

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES
E EQUIPAMENTOS DE REDE**

ADRIANA CRISTINE ALVES RUOSO

**INFRAESTRUTURA DE REDES WANs UTILIZANDO AS
TECNOLOGIAS FRAME RELAY E MPLS**

MONOGRAFIA

Curitiba
2014

ADRIANA CRISTINE ALVES RUOSO

**INFRAESTRUTURA DE REDES WANs UTILIZANDO AS TECNOLOGIAS FRAME
RELAY E MPLS**

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Prof. M.e. Fabiano Scriptori de Carvalho

CURITIBA
2014

RESUMO

RUOSO, Adriana Cristine Alves. 2013. 63 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Esta monografia objetivou o estudo das redes WANs, com a descrição e implementação das tecnologias de redes de longa distância. Modelos de referência e padrões foram abordados com tópicos resumidos sobre redes IP e roteamento. O trabalho teve como tema principal o estudo da transição entre a tecnologia Frame Relay e MPLS. Durante anos o Frame Relay foi utilizado pelas operadoras de telecomunicações como tecnologia chave para oferecer redes WANs para seus clientes. Com o surgimento de redes convergentes, que utilizam voz, dados e vídeos foi necessária a implementação de técnicas de QoS e Engenharia de Tráfego, o MPLS surgiu como suporte para estas demandas. Para o desenvolvimento do trabalho foram realizadas simulações de infraestrutura de redes Wans por meio do software GNS3 e Wireshark.

Palavras-chave: Redes WANs, Frame Relay, MPLS.

ABSTRACT

Ruoso , Adriana Cristine Alves . 2013. 53 f . Monograph (Specialization in Configuration and Server Equipment and Network Management) . Federal Technological University of Paraná . Curitiba , 2013.

This thesis aimed to study the WANs, with the description and implementation of wide area networks technologies. Reference models and standards were summarized topics covered in IP networks and routing. The work had as main theme the study of the transition between the Frame Relay and MPLS technology. For years Frame Relay was used by telecom operators as a key technology for WANs provide for their clients. With the emergence of converged networks, using voice, data and video was necessary to implement techniques QoS and Traffic Engineering, MPLS has emerged as support for these demands. For the development of infrastructure work simulations Wans networks were performed using GNS3 and Wireshark software.

Keywords : Networks WANs , Frame Relay , MPLS

LISTA DE ILUSTRAÇÕES

Figura 1: Pilha de protocolo de internet e modelo de referência OSI.....	16
Figura 2: Datagrama na camada de internet.....	17
Figura 3: Cabeçalho IPV4	18
Figura 4: Cabeçalho IPV6	19
Figura 5: Relacionamento lógico entre camada de rede, transporte e aplicação	19
Figura 6: Pacote de dados na camada de transporte.....	20
Figura 7: Camada de aplicação.....	21
Figura 8: Rede de interconexão WAN	22
Figura 9: Opção de tecnologia WAN.....	23
Figura 10: Rede comutada por circuito	23
Figura 11: Rede comutada por pacotes	24
Figura 12: Acesso de rede integrado usando canais dedicados.....	27
Figura 13: Acesso de rede integrado usando WAN pública comutada	28
Figura 14: Quadro padrão Frame Relay	28
Figura 15: Tabela de encaminhamento de pacotes baseados em rótulos.....	30
Figura 16: Cabeçalho MPLS	32
Figura 17: Operação MPLS.....	33
Figura 18: Inserção dos rótulos aos pacotes IPs.....	33
Figura 19: Componentes da arquitetura InteServ.....	34
Figura 20: Arquitetura de serviços DiffServ	35
Figura 21: Balanceamento de carga MPLS-TE	36
Figura 22: GNS3	37
Figura 23: Wireshark.....	37
Figura 24: Infraestrutura de rede Utilizando o Frame-Relay	38
Figura 25: Teste de conectividade entre Matriz e Filial	47
Figura 26: Análise de pacotes Wireshark.....	47
Figura 27: Configuração PVC Frame-relay	48
Figura 28: Configuração PVC Frame-Relay.....	48
Figura 29: Configuração PVC Frame-Relay, Switch Frame-relay PVC 102	49
Figura 30: Configuração PVC Frame-Relay, Switch Frame-Relay PVC 201	49
Figura 31: Configuração do cenário implementado com a tecnologia MPLS	50

LISTA DE TABELAS

TABELA 1 - CONFIGURAÇÃO DO ROTEADOR DA MATRIZ	39
TABELA 2 - CONFIGURAÇÃO DO ROTEADOR DA FILIAL	40
TABELA 3 - CONFIGURAÇÃO DO SWITCH FRAME RELAY - OPERADORA.....	41
TABELA 4 - CONFIGURAÇÃO DO ROTEADOR DE BORDA MATRIZ	42
TABELA 5 - CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ.....	43
TABELA 6 - CONFIGURAÇÃO DO ROTEADOR DA BORDA DA FILIAL.....	44
TABELA 7 - CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ.....	50
TABELA 8 - CONFIGURAÇÃO PE1	53
TABELA 9 - CONFIGURAÇÃO DO ROTEADOR P1	55
TABELA 10 - CONFIGURAÇÃO DO ROTEADOR P2	58
TABELA 11 - CONFIGURAÇÃO DO ROTEADOR PE2	60
TABELA 12 - CONFIGURAÇÃO DA FILIAL	65
TABELA 13 - LISTA DAS INTERFACES EM PE1	69
TABELA 14 - LISTA DAS INTERFACES P1	69
TABELA 15 - LISTA DAS INTERFACES EM PE2.....	69
TABELA 16 - LISTAS DE INTERFACES EM PE2.....	69
TABELA 17 - LISTAS DAS TABELAS DE ROTEAMENTO DE PE1	70
TABELA 18 - LISTAS DAS TABELAS DE ROTEAMENTO DE P1.....	70
TABELA 19 - LISTAS DE TABELAS DE ROTEAMENTO DE PE2.....	70
TABELA 20 - LISTAS DE TABELAS DE ROTEAMENTO DE PE2.....	71
TABELA 21 - ROTEAMENTO ENTRE MATRIZ E FILIAL	71
TABELA 22 - ROTEAMENTO ENTRE MATRIZ E FILIAL	71

LISTA DE SIGLAS

ARPANET	Advanced Research Projects Agency
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification
CVC	Circuito Virtual Comutado
CR	Comandnd Response
DE	Discart Eligibility
DHCP	Dynamic Host Configuration Protocol
DLCI	Danta Link Connection Identifier
DNS	Domain Name System
DCE	Data Circuit-Terminating Equipment
DTE	Data Terminal Equipament
EA	Extended Address
EXP	Experimental Bits
FECN	Forward Explicit Congestion Notification
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	HyperText Transfer Protocol Security
Gbps	Gigabits por segundo
ISO	Internetal Standards Organization
LABEL	Rótulo
LAN	Local Area Network
LAP	Link Access Procedure
LAPB	Link Access Procedure Balanced
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISP	Internet Service Provider
ITU-T	International Telecommunicatios Union
MAN	Metropolitan Area Network
Mbps	Megabit por segundo
MPLS	Multiprotocol Label Switching

NFS	National Science Foundation
PVC	Circuito Virtual Permanente
QOS	Quality of service
RIP	Routing Information Protocol
RDSI	Rede Digital de Serviços Integrados
RFC	Request For Comments
RPTC	Rede pública de telefonia comutada
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SVC	Circuito Virtual Comutado
TCP	Transmission Control Protocol
TELNET	Terminal Virtual
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VC	Virtual Circuit / Channel
VCI	Virtual Circuit Identifier
VOIP	Voice over IP
VPI	Virtual Path Identifier
WAN	Wide Área Network

SUMÁRIO

1 INTRODUÇÃO	12
1.1 JUSTIFICATIVA	13
1.2 OBJETIVO GERAL	13
1.3 OBJETIVOS ESPECÍFICOS	13
2 REFERENCIAL TEÓRICO	14
2.1 REDES DE COMPUTADORES	14
2.2 PILHA DE PROTOCOLOS TCP/IP	15
2.2.1 Camada Física	16
2.2.2 Camada de Enlace	16
2.2.3 Camada de Rede	17
2.2.4 Transporte	19
2.2.5 Aplicação	20
2.3 LOCAL AREA NETWORK – LAN	21
2.3.1 Wide Area Network - WAN	22
2.3.2 Técnicas de Comutação	23
2.4 Roteamento	25
2.4.1 Roteamento Estático	25
2.4.2 Protocolos de Roteamento Dinâmicos	25
2.4.3 RIP	25
2.4.4 EIGRP	26
2.4.5 OSPF	26
2.5 TECNOLOGIAS DE REDES DE LONGA DISTÂNCIA	26
2.5.1 Frame Relay	27
2.5.2 MPLS	29
2.5.2.1 Terminologia de MPLS	30
2.5.2.2 Cabeçalho MPLS	31
2.5.2.3 Funcionamento	32
2.5.2.4 Qualidade de Serviços (QoS)	34
2.5.2.5 Engenharia de Tráfego (TE)	35
2.5.2.6 Ferramentas	36
3 IMPLEMENTAÇÃO	38
3.1 CENÁRIO DE IMPLEMENTAÇÃO COM TECNOLOGIA FRAME RELAY	38
3.2 CENÁRIO COM IMPLEMENTAÇÃO MPLS	50
4. CONSIDERAÇÕES FINAIS	73
REFERÊNCIAS	75

1 INTRODUÇÃO

As redes de computadores surgiram com a pretensão de transferir informações de um computador para outro, mas com o rápido progresso tecnológico a história mostrou que isso era apenas o começo do que seria essencial. Através dos anos as redes passaram por um longo processo de evolução, fruto da busca em atender a demanda por maior agilidade entre coleta, armazenamento, processamento das informações e as conexões entre pequenas e extensas áreas geográficas.

O primeiro passo foi dado com o surgimento das redes locais (*Local Area Network – LANs*), que nasceram nos ambientes acadêmicos, com o intuito de viabilizar a interconexão de equipamentos de comunicações em uma área geográfica restrita.

A padronização dos protocolos em padrões abertos permitiu que redes de diferentes fabricantes fossem interconectadas, sendo possível ampliar a área de abrangência nas implementações, surgindo, assim, os conceitos de redes metropolitanas (*Metropolitan Area Network – MANs*), que tornaram possível interligar redes e equipamentos em diversos locais e pontos diferentes em uma cidade ou uma área metropolitana e as redes geograficamente distribuídas (*WANs*), que propiciaram conexão de redes, permitindo a comunicação de longa distância, possibilitando abranger locais em várias cidades, países ou continentes.

A demanda por constante evolução fez surgir o Frame Relay, uma nova tecnologia para redes WANs, com o uso de circuitos virtuais, utilizada durante anos pelas empresas de telecomunicações para interligar seus clientes. Passados alguns anos, surgiu a tecnologia Asynchronous Transfer Mode (ATM), que veio com o objetivo de oferecer altas velocidades nas conexões das redes. Mesmo com o surgimento do ATM, a tecnologia Frame Relay continuou sendo utilizada para interligar LANs por meio das operadoras de Telecomunicações.

A necessidade de as redes WANs oferecerem Qualidade de Serviço (QoS) e Engenharia de tráfego (TE) possibilitou o desenvolvimento do Multiprotocol Label Switching (MPLS) que opera com encaminhamento de rótulos (labels), com a capacidade de propiciar agilidade, com o envio dos pacotes e oferecer recursos de QoS e TE.

Este projeto foi desenvolvido por meio de levantamento bibliográfico presente nos veículos de comunicação como livros e artigos. Serão apresentados alguns conceitos já sedimentados que serviram para o entendimento do tema tratado por essa monografia.

1.1 JUSTIFICATIVA

Atualmente, as empresas de telecomunicações oferecem diversos serviços de interligação WANs para que os clientes possam fazer a conexão entre os equipamentos. É necessário ter uma infraestrutura de redes de telecomunicações que possa oferecer serviços, atendendo às exigências atuais. As tecnologias têm passado por mudanças no intuito de atender às demandas no que se refere a melhor desempenho das redes IPs, QoS e engenharia de tráfego na transferência das informações. É necessário fazer um estudo da tecnologia MPLS para verificar quais as vantagens na implementação desta tecnologia em relação ao Frame Relay. Foram feitos testes e simulações nos cenários de implementação de infraestrutura de redes que utilizam as tecnologias Frame Relay e MPLS, para verificar as características de implementação de cada tecnologia.

1.2 OBJETIVO GERAL

Implementar e analisar uma infraestrutura de redes WANs utilizando as tecnologias Frame-Relay e MPLS.

1.3 OBJETIVOS ESPECÍFICOS

- ✓ Fazer o levantamento do estado da arte das tecnologias WANs utilizadas na pesquisa;
- ✓ analisar as ferramentas que serão utilizadas como suporte ao trabalho;
- ✓ planejar cenários de interconexão das redes empresariais por meio das WANs;
- ✓ implementar os cenários por meio de roteadores ou *softwares* de simulação/emulação;
- ✓ analisar as características das redes WANs implementadas.

