padrões de mercado e evoluir a tecnologia para que os provedores de acesso pudessem investir nessa área [28].

Uma diferença significativa entre o MPLS e as outras tecnologias de redes WANs é a forma como os rótulos são associados e a capacidade de se carregar uma pilha de rótulos anexados aos pacotes trafegados na rede. O conceito de pilha de rótulos permite que as redes MPLS utilizem novas aplicações como Engenharia de Tráfego, Redes Privadas Virtuais (VPNs) e recuperação em caso de falhas com rápido re-roteamento de pacotes [24,28].

4.2.1 Arquiteturas de dispositivos MPLS

Numa rede MPLS a arquitetura de um nó, ilustrada na Figura 15 é definida por dois componentes. O componente de encaminhamento conhecido como *Data Plane* e o componente de controle chamado de *Control Plane*. O componente de encaminhamento utiliza uma base de dados mantida por um comutador que faz o encaminhamento dos pacotes de acordo com os rótulos carregados por eles. Já o componente de controle é responsável pela criação e manutenção da informação rotulada encaminhada entre um grupo de dispositivos interconectados. A Figura 16 mostra uma arquitetura básica de um nó MPLS fazendo roteamento IP.

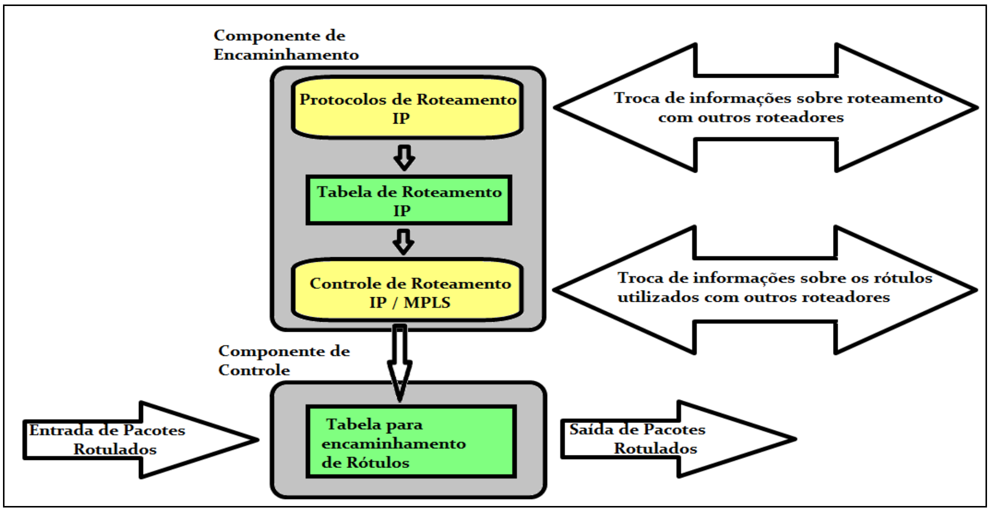


Figura 15: Arquitetura de um Nó MPLS/IP [28]

Cada nó MPLS deve ser capaz de lidar com um ou mais protocolos de roteamento, assim trocam informações para que o encaminhamento dos pacotes seja feito entre os nós MPLS pertencentes à rede. Desta forma, todo nó MPLS é um roteador IP em seu plano de controle. Os protocolos de roteamento fornecem dados para que as tabelas de roteamento sejam preenchidas [26,27,28].

Nos roteadores IP, as tabelas de roteamento servem para armazenar os endereços IP numa memória temporária, formando assim uma *cache* de endereços. Num nó MPLS, a tabela de roteamento é utilizada para determinar a troca de rótulos, onde nós adjacentes trocam rótulos na sub-rede que está contida na tabela de roteamento. A troca de rótulos para destinos *unicast* pode ser feita através do protocolo proprietário da Cisco TDP (*Tag Distribution Protocol*) ou pelo protocolo especificado pela IETF, o LDP (*Label Distribuition Protocol*) [26,28].

O processo de controle de roteamento IP MPLS utiliza os rótulos trocados entre nós adjacentes para construir uma tabela de encaminhamento, que é a base de dados do componente de controle, que é usado para encaminhar pacotes rotulados pela rede MPLS [28].

O LSR (*Label Switch Router*) pode ser qualquer dispositivo, roteador ou comutador, que implemente os procedimentos de distribuição de rótulos e seja capaz de encaminhar pacotes de acordo com as descrições de cada rótulo. A função do LDP é permitir que o LSR distribua seus rótulos para outros LRS's da rede [26,27,28].

Existem alguns tipos de LSR que são diferenciados pela funcionalidade que eles provêem para uma determinada infra-estrutura da rede. Alguns tipos de LSR são Edge-LSR, ATM-LSR, ATM edge-LSR e a distinção entre eles é puramente arquitetural. Um único dispositivo pode fazer vários desses papéis [25,26].

Um Edge-LSR ou roteador de borda é um roteador que fixa ou retira o rótulo de um pacote que está na borda da rede MPLS. A colocação de um rótulo em um pacote é o ato de fixá-lo no nó de origem, considerando que o fluxo do tráfego seja de uma determinada origem para um destino em um domínio MPLS. A retirada do rótulo acontece quando o pacote atinge o destino. Qualquer roteador de borda que possui vizinhos que não são do domínio MPLS é considerado Edge-LSR

[25,26].

Os roteadores de borda utilizam uma tabela de roteamento IP adicionados da capacidade de rotular ou remover rótulos de pacotes IP, antes de encaminhá-los para nós não MPLS. A arquitetura de um roteador de borda é representado na Figura 16 [26].

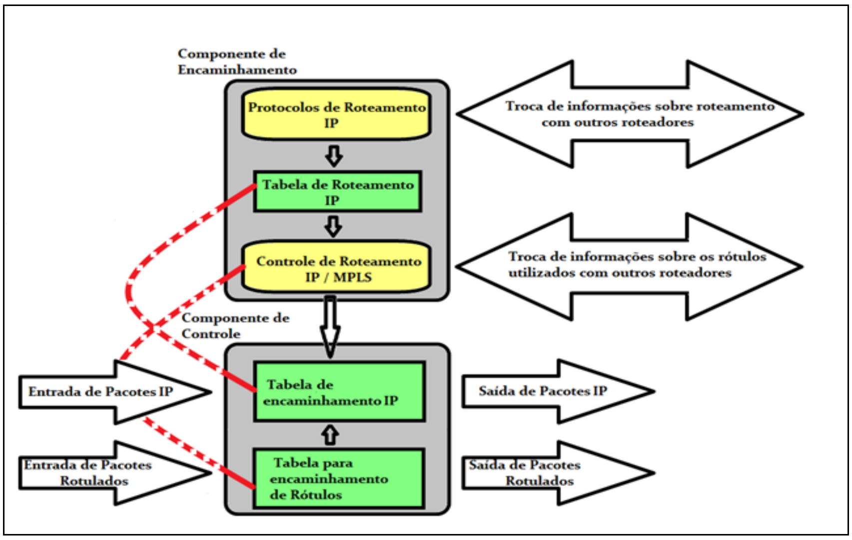


Figura 16: Arquitetura de um LSR de borda [28]

A arquitetura de um roteador de borda herda características da arquitetura de um nó MPLS adicionado de algumas alterações no componente de controle de dados. A tabela de encaminhamento IP é formada a partir da tabela de roteamento IP que é acrescida do rótulo MPLS. Pacotes IP que chegam poderão ser encaminhados como pacotes IP ou serem rotulados e encaminhados como pacotes para outros nós MPLS. Os pacotes que já chegam rotulados também são encaminhados para outros nós MPLS. Pacotes rotulados que sairão para um nó não MPLS perdem seu rótulo e uma busca de camada 3, para encontrar o destino não MPLS, é feita [28].

Um roteador de borda, basicamente, é capaz de receber um pacote IP, fazer buscas de camada 3 além de, rotular ou retirar rótulos de pacotes que serão encaminhados dentro do seu domínio [25].

4.2.2 Fixação de Rótulos

A imposição de rótulos pode ser descrita como sendo o ato de inserir um rótulo em um pacote assim que ele chega ao domínio MPLS. A atribuição inicial de um rótulo ocorre no limite da rede, isto significa que pacotes são rotulados antes de serem encaminhados por um domínio MPLS [24].

Para efetuar esta função o roteador de borda precisa identificar o cabeçalho do pacote IP e qual o rótulo ou pilha de rótulos, deve ser associada ao pacote. No roteamento convencional, para cada salto na rede é feita uma busca na tabela de roteamento através do endereço IP destino que fica armazenado no cabeçalho do pacote. O roteador então seleciona o próximo salto a cada iteração de busca, na tabela roteamento. Com as informações obtidas como resultado da busca, envia o pacote através de uma interface para o destino final [23,24].

