UNIVERSIDADE POLITÉCNICA

A POLITÉCNICA

Escola Superior de Gestão, Ciências e Tecnologias

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

DIMENSIONAMENTO DE UMA VPN BASEADA NA TECNOLOGIA MPLS PARA INTERLIGAR A SEDE DA UNIVERSIDADE A POLITÉCNICA EM MAPUTO E SUA DELEGAÇÃO NA CIDADE DE QUELIMANE

CASO DE ESTUDO: UNIVERSIDADE A POLITÉCNICA

ANDERSON JOSÉ COSSA

MAPUTO

2019

UNIVERSIDADE POLITÉCNICA

A POLITÉCNICA

Escola Superior de Gestão, Ciências e Tecnologias

LICENCIATURA EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

DIMENSIONAMENTO DE UMA VPN BASEADA NA TECNOLOGIA MPLS PARA INTERLIGAR A SEDE DA UNIVERSIDADE A POLITÉCNICA EM MAPUTO E SUA DELEGAÇÃO NA CIDADE DE QUELIMANE

CASO DE ESTUDO: UNIVERSIDADE A POLITÉCNICA

ANDERSON JOSÉ COSSA

SUPERVISOR: Engº. Faustino Pioris

Monografia apresentada a Escola Superior de Gestão e Tecnologias – Universidade Politécnica, como parte dos requisitos para obtenção do grau de licenciatura em Engenharia Informática e de Telecomunicações.

MAPUTO

2019

PARECER DO SUPERVISOR

TEMA: DIMENSIONAMENTO DE UMA REDE VPN BASEADA NA TECNOLOGIA MPLS PARA INTERLIGAR A SEDE DA UNIVERSIDADE A POLITÉCNICA EM MAPUTO E SUA DELEGAÇÃO NA CIDADE DE QUELIMANE

PARECER DO SUPERVISOR

CANDIDATO: ANDERSON J. COSSA

A evolução tecnológica tem sido um factor determinante no *modus operandi* de pequenas e grandes organizações, tornando deste modo um dos factores chave para o sucesso das mesmas. E é com base nestes conceitos que o candidato Anderson Cossa, aqui apresenta um trabalho de defesa com o tema "**Dimensionamento De Uma Rede VPN Baseada Na Tecnologia MPLS Para Interligar A Sede Da Universidade A Politécnica Em Maputo E Sua Delegação Na Cidade De Quelimane**", que teve como objectivo garantir a interligação entre a sede da Universidade A Politécnica de Maputo e sua delegação na cidade de Quelimane, recorrendo às ferramentas e soluções actualmente existentes.

Outro objectivo não directamente escrito no trabalho, é consolidar os conhecimentos obtidos no curso de *Engenharia Informática e de Telecomunicações* ao longo de todo o processo pedagógico.

De um modo geral, o candidato mostrou vontade, dedicação e acima de tudo empenho no estudo da matéria, na pesquisa de informação, na implementação da solução proposta por forma a garantir a interligação com a delegação de Quelimane, na investigação de ferramentas de suporte nunca antes aprendidas durante o processo de aprendizado, o que obviamente criou algumas dificuldades e na consolidação de conhecimentos que tinha da matéria abordada na investigação.

Dado que o objectivo primordial da investigação em teses de licenciatura é a consolidação dos conhecimentos obtidos durante a formação regular e desenvolvimento da capacidade de pesquisa, o candidato mostrou seu cometimento, apreciando-se também o esforço que teve que empreender no estudo sem supervisão directa, apresentando sempre progressos que ia tendo durante a fase de investigação.

O candidato usou como caso de estudo uma situação prática vivida no dia-a-dia na Universidade A Politécnica, tendo apresentado uma solução teórico-prática que pode ser muito aproveitada para implementar nesta instituição ou em qualquer delegação que precise de serviços similares.

O trabalho se resumiu num grande esforço desencadeado pelo candidato por forma a garantir interligação com a delegação de Quelimane, resolvendo deste modo o problema interligação detectado nesta delegação da Universidade Á Politécnica

A estrutura do trabalho apresenta-se numa estética boa o que facilita a sua leitura.

Alguns conselhos ficam para o candidato:

- Em situações futuras de trabalhos do género deve envolver um linguista desde o início por forma a ajudar a harmonizar a linguagem do documento final e reduzir erros ortográficos que de forma geral não influenciam na percepção do trabalho mas poderiam retirar algum brilho do mesmo.
- Deve reservar algum tempo no fim para uma revisão geral do trabalho com objectivo de detectar inconsistências causadas por rotina de leitura do trabalho.

Contudo, pelo conteúdo científico apresentado aceita-se que o trabalho proposto seja avaliado como trabalho de fim de curso, dado que o candidato mostrou:

- Bom conhecimento e domínio do tema em estudo;
- Boa articulação, compreensão e aplicação da teoria para a prática;
- Conclusão satisfatória.

Maputo, 07 de Fevereiro de 2019

O Supervisor do Trabalho

Eng.º Faustino D. Pioris

DECLARAÇÃO DE HONRA

Eu, Anderson José Cossa declaro por minha honra que o presente Projecto Final do Curso é exclusivamente de minha autoria, não constituindo cópia de nenhum trabalho realizado anteriormente e as fontes usadas para a realização do trabalho encontram-se referidas na bibliografia.

Maputo, Fevereiro de 2019

Assinatura:_____

(Anderson José Cossa)

DEDICATÓRIA

Dedico a Ti meu Deus para que os homens se lembrem: "*Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível*".

Dedico este trabalho aos meus pais Maria Júlia Fernando e José Armindo Cossa, irmã Evelyn da Glória José Cossa, aos meus amigos e companheiros em especial ao Engº. Inocêncio Zunguze pela força, apoio, carinho e esperança durante o meu período estudantil. Não deixo passar a minha dedicatória ao meu tutor Engenheiro Faustino Pioris, pelo incentivo e pela atenção disponibilizada e que desde o início do curso foi uma imagem profissional.

AGRADECIMENTOS

Agradeço a Deus por olhar por mim e me ter dado forças para não desistir da minha formação, agradeço a minha família em especial a minha mãe Maria Júlia Fernando e pai José Armindo Cossa, aos meus primos Dennys Bento, Aiken Vicente, Gerson Fernando, Rivaldo Ngoca, Fernando Ngoca e a minha companheira, tomo a vocês amigos Dércio Mafunhana, José Kandhea, João Jorge, Vasco Filipe, Hélio Pequenino, Horácio Aires, Inocêncio Zunguze e Ivan Bana pelo apoio incondicional.

Ontem fui uma criança, um adolescente e hoje um jovem, pode até parecer uma história para emocionar, mas grandes lutas se levantaram e eu estou com aquele que me fortalece:

> "*Não temas porque eu sou contigo, não te assombres, porque eu sou o teu Deus; eu te esforço (fortaleço) e te ajudo, e te sustento com a destra da minha justiça"*. (Isaías 41:10).

Agradeço de forma especial ao meu supervisor Engº Faustino Pioris que de forma incondicional ajudou-me a desenvolver este projecto e sempre me acolhendo e recebendo, o meu muito obrigado, a Universidade A Politécnica e aos seus colaboradores por me ter formado um Homem e não um menino.

RESUMO

O presente trabalho consiste em estudar e analisar as redes VPN's (*Virtual Networks*) baseadas na tecnologia MPLS (*Multiprotocol Label Switching*), de modo a elaborar um projecto de redes que consiste em dimensionar um enlace[1] que permita e facilite a comunicação entre a sede da universidade A Politécnica e a sua delegação na cidade de Quelimane. O estudo também pode servir como referência para outras empresas de grande e médio porte que queiram economizar, ganhar agilidade e disponibilidade nas suas redes a menor custo e uma boa QoS (Qualidade de Serviço). Assim sendo, esta tecnologia mostra-se como uma solução atractiva para soluções de VPN's com alto nível de escalabilidade. Para a realização do presente trabalho, foi usada a metodologia descritiva, pois foram feitas entrevistas aos funcionários da Universidade A Politécnica para a colecta de informação essencial para o alcance dos objectivos previstos. Também foi realizada uma análise bibliográfica sobre a tecnologia MPLS, com vista a adquirir melhores conhecimentos teóricos sobre a mesma. O desempenho desta rede foi comprovado mediante uma simulação utilizando o *software* GNS3, que consistiu na configuração da VPN sobre a rede MPLS. Foram realizados testes de conectividade entre os pontos Maputo e Quelimane para verificar se havia comunicação entre ambos, e com os resultados dos testes foi possível comprovar a credibilidade do presente dimensionamento.