2 REFERENCIAL TEÓRICO

O desenvolvimento das redes aconteceu a partir de pesquisas dentro do departamento de Defesa dos Estados Unidos, chamado *Advanced Research Projects Agency Network* (ARPANET), que possibilitou a conexão de universidades e repartições públicas por meio de linhas telefônicas privadas. Com a ampliação das redes, utilizando rádio e satélite, os problemas dos protocolos existentes começaram a ser conhecidos. Surgiu, então, a necessidade de criar uma nova arquitetura de referência, com capacidade de conectar diversas redes simultaneamente e, assim, nasceu o protocolo TCP/IP, que se tornou protocolo oficial da ARPANET em 1983. O TCP/IP foi interconectado à *National Science Foundation* (NSF), o que possibilitou a expansão dessas redes, não mais se restringindo a ambientes acadêmicos, propiciando a sua disseminação.

Em 1990 surgiu a *World Wide Web* (WWW) que revolucionou diversos aspectos da rotina diária em ambientes corporativos e pessoais. A conexão com a Internet possibilitou a conexão com uma rede mundial. A Internet serviu também como plataforma para habilitação e a disponibilidade de novas aplicações (Kurose, 2010).

A ampliação das redes permitiu que as informações e dados estivessem disponíveis em tempo real, mas essa evolução desencadeou uma crescente demanda por banda, exigindo da Internet Service Provider (ISPs) soluções eficientes.

O aumento no número de usuários remotos, o acesso à *Internet*, a complexidade de aplicações em ambientes virtualizados ou em *cloud computing* tem exigido, a cada dia, serviços mais especializados e específicos.

As operadoras de telecomunicações têm como desafio constante buscar novas tecnologias com o objetivo de assegurar um mínimo de qualidade e segurança nos serviços disponibilizados.

2.1 REDES DE COMPUTADORES

As Redes de Computadores surgiram da necessidade de interligar dois ou mais computadores, formando um conjunto de computadores interligados

fisicamente, entre uma pequena distancia ou até milhares de quilômetros, interconectados por meio de sistemas de comunicação, realizando trabalhos de processamento de dados ,de forma isolada ou compartilhadas.

2.2 PILHA DE PROTOCOLOS TCP/IP

A pilha de protocolos *Transmission Control Protocol/ Internet Protocol* (TCP/IP) é a mais utilizada atualmente. As tarefas envolvendo o processo de comunicação são distribuídas entre protocolos, organizados nas cinco camadas distintas: Física, Enlace, Rede, Transporte e Aplicação. Cada protocolo da pilha possui uma função distinta no processo de comunicação, onde a camada inferior oferece serviço à camada superior, usando como base o conceito de uma pilha de protocolos independentes.

O TCP/IP executa protocolos que controlam o envio e o recebimento de informações dentro da Internet, sendo capaz de diferenciar uma aplicação da outra; antes de fechar a conexão ele garante a entrega confiável de todos os dados. É responsável por fornecer a conexão direta de um aplicativo do *host* de origem para o *host* de destino, sendo chamado de um protocolo fim-a-fim. Cada mensagem é encapsulada em um datagrama IP que é utilizado para o transporte, mas, apesar de ser utilizado para transportar, ele não é capaz de interpretar as mensagens.

O protocolo IP especifica o formato dos pacotes que são enviados e recebidos entre roteadores e sistemas finais, sendo o responsável por encaminhar um bloco de dados de um *host* de origem para um *host* de destino e, no caso do *host* de destino estar em outra rede, o IP utiliza o roteador. Segundo (Comer, 2007):

O TCP/IP fornece um serviço de transporte de stream orientado a conexão, full-duplex e completamente confiável (nenhuma duplicação ou perda de dados), o que permite a dois programas aplicativos formarem uma conexão, enviar dados em uma ou outra direção e então terminar a conexão.

Na figura 1 é possível visualizar a pilha de protocolo de Internet e modelo de referência OSI.

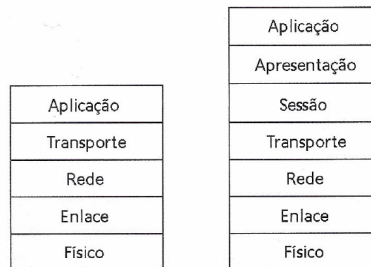


Figura 1: Pilha de protocolo de internet e modelo de referência OSI

Fonte: (Kurose, 2010 p.38)

2.2.1 Camada Física

A camada física é responsável por converter os dados em sinais numéricos nos meios de comunicação, tem a função de encontrar o caminho mais curto e confiável, com o objetivo de transmitir um fluxo bruto de bits (sinal elétrico, óptico ou microondas) de uma camada para outra.

Para (Kurose; Ross, 2006) "esta camada é responsável por movimentar bits individuais que estão dentro do quadro de um nó para o seguinte". Para (Stallings, 2005) "a camada física abrange a interface física entre um dispositivo de transmissão de dados ou um meio de transmissão de rede".

2.2.2 Camada de Enlace

É de responsabilidade da camada de enlace detectar e corrigir erros que possam ter ocorrido na camada física, fornecer uma interface de serviço bem definida à camada de rede e regular o fluxo de dados, para que não seja enviada uma quantidade excessiva de dados, entre receptores e transmissores.

Segundo (Tanenbaum, 2003):

A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los se necessário em unidades menores, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade.

Os bits a serem enviados ao nível físico são particionados em quadros, cada um contendo uma forma de redundância para detecção de erros, sendo possível criar e reconhecer os limites dos quadros e, para evitar que o transmissor envie mais dados que o receptor possa processar, é utilizado um mecanismo de controle de fluxo que possibilita saber qual o espaço disponível no *buffer*.

2.2.3 Camada de Rede

Na camada de Rede existe o protocolo IP (*Internet Protocol*) que foi projetado com o objetivo de interligar as redes. Para (Taneunbaum, 2003):

A tarefa do IP é fornecer a melhor forma possível de transportar datagramas da origem para o destino independentemente de essas máquinas estarem na mesma rede ou de haver outras redes entre elas.

Esta camada é responsável por receber os pacotes da camada de transporte e adicionar o endereçamento virtual, ou seja, o endereço IP, acrescentando informações de endereço do computador de origem e de destino.

Para (Kurose; Ross, 2006) a camada de Rede é composta por dois componentes principais. Um deles o protocolo IP que define os campos no datagrama e o modo de agir nesses campos entre sistemas finais e roteadores. O outro componente importante é o protocolo de roteamento que determina as rotas que os datagramas seguem entre origens e destinos.

Apesar de também conter numerosos protocolos de roteamento, (Kurose; Ross, 2006) essa camada é denominada como camada IP, refletindo o fato de que ela é o elemento fundamental que mantém a integridade da Internet.

Na Figura 2 é possível visualizar o datagrama na camada da Internet.

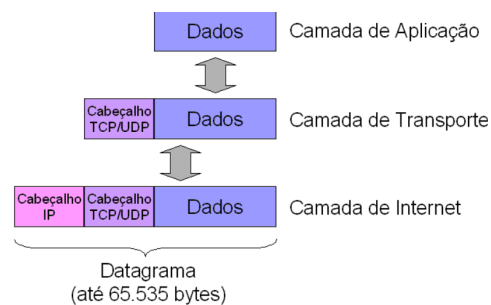


Figura 2: Datagrama na camada de internet

Fonte: (Clube do Hardware, 2013)

Na Internet cada equipamento tem de ser codificado com seu número de rede e seu endereço IP. A princípio, a combinação é exclusiva, não sendo possível haver dois equipamentos com o mesmo endereço IP.

Há duas versões do protocolo IP em uso atualmente:

Os computadores se comunicam na *Internet* por meio do *Internet Protocol* (IP).

A figura 3 mostra o formato do cabeçalho Internet Protocol Versão 4 (IPv4).

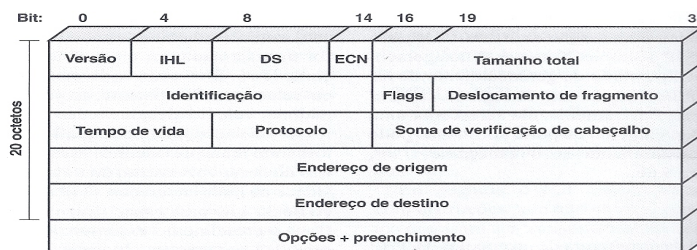


Figura 3: Cabeçalho IPv4

Fonte: (Stallings, 2005 p.85).

IPv4: o IPv4 utiliza um endereço de 32 bits para especificar uma origem ou destino. Apesar do seu desempenho durante anos, os problemas apresentados pelo IPv4 têm se tornado relevantes. O principal deles é a falta de endereços, pois o IP utiliza um endereço de 32 bits para especificar uma origem ou destino, sendo insuficiente para atender todos os sistemas que precisam de endereços.

IPv6: o protocolo IPv6 surgiu como uma necessidade de atender um número maior de endereços. O cabeçalho usa uma série de formato fixo, o espaço de endereçamento é maior, tem 128 bits de comprimento o que possibilita criar níveis de hierarquia adicional. O formato de cabeçalho flexível possibilita incluir um conjunto de cabeçalhos opcionais e a inclusão de informações pelo datagrama. Permite uma abstração de fluxo e bits para a especificação de serviço diferenciado (Diffserv), assim como no IPv4.

Na Figura 4 é possível visualizar o cabeçalho IPv6.

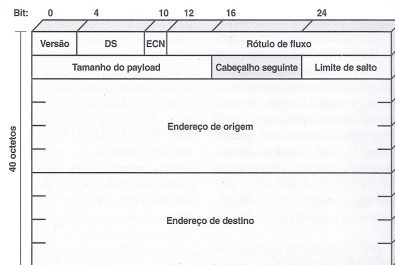


Figura 4: Cabeçalho IPv6

Fonte: (Stallings, 2005 p.85)

2.2.4 Transporte

A camada de Transporte é responsável por fornecer um meio de transporte lógico aos dados transmitidos na rede, este transporte pode ser orientado a conexão ou não orientado. Para (Comer, 2006) “a principal tarefa da camada de transporte é prover comunicação de um programa aplicativo para outro”.

Essa camada tem a responsabilidade de oferecer um serviço confiável e eficiente aos processos presentes na camada de aplicação, para tanto ela utiliza alguns serviços oferecidos pela camada de rede, esses serviços são chamados de entidade de transporte. Podemos localizar a entidade de transporte em um processo do usuário, no núcleo de sistema operacional, em um pacote de bibliotecas vinculado a aplicações de rede ou na placa de interface de rede. O relacionamento lógico existente entre as camadas está ilustrado na Figura 5.

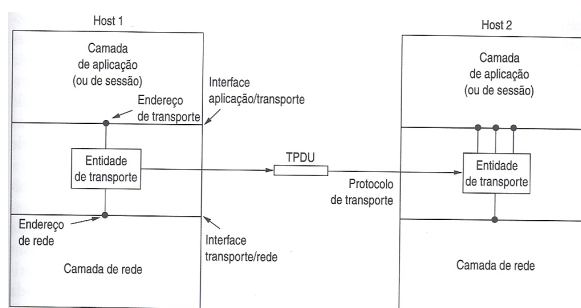


Figura 5: Relacionamento lógico entre camada de rede, transporte e aplicação

Fonte (Tanenbaum, 2003 p.513)

Essa camada trabalha com dois protocolos: o *User Datagram Protocol* (UDP) e o *Transmission Control Protocol* (TCP). O protocolo UDP é não confiável e não orientado à conexão. Fornece apenas os serviços de endereçamento e fragmentação, não provendo controle do fluxo, confiabilidade e erro. Se houver

congestionamento na rede, um datagrama pode ser perdido, pois o UDP não informa as aplicações desta ocorrência. No caso de congestionamento em uma rota da rede o pacote pode chegar ao seu destino em uma ordem diferente daquela que foi enviada. Este protocolo trabalha sem estabelecer conexões entre os *softwares* que estão se comunicando. É ideal para aplicações onde a velocidade é mais importante que a confiabilidade, como em aplicações multimídia: *Trivial File Transfer Protocol (TFTP)*, *Routing Information Protocol (RIP)*, *Simple Network Management Protocol (SNMP)* e *Domain Name System (DNS)*, pois o UDP tem um cabeçalho menor, o que requer menos *overhead*, significando menos atraso.

Segundo (Taneubaum, 2003) "o TCP foi projetado para se adaptar dinamicamente às propriedades da inter-rede e ser robusto diante de muitos tipos de falhas que podem ocorrer". O Protocolo TCP é um protocolo orientado à conexão, confiável que permite a entrega sem erros de um fluxo de bytes de um computador de origem a um computador de destino, gerenciando fluxos e interfaces TCP para a camada IP.

Na Figura 6 é possível visualizar o pacote de dados da camada de transporte.