A escolha de um destino, para um pacote IP, depende da combinação de duas funções. A primeira, divide o conjunto de prováveis pacotes num conjunto de acordo com os prefixos IP do destino. A segunda função mapeia cada destino para o endereço IP do próximo salto. Isto significa que cada destino da rede pode ser alcançado por um caminho de acordo com o fluxo do tráfego [24,25].

Na arquitetura MPLS, a primeira função é conhecida como FECs (*Fowarding Equivalence Classes*). Pode ser vista como um grupo de IPs que são encaminhados da mesma maneira pelo mesmo caminho com o mesmo tratamento de encaminhamento. Uma FEC pode corresponder a uma sub-rede destino, como também, pode corresponder a qualquer classe de tráfego considerada relevante pelo roteador de borda. Podem ser considerados exemplos de FEC, o tráfego correspondente a um único destino ou um tráfego todo originado de uma origem única. Uma FEC pode ser também um subconjunto de uma tabela BGP (*Border Gateway Protocol*), incluindo todos os destinos alcançáveis pelo mesmo ponto de saída, no caso o roteador BGP [24,26,29].

No roteamento IP convencional, o processamento do pacote é feito a cada salto na rede. Já no MPLS, um determinado pacote é associado a uma determinada FEC assim que ele entra no domínio MPLS. Este processo ocorre no dispositivo de fronteira da rede. O pacote, de uma determinada FEC, é então codificado com um pequeno identificador de tamanho único chamado de rótulo [26,29].

Quando um pacote é encaminhado para seu destino, o rótulo já é fixado ao pacote IP para que o próximo dispositivo no caminho possa também encaminhá-lo de acordo com as informações contidas em seu rótulo e não pelas informações do roteamento IP.

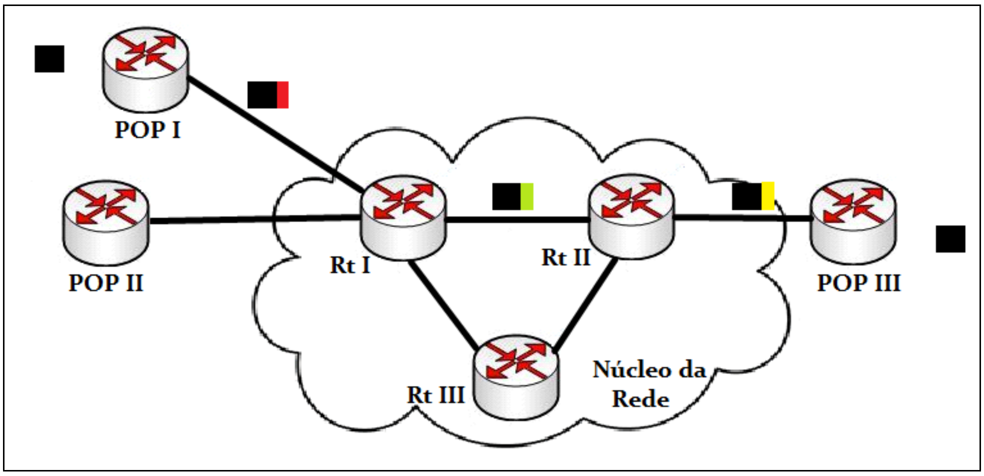


Figura 17: Representação da fixação de rótulos e Label Swapping [26]

O processo de fixação de rótulo num pacote está ilustrado na figura acima. Este processo pode ser descrito em alguns passos [26]:

Passo 1 – O pacote IP chega ao roteador do POP I;

Passo 2 – O roteador do POP II, faz uma busca na tabela de roteamento, fixa um rótulo e encaminha o pacote para o roteador Rt I, localizado no núcleo da rede MPLS;

Passo 3 – O roteador Rt I faz uma busca na tabela de rótulos, retira o antigo rótulo, fixa seu rótulo e encaminha o pacote para o roteador Rt II;

Passo 4 – O roteador Rt II verifica a tabela de rótulos, retira o antigo rótulo, fixa seu rótulo e encaminha o pacote para o roteador do POP III;

Passo 5 – O roteador do POP III verifica a tabela de rótulos, retira o rótulo do pacote, efetua uma busca na tabela de roteamento IP e então encaminha o pacote para seu destino.

4.2.3 Encaminhamento de pacotes MPLS

Cada pacote que entra numa rede MPLS através de um roteador de borda, de origem e sai por um roteador de borda destino, cria um caminho conhecido como LSP (*Label Switch Path*), que descreve o conjunto de roteadores que o pacote rotulado passou até chegar ao roteador destino. O LSP é unidirecional o que significa que um LSP é usado para que o tráfego retorne, numa determinada FEC. Na Figura 20, o *Label Switch Path* é representado pelo caminho traçado entre o roteador de borda de entrada, LSR I, e o roteador de saída LSR III, passando pelo roteador LSR II [29].

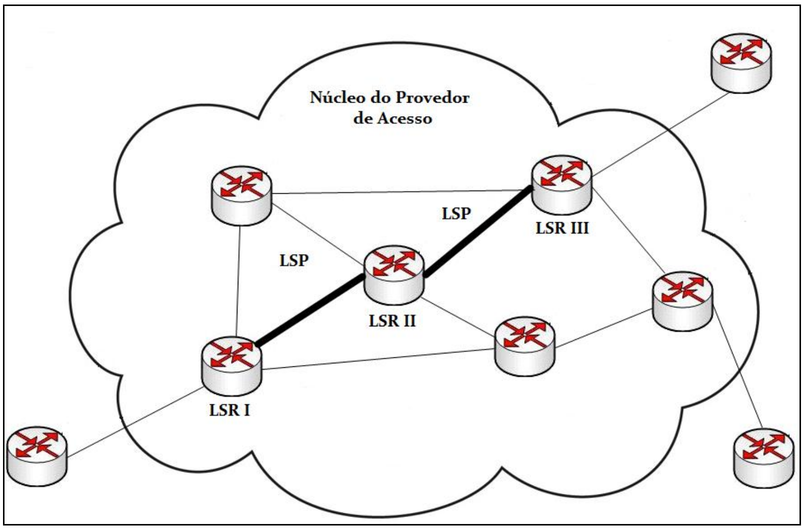


Figura 18: Caminho LSP formado entre os dispositivos LSR I e LSR III

A criação do LSP depende de um esquema orientado a conexão porque o caminho é definido antes de qualquer fluxo de informação. No entanto, o início dessa conexão é baseado na topologia da informação e não um requisito para o fluxo de tráfego. Ou seja, o caminho é criado independente de qualquer tráfego que esteja sendo trafegado nesse instante.

Cada roteador mantém duas tabelas com informações sobre o encaminhamento de pacotes numa rede MPLS. A primeira é conhecida como LIB (*Label Information Base*), responsável por manter todos os rótulos associados pelo seu roteador além de armazenar o mapeamento desses rótulos quando enviados para um roteador destino. A segunda tabela é conhecida como LFIB (*Label Forwarding Information Base*), utilizada durante um encaminhamento de pacotes e armazena apenas os rótulos que estão em uso, em determinado momento, pelo componente de encaminhamento [25,26,29].

4.3 GMPLS

O MPLS envolve a configuração de um caminho específico para que uma seqüência de pacotes sejam rotulados, desta maneira a tabela de roteamento não precisa ser consultada para que os pacotes MPLS sejam encaminhados através do *backbone*. Pesquisadores desta tecnologia provaram que um rótulo poderia ser mapeado numa cor específica no espectro e que pacotes MPLS poderiam ser diretamente ligados a rede óptica. Com a evolução das pesquisas, surgiu o termo redes ópticas inteligentes, termo que se refere a forma como a rede deveria ser controlada dentro do meio óptico [21, 24].

O protocolo GMPLS (*Generalized Multiprotocol Label Switching*), melhorou a arquitetura MPLS separando o componente de encaminhamento ou plano de dados (*Data Plane*) do componente de controle ou plano de controle (*Control Plane)*[24]. O plano de dados é por onde a informação de fato vai passar. Esse plano pode ser híbrido, dessa forma temos esses diferentes planos se comunicando. O plano de dados está dividido em camadas onde cada camada representa um tipo de comutação, como por exemplo, *Ethernet*, ATM ou fibra ótica. O plano de controle é onde os protocolos de sinalização vão funcionare. É por ele que serão alocados os recursos e definidos os LSPs.

Para cumprir a tarefa de controlar redes núcleo foi necessário o desenvolvimento de vários protocolos e interfaces. O GMPLS não é apenas um único protocolo, mas sim, um conjunto de diferentes padrões escritos por diferentes entidades em prol de um único objetivo. A sua maior contribuição foi a extensão e generalização do seu componente de controle de tráfego para servir como plano de controle para outros tipos de redes de transporte, incluindo redes ópticas com multiplexação por divisão de tempo e serviços de comprimento de onda. Por isso é considerada a melhor proposta para integrar as tecnologias IP e WDM, primeiro porque ele pode ser usado como poderoso instrumento para a engenharia de tráfego, e segundo porque ele é facilmente adequado à tecnologia WDM quando lambdas são utilizadas como rótulos [21,24].