Palavras-chave: Rede Virtual Privada, Comutação de Rótulos Multiprotocolo, Tecnologia, Redes.

[1] Enlace se refere à ligação entre dispositivos de comunicação entre dois ou mais locais, possibilitando deste modo a transmissão e recepção de informações.

ABSTRACT

The present work consists of studying and analyzing the virtual networks (VPN's) based on the Multiprotocol Label Switching (MPLS) technology, in the order to elaborate a network project that consists in designing a link that allows and facilitates the communication between the headquarters of the university A Politécnica and its delegation in the city of Quelimane. The study can also serve as reference for other and mid-sized companies that want to save money, gain agility and availability in their networks at lower cost and a good Quality of Service (QoS). As such, this technology proves to be an attractive solution for VPN solutions with a high level of scalability. For the accomplishment of the present work, the descriptive methodology was used, since interviews were made to the employees of the A Politécnica University to collect essential information to reach the objectives. A bibliographic analysis was also carried out on MPLS technology, aiming to acquire better theoretical knowledge about it. The performance of this network was verified through a simulation using the GNS3 software, which consisted of the configuration of the VPN over the MPLS network. Connectivity tests were carried out between Maputo and Quelimane points to verify if there was communication between them, and with the results of the tests it was possible to prove the credibility of the present design.

Keywords: Virtual Private Network, Multi-Protocol Label Switch, Technology, Network.

LISTA DE ACRÓNIMOS

AS	*Sistema Autônomo*
CE	*Costumer Edge*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
FEC	*Forwarding Equivalence Class*
FIB	*Forwarding Information Base*
LIB	*Label Information Base*
LER	*Label Edge Router*
LFIB	*Label Forwarding Information Base*
LDP	*Label Distribution Protocol*
LSR	*Label Switch Router*
LSP	*Label Switch Path*
MPLS	*Multi Protocol Label Switch*
OSI	*Open System Interconection*
PABX	*Private Automatic Branch Exchange*
PE	*Provider Edge*
QoS	*Quality of Service*
RIP	*Routing Information Protocol*
RD	*Route Distinguisher*
RFC	*Request for Comments*
RSVP	*Resource Reservation Protocol*
VPN	*Rede Virtual Privada*
VRF	*Virtual Routing and Forwarding table*
xDSL	*Digital Subscriber Line*

LISTA DE FIGURAS

Figura 1 - VPN intranet 9

Figura 2 – VPN Extranet 10

Figura 3 – VPN Acesso Remoto 10

Figura 4 – Tunelamento 11

Figura 5 – Modelo Overlay 12

Figura 6 – Modelo Ponto-a-Ponto 12

Figura 7 – Cabeçalho MPLS 14

Figura 8 - Associação Pacote-Rotulo-FEC-LSP 15

Figura 9 - Componentes da arquitectura MPLS 16

Figura 10 - Etapas de operação do MPLS 18

Figura 11 – Visão Geral de uma VPN MPLS 20

Figura 12 - Arquitectura VPN MPLS 21

Figura 13 - Arquitectura de uma rede VoIP 23

Figura 14 – Estrutura Orgânica da Universidade A Politécnica de Maputo 30

Figura 15 – Estrutura Orgânica da Universidade A Politécnica de Quelimane 31

Figura 16 – Cisco 1941Series Integrated Services Routers 40

Figura 17 – Diagrama da VPN-MPLS proposta pela Teledata 40

Figura 18 – Arquitectura da Rede VPN-MPLS 42

Figura 19 – Arquitectura da Rede VPN-MPLS 42

Figura 20 – Custo do *Router* Cisco 3725 Series. 74

Figura 21 – Cisco 3700 Series *multiservice-access-router Interfaces* 75

LISTA DE TABELAS

Tabela 1. Especificação das classes de serviço e portas UDP/TCP para aplicações. Fonte: Autor 36

Tabela 2. Codecs de voz que podem ser usados para dimensionarem a largura e banda VoIP.... 37

Tabela 3 – Tabela de Preços para a Proposta de VPN-MPLS. Fonte: (TELEDATA 2018) 41

Tabela 4 - Detalhe da VRF. 55

Tabela 5 – Características do *Router* Cisco 1941. 72

Tabela 6 – Custo do *Router* Cisco 3725 Series..... 74

Índice

PARECER DO SUPERVISOR I
DECLARAÇÃO DE HONRA III
DEDICATÓRIA IV
AGRADECIMENTOS V
RESUMO VI
ABSTRACT VII
LISTA DE ACRÓNIMOS VIII
LISTA DE FIGURAS IX
LISTA DE TABELAS X
CAPÍTULO 1 – INTRODUÇÃO 1
1.1 Objectivos 2
1.1.1 Objectivo Geral 2
1.1.2 Objectivos Específicos 2
1.2 Problema 3
1.3 Perguntas de pesquisa e hipóteses a considerar 4
1.3.1 Formulação das perguntas a investigar 4
1.3.2 Hipóteses H0 e H1 4
1.4 Justificação do tema 5
1.5 Delimitações do trabalho 5
Capitulo II – Marco Teórico-Conceitual da Investigação 6
2.1 Antecedentes que nortearam o surgimento da tecnologia MPLS 6
2.1.1 Frame relay 6
2.1.2 Asynchronous transfer mode 7
2.2 Bases teóricas de investigação 7
2.2.1 Rede virtual privada 7
2.2.2 MPLS 13
2.2.3 VPN-MPLS 20
2.2.4 Voice over IP 22
2.3 Determinação das variáveis de investigação 23
2.3.1 Qualidade de Serviço (QoS) 23

2.3.2 Escalabilidade 26
2.3.3 Segurança 27
CAPÍTULO III – MARCO CONTEXTUAL DA INVESTIGAÇÃO 29
3.1 A Organização 29
3.1.1 Missão 29
3.1.2 Objectivos 29
3.1.3 Valores 29
3.1.4 Organograma da Universidade A Politécnica 30
CAPÍTULO IV – METODOLOGIA DE RESOLUÇÃO DO PROBLEMA E APRESENTAÇÃO DE RESULTADOS 33
4.1 Entrevista 33
4.2 Especificação das aplicações a considerar no dimensionamento 34
4.2.1 Divisão das aplicações em múltiplas classes de serviço 34
4.3 CODEC 36
4.4 Determinação da tecnologia de acesso 38
4.5 Orçamento proposto do projecto 39
4.5.1 Proposta técnica 39
4.5.2 Serviço de dados MPLS 39
4.5.3 Diagrama de rede 40
4.5.4 Proposta comercial da teledata 41
4.6 Simulação da VPN-MPLS 41
4.6.1 Endereçamento IPv4 43
4.6.2 Escopo do projecto de instalação e configuração no ambiente real 44
4.6.3 Simulação no GNS3, escopo de configuração: 44
4.6.4 Configuração da VPN-MPLS 45
4.6.5 Voz sobre IP 61
4.7.6.1 Configuração da infra-estrutura de tráfego de voz 61
CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES 66
REFERÊNCIAS BIBLIOGRÁFICAS 68
BIBLIOGRAFIA 70
ANEXOS 71

CAPÍTULO 1 – INTRODUÇÃO

Nos dias de hoje a comunicação é um elemento chave no processo de troca de informação bem como na partilha de recursos de rede e por meio desta rede e com o suporte de tecnologias apropriadas, garante-se a escalabilidade, fidelidade, segurança e a QoS (*Quality of Service*).

Das tecnologias existentes que garantem a comunicação entres dois ou mais lugares, a MPLS vem se mostrando como uma alternativa de suporte à VPN (*Virtual Private Network*), pois constitui uma das formas de reduzir o tempo e garantir a fidelidade de informação, para além de ser uma tecnologia de encaminhamento por pacotes baseada em rótulos, desenvolvida com o objectivo de acelerar o transporte de pacotes em *routers*.