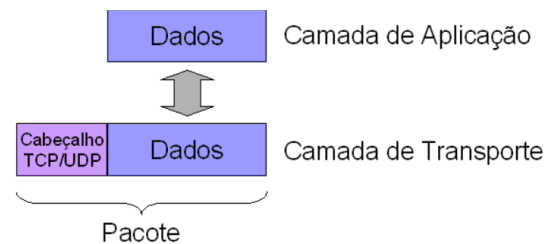


Figura 6: Pacote de dados na camada de transporte

Fonte: (Clube do Hardware, 2013)

2.2.5 Aplicação

A camada de aplicação é a camada que está mais perto do usuário. Contém os protocolos de nível mais alto e define como os processos de aplicação trocam as mensagens. É responsável por fornecer uma interface entre as aplicações que são utilizadas para enviar os dados para a rede pela qual as mensagens são transmitidas. "Contém a lógica necessária para dar suporte a diversas aplicações do usuário" (Stallings,2005). Esta camada possibilita que o aplicativo escolha o estilo de transporte a ser usado, podendo ser fluxo contínuo

de bytes ou uma sequência de mensagens individuais. Os processos que rodam são particulares da aplicação, os dados são transmitidos no formato interno e, após, são codificados no padrão do protocolo.

A Figura 7 apresenta o datagrama da camada de aplicação.

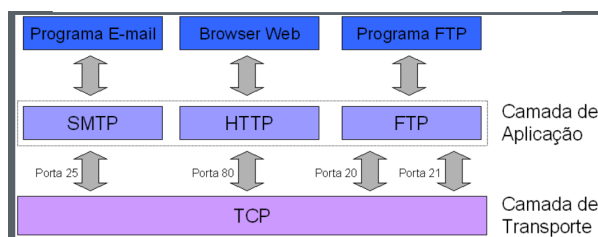


Figura 7: Camada de aplicação

Fonte: (Clube do Hardware, 2013)

Dentre alguns protocolos que fazem parte da camada de aplicação e aceitam diretamente as aplicações do usuário pode-se citar:

- ✓ *Hyper Text Transfer Protocol (HTTP);*
- ✓ *HyperText Transfer Protocol Security (HTTPS);*
- ✓ *File Transfer Protocol (FTP);*
- ✓ *Simple Mail Transfer Protocol (SMTP);*
- ✓ *Terminal Virtual (TELNET);*
- ✓ *Domain Name System (DNS);*
- ✓ *Dynamic Host Configuration Protocol (DHCP).*

2.3 LOCAL AREA NETWORK – LAN

As LANs são redes com uma extensão geográfica restrita, privada, com o objetivo de interligar computadores localizados na mesma sala, edifício ou campus, possuindo uma distância máxima de alguns quilômetros entre as estações mais distantes. Segundo Soares (1997) “são redes privadas, que permitem a interconexão de equipamentos de comunicação de dados numa pequena região”.

As LANs funcionam com taxas de transmissão que variam de 10 Mbps a 10Gbps, tendo como características o baixo retardo a baixa taxa de erro de bits. Para (Comer, 2007):

As redes que permitem que múltiplos computadores compartilhem um meio de comunicação são usadas para comunicação local. As conexões ponto a ponto são usadas para redes de longa distância e para alguns outros casos especiais.

2.3.1 Wide Area Network - WAN

As WANs têm uma abrangência geográfica maior que uma LAN, funcionam além do escopo geográfico, não sendo restrito a um mesmo lugar ou prédio. A escalabilidade é o aspecto chave da WAN, pois ela deve ser capaz de crescer o quanto for necessário, permitindo que os computadores se comuniquem simultaneamente, utilizando conexões seriais de vários tipos para fornecer acesso à largura de banda em grandes áreas geográficas. Como não é possível conectar computadores em um país ou em todo o mundo, da mesma forma que os computadores são conectados em uma rede local, foi necessária a busca por tecnologias diferentes para atender a essa necessidade.

A Figura 8 apresenta a composição de uma rede WAN.

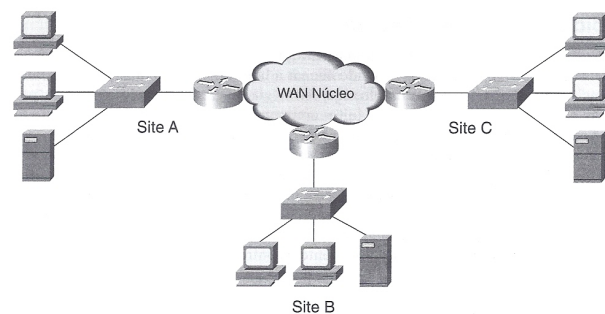


Figura 8: Rede de interconexão WAN

Fonte: (Birkner, 2003)

Dependendo da utilização, o usuário tem diversas opções para contratar enlaces WANs. As principais tecnologias de redes de longa distância são divididas em dois tipos distintos de comutação: redes comutadas por circuitos e redes comutadas por pacotes.

A Figura 9 mostra como são divididas as redes de longa distancia.

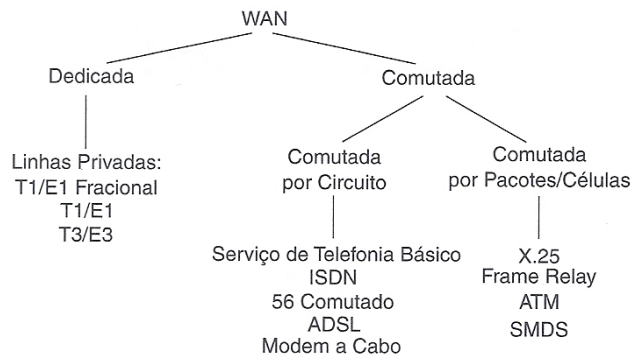


Figura 9: Opção de tecnologia WAN

Fonte:(Birkner, 2003 p.244)

2.3.2 Técnicas de Comutação

Para (Stallings, 2005):

Na transmissão de dados para além de uma rede local, a comunicação normalmente se dá mediante a transmissão de dados da origem ao destino por uma rede de nós de comutação intermediários.

Estes nós intermediários podem encaminhar os pacotes utilizando os conceitos de comutação por circuitos e comutação por pacotes. A Figura 10 apresenta uma rede comutada por circuito.

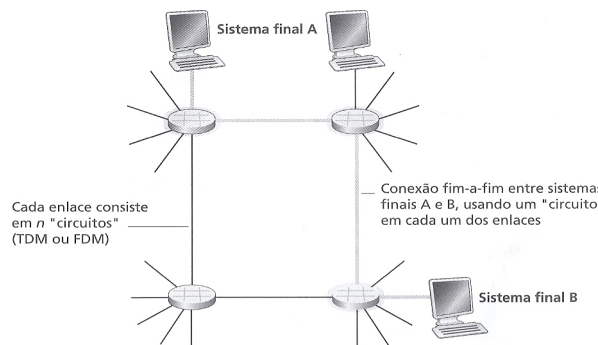


Figura 10: Rede comutada por circuito

Fonte:Kurose, Ross, 2006, p.13

Na comutação por circuitos, um circuito físico e dedicado é estabelecido entre a origem e o destino, por meio de protocolos de sinalização. Este circuito é mantido durante todo o período de transmissão das informações. A vantagem na utilização deste tipo de comutação é que o enlace é dedicado para as estações na transmissão das informações. A desvantagem é que a infraestrutura da

empresa de telecomunicações não é utilizada de forma a maximizar o envio de dados entre as estações. Assim, se um usuário não enviar informações pela rede, mesmo assim o enlace está dedicado e garantido para ele. A rede de telefonia utiliza a infraestrutura de comutação por circuitos para oferecer os serviços aos seus usuários. De acordo com (Stallings, 2005) “uma importante característica das redes de comutação de circuitos é que os recursos dentro da rede são dedicados a chamadas específicas”. As tecnologias utilizadas na comutação de circuitos são: a Rede Digital de Serviços Integrados (RDSI) e a Rede Pública de Telefonia Comutada (RPTC).

A figura 11 é possível visualizar a configuração de uma rede comutada por pacotes.

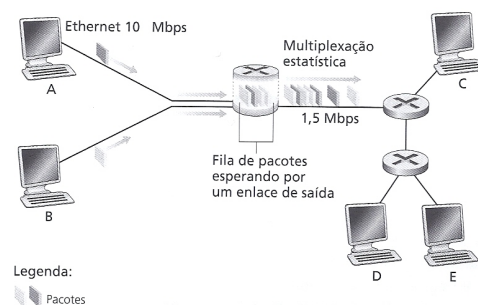


Figura 11: Rede comutada por pacotes

Fonte: Kurose, Ross, 2006, p.15

Na comutação por pacotes não existem circuitos físicos dedicados para a transmissão de informações entre as estações. As informações a serem transmitidas são divididas em pacotes e enviadas separadamente. Estes pacotes contêm informações suficientes para que as informações possam ser roteadas entre os nós intermediários, possibilitando o encaminhamento das informações entre estas redes. As desvantagens na utilização de uma rede comutada por pacotes são a falta de Qualidade de Serviço (QoS), a entrega desordenada de pacotes (alguns pacotes podem chegar depois de outros) e o possível descarte de pacotes em situações de sobrecarga. As tecnologias de redes WANs que utilizam a comutação por pacotes são X25, Frame-Relay e ATM.

2.4 Roteamento

Os roteadores encaminham as informações em uma rede comutada por pacotes, analisando o endereço IP de destino. Eles preenchem as tabelas de roteamento com base nas informações destas redes de destino. O roteamento pode ser dividido de duas formas: estático e dinâmico.

2.4.1 Roteamento Estático

No roteamento estático, o administrador deve fazer um projeto lógico indicando quais as rotas que os pacotes devem percorrer, na infraestrutura de rede, para alcançar a rede destino. Depois, deve configurar manualmente as rotas em cada roteador para que as informações consigam trafegar da origem ao destino. É indicado para redes de menor porte, porque em cada alteração da topologia, as modificações devem ser feitas manualmente. A vantagem é o menor *overhead*, porque não precisa enviar informações de controle para gerenciar o estado do enlace, nem fazer convergência da rede.

2.4.2 Protocolos de Roteamento Dinâmicos

Os protocolos de roteamento dinâmicos servem para estabelecerem um mapeamento da rede e preenchimento da tabela de roteamento de forma dinâmica, fazendo com que todas as alterações na topologia da rede possam ser modificadas sem a interferência do administrador da rede. Estes protocolos trocam informações (*updates*) formando adjacências entre os roteadores para montar as tabelas de roteamento e possibilitar o encaminhamento das informações na rede. Dentre os protocolos de roteamento mais utilizados atualmente estão o RIP, EIGRP e OSPF.

2.4.3 RIP

É um protocolo de roteamento vetor distância que troca informações entre os roteadores (*updates*) a cada 30 segundos. O RIP tem duas versões: 1 e 2. A versão 1 é Classful e não permite a utilização de máscara de rede de

tamanho variável (VLSM). Já a versão 2 permite a utilização de VLSM e redes não contíguas. É um protocolo definido pelo *Internet Engineering Task Force* (IETF). Com isto, é possível implementar o RIP em roteadores de diversos fabricantes (Cisco, HP, 3Com). As desvantagens do RIP são: convergência muito lenta, em alguns casos o RIP leva minutos até que a rede faça a convergência total. Um limite máximo de 15 roteadores, impedem que este protocolo possa ser utilizado em redes de grande dimensão.

2.4.4 EIGRP

É um protocolo vetor distância de roteamento desenvolvido pela empresa Cisco. Tem um melhor desempenho do que o protocolo RIP, podendo ser implementado em redes com centenas de roteadores. Tem suporte a VLSM e redes não contíguas. A sua convergência é rápida, devido a alguns mecanismos internos que fazem com que o desempenho seja maximizado, para que a rede possa fazer a convergência de forma rápida. Sua desvantagem é que todos os roteadores utilizados para a implementação devem ser da fabricante Cisco. Isto porque é um protocolo proprietário.

2.4.5 OSPF

É um protocolo de roteamento de estado de enlace (*link state*) aberto desenvolvido pelo *Internet Engineering Task Force* (IETF). É um protocolo de roteamento *classless*, que utiliza máscara de rede de tamanho variável. Tem uma característica hierárquica, com uma área de Backbone (área 0) e as outras áreas conectadas a esta área. Por causa desta característica hierárquica, pode-se construir redes de grandes dimensões, como por exemplo do tamanho de um continente. O OSPF tem uma convergência rápida, fazendo com que qualquer alteração na topologia da rede seja propagada para os roteadores envolvidos.

2.5 TECNOLOGIAS DE REDES DE LONGA DISTÂNCIA

É responsável por interligar redes em áreas amplas, geograficamente distribuídas, com o dever de propiciar o tráfego de dados, voz e imagem em altas

velocidades, interconectando diversos pontos; sendo possível utilizar diversas tecnologias de transportes na busca por melhor desempenho no tráfego dos dados.

2.5.1 Frame Relay

Foi desenvolvido para suprir ineficiências existentes no X25, buscando eficiência relacionada a custos de projetos de WAN. É um protocolo de rede geograficamente distribuída, foi muito utilizada para interligações empresariais. Opera na camada física e enlace do modelo de referência OSI. O conceito de comutação de pacotes é utilizado para encaminhar as informações por meio das redes de forma simples e rápida. Pode ser utilizado por meio de uma linha dedicada para proporcionar a utilização da técnica de multiplexação flexível e conveniente, criando uma malha lógica de circuito Virtual (*Virtual Circuit – VC*). Os VCs fornecem um caminho de comunicação bidirecional de um dispositivo ao outro e são identificados por DLCIs.