Com a evolução do GMPLS, novos procotolos foram criados e os que já existiam evoluíram. O protocolo de gerenciamento de enlace surgiu como consequência da evolução do GMPLS, assim como o protocolo roteamento OSPF (*Open Shortest Path First*) e o protocolo de roteamento entre domínios distintos IS-IS (*Intermediate System-to-Intermediate System Protocol*) [24].

A rede GMPLS é uma importante rede óptica pois num cabo de fibras centenas de enlaces paralelos podem coexistir entre dois nós da rede, passando por uma única fibra. Isso mostra a grande capacidade de crescimento de uma rede GMPLS sem que grandes mudanças sejam feitas em sua infra-estrutura [24].

O desafio consiste em definir como o plano de controle vai alocar os recursos de maneira eficiente, e como vai controlar os nós da rede. De maneira similar ao MPLS, temos uma versão aprimorada do RSVP, o RSVP-TE, onde TE indica engenharia de trafego, que serve como protocolo de sinalização. E temos também um novo protocolo, o LMP (*Link Management Protocol*), que como o nome indica, serve para gerenciar os links de TE, links que governam a engenharia de trafego na rede.

4.4 Engenharia de Tráfego

A engenharia de tráfego é um dos maiores benefícios oferecidos pelo MPLS. Este termo refere-se à habilidade para controlar o tráfego da rede com objetivo de reduzir problemas de congestionamento e conseguir um melhor aproveitamento dos recursos de rede disponíveis. Assim a operação de troca de informação poderá ser eficiente, confiável e otimizada. Ela também é considerada fundamental nas redes de grande porte, onde a qualidade de serviço tem se tornado cada vez mais necessária [22,23].

O tronco de tráfego é uma agregação do fluxo de tráfego de uma mesma classe dentro de um LSP. As classes de tráfego são representações abstratas de tráfego onde algumas características são semelhantes [23]. O tronco de tráfego difere do LSP. O LSP é apenas a identificação do caminho roteado por rótulos por onde o tráfego passa.

O MPLS é propício à aplicação de Engenharia de Tráfego, pois é capaz de prover e suportar grande quantidade dos seus requisitos. A facilidade de utilização da Engenharia de Tráfego em redes MPLS se deve a alguns fatores, relacionados abaixo [23]:

- Roteamento baseado nos rótulos;
- Gerenciamento eficiente dos LSPs;
- Troncos de tráfego podem ser mapeados em LSPs com facilidade;
- MPLS permite tanto tráfego agregado quanto não agregado;
- Uma boa implementação MPLS pode reduzir o cabeçalho para a Engenharia de tráfego.

O administrador da rede pode desenvolver políticas de fluxo de tráfego baseadas em como e onde as informações entram na rede. Nas redes convencionais o roteador é o ponto de monitoração e avaliação da informação trafegada na rede. Estudos mais detalhados sobre o tráfego da rede permitem maior nível de controle por parte de quem gerencia a rede e assim maior objetividade e precisão nos níveis de serviços [22,23].

4.5 Segurança em Redes MPLS

Uma rede privada virtual ou VPN(*Virtual Private Network*) é uma rede que utiliza uma infra-estrutura de rede compartilhada provendo segurança e privacidade semelhante a uma rede cabeada alugada. No passado VPNs eram associadas a redes túneis IPSec sobre a Internet, ou PPTP(*Point-to-Point Tunneling Protocol*), VPN L2TP(*Layer 2 Tunneling Protocol*) discada numa intranet [29].

Uma das formas de aplicações do MPLS é como uma infra-estrutura de serviços IP VPN, freqüentemente denominada BGP/MPLS VPN. Essa aplicação é especificada pela RFC 2547 e muitas redes comerciais estão em produção com essa aplicação [29].

Provedores de serviço de Internet fornecem sua infra-estrutura como núcleo de rede para vários clientes coorporativos. Uma VPN IP é utilizada para que os dados de várias empresas trafeguem, de forma segura, por uma mesma infra-estrutura de rede.

Alguns termos são utilizados para denominar os ativos da VPN de acordo com sua localização na rede e fluxo do tráfego. A figura XX representará uma VPN MPLS usando alguns termos abaixo [29]:

- Intranet – VPN que interliga sites de uma corporação;
- Extranet – VPN que conecta um site corporativo ou sites externos de parceiros ou fornecedores. Pode-se afirmar que a Internet é a última VPN Extranet insegura;
- Roteador de Borda do Cliente (CE) – Roteador localizado no site do cliente que o conecta ao ISP através de um ou mais roteadores de borda do provedor;
- Roteador de Borda do Provedor (PE) – Roteador localizado na rede do Provedor de serviço por onde se conecta o cliente;
- Roteador de núcleo do Provedor (Core) – Roteador localizado na rede do Provedor de serviço que interliga os roteadores de borda;
- Roteadores de borda de entrada e saída (PEE, PES) – São os roteadores de borda

por onde os pacotes saem ou entra na rede do Provedor de serviço;

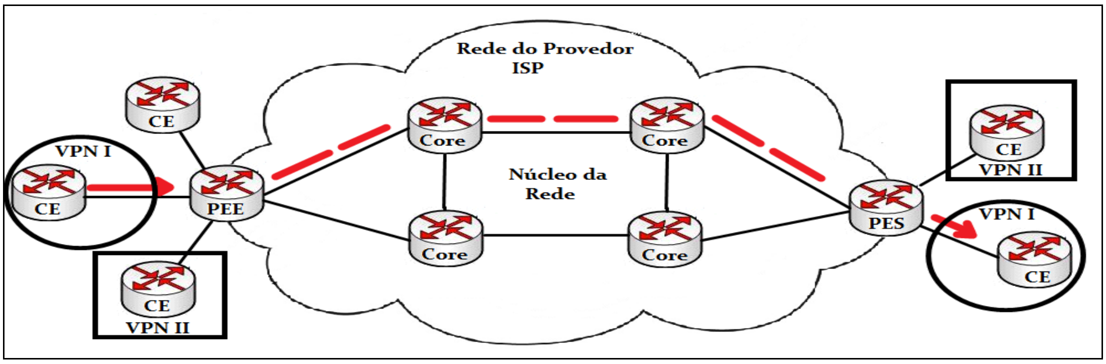


Figura 19: Representação de uma rede VPN-MPLS[29]

Na Figura 19, pode-se considerar os roteadores CE, que estão trafegando informação, participam de uma VPN, VPN I, e os outros participam de outra, VPN II. O tráfego da VPN I é ilustrado pelas setas que saem do roteador CE, localizado na VPN I, no cliente, com destino ao roteador de borda de entrada PEE, localizado na rede do ISP [29].

Na implementação da VPN MPLS, cada ponto da rede, uma localidade ou site, possui uma numeração chamada RD (*Route Destinguer*). O RD é um número de 8 bytes utilizado como prefixo para o endereço IP do *site*. Ele é configurado na interface conectada ao *site* ou localidade. Com esse número é possível distinguir duas sub-redes com mesmo endereço IP num domínio MPLS. Por exemplo, a VPN I possui o endereço de rede 10.5.1.0 e a VPN II também possui o mesmo endereço. Para que os pacotes sejam encaminhados para a VPN correta utiliza-se um RD como um código de identificação para cada VPN. A VPN I possui o RD de número 22 e a VPN II possui o RD de número 08. No ponto de vista do provedor de acesso a VPN I possui o endereço 22:10.5.1.0 e a VPN II possui o endereço 08:10.5.1.0. Numa VPN baseada em IPV4 os 8 bytes do prefixo RD são adicionados aos 4 bytes do endereço IP, resultando num endereço de roteamento de 12 bytes [29].

O MBGP (*Multiprotocol BGP*) é uma extensão do multiprotocolo BGP4(*Border Gateway Protocol versão 4*) e foi criado para carregar informações de roteamento entre um par de roteadores. Por questões de segurança e escalabilidade o MBGP só trafega informações sobre uma VPN para roteadores que tenham o mesmo número RD em suas interfaces. Assim as chances de vazamento de informações de um cliente A para um cliente B. Cada roteador de borda traça rotas para os clientes conectados a ele e não para todo o conjunto de clientes conectados ao provedor.

Essa característica demonstra o grande poder de escalabilidade da rede [29].