Para o desenvolvimento do tema proposto será elaborada uma análise sobre os aspectos relacionados com a actual infra-estrutura de rede da Universidade A Politécnica de Maputo e de Quelimane. Deste modo será feita a virtualização da infra-estrutura de rede actual, onde será também abordado o conjunto de equipamentos activos e passivos de rede.

A grande motivação para o desenvolvimento e implementação das tecnologias VPN baseada nas tecnologias MPLS provém do facto de estas tecnologias fornecerem Qualidade de serviços, maior escalabilidade em termos de gestão e operações sendo deste modo uma rede completamente conectada e possibilita que o cliente possa criar uma rede privada sem nenhuma criptografia.

Espera-se que ao adoptar esta tecnologia, a Universidade A Politécnica possa reduzir os custos com a utilização de VPN baseada no protocolo IP com ganhos na garantia de escalabilidade, flexibilidade, segurança de informação e qualidade de Serviços.

1.1 Objectivos

1.1.1 Objectivo Geral

Dimensionar uma rede VPN baseada na tecnologia MPLS por forma a prover a comunicação entre a sede da Universidade A Politécnica em Maputo a sua delegação em Quelimane.

1.1.2 Objectivos Específicos

- Determinar os fundamentos teóricos da tecnologia MPLS como solução para VPN;
- Descrever a situação actual da rede da Universidade A Politécnica em Maputo e da delegação na cidade de Quelimane;
- Estimar o orçamento para a implementação da rede VPN-MPLS;
- Simular o enlace proposto para testar a conectividade entre a sede e a delegação.

1.2 Problema

A evolução das redes e tecnologias de comunicação vem crescendo gradualmente nos últimos tempos, faz com que, as corporações, pequenas, médias e grandes empresas necessitem cada vez mais de soluções de comunicações modernas nas suas redes que garantam comunicações ágeis, seguras e com boa disponibilidade de serviço. Actualmente existe uma grande diversidade de soluções de redes para garantir o tráfego de informação; Estas soluções são dirigidas a resolução de problemas, avaliação de parâmetros e serviços concretos de redes de comunicações. As VPN's baseadas na tecnologia MPLS representam uma dessas soluções de comunicação que proporcionam uma melhoria considerável nas aplicações e serviços utilizados nas redes de comunicação.

A Universidade A Politécnica possui uma rede de computadores em operação neste momento com o objectivo de partilhar os recursos e serviços de rede existentes como: ficheiros, impressoras, partilha de dados e correio electrónico, e outros recursos da rede, neste contexto observa-se que a gestão de recursos de rede é descentralizada ou seja resume-se na falta de:

Uma rede de dados interligada a nível nacionais para permitir a comunicação entre a sede da Universidade A Politécnica de Maputo e à sua delegação na cidade de Quelimane, com capacidade de integrar os recursos de rede bem como integrar as informações existentes ao nível da sede e da delegação.

`

1.3 Perguntas de pesquisa e hipóteses a considerar

1.3.1 Formulação das perguntas a investigar

- Quais são os fundamentos teóricos da rede VPN baseada na tecnologia MPLS?
- Quais as necessidades de dimensionar uma rede VPN baseada na tecnologia MPLS para proverem a comunicação entre a sede da Universidade A Politécnica em Maputo e a sua delegação na Quelimane?
- Que benefícios verificar-se-ão com o dimensionamento de uma rede VPN baseada na tecnologia MPLS para prover a comunicação entre a sede da Universidade A Politécnica em Maputo e a sua delegação em Quelimane?

1.3.2 Hipóteses H0 e H1

H0: Se se dimensionar uma rede VPN baseada na tecnologia MPLS, aproveitando as vantagens de engenharia de tráfego, ou seja, encaminhamento eficiente do tráfego e utilização eficiente da banda não haverá alteração da infra-estrutura interna da Universidade.

H1: Se se dimensionar uma rede VPN baseada na tecnologia MPLS, aproveitando as vantagens de engenharia de tráfego, ou seja, encaminhamento eficiente do tráfego e utilização eficiente da banda, poderá permitir a partilha de informação entre a sede e a delegação com ganhos na garantia de escalabilidade, flexibilidade e segurança.

1.4 Justificação do tema

A crescente evolução da tecnologia e o uso das tecnologias de comunicação, levam com que sejam estudadas melhores formas de tratamento do tráfego e escoamento de informação. Deste modo, esta evolução representa um diferencial no mercado sobre a realidade e representam uma nova promessa para o futuro.

Foi com base nas vantagens e tendências para o futuro das tecnologias que surgiu a motivação para realização deste projecto, utilizando como referência um estudo de caso a Universidade A Politécnica com vista a melhorar a qualidade de serviços e disponibilidade melhorada dos serviços aos utilizadores bem como facilitar o acesso e reduzir os custos da própria infra-estrutura da instituição.

1.5 Delimitações do trabalho

Referenciado anteriormente, as corporações, empresas de médio e grande porte necessitam cada vez mais de soluções de comunicação de dados modernas para suas redes que garantam comunicações ágeis, seguras e com boa disponibilidade de serviço. Desta feita com o presente trabalho, pretende-se prover a comunicação entre a sede da Universidade A Politécnica em Maputo e a sua delegação na cidade de Quelimane de modo a que se garanta que haja confiabilidade, segurança, valor de rede aos seus utilizadores e escalabilidade, aumentando deste modo a disponibilidade, pois em vez de adicionar largura de banda para a gestão do aumento de tráfego, esta utilizará a largura de banda existente de forma mais eficiente, permitindo desta maneira com que os pacotes sejam encaminhados por rotas explícitas e com uma largura de banda específica garantida.

Capitulo II – Marco Teórico-Conceitual da Investigação

Este trabalho tem como objectivo garantir a comunicação entre a sede da Universidade A Politécnica de Maputo e sua delegação na cidade de Quelimane.

Neste capítulo são abordados os fundamentos teóricos gerais, princípios e teorias sobre a tecnologia em causa para que o leitor tenha uma melhor compreensão dos procedimentos seguidos na elaboração deste trabalho.

2.1 Antecedentes que nortearam o surgimento da tecnologia MPLS

No surgimento das redes de dados, o transporte da informação no formato de pacotes utilizava a rede telefónica como meio de transmissão. Porém, limitações causadas pelas inadequações da rede dimensionada para o transporte de voz e não de dados, como baixas taxas de transmissão, motivaram o surgimento de técnicas que aumentassem essa capacidade. Nesse cenário surgiu nas redes de telecomunicações uma variedade de tecnologias de comutação de dados baseadas em quadros[2] (*frames*), células[3] (*cells*) e pacotes[4] (*packets*). (NAKAMURA 2009)

De o acordo com Nakamura (2009), em termos cronológicos, as tecnologias mais importantes foram a *Frame Relay*, a ATM e a tecnologia MPLS, que tinham como objectivo principal o transporte de todos tipos de aplicações numa única plataforma e seguindo padrões internacionais.

2.1.1 Frame relay

De acordo com Mendes (2011), o *Frame Relay* é um serviço de comunicação de dados baseado na tecnologia de comutação de pacotes orientados à conexão, provido por redes de suporte às interfaces de acesso às terminais de usuários. Essa tecnologia assegura serviços com velocidades de acesso de 64kbps à 2Mbps interligando redes dispersas geograficamente que precisam transferir diferentes tipos de dados.

Derivado da tecnologia X.25, o *Frame Relay* é uma tecnologia definida nas camadas 1 (física) e 2 (enlace) do modelo OSI (*Open System Interconection*), da qual possui a característica de menor ocorrência de falhas e maior custo-beneficio. (FILIPPETTI 2002)

[2] Quadros informação que é traduzida e transmitida entre dois ou mais pontos da rede.
[3] Células pacotes relativamente pequenos transferidos na rede.
[4] Pacotes dados transmitidos pela rede.

Com o avanço da tecnologia, surgiu a necessidade de se atingir velocidades mais altas do que se podia atingir com o *Frame Relay*. Como forma de aumentar as capacidades de transmissão, foi desenvolvida a tecnologia ATM (*Asynchronous Transfer Mode*), com capacidades para a transmissão de voz, vídeo e dados, por meio de redes públicas e privadas, à velocidades consideravelmente altas.