O Frame Relay, assim como o X25, permite a comunicação em circuitos: circuito virtual permanente (PVC) e circuito comutado virtual (SVC). O circuito virtual na rede é identificado por um número *Data Link Connection Identifier* (DLCI).

A Figura 12 apresenta a rede que utiliza os canais dedicados.

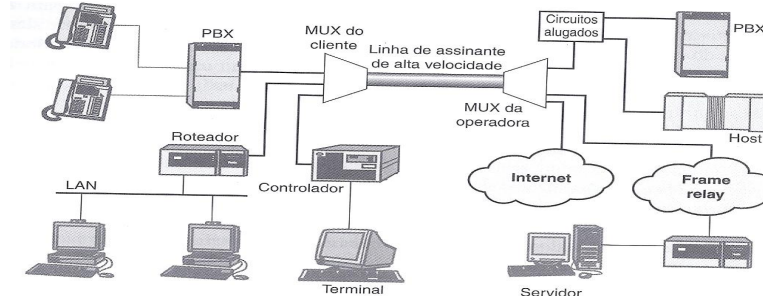


Figura 12: Acesso de rede integrado usando canais dedicados

Fonte:(Stallings,2005 p.274)

De acordo com (Birkner, 2003) “o Frame Relay foi planejado como uma alternativa eficaz em termos de custo a projetos de WAN ponto-a-ponto de linha privada”. Para (Stallings, 2005) “o Frame Relay é projetado para fornecer um esquema de tráfego mais eficiente do que a comutação de pacotes tradicional”.

A Figura 13 mostra uma rede WAN comutada.

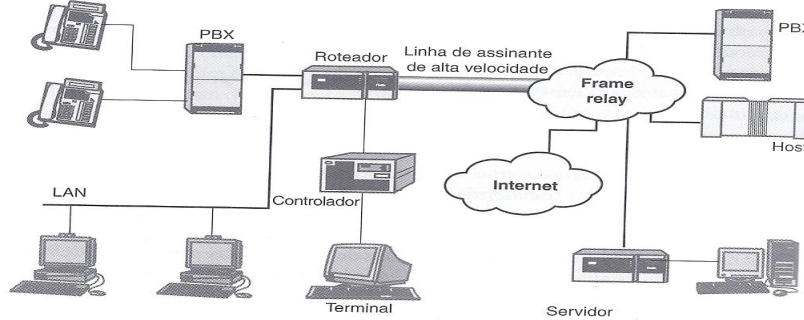


Figura 13: Acesso de rede integrado usando WAN pública comutada

Fonte: (Stallings, 2005 p.274).

O Frame Relay substituiu o antigo protocolo X25, oferecendo uma forma mais rápida de transmitir as informações e não tendo todo o controle de erros em todos os nós da rede, característica do X25. Isto se deve aos meios de transmissão utilizados atualmente. Com a utilização das fibras ópticas, as taxas de erros de bits, nas comunicações de dados ficaram menores. Isto permitiu que o controle de erros fosse feito fim-a-fim, ou seja nas máquinas finais. Os campos que compõem o Frame Relay são:

- ✓ **DLCI (Data link Connection Identifier):** é o identificador de enlace de dados, à conexão virtual entre o dispositivo DTE e *switch*, contém 10 bits de cabeçalho definido pelo padrão. Os primeiros 6 bits são dedicados a parte 1 do identificador, a segunda parte do DLCI usa quatro primeiros bits do segundo byte. A importância dos valores do DLCI é local, o que significa que a mesma conexão virtual pode ter valores diferentes em extremidades opostas, sendo exclusivo apenas no canal físico a que pertence;

Na Figura 14 abaixo é possível visualizar o quadro padrão do Frame Relay.

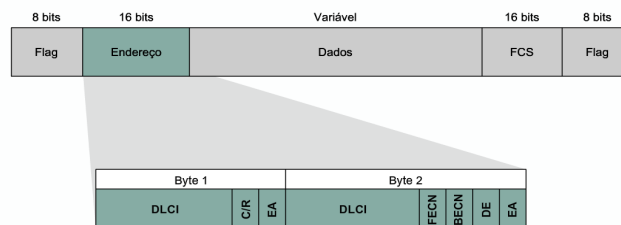


Figura 14: Quadro padrão Frame Relay

Fonte: (CCNA Exploration – Acessando a WAN – Módulo 4 - Slide 3.1.3.1).

- ✓ Bit de endereço estendido (*Extended Address – EA*): permite DLCIs mais longos. O bit EA indica se o byte atual tem o endereço final. Se o bit EA for igual a 1 indica que o byte atual contém o endereço final. Se bit EA for igual a 0 significa que deve ser esperado outro *byte* de endereço. O oitavo bit de cada byte do campo de endereço indica o EA;
- ✓ Bit de Comando-Resposta (*Command Response - C/R*): permite as camadas mais altas identificarem o frame. O bit C/R geralmente não é utilizado pelo Frame Relay;
- ✓ Bit (*Discart Eligibility – DE*): o *Bit* DE é responsável por indicar o nível de prioridade do frame. Para manter a rede livre da sobrecarga, às vezes se faz necessário o descarte dos frames pelos nós de comutação. Quando o bit DE for igual a 1 significa que o frame deve ser descartado no caso de congestionamento. Este bit pode ser configurado durante o percurso pela origem dos dados ou pelos nós de comutação;
- ✓ *Forward Explicit Congestion Notification (FECN)*: é responsável por indicar que o tráfego está congestionado, pode ser configurado por qualquer nó de comutação. Informa ao nó de destino de dados que ocorreu um congestionamento no circuito;
- ✓ *Backward Explicit Congestion Notification (BECN)*: o Bit BECN é responsável por informar ao nó de origem se há congestionamento;
- ✓ Local Management Interface (LMI): é responsável pelo gerenciamento. Possui mecanismos de *keepalive* que possibilita verificar se os dados estão fluindo na rede. (CCNA Exploration – Acessando a WAN)

2.5.2 MPLS

O Multiprotocol Label Switching (MPLS) evoluiu por meio de esforços que foram realizados pela indústria, na segunda metade dos anos 1990, visando aperfeiçoar a velocidade de distribuição dos roteadores IP, adotando um novo conceito de redes de circuitos virtuais, um conceito de rótulo de tamanho fixo (Kurose, Ross, 2006).

O MPLS é um mecanismo definido nas RFCs 3031 e 3032, que faz o encaminhamento das informações por meio de um rótulo (label) de tamanho fixo, que torna o processo de encaminhamento dinâmico. Com a implementação e utilização do MPLS a rede passa a ter um melhor desempenho no

encaminhamento das informações, o que permite a implementação de políticas de Qualidade de Serviço (QoS) para diferenciar os diversos fluxos de informações que trafegam na rede (dados, voz, vídeo), fazendo com que os fluxos mais importantes (voz, vídeo) tenham maior prioridade. Isto tem impacto na utilização de determinados serviços, como Voz sobre IP (VoIP), que necessita de determinadas características como baixo *delay/jitter* e fluxo contínuo, com poucas perdas de pacotes, para que a aplicação tenha um melhor desempenho. A Figura 15 apresenta a Tabela de encaminhamento de Pacotes baseada em rótulos.

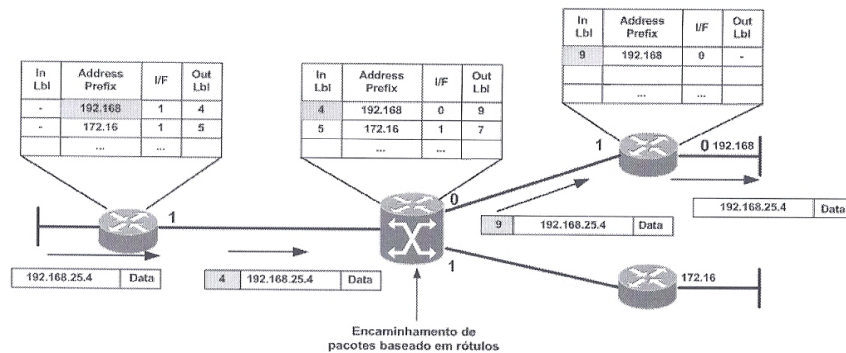


Figura 15: Tabela de encaminhamento de pacotes baseadas em rótulos

Fonte:(Oliveira,Lins, Mendonça, 2012 p.35).

A forma de comutar dados por meio de uma rede é definida por uma consulta a um pequeno rótulo ou etiqueta em cada pacote de dados. Após retirar o rótulo do pacote é realizada uma consulta em uma tabela para determinar o próximo salto e um novo rótulo é adicionado ao pacote (Farrel, 2005).

2.5.2.1 Terminologia de MPLS

Para estudar o MPLS é importante conhecer o hermetismo científico da terminologia a ele aplicado (Osborne; Simnha, 2003). Segue abaixo a demonstração de alguns termos.

- ✓ *Upstream*: um roteador que está mais próximo da origem de um pacote que outro roteador;
- ✓ *Downstream*: Um roteador que está mais distante da origem de um pacote que outro;
- ✓ Plano de Controle: são trocadas as informações de roteador e rótulo;

- ✓ Plano de Dados de Encaminhamento: é realizado o encaminhamento, após ser realizado o controle;
- ✓ Rótulo (*Label*): uma tag tamanho fixo, em que o MPLS é baseado;
- ✓ Vínculo de Rótulos: uma associação de um FEC (prefixo) a um rótulo;
- ✓ Imposição de Rótulo: acrescenta um rótulo a um pacote de dados;
- ✓ Descarte de Rótulo: remove o rótulo de um pacote de dados;
- ✓ Troca de Rótulos: Muda o valor do rótulo no cabeçalho;
- ✓ *Label Switch Router* (LSR): dispositivo que comuta pacotes com base no rótulo, existe três tipos de LSR: de Borda de Entrada, de Trânsito e de Borda de Saída;
- ✓ *Label Edge Router* (LER): roteador de rótulo de borda;
- ✓ *Forwarding Equivalence Class* (FEC): classe de equivalência de encaminhamento;
- ✓ *Label Switched Path* (LSP): Caminho de comutação de rótulos;
- ✓ Pilha de rótulos (*Label Stak*): é um conjunto de rótulos utilizado;
- ✓ *Forwarding Information Base* (FIB): tabela de informação de encaminhamento;
- ✓ *Label Forwarding Information Base* (LFIB): é uma tabela com o indicativo de como e onde encaminhar os pacotes.
- ✓ *Label Information Base* (LIB): tabela de armazenamento de vínculos de rótulos;
- ✓ *Tag Information Base* (TIB): base de informação de tag;
- ✓ *Label Distribution Protocol* (LDP): distribui os vínculos de rótulo entre LSR e seu vizinho;
- ✓ *Tag Distribution Protocol* (TDP): protocolo de distribuição da tag;
- ✓ *Resource Reservation Protocol* (RSVP): protocolo de reserva de recursos, originalmente serviu como protocolo de sinalização para modelo de qualidade de serviço (QoS);
- ✓ *Constrained Routing LDR* (CR-LDP): roteamento restrito.

2.5.2.2 Cabeçalho MPLS

O rótulo é um identificador de 4 Bytes, com significado local no roteador que é usado para identificar um conjunto de pacotes IPs, *Forwarding Equivalent*

Class (FEC), que são enviados de forma idêntica. No geral, uma FEC é equivalente a uma rota. Se os pacotes forem roteados usando apenas o endereço IP do destino, a definição da FEC pode mudar. Na Figura 16 podemos visualizar os campos do cabeçalho MPLS. Em seguida será descrito a função de cada campo.

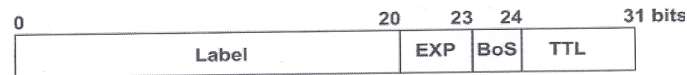


Figura 16: Cabeçalho MPLS

Fonte:(Oliveira, Lins, Mendonça, 2012 p.29).

- ✓ **Label (Rótulo):** contém o valor do rótulo MPLS e possui o tamanho de 20 *Bits*;
- ✓ **Experimental Bits (EXP):** é utilizado para o enfileiramento (*queuing*) e o algoritmo de descarte de pacotes. Este campo possui 3 bits e é usado por classe de serviços (CoS);
- ✓ **Bottom of Stack (BoS):** permite a criação hierárquica de rótulos em uma pilha. Possui o tamanho de 1 *bit*, o valor 1 indica que é a base da pilha de rótulos; se valor for 0, o roteador terá condições de decidir se o próximo encaminhamento será baseado em MPLS ou IP;
- ✓ **Time To Live (TTL):** determina a quantidade de saltos que o pacote MPLS pode executar. Possui 8 *Bits*.

2.5.2.3 Funcionamento

Nas redes MPLS, os pacotes são rotulados assim que entram na rede e são encaminhados apenas com base no conteúdo desses rótulos ao longo do caminho. Com intuito de evitar o intenso processo de pesquisa de dados do roteamento convencional, as decisões de encaminhamento são tomadas com base nestes rótulos (Oliveira; Lins; Mendonça, 2012).