Capítulo 5 – AMBIENTE DE REDE DA SER-PB

Para se adequar às novas tecnologias de mercado e melhorar o desempenho de sua rede interna, a Secretaria de Estado da Receita da Paraíba, juntamente com a provedora de serviços de Internet Oi, implantaram uma rede MPLS para que um bom nível de serviço seja oferecido aos usuários da rede da SER-PB. Neste capítulo será feita uma contextualização sobre o ambiente de rede, projetos e problemas enfrentados pela SER-PB durante a implantação do protocolo MPLS em sua rede.

5.1 A Instituição SER-PB

A Gerência de Tecnologia da Informação (GTI), da Secretaria de Estado da Receita (SER) está localizada no Centro Administrativo Integrado do Governo do Estado da Paraíba. A SER é uma instituição governamental que viabiliza financeiramente as ações do estado junto com as Gerências Regionais, Recebedorias, Coletorias, Postos Fiscais e Agências. A GTI é responsável pela manutenção, desenvolvimento e gerenciamento de todo o parque tecnológico da SER. Nela estão presentes todos os servidores e ativos da rede.

Dentre as atividades que desempenha, destacam-se:

- Gerenciar as atividades pertinentes aos setores de Suporte e Desenvolvimento através de suas sub-gerências.
- Instalação e configuração de servidores, serviços de internet (HTTP, SMTP, DNS), serviços de intranet (Banco de dados, DHCP, PDC, BDC, Proxy, SSH);
- Definição da política de segurança e projetos para a rede;
- Propor melhorias do parque tecnológico, com o objetivo de manter a instituição constantemente atualizada e competitiva;
- Acompanhamento permanente dos trabalhos no que tange a instalação física dos equipamentos, linhas de comunicação de dados, assistência técnica, operação e manutenção dos ativos, visando melhor desempenho da rede.

5.2 Rede da Instituição SER-PB

A rede da SER-PB tem como objetivo interligar todos os órgãos que compõem a Secretaria da Receita do Estado da Paraíba. Estes órgãos estão dispostos por todo o estado da Paraíba, por esse motivo a rede SER é considerada uma rede geograficamente distribuída. Num contexto mais específico, a rede é delimitada por dois firewalls que provêem seu acesso as redes CODATA, RIS, INTERNET e sua VPN OI.

Cada rede citada provê uma funcionalidade específica para a rede da SER-PB. A rede RIS é provida e mantida pelo SERPRO oferecendo todo o ambiente necessário para que a SER-PB esteja inserida no projeto nacional de notas fiscais eletrônicas (NFe). A rede CODATA é mantida pela Companhia de Processamento de Dados da Paraíba (CODATA), que é o órgão responsável por gerir a Tecnologia da Informação do Estado, desta forma a rede SER deve ter um ponto de acesso a esta rede. Todas as secretarias do estado devem estar interligadas a rede CODATA. A rede INTERNET provê acesso à rede mundial de computadores, INTERNET, aos usuários da rede SER, além de inseri-la num contexto mundial. Para que a rede SER seja acessada remotamente, de forma segura, foi contratado o serviço de VPN oferecido pela provedora OI.

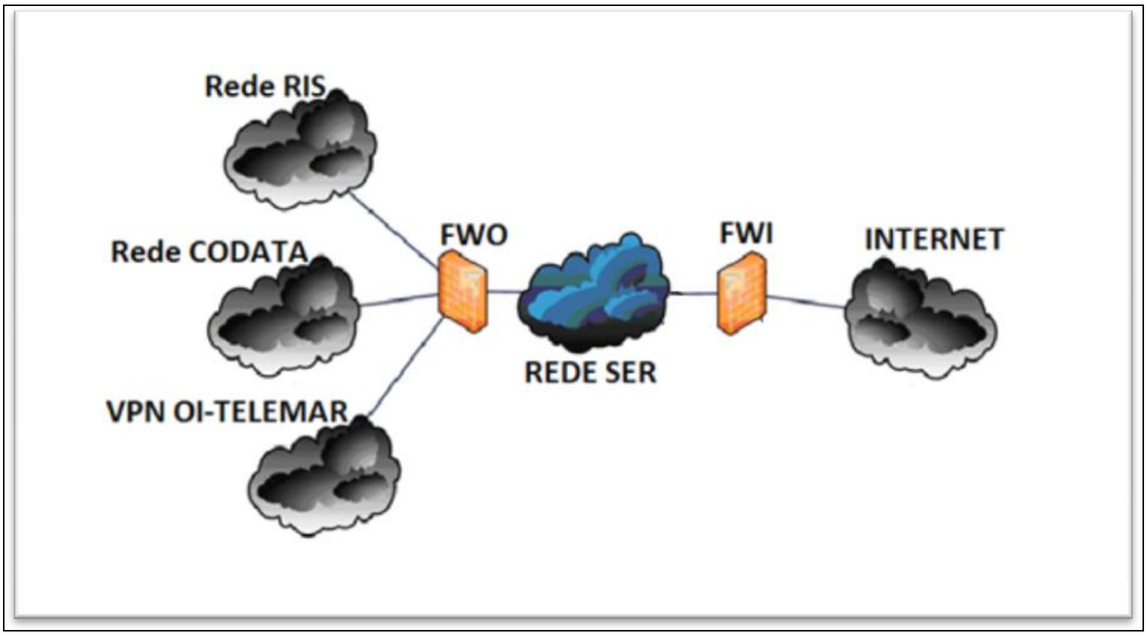


Figura 20: Estrutura Lógica onde a rede da SER-PB está inserida

A rede da SER-PB é composta por algumas sub-redes que estão organizadas de acordo com uma topologia em estrela, onde um roteador central concentra todo o tráfego da rede. As principais sub-redes são Intranet, Sede, GTI, Atendimento, Backup, DMZ e Rádios.

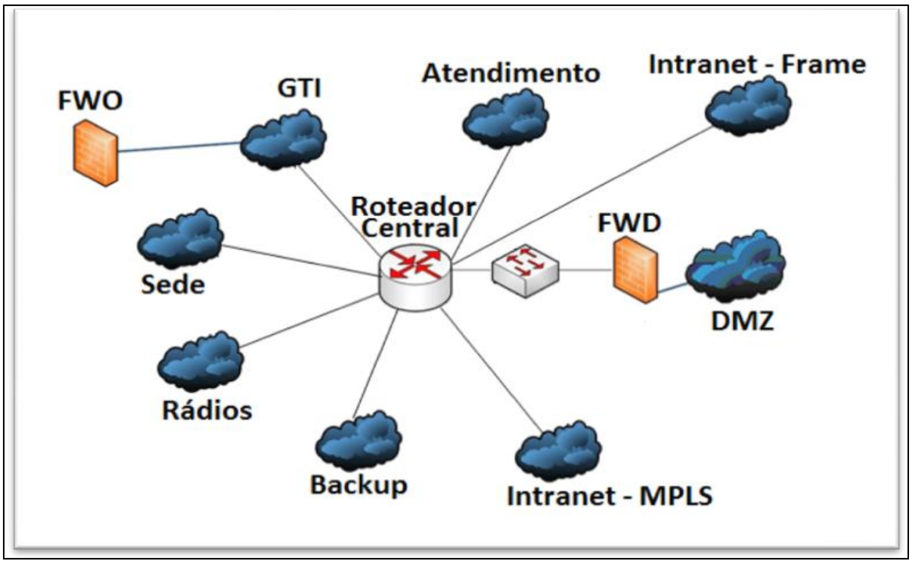


Figura 21: Estrutura lógica da Rede SER-PB

A sub-rede Intranet é o objeto de estudo deste trabalho e por esse motivo será detalhada no sub-tópico 5.2.1.

5.2.1 Sub-rede Intranet

Esta sub-rede abrange todo o estado com aproximadamente oitenta e oito pontos de acesso. Como já mencionado, a sub-rede Intranet é responsável por prover comunicação entre os Postos Fiscais, representados na Figura 22, Coletorias e Superintendências, órgãos da SER-PB e a unidade Sede localizada em João Pessoa. A sub-rede inicialmente possuía uma infra-estrutura composta pela técnica de comutação de quadros *Frame-Relay* provida pela provedora de serviços de Internet Oi. Na Figura 22, estão os Postos Fiscais do estado da Paraíba que são os principais pontos de acesso a rede *Frame Relay*. A sub-rede Intranet (*Frame Relay*) provia os seguintes serviços:

- Acesso aos sistemas corporativos – ATF, ATFd, ATOMO;
- Acesso ao Banco de dados central;
- Acesso ao sistema de correio eletrônico – Postfix + MailScanner + Spamassassin + Clamav + Openwebmail;
- Acesso à Internet;