2.1.2 Asynchronous transfer mode

Segundo Lewis (1999), a tecnologia ATM foi desenvolvida com o objectivo de se estabelecer um protocolo para transmissões de voz, vídeo e dados a altas velocidades, em redes públicas e privadas, permitindo a interoperabilidade entre equipamentos de diversos fornecedores.

Para Nakamura (2009), quando a tecnologia ATM foi lançada ao mercado, esperava-se que ela dominasse o cenário mundial devido às suas altas taxas de transmissão, consideravelmente maiores que as atingidas pela *Frame Relay* e pela agregação de múltiplos tipos de serviços como voz, vídeo e dados em uma pequena célula de tamanho fixo. Mas, devido ao facto de essa tecnologia não se integrar muito bem com o protocolo de rede mais difundido no mundo (o IP), e ainda possuir grandes problemas de escalabilidade na utilização IP (*Internet Protocol*) sobre ATM, uma tecnologia híbrida começou a surgir como forma de resolver esse problema. Tal tecnologia permitia agregar as características boas do ATM ao IP e criar a tecnologia IP + ATM. As vantagens dessa agregação são a gestão de uma rede única, ao invés da rede ATM e da rede IP, a resolução do problema de escalabilidade com a criação de mecanismos de estabelecimento automático de conexões e agregação de QoS ao IP tradicional. Essa tecnologia híbrida é denominada MPLS.

2.2 Bases teóricas de investigação

Para melhor percepção do objecto de investigação, são apresentados alguns conceitos a destacar:

2.2.1 Rede virtual privada

Antigamente, as instituições que quisessem utilizar uma rede de computadores para troca de informações entre filiais e matriz, distantes entre si, deveriam montar sua própria infra-estrutura particular demandando uma grande quantidade de recursos tanto financeiros quanto humanos para a implantação e manutenção desta rede. A Internet era inviável de ser utilizada por ser de

domínio público e portanto podendo ser monitorada por entidades não desejáveis. Neste contexto surge a proposta das VPNs, visando reduzir sensivelmente os custos por utilizar toda a infra-estrutura da internet, uma rede de alcance global, eliminando a necessidade de linhas dedicadas de longa distância e mantendo a segurança necessária pela instituição. (Marleta 2007)

As VPNs constituem um elemento muito importante na infra-estrutura de comunicações de uma organização. De facto, não só permitem aos utilizadores remotos o acesso à rede interna, como são um meio de estender a rede a locais geograficamente afastados como, filiais ou qualquer outra instalação de dimensão variável. (Boavida *et al.* 2009)

De acordo com Celestino (2005 p:40) VPNs "são tuneis de criptografia entre pontos autorizados, criados através da internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos."

Para Silva (2002),

> "*Virtual Private Network* (VPN), ou Rede Privada Virtual, é uma rede privativa (com acesso restrito) construída sobre a infra-estrutura de uma rede pública, geralmente a Internet. Utiliza as mais avançadas tecnologias de criptografia, assegurando privacidade e integridade das comunicações, substituindo com vantagem os *links* dedicados e de longa distância. Além da redução dos custos com *links*, permite que as empresas criem uma rede totalmente integrada, conectando escritórios, filiais e fábricas, com tráfego de voz, dados e vídeo."

Desta feita, concordando com as definições a cima citadas, pode-se considerar VPN uma rede que possibilita um acesso privado ou particular de comunicação, que faz o uso da infra-estrutura de telecomunicação públicas já existentes como Internet, reservando a privacidade através do uso de protocolos de tunelamento e procedimentos de segurança.

2.2.1.1 Tipos de VPN

Existem vários tipos de implementação de VPN's, onde cada implementação contém especificações próprias bem como características que requerem certa atenção na hora de implementar.

A seguir são apresentados os três tipos principais de VPN's:

a) VPN Intranet

É utilizada para facilitar a comunicação entre departamentos de uma empresa, conforme ilustra a figura 1 a seguir. Um dos requisitos básicos a considerar é a necessidade de uma criptografia rápida para não sobrecarregar a rede (que deve ser rápida). Outro requisito essencial é a confiabilidade a fim de garantir a prioridade de aplicações críticas, como por exemplo, sistemas financeiros e banco e dados. (Miranda 2002)

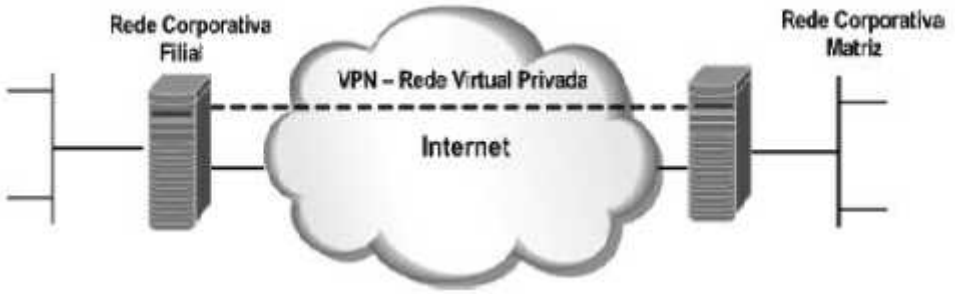

Figura 1 - VPN intranet. Fonte: (Oliveira et al. 2012)

b) VPN Extranet

É implementada para conectar uma empresa aos seus sócios, fornecedores, clientes, e outros conforme ilustrado na figura 2. Para isso é necessário uma solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Outro ponto muito importante a se considerar é o controlo de tráfego, o que minimiza os efeitos dos gargalos[5] existentes em possíveis nós entre as redes, e ainda garante uma resposta rápida e suave para aplicações críticas. (Miranda 2002)

[5] Gargalos limitação de banda em uma rede.

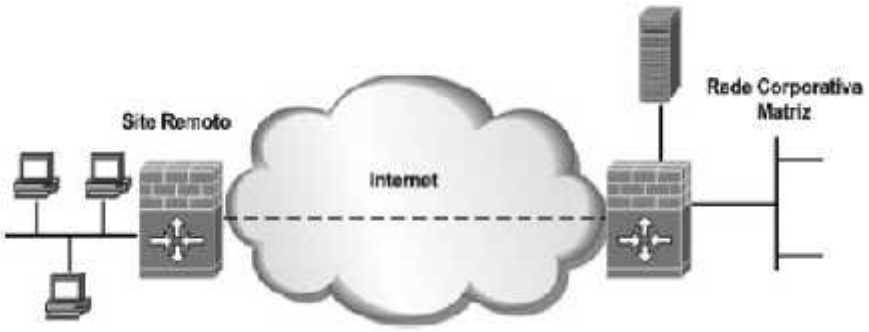

Figura 2 – VPN Extranet. Fonte: (Oliveira et al. 2012)

c) VPN Acesso Remoto

De acordo com Miranda (2002), uma VPN de acesso remoto conecta uma empresa aos seus empregados que estejam distantes fisicamente da rede conforme mostra a figura 3. Neste caso torna-se necessário um *software* cliente de acesso remoto. Quanto aos requisitos básicos, o mais importante é a garantia de QoS (*Quality of Service*), isto porque geralmente quando se conecta remotamente de um computador portátil, você está limitado à velocidade do *modem*. Outro item não menos importante é uma autenticação rápida e eficiente que garanta a identidade do utilizador remoto e por último, um factor importante é a necessidade de uma administração canalizada desta rede, já que ao mesmo tempo, pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticados por exemplo, estejam centralizadas num único lugar.