A Figura 17 demonstra as quatro etapas que compõem a operação MPLS:

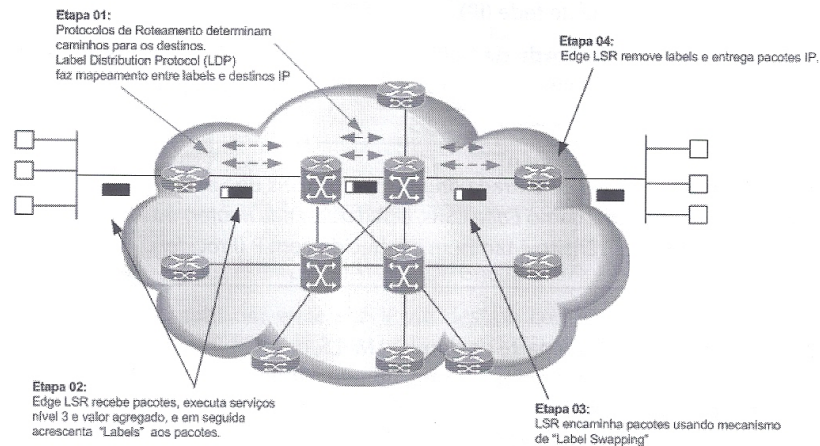


Figura 17: Operação MPLS

Fonte: (Oliveira,Lins, Mendonça, 2012 p.38)

- ✓ Construção das tabelas de roteamento: servem para determinar os melhores caminhos para atingir as redes de destino com a utilização das tabelas desenvolvidas pelos protocolos de roteamento;
- ✓ ingresso dos pacotes na rede: após o recebimento dos pacotes que irão entrar na rede o roteador de borda executa o serviços de nível 3, adiciona valor como QoS e o rótulo ao pacote;
- ✓ encaminhamento do pacote na rede: o pacote é encaminhado utilizando o mecanismo de troca de rótulos (*Label Swapping*). Após receber e ler o rótulo o LSR encaminha depois de realizar a alteração de acordo com a tabela LFIB;
- ✓ saída de pacote na rede: a entrega é realizada pelo pacote IP após a remoção do rótulo pelo LSR de saída.

A figura 18 mostra a inserção de rótulos aos pacotes IPs que são anunciadas para os roteadores vizinhos pelo protocolo LDP.

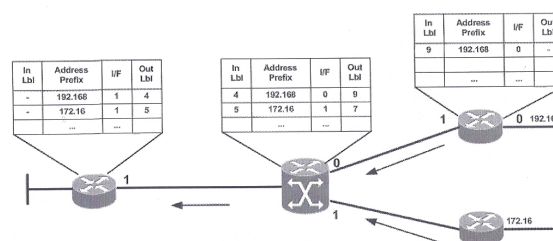


Figura 18: Inserção dos rótulos aos pacotes IPs

Fonte: (Oliveira,Lins, Mendonça, 2012 p.40).

2.5.2.4 Qualidade de Serviços (QoS)

A Internet trabalha com o protocolo IP, onde toda transmissão de dados e fluxos são compartilhados pela largura da banda que opera com melhor esforço (*best effort*). Os pacotes que trafegam na Internet são tratados da mesma forma sem distinção ou prioridades.

O QoS surgiu da necessidade de criar mecanismos para gerenciar o tráfego da largura de banda, atraso e congestionamento em toda a rede, sendo possível desenvolver critérios, prioridades e a distinção entre as classes. Para (Oliveira, Lins e Mendonça, 2012); QoS em redes IPs são mecanismos que permitem o controle e a manipulação dos parâmetros de banda, atraso (*delay*), variação de atraso (*jitter*) e perda de pacotes, sendo uma arquitetura fim a fim. Duas arquiteturas são utilizadas para a aplicação de QoS nas redes:

- ✓ Serviços integrados (*Integrated Services – IntServ*): têm como base quatro componentes: escalonador de pacotes, controle de admissão, classificador de pacotes e policiamento. No modelo IntServ são propostas duas classes de serviços: serviço garantido (*guaranteed service*) e serviço de carga controlada (*controlled load service*). A reserva de recursos é que garante a qualidade de serviços. É tipicamente utilizado para garantir que um fluxo, em especial, receba o nível de QoS apropriado ao longo da rede inteira, antes de enviar esse tráfego. (Oliveira; Lins; Mendonça, 2012).
- ✓ Serviços diferenciados (*Differentiated Services – DiffServ*): possibilita definir as prioridades dos pacotes de forma diferenciada com o auxílio de dois componentes: condicionamento de tráfego e comportamentos por salto;

Na figura 19 é possível visualizar os componentes da arquitetura IntServ .

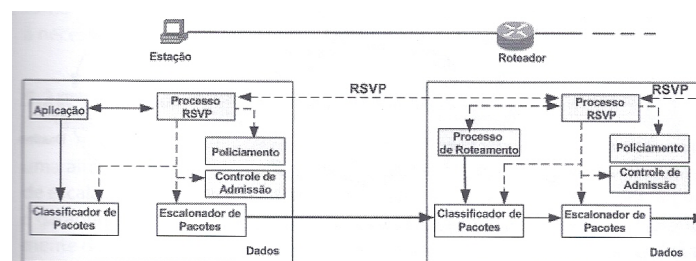


Figura 19: Componentes da arquitetura IntServ

Fonte: (Oliveira, Lins, Mendonça, 2012 pg 65).

- ✓ Escalonador de pacotes: usa uma política de atendimento para gerenciar o

buffer das filas de saída;

- ✓ Controle de admissão: cada nova solicitação de QoS implementa o algoritmo para verificar se a solicitação pode ser atendida sem interferir nos outros fluxos;
- ✓ Classificador de pacotes: identifica e mapeia os fluxos em suas categorias distintas e, se estiverem de acordo com as normas do policiamento, são colocadas nos *buffers* da fila de saída apropriada;

Policiamento: verifica se o fluxo esta de acordo com as normas especificadas. Fluxos fora do acordo têm seus pacotes descartados para evitar congestionamento (Oliveira; Lins e Mendonça,2012).

A figura 20 apresenta a arquitetura de serviços DiffServ.

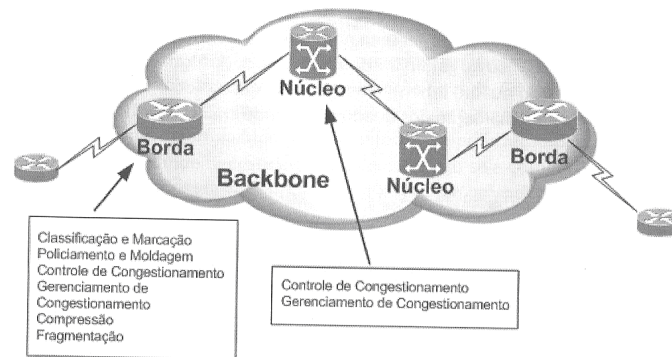


Figura 20: Arquitetura de serviços DiffServ

Fonte: (Oliveira, Lins, Mendonça, 2012 p.71).

Os roteadores de núcleo são responsáveis por verificar o DSCP marcado em seus cabeçalhos, classificar e encaminhar se estiverem de acordo.

2.5.2.5 Engenharia de Tráfego (TE)

A engenharia de tráfego explora os mecanismos de funcionamento, define os rótulos e o comportamento dos roteadores ao receber os rótulos; sendo possível criar mecanismos para atender questões críticas dos serviços com o objetivo de propiciar a eficiência, confiabilidade nas operações e otimizar a utilização de recursos e desempenho na transmissão dos dados. É possível garantir que diversos caminhos possam ser utilizados para o envio do tráfego sem

sobrecarregar um determinado caminho, deixando o outro subutilizado (Oliveira; Lins e Mendonça, 2012). É possível visualizar, na figura 21, o balanceamento de carga MPLS-TE.

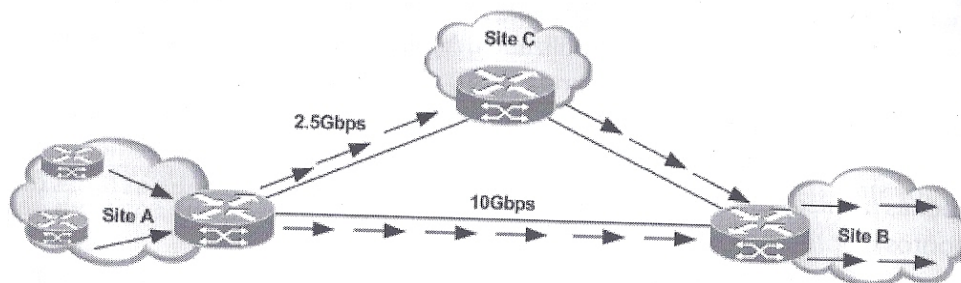


Figura 21: Balanceamento de carga MPLS-TE

Fonte: (Oliveira,Lins, Mendonça, 2012 pg 88).

A engenharia de tráfego possibilita criar túneis, para permitir o balanceamento de carga entre caminhos alternativos com diferentes taxas de transmissão, após análise do tráfego.

2.5.2.6 Ferramentas

Para a elaboração deste trabalho foi utilizado o simulador gráfico de redes GNS3 que permite projetar topologias de redes, com a emulação de equipamentos ativos de uma rede. Com o GNS3 é possível executar simulações ou configurar dispositivos, emular o *Internetworking Operating System* (IOS) de um *Router* real e realizar as respectivas configurações. Para a simulação da tecnologia, foram utilizados roteadores Cisco da série 3700, com o IOS c3725-advipservicesk9-mz.124-18.

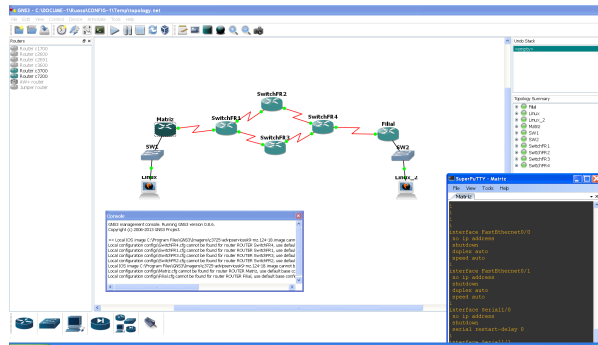


Figura 22: GNS3

Fonte: Autoria própria.

Para analisar os protocolos e capturar de forma interativa o tráfego da rede, foi utilizado o Wireshark, pois através dele é possível capturar o tráfego em tempo de execução e apresentar as informações em um formato legível.

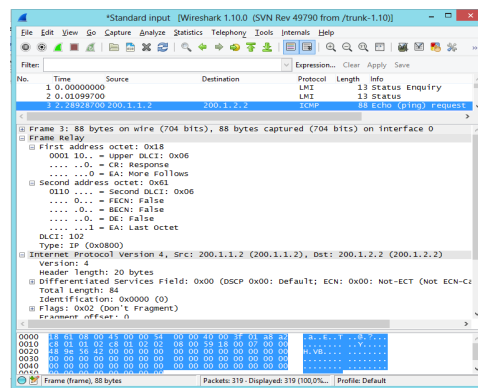


Figura 23: Wireshark

Fonte: Autoria própria

3 IMPLEMENTAÇÃO

Neste capítulo serão mostrados os testes de simulação das infraestruturas de redes, utilizando as tecnologias Frame Relay e MPLS. Para a simulação da tecnologia, foi utilizado o software GNS3 com roteadores Cisco, da série 3700, com o *Internetworking Operating System (IOS)*. O GNS3 é um simulador gráfico de redes que permite a emulação de redes complexas. Este programa cria um ambiente virtual no computador, permitindo a realização de testes no laboratório. O *software* também pode ser usado para projetar redes e simular tecnologias de redes.

3.1 CENÁRIO DE IMPLEMENTAÇÃO COM TECNOLOGIA FRAME RELAY

Cenário 1: implementação de uma topologia de rede utilizando a tecnologia Frame Relay.

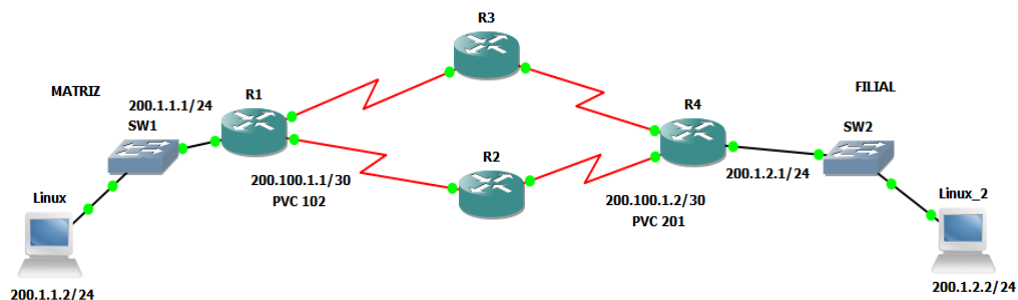


Figura 24: Infraestrutura de rede Utilizando o Frame-Relay

Fonte: autoria própria

A topologia indicada na figura 23 mostra a implementação de uma infraestrutura de rede WAN, utilizando a tecnologia Frame Relay para fazer o encaminhamento dos pacotes por meio de uma rede comutada por pacotes. Na figura, pode-se verificar a interligação da Matriz a uma Filial, utilizando a infraestrutura de uma empresa de Telecomunicações. Nesta implementação foi

configurado um Circuito Virtual Permanente (PVC) nos roteadores R1 ↔ R2 ↔ R4, fazendo com que as informações sigam este caminho. A tecnologia Frame Relay não implementa, nativamente, Qualidade de Serviço (QoS) aos diferentes fluxos de informações (voz, dados, vídeo).