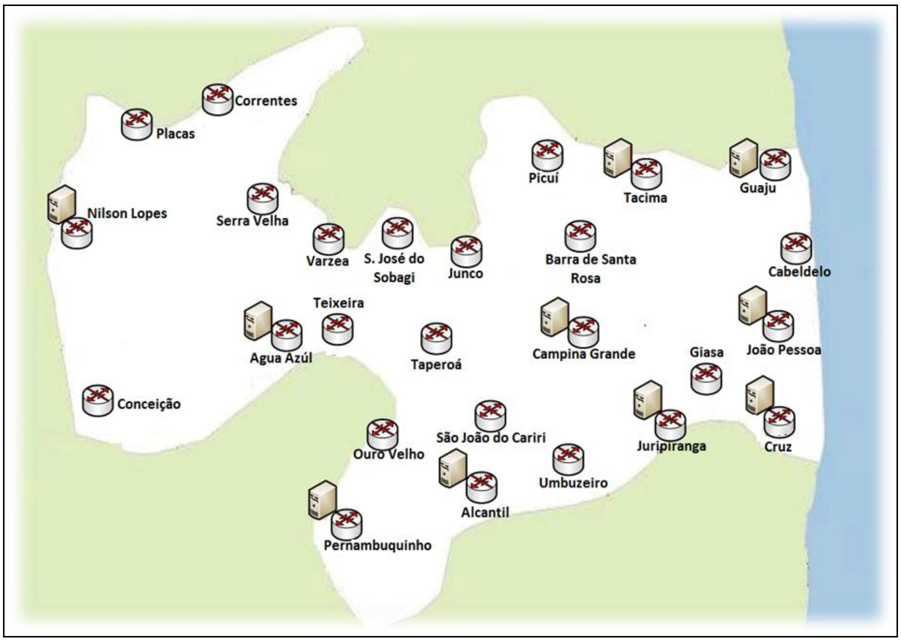


Figura 22: Postos Fiscais interligados pela Intranet Frame e MPLS

5.2.1.1 *Implantação da Rede MPLS*

A implantação da rede MPLS trouxe uma série de vantagens para a rede da SER-PB. Principalmente por solucionar grande parte dos problemas elencados no tópico 5.2.1.3- Problemas e Necessidade de Evolução. O projeto de implantação se iniciou na capital e os pontos localizados em João Pessoa foram priorizados. Durante a implantação tínhamos que o processo de migração consistia de 4 fases para cada localidade:

1ª Fase – Instalação dos equipamentos necessários nas localidades (Roteadores);

2ª Fase – Configuração do equipamento;

3ª Fase – Configuração do protocolo BGP;

4ª Fase – Testes de conectividade.

A primeira fase é realizada pela equipe de configuração da provedora de serviços de Internet, Oi, que se dirige até a localidade e instala o roteador de acesso a rede MPLS. Em seguida, um técnico da provedora de serviços de Internet, juntamente com um técnico do cliente, SER-PB, iniciam a configuração lógica dos equipamentos instalados, que consistem da configuração do nome, endereço IP da interface *Ethernet*, endereço da interface *Serial*, configuração do serviço

DHCP(*Dynamic Host Configuration Protocol*), dentre outras. A terceira fase consiste da configuração, por intervenção manual, da rota padrão para o roteador estático central da SER, pela equipe técnica da provedora de serviços de rede. A última fase se caracteriza pelos testes da rede. Testes são necessários para que seja verificado dinamicamente a operação da rede. Os testes de conectividade foram realizados a medida em que as localidades eram migradas para a rede MPLS, se caracterizando como testes não intrusivos. Pois foram realizados sem interromper os serviços da rede. Um procedimento padrão de testes foi elaborado para que a conectividade entre os domínios fosse devidamente testada por várias equipes diferentes que atuaram em todo o estado.

5.2.1.2 *Qualidade de Serviço e Priorização do Tráfego*

A rede Intranet Frame era compartilhada e funcionava num regime de melhor esforço. Um cliente podia gerar tráfego concorrente na rede, o que acarretava uma série de congestionamentos e reclamações por parte dos próprios usuários da rede. Uma das propostas da nova rede MPLS foi o melhor gerenciamento do tráfego da rede, o que possibilitaria a SER escolher quais aplicações críticas deveriam ser priorizadas no novo domínio.

Foram propostos vários perfis de priorização QoS para as aplicações da SER. A GTI teve que escolher um dos perfis e aplicar as suas necessidades. Os perfis propostos são classificados de acordo com os tipos de serviços e o percentual que ocuparão do enlace (*Traffic Shapping*).

	Classes de Serviço				
	Voz	Vídeo	Críticos	Prioritário	Melhor Esforço
DA	-	-	-	-	100%
DB	-	-	-	50%	50%
DC	-	-	50%	40%	10%
DVA	30%	-	-	-	70%
DVB	30%	-	-	50%	20%
DVC	30%	-	40%	20%	10%
DVVA	10%	30%	-	-	60%
DVVB	10%	30%	-	40%	20%
DVVC	10%	30%	30%	20%	10%

Tabela 2- Quadro de perfis para o serviço de QoS

A tabela acima mostra as classes e os perfis possíveis para qualidade de serviço. Quanto mais classes de priorização tiver o perfil mais caro o serviço prestado. A classe DA não oferece priorização e o tráfego é disputado pelas aplicações em melhor esforço. A classe DB prioriza o tráfego escolhido como prioritário, ou seja, ao alcançarem o roteador, os pacotes das aplicações escolhidas como prioritárias tem prioridade sobre o restante dos pacotes que estão na fila. Essa classe só garante a priorização selecionada para 50% do enlace, os outros 50% serão disputados pelas aplicações restantes em melhor esforço. A classe DC divide o tráfego em dados críticos, dados prioritários e dados sem priorização. Os dados críticos tem prioridade sobre os dados prioritários e pode consumir 50% da banda. Os dados prioritários utilizarão 40% do enlace, outros 10% serão utilizados pelas aplicações concorrentes. Outras classes estão disponíveis e seguem a mesma linha de raciocínio, no tocante a divisão de banda e priorização de pacotes. A tabela acima mostra como estão divididas o restante das classes de QoS disponíveis pela provedora de serviços de rede.

A GTI escolheu a classe DB para ser o seu perfil de QoS e priorização. Assim a fornecedora garante que até 50% do enlace, os pacotes prioritários terão prioridade sob o restante dos pacotes da rede. Além de escolher o seu perfil, a GTI teve de elencar as aplicações que seriam consideradas prioritárias.

O tráfego das aplicações prioritárias é composto pelos principais serviços oferecidos pela GTI. Tráfego de replicação de dados do controlador de domínio, atualização de anti-vírus, aplicação corporativa (ATF), ATOMO, tráfego de backup, serviço de mensagens (e-mail), dentre outros. Para a priorização são necessárias informações sobre a porta em que a aplicação está habilitada para funcionar, o endereço IP do servidor e o nome da aplicação.

A Tabela 3 mostra as informações de QoS da SER. Informações como IP e Porta não estão disponibilizados por questões de segurança da informação.

Nome da Aplicação	Uso	Prioridade
ATF/Aplicação		
Replicação do BD/informix		
Legado-Postof/telnet		
Legado/telnet		
Replicação do BD-Legado/informix		
PORTAL FISCAL		
PASE INTERESTADUAL	DADOS	Priority
IPVA (DETRAN/CODATA)		
Legislação		
E-MAIL		
Intranet/http		
Antivírus		
Replicação pdc/bdc		

Tabela 3 – Tabela de Aplicações escolhidas pela SER

O ATF é o sistema corporativo da SER. Todas as transações e procedimentos de fiscalização do estado são realizadas através dele. Como é um sistema WEB que serve todo o estado, tráfego gerado por ele é considerado crítico. A replicação do banco de dados é a operação que origina o *backup* das informações coletadas através do ATF. Caso seu tráfego não seja priorizado o backup pode não ser concluído por questões de congestionamento. O sistema legado ATOMO faz uso de várias conexões remotas, via telnet, para as localidades onde ela está ramificada. Existe uma base central na sede que armazena os dados coletados em todos os postos fiscais do estado em determinada hora do dia.

Observando a tabela acima pode-se constatar que os principais serviços da SER foram elencados como críticos, portanto, disputarão entre si metade do enlace disponível. O restante das aplicações como vídeo, áudio, streaming sob demanda, voz sobre ip, p2p, torrent, web messengers, estarão disputando a outra metade do enlace através do melhor esforço.

5.2.1.3 *Problemas e Necessidade de Evolução*

A necessidade de inovação tecnológica em seu *backbone*, fez com que a provedora aderisse a tecnologia MPLS e solicitasse a adequação de todos os seus clientes à essa tecnologia. Além dessa causa inicial, a SER teve outras causas determinantes para a migração de tecnologia.