Figura 3 – VPN Acesso Remoto. Fonte: (Oliveira *et al.* 2012)

Todos os tipos de VPNs citados anteriormente baseiam-se na tecnologia de tunelamento, que pode ser definida como o processo de encapsular um protocolo dentro de outro; porém, antes de capsular, este deverá ser criptografado, de forma que, caso seja interceptado durante o transporte, não possa ser lido. O pacote que é criptografado e encapsulado é enviado pela Internet até ao destino, onde é descapsulado e desencriptografado, para entrega ao destinatário. Portanto, o túnel é a denominação do caminho lógico que é percorrido pelos pacotes ao longo da rede. Após alcançar o destino, o pacote é descapsulado e encaminhado ao seu destino final, conforme ilustrado na figura. (Oliveira *et al.* 2012)

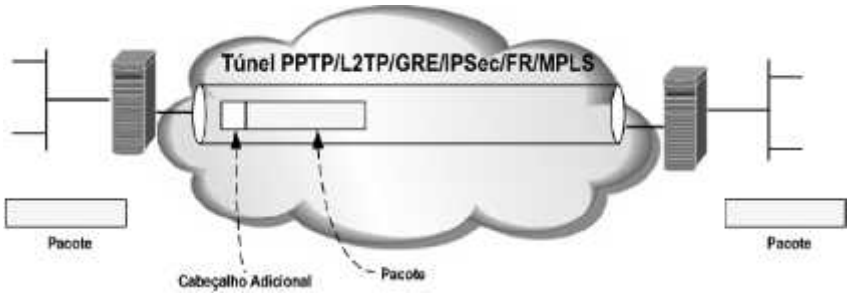

Figura 4 – Tunelamento. Fonte: (Oliveira *et al.* 2012)

2.2.1.2 Modelos VPN

A seguir são apresentados os dois modelos principais de VPN:

a) Modelo Overlay

De acordo com Oliveira *et al.* (2012), no modelo *overlay* para VPN's, toda a lógica funcional das VPNs ocorre nos equipamentos dos utilizadores, limitando a operadora de telecomunicações a fornecer circuitos físicos como, por exemplo, E1,E2 e STM ou circuitos virtuais de redes como *Frame Relay* ou ATM, neste modelo, nenhum processo de roteamento ocorre entre o roteador do cliente e o provedor de serviços; dessa forma o provedor de serviços nunca visualiza as rotas do cliente.

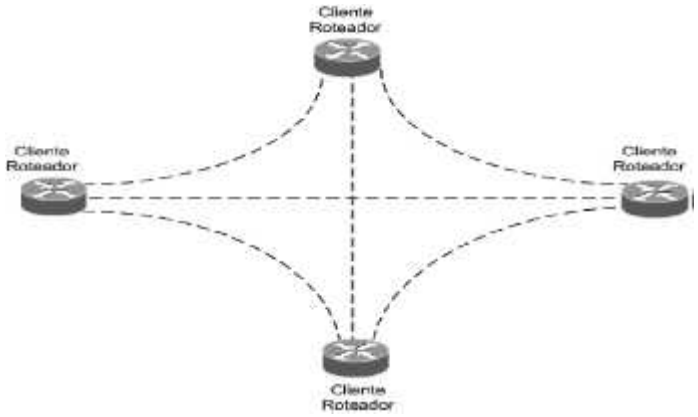

Figura 5 – Modelo Overlay. Fonte: (Oliveira *et al.* 2012)

b) Modelo Ponto-a-Ponto

De acordo com Oliveira *et al.* (2012), no modelo ponto-a-ponto, "as operadoras de telecomunicações participam directamente dos mecanismos funcionais das VPN's, proporcionando o roteamento entre os roteadores dos clientes e da operadora de comunicações".

Figura 6 – Modelo Ponto-a-Ponto. Fonte: (Oliveira *et al.* 2012)

2.2.2 MPLS

MPLS é uma tecnologia de comutação de pacotes que faz o encaminhamento eficiente de fluxos de tráfego na rede. Constitui uma solução para diminuir o processamento nos equipamentos de rede e interligar com maior eficiência redes de tecnologias distintas. (ROSEN *et al.* 2001)

Essa tecnologia, foi apresentada inicialmente como uma solução que permitia melhorar o desempenho das redes IP na função de encaminhamento de pacotes IP, combinando o processo de roteamento de nível 3 com a comutação de nível 2 para realizar o encaminhamento de data gramas através de pequenos rótulos de tamanho fixo. (ROSEN *et al.* 2001)

a) Cabeçalho da Tecnologia MPLS

De acordo com OLIVEIRA *et al.* 2012, "o item mais importante para o MPLS é o rótulo". Os rótulos são pequenos identificadores de tamanho fixo, colocados nos pacotes durante seu tráfego pela rede, sendo facilmente processáveis.

De acordo com Oliveira *et al.* (2012), o cabeçalho MPLS é composto pelo seguinte:

- ***Label* (rótulo):** este campo é considerado como sendo a peça chave da componente de encaminhamento, pois, serve de índice para o próximo endereço de roteamento. Seu tamanho é de 20 *bits*;
- **EXP (*Experimental Bits*):** este campo é composto por 3 *bits* e é utilizado para alterar os algoritmos de enfileiramento e descarte. Dessa forma é possível dar prioridade a determinados pacotes. Este campo é actualmente usado para prover classes de serviços (CoS);
- **BoS (*Bottom of Stack*):** este campo é formado por apenas 1 *bit*, e permite a criação de uma pilha hierárquica de rótulos. Ele indica se o cabeçalho ao qual o pacote pertence é o último da pilha MPLS. Todos os cabeçalhos MPLS devem ter esse *bit* em 0, e através desse campo um *router* de saída tem condições de decidir se o próximo encaminhamento será baseado em MPLS ou IP;
- **TTL (*Time To Live*):** este campo é formado por 8 *bits* e funciona de maneira semelhante ao TTL do protocolo IP. Ele especifica um limite de quantos saltos o pacote pode atravessar. Quando um data grama entra em um *router* de borda MPLS, o valor inicial do TTL no cabeçalho MPLS deve ser igual ao valor do TTL do

cabeçalho IP e decrementado de 1 em cada *router*. Na saída do caminho, o *router* deve copiar o valor do TTL do cabeçalho MPLS para o TTL do cabeçalho IP.

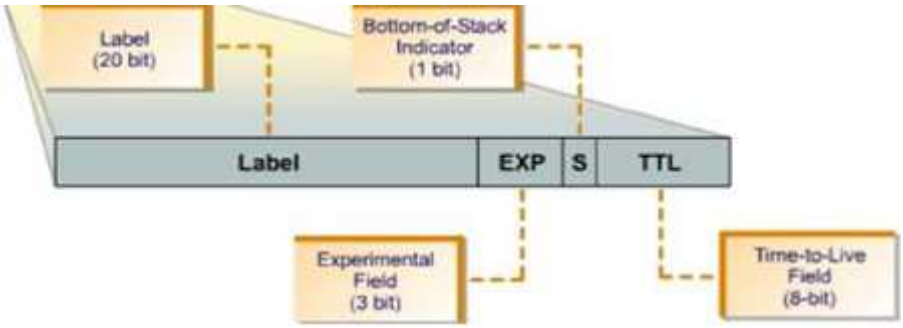

Figura 7 – Cabeçalho MPLS. Fonte: (CABRERA 2015)

b) Componentes da Arquitectura da Tecnologia MPLS

A seguir são descritos os principais termos e componentes de uma arquitectura MPLS, de acordo com (OLIVEIRA *et al.* 2012):

- **LDP (*Label Distribution Protocol*):** o protocolo LDP é o responsável pela distribuição de rótulos para os prefixos IP em uma rede MPLS. Todos os prefixos anunciados pelo mesmo equipamento vizinho recebem o mesmo rótulo. Com isso, os elementos intermediários em uma rede MPLS (chamados P) não precisam conhecer a tabela de roteamento completa da rede.
- **LIB (*Label Information Base*):** é uma tabela que contém os diversos vínculos de rótulos que um LSR recebe sobre o protocolo LDP, ou seja, uma tabela que apresenta informações correlacionando os rótulos às interfaces do *router*. É através desta tabela que o LSR determina para qual interface deverá encaminhar o pacote recebido.
- **FIB (*Forwarding Information Base*):** é uma tabela que controla a decisão de encaminhamento de um *router*. Para todo possível endereço IP de destino, uma pesquisa de prefixo longo é executada pela FIB. Se um endereço é localizado na tabela, o *router* saberá para qual interface de saída deverá enviar o pacote. Se nenhum endereço é localizado, o pacote é descartado.