TABELA 1 - CONFIGURAÇÃO DO ROTEADOR DA MATRIZ

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 200.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 1/0
R1(config-if)#ip address 200.200.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#encapsulation frame-relay
R1(config-if)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip address 200.100.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay map ip 200.1.1.2 102 broadcast
R1(config-if)#exit
R1(config)#
R1(config)#router eigrp 100
R1(config-router)#network 200.1.1.0
R1(config-router)#network 200.100.1.0
R1(config-router)#network 200.200.1.0
R1(config-router)#no auto-summary
R1(config-router)#exit
```

FONTE: AUTORIA PRÓPRIA

Na TABELA 1 é possível visualizar a configuração do roteador da Matriz, com a configuração da FastEthernet 0/0, na interface serial 1/0, serial 1/1 com os IPs e máscara de rede atribuídos. O comando de configuração de interface encapsulation frame-relay habilita o encapsulamento frame-relay e possibilita o processamento na interface suportada.

Através do comando frame-relay map ip é possível mapear o vc para R2 e

o broadcast é uma maneira simplificada de encaminhar as atualizações de roteamento para a rede.

Com o comando `router eigrp` é configurado o protocolo de roteamento que será utilizado pela rede, publicando as redes através do comando `network`.

TABELA 2 - CONFIGURAÇÃO DO ROETADOR DA FILIAL

```

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#hostname Filial
Filial(config)#interface fastEthernet 0/0
Filial(config-if)#ip address 200.1.2.1 255.255.255.0
Filial(config-if)#no shutdown
Filial(config-if)#exit
Filial(config)#interface serial 1/3
Filial(config-if)#encapsulation frame-relay
Filial(config-if)#ip address 200.200.1.2 255.255.255.252
Filial(config-if)#no shutdown
Filial(config-if)#exit
Filial(config)#interface serial 1/2
Filial(config-if)#encapsulation frame-relay
Filial(config-if)#ip address 200.100.1.2 255.255.255.252
Filial(config-if)#no shutdown
Filial(config-if)#frame-relay map ip 200.1.1.1 201 broadcast
Filial(config-if)#exit
Filial(config)#router eigrp 100
Filial(config-router)#network 200.1.2.0
Filial(config-router)#network 200.200.1.0
Filial(config-router)#network 200.100.1.0
Filial(config-router)#no auto-summary
Filial(config-router)#exit
Filial(config)#end

```

FONTE: AUTORIA PRÓPRIA

Na TABELA 2 é possível visualizar a configuração de R4, com o comando `hostname filial` é definido que R4 será alterado para filial. A interface FastEthernet 0/0 é configurada através do comando `ip address` com a inserção do endereço Ip e máscara de rede;o comando `no shutdown` é realizado para deixar operacional a

interface.

O comando de configuração de interface encapsulation frame-relay habilita o encapsulamento frame-relay na interface serial 1/3 e interface serial 1/2 .

Através do comando frame-relay map ip é possível mapear o vc para rede 201 e o broadcast é uma maneira simplificada de encaminhar as atualizações de roteamento para a rede.

Com o comando router eigrp é configurado o protocolo de roteamento que será utilizado pela rede.

TABELA 3 - CONFIGURAÇÃO DO SWITCH FRAME RELAY - OPERADORA

```
SwitchFR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchFR(config)#hostname SwitchFR
SwitchFR(config)#frame-relay switching
SwitchFR(config)#interface serial 1/1
SwitchFR(config-if)#encapsulation frame-relay
SwitchFR(config-if)#frame-relay route ?
SwitchFR(config-if)#frame-relay route 102 interface serial 1/2 201
SwitchFR(config-if)#exit
SwitchFR(config)#interface serial 1/2
SwitchFR(config-if)#encapsulation frame-relay
SwitchFR(config-if)#frame-relay intf-type dce
SwitchFR(config-if)#frame-relay route 201 interface serial 1/1 102
SwitchFR(config)#interface serial 1/2
SwitchFR(config-if)#encapsulation frame-relay
SwitchFR(config-if)#frame-relay intf-type dce
SwitchFR(config-if)#frame-relay route 201 interface serial 1/1 102
SwitchFR(config)#
```

FONTE:AUTORIA PRÓPRIA

A TABELA 3 apresenta a configuração do Roteador de Borda da matriz, o comando *hostname* configura o R1 como SwitchFR e a configuração das interfaces. Para configurar a interface como Frame-Relay DCE é utilizado o comando *frame-relay intf-type DCE*. O comando *frame-relay route 201 interface serial 1/1 102*, configura o roteador para encaminhar o tráfego de entrada na interface serial 1/1 com a DLCI de saída 102.

TABELA 4 - CONFIGURAÇÃO DO ROTEADOR DE BORDA MATRIZ

```
R1#show running-config
Building configuration...
Current configuration : 1411 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 200.1.1.1 255.255.255.0
 duplex auto
 speed auto
```

FONTE:AUTORIA PRÓPRIA

A TABELA 4 exibe a configuração do roteador de borda da Matriz. No comando `version 12.4` é determinada a versão que o sistema será executado. Com o comando `service timestamps debug datetime msec` é possível configurar, data, hora e milésimoS de segundos de serviços de registro no arquivo de log.

Para definir o nome do roteador é executado o comando `Hostname` . O início e o fim da seção de inicialização é configurado pelo comando `boot-start-`

marker e boot-end-marker. O comando `ip address 200.1.1.1 255.255.255.0` é utilizado para configurar o ip na interface FastEthernet.

TABELA 5 - CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ

continua

```
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
encapsulation frame-relay
shutdown
serial restart-delay 0
clock rate 64000
interface Serial1/1
ip address 200.100.1.1 255.255.255.252
encapsulation frame-relay
serial restart-delay 0
clock rate 64000
frame-relay map ip 200.100.1.1 102
frame-relay map ip 200.100.1.2 102 broadcast
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router eigrp 100
network 200.1.1.0
network 200.100.1.0
no auto-summary
!
ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
```

TABELA 5 – CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ

conclusão

```
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
end
```

FONTE:AUTORIA PRÓPRIA

A TABELA 5 apresenta a configuração do roteador de borda da matriz. Na linha com o comando `router eigrp 100` é habilitado o eigrp no roteador e com o comando `network` são especificados as redes conectadas no roteador. Ao configurar `line vty 0 4` será permitido o acesso telnet para até cinco usuários.

TABELA 6 - CONFIGURAÇÃO DO ROTEADOR DA BORDA DA FILIAL

continua

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Filial
!
boot-start-marker
```

TABELA 6 – CONFIGURAÇÃO DO ROTEADOR DA BORDA DA FILIAL

```
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 200.1.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
ip address 200.100.1.2 255.255.255.252
encapsulation frame-relay
serial restart-delay 0
clock rate 64000
frame-relay map ip 200.100.1.1 201 broadcast
frame-relay map ip 200.100.1.2 201
```

TABELA 6 – CONFIGURAÇÃO DO ROTEADOR DA BORDA DA FILIAL**conclusão**

```

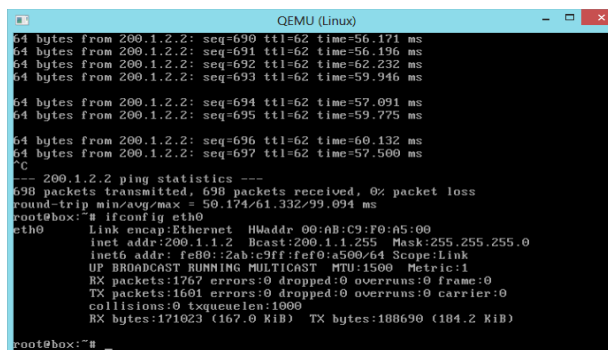
!
interface Serial1/3
no ip address
encapsulation frame-relay
shutdown
serial restart-delay 0
!
router eigrp 100
network 200.1.2.0
network 200.100.1.0
no auto-summary
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
! end

```

FONTE: AUTORIA PRÓPRIA

Pode-se verificar, nas tabelas, as configurações utilizadas nos equipamentos para a implementação da topologia da infraestrutura de redes, utilizando a tecnologia Frame Relay. O roteador R2 foi modificado para trabalhar como um switch Frame Relay. Isto foi possível com a utilização do comando “frame-relay switching”. Com isto, é possível fazer as configurações dos PVCs e a comutação entre Matriz e Filial. Pode-se verificar também, a configuração estática do encaminhamento dos pacotes entre a Matriz e a Filial e a utilização do

protocolo de roteamento dinâmico EIGRP.



```

64 bytes from 200.1.2.2: seq=690 ttl=62 time=56.171 ms
64 bytes from 200.1.2.2: seq=691 ttl=62 time=56.196 ms
64 bytes from 200.1.2.2: seq=692 ttl=62 time=62.232 ms
64 bytes from 200.1.2.2: seq=693 ttl=62 time=59.946 ms

64 bytes from 200.1.2.2: seq=694 ttl=62 time=57.091 ms
64 bytes from 200.1.2.2: seq=695 ttl=62 time=59.775 ms

64 bytes from 200.1.2.2: seq=696 ttl=62 time=60.132 ms
64 bytes from 200.1.2.2: seq=697 ttl=62 time=57.500 ms
^C
--- 200.1.2.2 ping statistics ---
690 packets transmitted, 690 packets received, 0% packet loss
round-trip min/avg/max = 50.174/61.332/99.094 ms
root@box:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0B:C9:F0:A5:00
          inet addr:200.1.1.2  Bcast:200.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::2ab:c9ff:fe0:a500/64  Scope:link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1767 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1601 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:171023 (167.0 KiB)  TX bytes:188690 (184.2 KiB)

root@box:~#

```

Figura 25: Teste de conectividade entre Matriz e Filial

Fonte: autoria própria

A figura 25 mostra um teste de conectividade entre a Matriz e a Filial. Pode-se verificar que o resultado do teste foi positivo, visto que a máquina de destino está pingando (ICMP).

A Figura 26 apresenta a análise de pacote realizado com o *software Wireshark*.

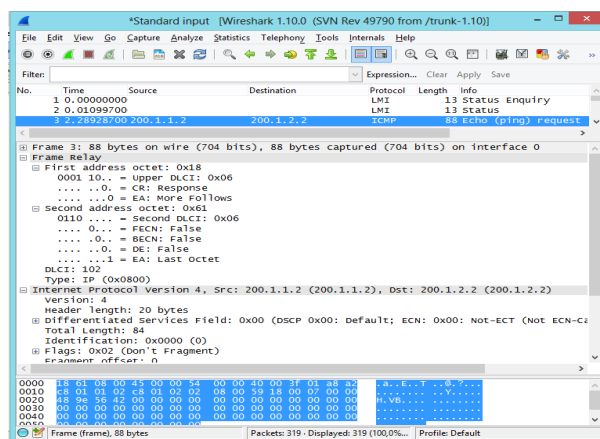


Figura 26: Análise de pacotes Wireshark

Fonte: autoria própria

Pode-se verificar os parâmetros utilizados para a implementação da topologia, utilizando o Frame Relay (DLCI, FECN, BECN, DE, EA).

Na Figura 27 é possível verificar a configuração Frame-Relay entre roteador de Borda e Filial.

```

R2
SwitchFR#show frame-relay pvc 102

PVC Statistics for interface Serial1/1 (Frame Relay DCE)

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial1/1

input pkts 2129      output pkts 2246      in bytes 186344
out bytes 191756    dropped pkts 0        in pkts dropped 0
out pkts dropped 0  out bytes dropped 0
in FECN pkts 0     in BECN pkts 0       out FECN pkts 0
out BECN pkts 0    in DE pkts 0         out DE pkts 0
out boast pkts 0   out boast bytes 0
30 second input rate 0 bits/sec, 1 packets/sec
30 second output rate 0 bits/sec, 1 packets/sec
switched pkts 2128
Detailed packet drop counters:
no out intf 0      out intf down 0      no out PVC 0
in PVC down 0     out PVC down 0       pkt too big 0
shaping Q full 0  pkt above DE 0      policing drop 0
pvc create time 00:48:25, last time pvc status changed 00:38:36
SwitchFR#

```

Figura 27: Configuração PVC Frame-relay

Fonte: autoria própria

A figura 28 demonstra a configuração PVC Frame-Relay do roteador de borda da Matriz.

```

R4
Filial#show frame-relay pvc

PVC Statistics for interface Serial1/2 (Frame Relay DTE)

Local      Active      Inactive      Deleted      Static
Switched   1           0             0            0
Unused     0           0             0            0

DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/2

input pkts 1759      output pkts 1878      in bytes 153976
out bytes 159516    dropped pkts 0        in pkts dropped 0
out pkts dropped 0  out bytes dropped 0
in FECN pkts 0     in BECN pkts 0       out FECN pkts 0
out BECN pkts 0    in DE pkts 0         out DE pkts 0
out boast pkts 37   out boast bytes 2368
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 1 packets/sec
pvc create time 00:37:25, last time pvc status changed 00:31:43

PVC Statistics for interface Serial1/3 (Frame Relay DTE)
Filial# show frame-relay map
Serial1/2 (up): ip 200.100.1.1 dlci 201(0xC9,0x3090), static,
                broadcast,
                CISCO, status defined, active
Serial1/2 (up): ip 200.100.1.2 dlci 201(0xC9,0x3090), static,
                CISCO, status defined, active
Filial#

```

Figura 28: Configuração PVC Frame-Relay

Fonte: autoria própria

Pode-se verificar na figura 28, que o enlace está ativo, indicando que o PVC foi estabelecido com sucesso. A figura mostra, também, a quantidade de tráfego no PVC.