O aumento de tráfego ocasionado pela utilização de novas funcionalidades da aplicação corporativa ATF e a utilização da nova plataforma WEB ATFd, fez com que a rede, em algumas localidades, parasse em horários de pico, devido a congestionamentos. Diante desse cenário os usuários solicitaram melhora da capacidade para os enlaces da rede. Algumas características mostravam a necessidade de uma renovação na infra-estrutura:

- Os CIRs (*Commited information rate*) garantido pela rede Frame eram muito baixos apesar dos enlaces possuírem boas capacidades
- O tráfego não tinha nenhum controle ou tipo de priorização;
- Tráfego inútil composto de aplicações P2P, streaming de vídeo e streaming de áudio;
- Aplicações coorporativas não estavam sendo bem suportadas;
- Aplicações de segurança não estavam sendo atualizadas;

Além das causas citadas acima, a rede SER teve de se adequar ao projeto nacional de notas fiscais eletrônicas (NFe), que exige maior velocidade e capacidade de banda de rede. Num prazo médio, cerca de 400 TB de dados serão despejados na Intranet da SER através das redes RIS e Internet. Que além de armazenar esses dados por no mínimo 6 anos deverá ter capacidade pra lidar com essa quantidade de dados sem que a rede perca desempenho ou até mesmo pare de oferecer seus serviços. Para o período de migração das redes ficou acordado que os dois ambientes, tanto o *Frame Relay*, quanto o MPLS deveriam existir. Assim os serviços da rede SER continuariam sendo prestados e o novo ambiente seria instalado sem maiores prejuízos.

5.2.2 Problemas detectados Pós-implantação MPLS

A implantação do *backbone* MPLS trouxe algumas vantagens para o ambiente de rede da SER. Melhoria na velocidade dos links, priorização dos pacotes de acordo com o tipo de tráfego, *links* redundantes para as localidades consideradas críticas pela SER. Mesmo com essas vantagens alguns problemas foram detectados com a utilização dos recursos da rede.

Da forma como o serviço é oferecido o monitoramento da rede é um ponto que foge do controle do cliente, visto que apenas o provedor tem acesso as configurações dos roteadores. Assim dúvidas com relação a eficiência da rede só são elucidadas caso o monitoramento da rede e comportamento da QoS seja efetuado. Com esse tipo de monitoramento a GTI estaria munida de informações necessárias para otimizar a rede de acordo com a necessidade de cada enlace variando os parâmetros de QoS dependendo da utilização da rede e das necessidades de cada localidade. Com o monitoramento da eficiência e comportamento do QoS pode-se analisar se a GTI está oferecendo um serviço eficiente. Além disso, pode-se verificar:

- A composição do tráfego em cada enlace da rede;
- Estatísticas sobre a carga de cada protocolo na rede;
- Qual protocolo está consumindo mais banda;
- Se o que foi proposto e configurado está sendo cumprido;
- Se as políticas de QoS estão ajudando a GTI prover um serviço consistente e com tempo de resposta aceitável para as aplicações críticas da SER;
- Se a eleição dos protocolos para o QoS foi correta;
- O tempo de resposta das aplicações rotuladas;

- Quais usuários estão tendo mal desempenho da aplicação devido a falhas de rede.
- Atualmente a Gerencia de Tecnologia da Informação da SER não possui informações detalhadas sobre o comportamento do tráfego.

O gerenciamento remoto da rede através dos roteadores não é possibilitado, visto que, o cliente não tem acesso aos roteadores MPLS nas localidades. Com isso a análise de problemas na rede, dependente da posição tomada pela central de atendimento da provedora do serviço. O que não é interessante para a GTI, que deve funcionar com carga de expediente de vinte e quatro horas por dia, sete dias por semana. Caso seja necessária a criação de uma nova sub-rede ou alguma modificação no endereçamento da rede, a equipe de técnicos do cliente deverá entrar em contato com a central de atendimento da provedora do serviço, o que torna o gerenciamento da rede menos eficaz e sempre dependente da ação do suporte de núcleo da rede.

O controle operacional da rede precisa de mecanismos que possibilitem um roteamento dinâmico e alternativo de modo que o nível de serviço não seja penalizado. A GTI possui uma rede com a arquitetura em estrela e um roteador centraliza todo o tráfego. O roteador central da GTI é um servidor Linux que faz roteamento estático para toda a rede. Para habilitar os pontos MPLS o protocolo BGP é alterado manualmente, pela equipe técnica da provedora. Este tipo de alteração é custosa e não eficiente pois a cada ponto adicionado uma nova intervenção é realizada no protocolo que pode funcionar de forma automática, caso o roteador central suportasse esse tipo de roteamento.

Algumas localidades da Intranet são consideradas pontos chaves de atuação da SER-PB no estado. Essas localidades receberam uma maior atenção no quesito capacidade de banda e redundância de links. A redundância de link deveria funcionar da seguinte forma, o link principal sempre possui maior capacidade que o link de backup e quando um dos dois cair, o outro deveria assumir automaticamente. Quando os dois estão em operação o link total fica nivelado pelo de menor capacidade. A atividade do link só é normalizada quando o link de menor capacidade é desligado. Este é um problema que está sendo analisado pela equipe da provedora de serviços.

Capítulo 6 – Ambiente de Gerenciamento de Rede para a SER-PB

Neste capítulo será proposto um ambiente de gerenciamento composto pela integração de um analisador de tráfego, que terá o papel de coletar os dados da rede e classificá-los, de um sistema de gerenciamento de rede, que terá o papel de monitorar o ambiente de rede gerando relatórios em tempo real e gráficos a partir dos dados coletados e um sistema de gerenciamento de banco de dados para que uma base histórica seja mantida.

6.1 Contextualização

Existem formas de gerenciamento de rede que solucionam grande parte dos problemas da rede da SER-PB com a ajuda de técnicas de coleta de tráfego e ferramentas de gerenciamento de redes. Alguns requisitos devem ser observados em um bom ambiente de gerenciamento:

- Flexibilidade de coleta de dados: As ferramentas que compõem o ambiente de gerenciamento precisam ser capazes de coletar dados de outras fontes além do SNMP. Muitos sistemas incluem maneiras de coletar dados a partir de quase todos os serviços de rede. Alguns deles são capazes de consultar bases de dados, verificar registros DNS e se conectar a servidores WEB.
- Qualidade da interface com o usuário: Um bom ambiente de gerenciamento deve prover uma interface gráfica de qualidade para seus administradores. Uma interface gráfica de qualidade não é apenas uma propaganda de marketing. Os administradores precisam de uma interface que retransmita as informações analisadas de uma maneira clara e simples.
- Valor: Existem ambientes de gerenciamento desenvolvidos por grandes empresas, como a plataforma de gerenciamento Open View da HP (Hewlett Packard). Essas ferramentas geralmente oferecem todos os requisitos que um bom sistema de gerenciamento pode ter, porém, o custo desse tipo de aplicação é muito elevado.
- Descoberta automatizada: Muitos sistemas oferecem a capacidade de identificar os hosts e dispositivos locais que compõem a rede gerenciada. Por meio de uma combinação de Pings de broadcast, solicitações SNMP, pesquisas de tabelas ARP

(Address Resolution Protocol) e consultas DNS.

- Recursos para geração de relatório: Muitos produtos podem enviar e-mails de alerta, enviar mensagens de texto para celulares, além de gerarem tíquetes para sistemas de rastreamento de problemas. Um bom ambiente de gerenciamento deve ser capaz de gerar relatórios de forma flexível, visto que não se sabe que plataformas e dispositivos serão integrados a rede num futuro próximo.
- Gerenciamento de configurações: Alguns ambientes podem ir além do monitoramento e alertas e são capazes de efetuar configurações reais de hosts e dispositivos
- Capacidade guardar informações: Um ambiente de gerenciamento deve suportar gerenciadores de bancos de dados (SGBDs) com a finalidade de armazenar informações históricas de forma organizada.
- Ponto central de gerenciamento: Um bom ambiente de gerenciamento deve ter um ponto único para acesso as informações.

Um problema enfrentado pela GTI é a não identificação do que está acontecendo em sua rede MPLS. Identificar quais os protocolos que são trafegados, descobrir quais aplicações são primordiais para a SER-PB, observar se o custo do investimento para manutenção do serviço de rede utilizado é realmente bem aproveitado, tornam o gerenciamento de rede um recurso indispensável para a SER-PB. Mesmo com a utilização de alguns sistemas de gerenciamento da rede, a GTI ainda não é capaz de dimensionar sua rede baseada no comportamento do tráfego. Além disso, a maioria dos requisitos de um bom ambiente de gerenciamento não atendidos pelos sistemas utilizados pela SER-PB. Com esses problemas

6.2 Sistemas sugeridos para o ambiente de gerenciamento proposto

A GTI precisa de um ambiente capaz de atender os requisitos de um bom ambiente de gerenciamento. Várias ferramentas exercem o papel de analisadoras de tráfego ou gerenciadores de rede, porém as escolhidas para composição do ambiente de gerenciamento proposto foram o analisador Wireshark, o sistema de gerenciamento de redes Zabbix e o sistema de gerenciamento de banco de dados MySQL. Uma breve descrição sobre as vantagens e características de cada um desses componentes será dada nessa seção com a finalidade de justificar a escolha de cada uma delas. Algumas ferramentas auxiliares podem ser elaboradas ou adicionadas para que a integração do ambiente seja facilitada.