- **LFIB (*Label Forwarding Information Base*):** é uma tabela que indica onde e como encaminhar os pacotes. É criada por equipamentos pertencentes a um domínio MPLS. A LFIB contém uma lista de entradas que consistem numa subentrada de ingresso e uma ou mais subentradas de ingresso, rótulo de saída, interface de saída, componentes de saída de nível de enlace. É baseada nas informações obtidas pelo LSR através da interacção com os protocolos de roteamento.
- **FEC (*Forwarding Equivalence Class*):** uma FEC consiste em um grupo de pacotes que podem ser tratados de forma equivalente para propósitos de encaminhamento. Pacotes de um mesmo fluxo de dados geralmente pertencem à mesma FEC. A FEC é representada por um rótulo e cada LSP é associado a uma FEC. Quando um LER recebe um pacote, verifica a qual FEC pertence e o encaminha através do LSP correspondente. Portanto, existe uma associação "pacote-rótulo-FEC-LSP" conforme ilustra a figura 8, e esta associação "pacote-FEC" ocorre apenas quando o pacote entra na rede MPLS, proporcionando grande flexibilidade e escalabilidade a este tipo de rede.

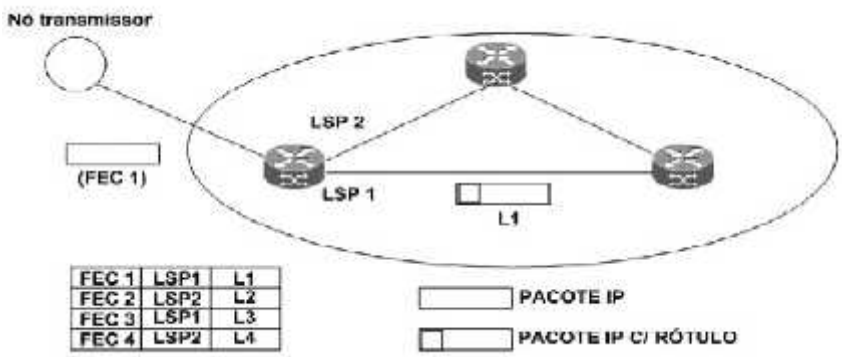

Figura 8 - Associação Pacote-Rotulo-FEC-LSP. Fonte: (OLIVEIRA et al. 2012)

- **LSR (*Label Switch Router*):** é um equipamento capaz de realizar encaminhamento de datagramas de rede através de rótulos MPLS. Ele participa activamente no estabelecimento de LSP, usando protocolos de sinalização de rótulo, tais como: LDP, RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) e BGP (*Border Gateway Protocol*), e no encaminhamento de tráfego baseado nos caminhos

estabelecidos. Ao receber um pacote, cada LSR troca o rótulo existente por outro, passando o pacote para o próximo *router* e assim por diante.

- **LSR de Borda de Entrada:** é um LSR (*router* ou *switch* com funções de roteamento) de entrada de uma rede MPLS. Ele realiza o processamento e a classificação inicial do pacote e aplica o primeiro rótulo na entrada (*ingress*) do pacote no domínio MPLS. Os *ingress* LSRs analisam as informações do cabeçalho de rede e associam cada datagrama à uma FEC. Toda FEC tem um rótulo associado que será utilizado no encaminhamento para o próximo nó.
- **LSR de Trânsito:** são LSR's intermediários que têm a função de apenas fazer a comutação, ou seja, a troca de rótulos, e encaminhar o datagrama para o próximo nó. Eles oferecem comutação em alta velocidade, sendo este o processo que mais contribui para o ganho de desempenho na utilização do protocolo MPLS, já que não precisam mais analisar cabeçalhos da camada de rede (IP).
- **LSR de Borda de Saída:** é um LSR responsável pela retirada do rótulo do pacote e encaminhamento ao seu destino final.
- **LSP (*Label Switched Path*):** um LSP é uma sequência ordenada de LSR's, sendo o primeiro um LSR de ingresso e o último um LSR de saída, ou seja, é o caminho entre o nó de ingresso, possíveis nós intermediários, e o nó de egresso de uma rede MPLS. (OLIVEIRA et al. 2012)

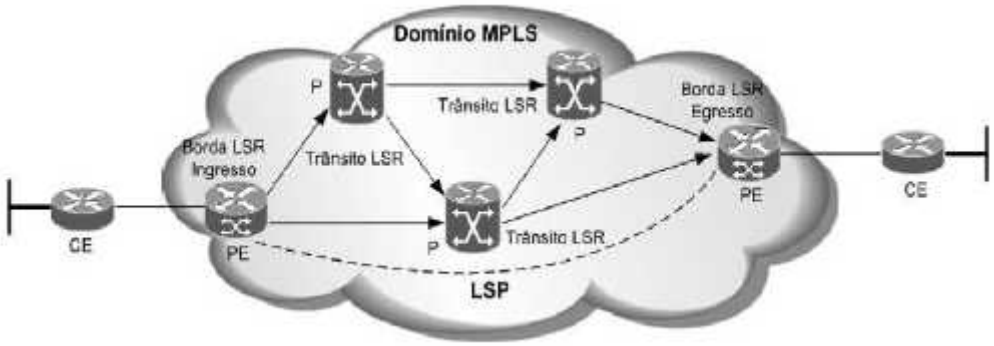

Figura 9 - Componentes da arquitectura MPLS. Fonte: (OLIVEIRA et al. 2012)

Os LSR's de Entrada (Ingresso) e os LSR's de Saída (Egresso) são também conhecidos como *Edge* LSR, LER (*Label Edge Router*) ou PE (*Provider Edge*). O LSR de Trânsito é também conhecido com P (*Provider*). Apesar de não fazerem parte do domínio MPLS, os *routers* que fazem parte do ambiente dos clientes possuem uma nomenclatura no cenário MPLS, sendo conhecidos como CE's (*Customer Edges*).

c) Funcionamento da Rede da Tecnologia MPLS

O modo de operação do MPLS diverge do modo de operação do IP, pois os pacotes são analisados na camada três somente quando entram ou quando saem do domínio MPLS. Este trabalho é feito pelo LER que além de analisar o cabeçalho IP faz a amarração do rótulo com a FEC de destino, e a partir daí o pacote é conduzido através da rede pelos LSR que manipulam apenas rótulos. (SANTOS 2003)

Segundo Oliveira *et al.* (2012), o funcionamento da rede MPLS consiste nas seguintes etapas:

- **1ª Etapa:** Construção das tabelas de roteamento
  Através de protocolos de roteamento, tais como OSPF (*Open Shortest Path First*) e IS-IS (*Intermediate System to Intermediate System*), são construídas as tabelas de roteamento, que irão determinar os melhores caminhos para atingir as redes de destino por toda a rede do provedor. Nesta etapa também há a actuação do protocolo LDP, que irá fazer o mapeamento entre rótulos e *IP's* de destino.
- **2ª Etapa:** Ingresso dos pacotes na rede
  O *router* de borda de ingresso recebe os pacotes que irão entrar na rede, executando serviços de nível 3 e de valor acrescentado, tais como QoS, e em seguida acrescenta o rótulo aos pacotes.
- **3ª Etapa:** Encaminhamento dos pacotes na rede
  O LSR encaminha os pacotes usando o mecanismo de troca de rótulos (*Label Swapping).* Ao receber o pacote com rótulo, o LSR lê o rótulo, o substitui de acordo com a tabela LFIB e o encaminha, sendo essa acção repetida por todos os *routers* no núcleo do *backbone*.
- **4ª Etapa:** Saída do pacote na rede
  O *router* de borda de saída remove o rótulo e entrega pacotes IP's.