A figura 29 apresenta a configuração PVC Frame- Relay, Switch Frame Relay PVC 102.

```

R1
R1#show frame-relay pvc
PVC Statistics for interface Serial1/0 (Frame Relay DTE)
PVC Statistics for interface Serial1/1 (Frame Relay DTE)
          Active      Inactive      Deleted      Static
Local          1           0             0             0
Switched       0           0             0             0
Unused         0           0             0             0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/1

input pkts 2025      output pkts 1907      in bytes 172404
out bytes 166904    dropped pkts 0        in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0      in BECN pkts 0      out FECN pkts 0
out BECN pkts 0     in DE pkts 0        out DE pkts 0
out bcast pkts 43    out bcast bytes 2752
5 minute input rate 0 bits/sec, 1 packets/sec
5 minute output rate 0 bits/sec, 1 packets/sec
pvc create time 00:44:48, last time pvc status changed 00:34:50
R1#show frame-relay map
Serial1/1 (up): ip 200.100.1.1 dlci 102(0x66,0x1860), static,
                CISCO, status defined, active
Serial1/1 (up): ip 200.100.1.2 dlci 102(0x66,0x1860), static,
                broadcast,
                CISCO, status defined, active
R1#

```

Figura 29: Configuração PVC Frame-Relay, Switch Frame-relay PVC 102

Fonte: autoria própria

A figura 30 apresenta as configurações PVC Frame-Relay, Switch Frame-Relay PVC 201.

```

R2
SwitchFR#show frame-relay pvc 201
PVC Statistics for interface Serial1/2 (Frame Relay DCE)
DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial1/2

input pkts 2296      output pkts 2177      in bytes 196132
out bytes 190592    dropped pkts 0        in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0      in BECN pkts 0      out FECN pkts 0
out BECN pkts 0     in DE pkts 0        out DE pkts 0
out bcast pkts 0     out bcast bytes 0
30 second input rate 0 bits/sec, 1 packets/sec
30 second output rate 0 bits/sec, 1 packets/sec
switched pkts 2296
Detailed packet drop counters:
no out intf 0        out intf down 0      no out PVC 0
in PVC down 0       out PVC down 0      pkt too big 0
shaping Q full 0    pkt above DE 0      policing drop 0
pvc create time 00:49:15, last time pvc status changed 00:39:29
SwitchFR#

```

Figura 30: Configuração PVC Frame-Relay, Switch Frame-Relay PVC 201

Fonte: autoria própria

Na implementação da topologia de rede utilizando a tecnologia Frame Relay, foi criado um circuito virtual permanente (PVC) entre os roteadores da matriz e a filial. Este caminho lógico será utilizado sempre que houver informações sendo transmitidas entre estes dois pontos. O protocolo de roteamento dinâmico EIGRP permite que os roteadores preencham a tabela de roteamento para decidir onde enviar as informações. Nesta implementação não há enlaces redundantes. O roteador R2 foi modificado para trabalhar como um

switch Frame Relay, com o comando Frame-Relay switching no modo de configuração global. Com isto o roteador passa a ter características de um switch Frame Relay, comutando endereços DLCI de camada 2. Neste equipamento, foi necessário fazer as configurações estáticas para o estabelecimento do PVC, dessa forma o encaminhamento das informações. Depois de configurados os equipamentos, foram feitos testes de conexão para a verificação do enlace, conforme as figuras 27, 28, 29, 30. Foi utilizado o *software* Wireshark para a captura de pacotes e análise das informações.

3.2 CENÁRIO COM IMPLEMENTAÇÃO MPLS

Cenário 2: implementação de uma topologia de rede utilizando a tecnologia MPLS

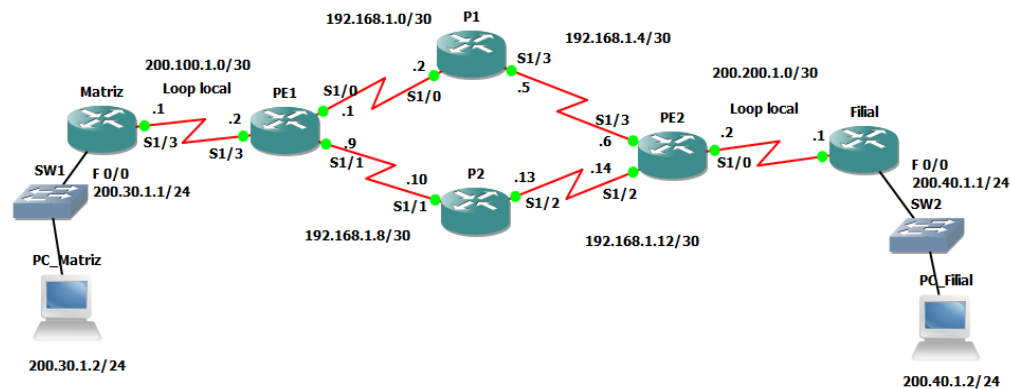


Figura 31: Configuração do cenário implementado com a tecnologia MPLS

Fonte: autoria própria

A topologia, indicada na figura 31, mostra a implementação de uma infraestrutura de rede WAN, com a tecnologia MPLS, fazendo a conexão entre matriz e filial. O roteador PE1 é o roteador de borda, o responsável por inserir o rótulo na entrada e retirar na saída. Pode-se dizer que é o roteador mais importante na arquitetura. O P1 é responsável por analisar e encaminhar os rótulos.

TABELA 7 - CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ

continua

```
Matriz#show running-config
Building configuration...
```


TABELA 7 – CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ

continuação

```
Current configuration : 1374 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Matriz
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
interface Loopback0
ip address 200.1.1.1 255.255.255.0
!
interface FastEthernet0/0
ip address 200.30.1.1 255.255.255.0
duplex auto
speed
auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
```

TABELA 7 – CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ

continuação

```
interface Serial1/0
  no ip address
  shutdown
  serial restart-delay 0
!
interface Serial1/1
  no ip address
  shutdown
  serial restart-delay 0

interface Serial1/2
  no ip address
  shutdown
  serial restart-delay 0
!
interface Serial1/3
  ip address 200.100.1.1 255.255.255.252
  serial restart-delay 0
!
router ospf 1
  log-adjacency-changes
  network 200.1.1.0 0.0.0.255 area 0
  network 200.30.1.0 0.0.0.255 area 0
  network 200.100.1.0 0.0.0.3 area 0
  ip forward-protocol nd
!
no ip http server
no ip http secure-server
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
```

TABELA 7 – CONFIGURAÇÃO DO ROTEADOR DE BORDA DA MATRIZ**conclusão**

login

End

FONTE: AUTORIA PRÓPRIA

Na Tabela 7, é possível visualizar a configuração do roteador de borda da matriz, com a configuração das interfaces. Com o comando `service timestamps debug datetime msec` é possível configurar a data, hora e milésimos de segundos de serviços de registro no arquivo de log. O comando `serial restart delay` é configurado para setar o tempo em milissegundos que o roteador irá aguardar, antes de tentar deixar operacional a interface. O protocolo de roteamento é configurado com o comando `router ospf 1`. O comando `ip CEF` habilita o Cisco Express forwarding, sistema operacional.

TABELA 8 - CONFIGURAÇÃO PE1**continua**

PE1#show running-config

Building configuration...

Current configuration : 1472 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname PE1

!

boot-start-marker

boot-end-marker

!

no aaa new-model

memory-size iomem 5

no ip icmp rate-limit unreachable

ip cef

!

no ip domain lookup

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

!

mpls label protocol ldp

!

TABELA 8 – CONFIGURAÇÃO PE1

continuação

```
ip tcp synwait-time 5
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
description Conexao com P1
ip address 192.168.1.1 255.255.255.252
mpls ip
serial restart-delay 0

interface Serial1/1
ip address 192.168.1.9 255.255.255.252
mpls ip
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
description Conexao com a Matriz
ip address 200.100.1.2 255.255.255.252
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.3 area 0
```

TABELA 8 – CONFIGURAÇÃO PE1**conclusão**

```

network 192.168.1.8 0.0.0.3 area 0
network 200.100.1.0 0.0.0.3 area 0
network 200.100.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

```

FONTE: AUTORIA PRÓPRIA

A tabela 8 exibe as configurações do roteador PE1. O protocolo de roteamento foi habilitado com o comando `router ospf 1`. O comando `line console 0` é configurado para alterar o modo de configuração da linha para console 0, que é a porta de console em switch Cisco. O comando `login` é configurado para obrigar o usuário a digitar a senha. Para habilitar o MPLS, no modo LDP, é configurado o comando `mpls label protocol ldp`. Com o comando `ip tcp synwait-time 5` é definido o período de tempo durante a tentativa de estabelecer uma conexão TCP, antes que espire.

TABELA 9 - CONFIGURAÇÃO DO ROTEADOR P1**continua**

```
P1#show running-config
```

TABELA 10 - CONFIGURAÇÃO DO ROTEADOR P1

continuação

```
Building configuration...
Current configuration : 1378 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
```

TABELA 9 – CONFIGURAÇÃO DO ROTEADOR P1

continuação

```
interface Serial1/0
description Conexao com PE1
ip address 192.168.1.2 255.255.255.252
mpls ip
serial restart-delay 0
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
description Conexao com PE2
ip address 192.168.1.5 255.255.255.252
mpls ip
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.3 area 0
network 192.168.1.4 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
```

TABELA 9 – CONFIGURAÇÃO DO ROTEADOR P1**conclusão**

```

exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end

```

FONTE: AUTORIA PRÓPRIA

Na tabela 9 é possível visualizar as configurações do roteador P1, que é responsável por analisar e encaminhar os rótulos. O comando no ip domain lookup foi utilizado para desativar o DNS. Com o comando router ospf 1 é habilitado o protocolo de roteamento. Para habilitar o MPLS no modo LDP é configurado o comando mpls label protocol ldp. Com o comando ip tcp synwait-time 5 é definido o período de tempo durante a tentativa de estabelecer uma conexão TCP, antes que expire.

TABELA 11 - CONFIGURAÇÃO DO ROTEADOR P2**continua**

```

P2#show running-config
Building configuration...
Current configuration : 1390 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup

```


TABELA 10 – CONFIGURAÇÃO DO ROTEADOR P2**continuação**

```
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
mpls label protocol ldp
ip tcp synwait-time 5
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial1/0
  no ip address
  shutdown
  serial restart-delay 0

interface Serial1/1
  description Conexao com PE1
  ip address 192.168.1.10 255.255.255.252
  mpls ip
  serial restart-delay 0
!
interface Serial1/2
  description Conexao com PE2
  ip address 192.168.1.13 255.255.255.252
  mpls ip
  serial restart-delay 0
!
interface Serial1/3
  no ip address
  shutdown
  mpls ip
  serial restart-delay 0
!
```

TABELA 10 – CONFIGURAÇÃO DO ROTEADOR P2**conclusão**

```
router ospf 1
log-adjacency-changes
network 192.168.1.4 0.0.0.3 area 0
network 192.168.1.12 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end
```

FONTE: AUTORIA PRÓPRIA

Na tabela 10 é possível visualizar as configurações do roteador P2, foi configurado o protocolo de roteamento ospf com o comando router ospf 1.