6.2.1 Zabbix

O Zabbix é um software, disponibilizado na Internet sob a licença GPL, utilizado para gerenciar e monitorar vários parâmetros de rede. Esse sistema utiliza vários mecanismos para manter informado o administrador ou equipe de monitoramento sobre o que está acontecendo na rede em determinado instante. Se destaca por incorporar, em uma única ferramenta, várias funcionalidades peculiares aos sistemas gerenciadores de rede sem alto custo além de permitir o monitoramento em tempo integral. Por oferecer flexibilidade na geração de relatórios e visualização de dados armazenados em tempo real o Zabbix é considerado uma boa ferramenta de planejamento, pois suporta polling, capacidade de captura de dados em determinado espaço de tempo além do trapping, que é a notificação via alarmes ou mensagens de texto para os administradores da rede.

Esta ferramenta é capaz de gerar gráficos a partir de dados coletados por scripts, ou outra ferramenta, integrando-se facilmente a outras aplicações e oferecendo suporte para vários ambientes como Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X. Essa característica faz com o que o ambiente proposto atinja o requisitos de flexibilidade de coleta de dados, de qualidade da interface com o usuário e de valor, já que esse sistema será o componente que fará a apresentação do estado da rede para seu administrador.

Uma característica marcante do Zabbix é a centralização do sistema de monitoramento, pois todas as informações como dados de configuração da ferramenta, dados sobre desempenho e dados históricos podem ser armazenados em uma base de dados relacional que será acessada por ele.

No ambiente proposto, o Zabbix tem a função de verificar sistemas de monitoramento de arquivos e logs, saídas do Wireshark, saídas de scripts e informar, em tempo real, ao setor responsável caso erros sejam identificados e que alguma anormalidade esteja ocorrendo na rede MPLS. O Zabbix é a saída padrão do ambiente de gerenciamento proposto já que possui uma interface bastante interativa, exibindo o conteúdo do tráfego da rede interna da SER-PB, coletado e classificado pelo Wireshark.

6.2.2 Wireshark

O Wireshark é um poderoso analisador de pacotes capaz de capturar o tráfego de uma rede. Pode ser caracterizado como uma ferramenta para detecção de problemas e melhor entendimento sobre o funcionamento de cada protocolo que pode ser usado, tanto para proteger seu sistema, quanto para capturar dados dos nós, em modo promíscuo, em uma rede de computadores. O tráfego coletado por essa ferramenta é organizado e separado por protocolos que são separados em uma lista de fácil navegação.

6.2.3 MySQL

O Mysql é um banco de dados relacional de código aberto que usa a linguagem Structured Query Language(SQL) para gerenciamento e busca de seus dados. Se baseia uma arquitetura cliente-servidor, onde o servidor é o sistema que manipula os dados contidos no banco. Os clientes não lidam diretamente com os dados do banco, ao invés disso, se comunicam com os servidores através dos códigos em SQL para realizar suas buscas. Uma característica chave do MySQL é que ele é um sistema *multithread,* capaz de executar várias processos de forma paralela, sendo esse o principal foco do seu desenvolvimento atualmente.Algumas características importantes ajudaram a torná-lo bastante popular:

- Portabilidade: O banco de dados é compatível com vários sistemas operacionais incluindo, Microsoft Windows 2000, Mac OS X, GNU/Linux, FreeBSD e Solaris. O software pode ser compilado e instalado caso não exista um pacote nativo para o sistema desejado;
- Suporte a diversas linguagens: Possui uma API compatível com diversificadas linguagens de programação. Aplicações escritas em C, C++, Eiffel, Java, Perl, PHP, Python e Tcl são capazes de acessar as bases de dados armazenadas no banco;
- União de bases de dados: Com o MySQL pode-se construir queries que utilizem tabelas de diferentes bases de dados.

Além das vantagens já citadas o MySQL é um produto de bom desempenho e barato, pois pode ser adquirido gratuitamente. O ambiente de gerenciamento de redes, da rede interna da SER-PB, poderá trabalhar com várias bases de dados, para que dados históricos da rede sejam armazenados por um período de tempo pré-estabelecido pela gerência de GTI.

6.3 Ambiente proposto

O ambiente proposto tem como objetivo sanar algumas deficiências observadas e relacionadas ao gerenciamento da rede MPLS da SER-PB, provendo um ambiente integrado capaz de oferecer os principais requisitos inerentes a um bom ambiente de gerenciamento de redes.

6.3.1 Arquitetura lógica do Ambiente Proposto

A Figura 23, mostra a arquitetura do ambiente proposto será divido em 3 camadas lógicas (IU, Coleta e Análise, Base) onde cada camada conterá um *software* que realizará uma ou mais funções específicas. A divisão do ambiente em uma arquitetura lógica facilita o entendimento do próprio ambiente e da função de cada um de seus componentes.

A ferramenta de gerenciamento de redes ZABBIX, além de prover suas funcionalidades convencionais será utilizada como componente da camada lógica IU (Interface com o Usuário). A camada lógica IU é responsável por prover a interface entre os usuários e o ambiente proposto. Ela foi escolhida por oferecer uma gama de funcionalidades gráficas como, criação de gráficos, mapas, visualização de relatórios e área para monitoramento via console gráfico. Outra propriedade que contribuiu para a escolha dessa solução foi sua grande capacidade de adaptação a outros sistemas. O ZABBIX aceita como entrada para criação de gráficos a saída de *Shell Scripts,* de analisadores de tráfego e de sistemas desenvolvidos pela GTI. A camada IU também servirá como ponto de centralização do ambiente, onde os usuários buscarão as informações coletadas, analisadas e armazenadas pelos componentes das outras camadas. A camada Coleta e Análise será composta pelo analisador de tráfego Wireshark, que terá a responsabilidade de coletar e classificar o tráfego da rede interna da SER-PB além repassar as informações coletadas para a camada IU, para que ela se encarregue da exibição dos dados através de gráficos. Os dados coletados por essa camada lógica poderão ser persistidos no banco de dados que compõe a camada lógica Base. A camada Base possui como seu componente o sistema gerenciador de banco de dados MySQL. O SGBD escolhido é suportado pelos componentes das outras camadas lógicas dessa forma tanto o Wireshark, quanto o Zabbix poderão utilizar o banco para que informações do tráfego e configurações do ambiente sejam persistidos de forma organizada.

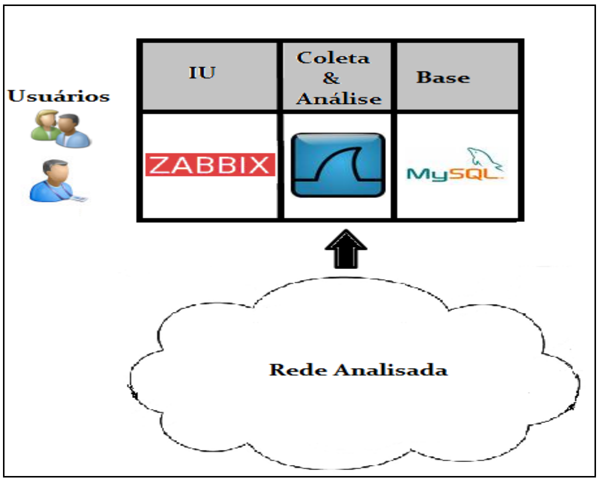


Figura 23: Arquitetura Lógica do Ambiente Proposto

A Figura 24 ilustra a comunicação entre as camadas, que representa interações que os usuários e sistemas integrados podem realizar no ambiente de gerenciamento proposto. A comunicação entre as camadas acontece em todas as vias, por exemplo, a camada IU tanto recebe solicitações, quanto exibe informações de forma estruturada e organizada, para os usuários do ambiente. Essa comunicação pode representar também um acesso feito por um usuário a determinado gráfico gerado. A camada IU também se comunica com as camadas de Coleta e Análise e a camada Base. Essa comunicação se dá em duas vias e pode representar a criação de um gráfico a partir das informações coletadas e seu posterior armazenamento numa base de dados.