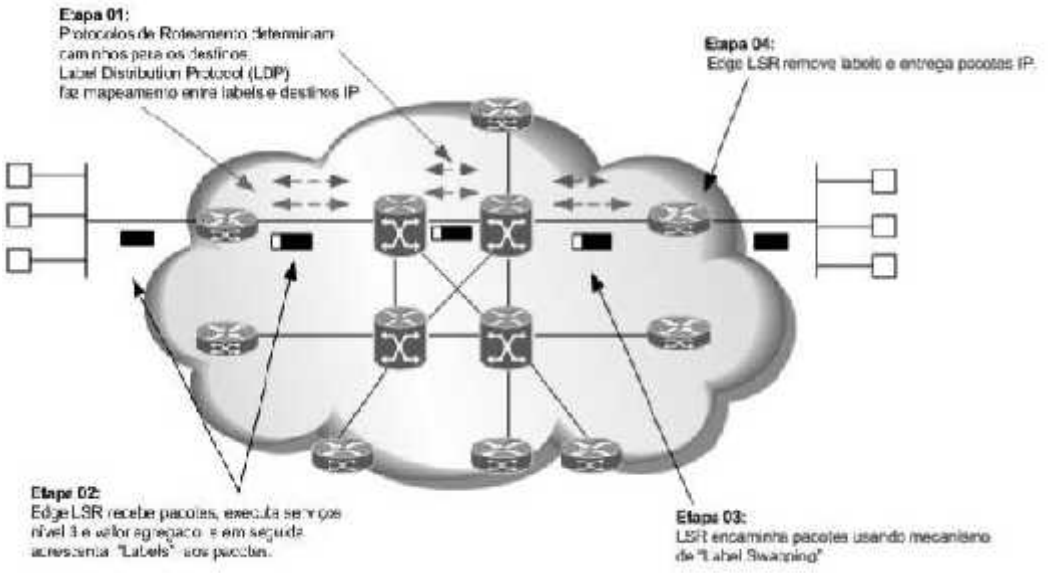

Figura 10 - Etapas de operação do MPLS. Fonte: (OLIVEIRA et al. 2012)

d) Roteamento na Internet

Segundo Kurose *et al.,* os protocolos de roteamento da internet, tem a função de "determinar o caminho tomado por um datagrama entre a *srcem* e o destino."

Um protocolo de roteamento intra-AS é usado para determinar como é rodado o roteamento dentro de um sistema autónomo (AS). Esses protocolos são também conhecidos como protocolos de roteadores internos (IGP – *Interior Gateway Protocols*). Historicamente, dois protocolos de roteamento têm sido usados para roteamento dentro de um sistema autónomo na Internet: o protocolo de informações de roteamento, RIP (*Routing Information Protocol*) e o OSPF (*Open Shortest Path Firs*t).

I) **Roteamento intra-AS na Internet: RIP**

Segundo Kurose et al. (P: 306), o RIP foi um dos primeiros protocolos de roteamento intra-AS da Internet, e seu uso é ainda muito disseminado. Sua *srcem* e seu nome vêm da arquitectura XNS (*Xerox Network Systems*).

II) **Roteamento intra-As na Internet: OSPF**

Como o RIP, o roteamento OSPF é bastante usado para roteamento intra-AS na Internet. O OSPF e o seu primo, IS-IS, muito parecido com ele, são em geral disponibilizados em ISP's de níveis mais altos, ao passo que o RIP está disponível em ISP's de níveis mais baixos e redes

corporativas. O "*Open*" do OSPF significa que as especificações do protocolo de roteamento estão abertas ao público (ao contrário do protocolo EIGRP da Cisco, por exemplo). A versão mais recente do OSPF, versão 2, está definida no RFC 2328, um documento público. (Kurose *et al.* P: 309)

O OSPF foi concebido como sucessor do RIP e como tal tem uma série de características avançadas. Em seu âmago, contudo, é um protocolo de estado de enlace que usa inundação de informação de estado de enlace e um algoritmo de caminho de menor custo de Dijkstra. Com o OSPF, um roteador constrói um mapa topológico completo (isto é, um grafo) de todo o sistema autónomo. O roteador então roda localmente o algoritmo do caminho mais curto de Dijkstra para determinar uma árvore de caminho mais curto para todas as sub-redes, sendo ele próprio o nó raiz. Os custos de enlaces individuais são configurados pelo administrador da rede […]. O administrador pode optar por estabelecer todos os custos de enlace em 1, conseguindo assim o roteamento com o mínimo de saltos, ou por designar para os enlaces pesos inversamente proporcionais à capacidade do enlace, de modo a desencorajar o tráfego a usar enlaces de largura de banda baixa. O OSPF não impõe uma política para o modo como são determinados os pesos dos enlaces (essa tarefa é do administrador da rede); em vez disso, oferece os mecanismos (protocolo) para determinar o caminho de roteamento de menor custo para um dado conjunto de pesos de enlaces. (Kurose *et al.* P: 309)

III) **BGP – O Protocolo de roteamento de Gateway exterior**

Em um único SA, o protocolo de roteamento recomendado na Internet é o OSPF (embora este não seja o único em uso). Entre SA's é usado outro protocolo, o BGP (*Border Gateway Protocol*). É necessário um protocolo diferente entre SAs, porque os objectivos de um protocolo de *gateway* interior e os de um protocolo de *Gateway* exterior não são os mesmos. Tudo o que um protocolo de *gateway* interior precisa fazer é movimentar pacotes da forma mais eficiente possível, da origem até o destino. Ele não precisa se preocupar com política. (Kurose et al. p: 353)

Os pares de roteadores BGP se comunicam entre si, estabelecendo conexões TCP. Esse tipo de operação possibilita uma comunicação confiável e oculta todos os detalhes da rede que está sendo utilizada.

De acordo com Tanenbaum (P:353), o BGP é fundamentalmente um protocolo de vector de distância, mas é bem diferente da maioria dos outros, como o RIP. Em vez de apenas manter o custo para cada destino, cada roteador BGP tem controlo de qual caminho está a ser usado. Da mesma forma, em vez de fornecer periodicamente a cada vizinho seu custo estimado para cada destino possível, o roteador BGP informa a seus vizinhos o caminho exacto que está usando.

2.2.3 VPN-MPLS

[…]. Uma VPN MPLS consiste de duas redes: a rede provedor e a rede do cliente. A rede do provedor é constituída de roteadores de borda (PE) que provêem serviços de VPN e conectividade para as redes dos clientes. As redes dos clientes são normalmente constituídas, fisicamente, por diferentes pontos de acessos. Os roteadores dos clientes que se conectam aos provedores dos serviços das VPN's são chamados de *Router Customer Edge* (CE) […]. Basicamente, uma VPN MPLS usa uma combinação dos benefícios das tecnologias não orientada a conexão (CE-PE) com a tecnologia orientada a conexão (PE-PE). Os protocolos de roteamento entre a CE e PE podem ser: EIGRP, RIPv2, Rota estática, BGP ou OSPF e entre os PE's é utilizado Multiprotocolo BGP (MP-BGP) (Boava 2004 p:31).

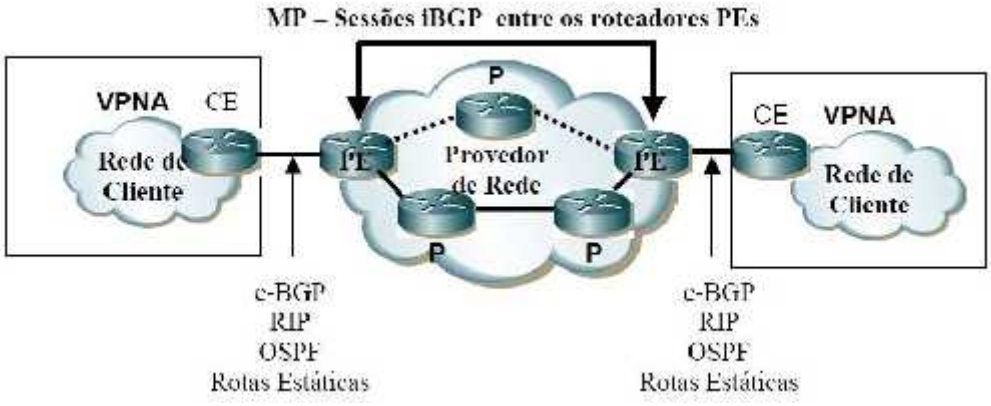

Figura 11 – Visão Geral de uma VPN MPLS. Fonte: (Boava 2004)

Da perspectiva do *router* do cliente (CE), apenas actualizações de rotas e dados são encaminhados para o router de entrada do provedor (PE). Nesse *router* do cliente não é necessária qualquer alteração das configurações da VPN, apenas é necessário habilitar um

protocolo de roteamento ou efectuar um roteamento estático para que este troque informações com o PE. (OLIVEIRA *et al*. 2012)

Segundo Oliveira *et al.* (2012),

> "O *router* PE executa múltiplas funções, pois ele deve ser capaz de isolar o tráfego se mais de um cliente estiver conectado a ele e, para cada cliente, é designada uma tabela de roteamento independente. O roteamento através do *backbone* é desempenhado usando um processo de roteamento na tabela de roteamento global.
>
> Esses *routers* de *backbone*, conhecidos como P (*Providers*), fazem comutação de rótulos entre os PE's e não requerem quaisquer configurações de VPN".