TABELA 12 - CONFIGURAÇÃO DO ROTEADOR PE2**continua**

```
PE2#show running-config
Building configuration...
Current configuration : 1464 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

TABELA 11- CONFIGURAÇÃO DO ROTEADOR PE2

continuação

```
!  
hostname PE2  
!  
boot-start-marker  
boot-end-marker  
no aaa new-model  
memory-size iomem 5  
no ip icmp rate-limit unreachable  
ip cef  
!  
no ip domain lookup  
ip auth-proxy max-nodata-conns 3  
ip admission max-nodata-conns 3  
!  
mpls label protocol ldp  
!  
ip tcp synwait-time 5  
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial1/0  
description Conexao com a Filial  
ip address 200.200.1.2 255.255.255.252  
serial restart-delay 0  
!  
interface Serial1/1  
no ip address  
shutdown  
serial restart-delay 0
```

TABELA 11- CONFIGURAÇÃO DO ROTEADOR PE2

continuação

```
!  
interface Serial1/2  
  description Conexao com P2  
  ip address 192.168.1.14 255.255.255.252  
  mpls ip  
  serial restart-delay 0  
!  
interface Serial1/3  
  description Conexao com P1  
  ip address 192.168.1.6 255.255.255.252  
  mpls ip  
  serial restart-delay 0  
!  
router ospf 1  
  log-adjacency-changes  
  network 192.168.1.4 0.0.0.3 area 0  
  network 192.168.1.12 0.0.0.3 area 0  
  network 200.200.1.0 0.0.0.3 area 0  
!  
ip forward-protocol nd  
!  
PE2# show ip ospf neighbor  
Current configuration : 1464 bytes  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname PE2  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
memory-size iomem 5  
no ip icmp rate-limit unreachable  
ip cef  
!
```

TABELA 11- CONFIGURAÇÃO DO ROTEADOR PE2

continuação

```
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
description Conexao com a Filial
ip address 200.200.1.2 255.255.255.252
serial restart-delay 0

interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
description Conexao com P2
ip address 192.168.1.14 255.255.255.252
mpls ip
serial restart-delay 0
!
interface Serial1/3
description Conexao com P1
```

TABELA 11 – CONFIGURAÇÃO DO ROTEADOR PE2**conclusão**

```
ip address 192.168.1.6 255.255.255.252
mpls ip
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 192.168.1.4 0.0.0.3 area 0
network 192.168.1.12 0.0.0.3 area 0
network 200.200.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
```

FONTE:AUTORIA PRÓPRIA

A tabela 11 exibe as configurações do roteador PE2, o nome do roteador foi configurado com o comando hostname PE2. Com o comando mpls ip é habilitado o encaminhamento nas interfaces.

TABELA 13 - CONFIGURAÇÃO DA FILIAL**continua**

```
Configuração da Filial
Filial#show running-config
Building configuration...
Current configuration : 1303 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Filial
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
```

TABELA 12 – CONFIGURAÇÃO DA FILIAL

continuação

```
ip address 200.200.1.1 255.255.255.252
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 200.10.1.0 0.0.0.255 area 0
network 200.200.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
```


TABELA 12 – CONFIGURAÇÃO DA FILIAL

continuação

```
line vty 0 4
 login
End
Filial#show running-config
Current configuration : 1352 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Filial
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 200.40.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 200.200.1.1 255.255.255.252
```

TABELA 12 – CONFIGURAÇÃO DA FILIAL**conclusão**

```
serial restart-delay 0
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1
log-adjacency-changes
network 200.10.1.0 0.0.0.255 area 0
network 200.40.1.0 0.0.0.255 area 0
network 200.200.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
no ip http server
no ip http secure-server
!
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
end
```

FONTE: AUTORIA PRÓPRIA

TABELA 14 - LISTA DAS INTERFACES EM PE1

```
PE1#show mpls interfaces
Interface      IP      Tunnel Operational
Serial1/0      Yes (Ldp) No      Yes
Serial1/1      Yes (Ldp) No      Yes
PE1#
```

FONTES: AUTORIA PRÓPRIA

TABELA 15 - LISTA DAS INTERFACES P1

```
P1#show mpls interfaces
Interface      IP      Tunnel Operational
Serial1/0      Yes (Ldp) No      Yes
Serial1/3      Yes (Ldp) No      Yes
```

FONTES: AUTORIA PRÓPRIA

TABELA 16 - LISTA DAS INTERFACES EM PE2

```
P2#show mpls interfaces
Interface      IP      Tunnel Operational
Serial1/1      Yes (Ldp) No      Yes
Serial1/2      Yes (Ldp) No      Yes
Serial1/3      Yes      No      No
```

FONTES: AUTORIA PRÓPRIA

TABELA 17 - LISTAS DE INTERFACES EM PE2

```
PE2#show mpls interfaces

Interface      IP      Tunnel Operational
Serial1/2      Yes (Ldp) No      Yes
Serial1/3      Yes (Ldp) No      Yes
```

FONTES: AUTORIA PRÓPRIA

Pode-se verificar nas tabelas 13, 14, 15,16 que a configuração do protocolo LDP, utilizado pela tecnologia MPLS está funcional.

TABELA 18 - LISTAS DAS TABELAS DE ROTEAMENTO DE PE1

```
PE1#show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	19	200.200.1.0/30	0	Se1/0	point2point
17	18	192.168.1.12/30	0	Se1/0	point2point
18	Pop tag	192.168.1.4/30	0	Se1/0	point2point
19	Untagged	200.30.1.0/24	792	Se1/3	point2point
20	Untagged	200.1.1.1/32	1652	Se1/3	point2point
21	22	200.40.1.0/24	0	Se1/0	point2point

FONTE: AUTORIA PRÓPRIA

TABELA 19 - LISTAS DAS TABELAS DE ROTEAMENTO DE P1

```
P1#show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	200.100.1.0/30	6009	Se1/0	point2point
17	Pop tag	192.168.1.8/30	5454	Se1/0	point2point
18	Pop tag	192.168.1.12/30	520	Se1/3	point2point
19	Pop tag	200.200.1.0/30	3292	Se1/3	point2point
20	20	200.1.1.1/32	1296	Se1/0	point2point
21	19	200.30.1.0/24	828	Se1/0	point2point
22	21	200.40.1.0/24	1104	Se1/3	point2point

FONTE:AUTORIA PRÓPRIA

TABELA 20 - LISTAS DE TABELAS DE ROTEAMENTO DE PE2

continua

```
P2#show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	18	192.168.1.0/30	0	Se1/2	point2point
17	Pop tag	192.168.1.4/30	0	Se1/2	point2point
18	16	200.100.1.0/30	0	Se1/2	point2point
19	Pop tag	200.200.1.0/30	0	Se1/2	point2point
20	20	200.1.1.1/32	0	Se1/2	point2point
21	19	200.30.1.0/24	0	Se1/2	point2point
22	21	200.40.1.0/24	0	Se1/2	point2point

FONTE: AUTORIA PRÓPRIA

TABELA 21 - LISTAS DE TABELAS DE ROTEAMENTO DE PE2

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	200.100.1.0/30	4895	Se1/3	point2point
17	17	192.168.1.8/30	0	Se1/3	point2point
18	Pop tag	192.168.1.0/30	0	Se1/3	point2point
19	21	200.30.1.0/24	0	Se1/3	point2point
20	20	200.1.1.1/32	0	Se1/3	point2point
21	Untagged	200.40.1.0/24	1056	Se1/0	point2point

FONTE: AUTORIA PRÓPRIA

As tabelas 17, 18, 19, 20 exibem as tabelas de encaminhamento dos rótulos MPLS. O comando Untagged indica que o rótulo será removido e encaminhado para o próximo salto.

TABELA 22 - ROTEAMENTO ENTRE MATRIZ E FILIAL

Tracing the route to 200.40.1.2

1	200.100.1.2	40 msec	40 msec	20 msec
2	192.168.1.2 [MPLS: Label 22 Exp 0]	72 msec	68 msec	72 msec
3	192.168.1.6 [MPLS: Label 21 Exp 0]	60 msec	60 msec	60 msec
4	200.200.1.1	72 msec	68 msec	72 msec
5	200.40.1.2	100 msec	96 msec	88 msec

FONTE: AUTORIA PRÓPRIA

TABELA 23 - ROTEAMENTO ENTRE MATRIZ E FILIAL

Tracing the route to 200.30.1.2

1	200.200.1.2	28 msec	44 msec	16 msec
2	192.168.1.5 [MPLS: Label 21 Exp 0]	80 msec	68 msec	84 msec
3	192.168.1.1 [MPLS: Label 19 Exp 0]	68 msec	56 msec	68 msec
4	200.100.1.1	92 msec	80 msec	80 msec
5	200.30.1.2	132 msec	88 msec	96 msec

FONTE: AUTORIA PRÓPRIA

Nas tabelas 21, 22 foram realizados testes de traceroute entre os dois pontos (Matriz e Filial). O teste deu resultado positivo, indicando quais os nós intermediários passam as informações.

4. CONSIDERAÇÕES FINAIS

As arquiteturas abordadas nesta monografia, apresentam características específicas que as diferem umas das outras, com relação à aplicabilidade, evolução e eficiência dessas tecnologias de rede. A tecnologia Frame Relay utiliza conexões lógicas sobre um único circuito físico, trabalha com orientação a conexão, porém, não garante a entrega dos pacotes, podendo descartar parte dos pacotes ou fluxos por ocorrências ou congestionamento. Foi utilizado por muitos anos como o principal serviço oferecido pelas redes de telecomunicações, mas apesar de atender a algumas necessidades dos usuários corporativos, esta tecnologia não atende as demandas atuais de redes convergentes, onde dados, voz e vídeo utilizam a mesma infraestrutura de redes para enviar estas informações.

A tecnologia MPLS surgiu como resposta à demanda por melhor desempenho das redes IPs. A necessidade de suprir as deficiências no que se refere à Engenharia de Tráfego (TE) e Qualidade de Serviços (QoS), e, tem sido implementada gradativamente em substituição da tecnologia Frame Relay.

Uma das grandes vantagens do MPLS é que pode ser implementado em cima das várias tecnologias existentes, como por exemplo, o Frame Relay. Isto faz com que as operadoras de telecomunicações não tenham que instalar uma infraestrutura nova, podendo utilizar os mesmos equipamentos já existentes, precisando, para isto, modificar o sistema operacional dos equipamentos para serem adaptados a nova estrutura da rede (MPLS).

Na implementação realizada nos testes, foi utilizado o mesmo modelo de roteador que poderia ser utilizado para a implementação das duas tecnologias abordadas no trabalho, modificando somente as configurações aplicadas em cada implementação.

A tendência é que as empresas de telecomunicações migrem as suas redes WANs para a tecnologia MPLS, visto que ela oferece maiores vantagens em relação ao Frame Relay. Em relação a custos, o núcleo de equipamentos utilizados no MPLS permite equipamentos menos robustos, devido ao maior trabalho que é realizado pela borda da rede.

O emulador de redes GNS3 foi essencial para o desenvolvimento das

implementações, visto que possibilitou as simulações e testes nas duas tecnologias aplicadas.

Trabalhos futuros podem explorar um detalhamento mais acentuado dessas tecnologias, bem como abordar outras arquiteturas de redes e, dessa forma, promover uma comparação, tendo como base esse trabalho. Uma das possíveis implementações futuras é a aplicação do MPLS utilizando Qualidade de Serviço (QoS) e Engenharia de Tráfego (TE), mostrando as vantagens desta tecnologia em relação ao Frame Relay.

REFERÊNCIAS

Biblioteca Digital da Unicamp. **Políticas e Mecanismos de Engenharia de Tráfego para redes MPLS/DS**. Disponível em:

<http://www.bibliotecadigital.unicamp.br/document/?code=vtls000431274&fd=y>.

Acessado em: 11 Nov 2013

BINKER, Matthew, H. **Projeto de Interconexão de redes**: Cisco Internetwork Design – CID. 1º Ed. São Paulo: Editora Pearson Education, 2003.

COMER, Douglas, E. **Interligação de Redes com TCP/IP: Princípios, protocolos e arquitetura**. 5º Ed. Rio de Janeiro: Editora Campos, 2006.

COMER, Douglas, E. **Redes de Computadores e Internet**. 4º Ed. Porto Alegre: Artmed Editora S.A., 2007

Comissão de Normalização de Trabalhos Acadêmicos. **Normas para Elaboração de Trabalhos Acadêmicos**. 1ª Ed. Curitiba: UTFPR, 2008.

Clube do Hardware. Como o protocolo TCP/IP funciona. Disponível em:

<http://www.clubedohardware.com.br/artigos/Como-o-Protocolo-TCP-IP-Funciona-Parte-1/1351/3>. Acessado em: 10 Out. 2013

Disciplina de redes de computadores II – Prof. M.Sc. Alessandro Kraeme UTFPR
Acessado em 01-12-13 : <http://kraemer.pro.br/outros/2010-2/redes2/framerelay.pdf>

FARREL, Adrian. **Internet e Seus Protocolos**. 1º Ed. Rio de Janeiro: Editora Campus, 2005.

FOROUZAN, Behrouz, E. **Comunicação de Dados e Redes de Computadores**, 4º Ed. Porto Alegre: Editora AMGH, 2010

KUROSE, F, James; ROSS, W, Keith. **Redes de Computadores e Internet: Uma Abordagem Top Down**. 5º Ed. São Paulo: Editora Pearson, 2010.

OSBORNE, Eric; Simba Ajay. **Engenharia de Tráfego com MPLS**. 1º Ed. Rio de Janeiro: Editora Campus, 2003.

Protocolos para Redes de pacote- Professor Luiz Augusto Pelisson – CEFET-PR
Acessado em 29-11-13 <http://www.dainf.ct.utfpr.edu.br/~pelisson/redes/x25.htm>

Slideshare.Net. **Redes Avançadas**. Disponível em:

<http://pt.slideshare.net/maurotapajios/redes-avançadas-5mpls>. Acessado em: 06 Jan 2014

SOARES, L,F,G; Lemos, G; Colcher, Sérgio. **Redes de Computadores das LANs, MANs e WANs às Redes ATM**. 13º Ed. Rio de Janeiro: Editora Campus, 1995

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados: Teoria e**

Aplicações Corporativas. 5ª Ed. Rio de Janeiro: Elsevier, Editora Campus, 2005.

TANEBAUM, Andrew S. **Redes de Computadores.** 4º Ed. Rio de Janeiro: Editora Campus, 1997.

TANEBAUM, Andrew S. **Redes de Computadores.** 3º Ed. Rio de Janeiro: Editora Campus, 2003.