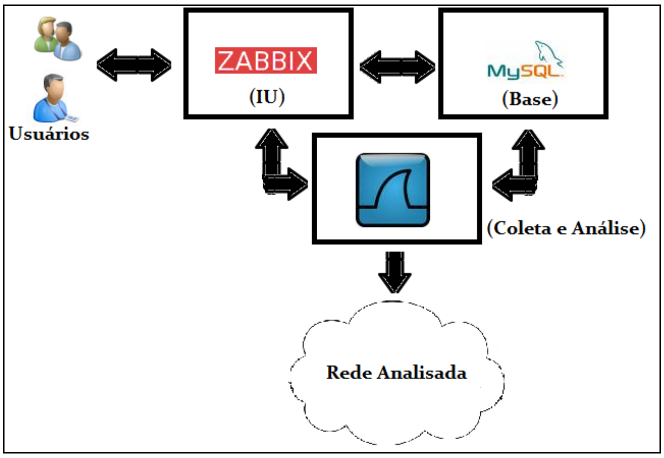


Figura 24: Comunicação entre camadas do Ambiente

6.3.2 Vantagens oferecidas

Com a implantação do ambiente proposto, espera-se que os administradores da rede SER-PB obtenham um ambiente capaz de atender os requisitos da rede SER-PB. Segue abaixo algumas vantagens que podem ser vislumbradas:

- Ambiente WEB e centralização das informações: A centralização do ambiente é um requisito pertinente que será oferecido pelo ambiente de gerenciamento proposto, pois, a equipe de gerenciamento da rede da SER-PB é reduzida. Com o ambiente centralizado o tempo de resposta para solução de chamados da rede SER-PB seria reduzido, visto que, as informações coletadas pelo ambiente estariam organizadas de forma que um único ponto do sistema pode exibi-las;
- Redução do número de servidores: O número de servidores de rede seria reduzido. Alguns servidores seriam desativados já que o ambiente proposto supriria a demanda deles;
- Custo ou valor: Outro ponto relevante para utilização deste ambiente proposto é que seu custo de implantação não será alto. Todas as ferramentas que o comporão o ambiente são softwares sob licença GPL e de código aberto que possuem versões gratuitas;
- Fácil adaptação a novos ambientes: A integração dos componentes de análise será facilitada, visto que todos possuem código aberto e trabalham em ambiente Linux nativamente provendo baixo custo, visto que as ferramentas estão prontas e só precisam de alguns ajustes e configurações para que funcionem de forma integrada, bastando a equipe de monitoramento ser devidamente treinada para operar corretamente os sistemas;
- Análise detalhada do tráfego: Identificação dos protocolos e carga de cada um deles na rede, funcionamento do QoS;
- Backup e dados históricos.

Capítulo 7 - Conclusão

Os administradores da rede da SER-PB estão enfrentando problemas no tocante ao gerenciamento de uma rede MPLS implantada recentemente. E por esse motivo necessitam de um ambiente de gerenciamento para melhorar seu nível de serviço oferecido e serem capazes de validar o serviço de rede utilizado que é prestado pela provedora Oi.

Com o estudo sobre as ferramentas de gerenciamento e os protocolos de gerenciamento e monitoramento, pode-se verificar que um bom ambiente de gerenciamento deve conter, como principais requisitos, a flexibilidade de coleta de dados, uma interface gráfica de qualidade, baixo custo, recursos para geração de relatórios. Itens que não são oferecidos pela provedora de serviço de Internet Oi.

Este trabalho propôs um ambiente de gerenciamento de rede que, se implantado, será capaz de fornecer a maioria dos requisitos definidos como imprescindíveis para um bom ambiente. Para levantar os requisitos foi necessário se fazer uma análise sobre as ferramentas de gerenciamento e monitoramento existentes, fazer um estudo sobre os protocolos de gerenciamento mais utilizados, além de fazer uma análise do ambiente da rede da SER com a finalidade de levantar seus problemas. O ambiente de rede proposto baseou-se na integração de um analisador de tráfego Wireshark, um sistema de gerenciamento de rede, ZABBIX e o sistema gerenciador de banco de dados MySQL. Cada um desses sistemas oferece um ou mais serviços para o ambiente proposto. O Wireshark é o responsável pela coleta e análise do tráfego, o ZABBIX é o responsável pela aprensentação do ambiente, nele serão exibidos os gráficos e mapas desejados pelos usuários do ambiente. O MySQL é o responsável pelo armazenamento das informações geradas e dos arquivos de configuração do ambiente.

É importante ressaltar que o ambiente integrado proposto não solucionará todos os problemas encontrados após a implantação da nova rede MPLS, porém, a identificação do tráfego poderá ser efetuada e dessa forma estratégias de priorização de tráfego, balanceamento de carga, deverão ser utilizadas para que os recursos da rede SER-PB sejam aproveitados da melhor maneira possível.

Referências Bibliográficas

[1] Optical Fiber communication – An Overview – Promana - journal of physics; Vol. 57, Nos 5 & 6 – Nov. & Dec. 2001 pp. 849-869

[2] A. S. TANENBAUM - Redes de Computadores, 4.ed, Rio de Janeiro, Campus, 2003

[3] Optical Networks Tutorial – ALCATEL

[4] A. L. G. CAMPOS - Fibras ópticas - uma realidade reconhecida e aprovada - Abril de 2002 | volume 6, número 2 - ISSN 1518-5974 – Rede Nacional de Ensino e Pesquisa

[5] M. A. MARTIGNONI - *http://www.lucalm.hpg.ig.com.br/cabos.htm* - Texto extraído da apostila Cabling I Instrutor da Impacta Tecnologia

[6] M. J. TELLES - A proposta dos Japoneses para nova Internet - Dissertação - Instituto de Informática - Universidade Federal do Rio Grande do Sul (UFRGS) - 2009

[7] J. F. KUROSE e K.W. Ross - Redes de Computadores e a Internet, uma abordagem top-down, 3.ed, São Paulo, Pearson Addison Wesley - 2005

[8] W. F. GIOZZA, E. CONFORTI, H. WALDMAN - Fibras Ópticas - Tecnologias e Projeto de Sistemas - Makrons Books

[9] U. D. BlACK - Sonet and T1: Architectures for Digital Transport Networks - 2nd Edition, Ed. Hardcover

[10] W. GORALSKI - Sonet/SDH Third Edition - 2002

[11] E. TITTEL - Coleção Schaum, Redes de Computadores - Ed. Bookman

[12] NCA Documents - All Optical Network - 2004

[13] M. MÉDARD, D. MARQUIS, S. R. CHINN - Attack Detection Methods for All-Optical Networks - Massachusetts Institute of Technology, Lincoln Laboratory

[14] P. E. GREEN, Jr. - “Optical Networkin IEEE Journal on Selected Areas in Communications, Vol. 14, No. 5, Jun. 1996

[15] S. ALEXANDER, R. BONDURANT, and et al. - A Precompetitive Consortium on Wide-Band All-Optical Networks, Journal of Lightwave Technology, Vol. 11, No. 5/6;

[16] F. R. DURAND - “Contributions for the analysis of hybrid WDM/OCDM Networks” - Universidade Estadual de Campinas . Faculdade de Engenharia Elétrica e de Computação – Tese Doutorado, Ano 2007, Páginas 23-24

[17] I. P. KAMINOW, A. T. LI, A. E. WILLNER, S. KARTAPOULOS - “ Next Generation Intelligent Optical Networks - From Access to Backbone “ 18 – 2008

[18] M. O’MAHONEY, C. (T.) POLITI, D. KLONIDIS, R. NEJABATI, D. SIMEONIDOU: "Future Optical Networks", Journal of Lightwave Technology, Vol. 24, Issue 12, December 2006

[19] P. HALL - Mesh-Based Survivable Networks; Options and Strategies for Optical, MPLS, SONET, and ATM Networking (2003)

[20] V. J. R. PAIXAO - Políticas e Mecanismos de Engenharia de Tráfego para Redes MPLS/DS

[21] E. J. C. GIMENEZ, R. R. VIEIRA, M. J. S. CARDOSO, G. A. FERRARRI 4 - Engenharia de Tráfego nas Redes MPLS: “Uma Análise Comparativa de seu Desempenho em Função de Suas Diferentes Implementações” - 2006 WCCSETE, March 19 - 22, 2006, São Paulo, BRAZIL - World Congress on Computer Science, Engineering and Technology Education

[22] R. P. ESTEVES, F. Y. NAGAHAMA, A. J. G. ABELEM - Adaptações na Sinalização GMPLS para Adequá-la às Redes OBS - - IV Congresso Brasileiro de Computação – CBComp 2004 Redes de Computadores

[23] L. D. GHEIN Cisco Press MPLS Fundamentals – A Comprehensive Introduction to MPLS, Theory and Practice – CCIE

[24] Cisco - Configuring a Basic MPLS VPN - URL: http://www.cisco.com/warp/public/105/mpls_vpn_basic.html

[25] W. D. GROVER - Mesh-Based Survivable Networks; Options and Strategies for Optical, MPLS, SONET, and ATM Networking (2003) – Multiprotocol Label – Prentice Hall

[26] SPRINGER - Next Generation Intelligent Optical Networks – 2008

[27] Optical Fiber Telecommunications - V Volume B - Systems And Networks - Feb 2008

[28] K. M. CAREN - Prentice Hall – Network Management – MIBS and MPLS – 2003