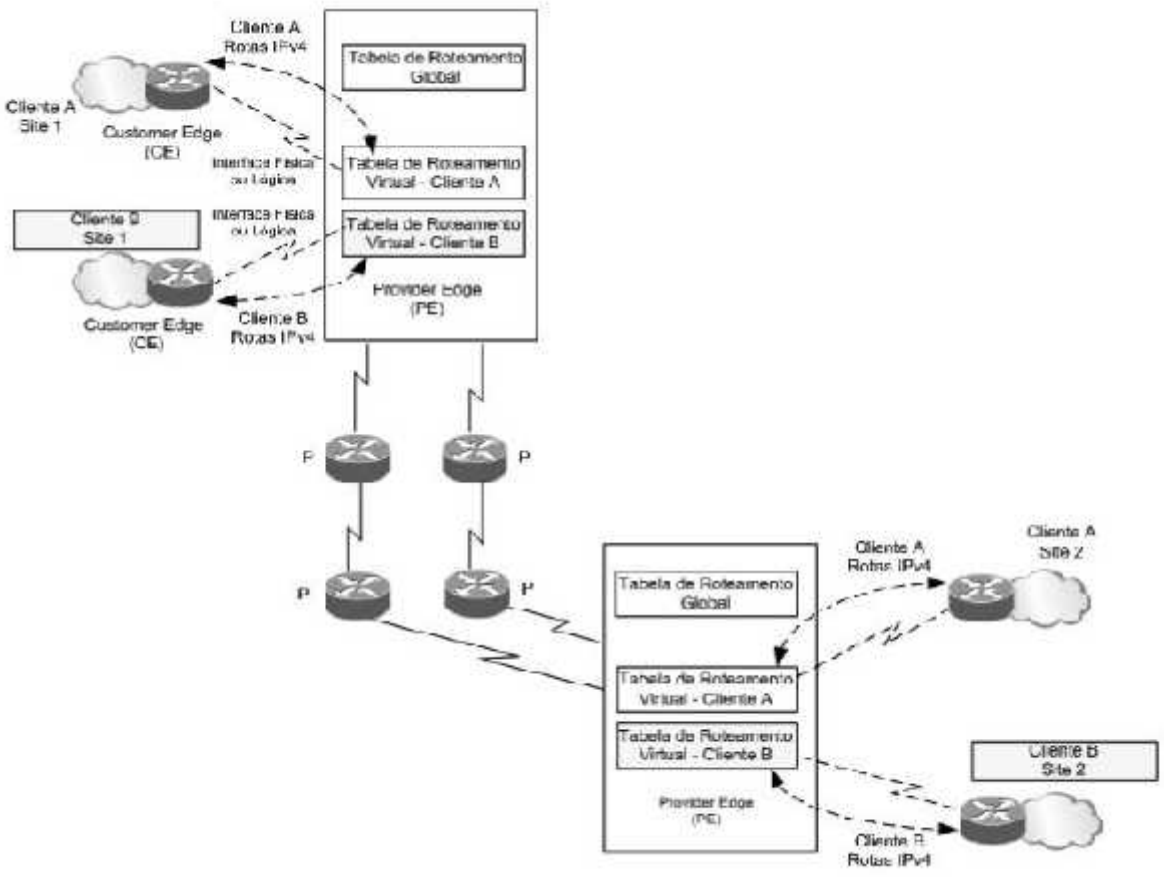

Figura 12 - Arquitectura VPN MPLS. Fonte: (OLIVEIRA et al. 2012)

Segundo Oliveira *et al.* (2012),

> "O isolamento do tráfego entre os clientes, que é realizado nos *routers* PE, faz uso de um conceito conhecido como tabela de roteamento virtual, também chamado de *Virtual Routing and Forwarding table* ou VRF. Um *router* PE tem uma instância de VRF para cada cliente conectado a ele. Funciona como se existissem *routers* dedicados para cada cliente que se conecta ao provedor de serviços, porém há compartilhamento de CPU, largura de banda e recursos de memória com outros *routers* virtuais pertencentes ao mesmo PE".

A função de uma VRF é similar a de uma tabela de roteamento global, portanto, todos os pontos conectados a um *router* PE devem fazer parte de uma VRF.

2.2.4 Voice over IP

Segundo Silva (2010),

> "VoIP (*Voice over IP*) significa o transporte da voz sob uma infra-estrutura IP. Esta infra-estrutura pode ser LAN ou WAN. Geralmente, quando se menciona VoIP, fala-se da integração do PABX com um *gateway* (*router* ou *switch*), que faz a conversão da voz tradicional para Voz sobre IP. Este conceito é um pouco diferente da Telefonia IP, em que não há mais a figura do PABX e os próprios telefones já fazem a conversão para VoIP".

O VoIP habilita o *Gateway* (*router* ou *switch*) para o transporte de tráfego de voz (por exemplo, chamadas telefónicas e faxes) sobre uma rede IP. O suporte de voz é implantado usando-se a tecnologia de pacotes de voz. No VoIP, o processador de sinais digitais segmenta o sinal de voz em quadros e os armazena em pacotes de voz. Esses pacotes de voz são transportados através da rede IP, de acordo com protocolos específicos, como o H.323 do ITU-T, também usado para a transmissão de vídeo através da rede IP. (SILVA 2010)

Como se trata de uma aplicação sensível a atrasos, é necessário o uso de equipamentos que suportam parâmetros de QoS.

A diferença entre as redes VoIP e as redes telefónicas tradicionais está na arquitectura de comutação, pois, enquanto as redes telefónicas tradicionais baseiam-se na comutação por circuitos, as redes VoIP baseiam-se na comutação por pacotes.

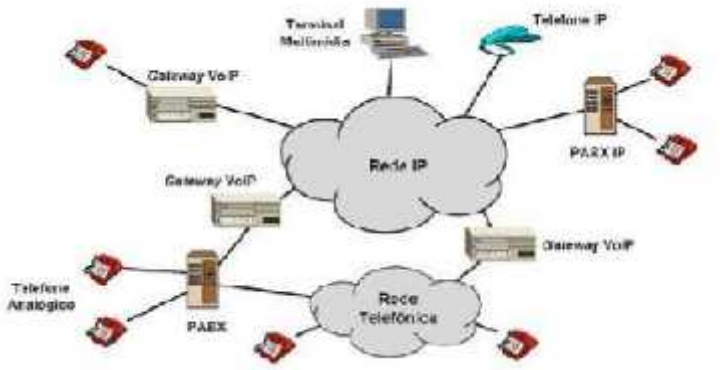

Figura 13 - Arquitectura de uma rede VoIP. Fonte: (SILVA 2010)

Voz sobre IP (Protocolo Internet) é a convergência da tradicional rede de voz e a rede de dados. A implementação de VoIP em uma VPN MPLS requer atenção com alguns parâmetros: disponibilidade de banda, perda de pacotes, atraso e *jitter* (variação do atraso). (Boava 2004 p:66)

2.3 Determinação das variáveis de investigação

Neste contexto será apresentada uma descrição dos conceitos básicos relacionados com às variáveis de investigação.

2.3.1 Qualidade de Serviço (QoS)

O QoS é uma medida colectiva de nível de serviço apresentado ao usuário. Pode ser considerado como sendo o nível de confiança na rede por determinada aplicação para atingir os requisitos necessários para o seu funcionamento (COLLINS 2004).

Para Silva (2010), QoS refere-se ao desafio de proporcionar um fluxo de dados que são sensíveis ao tempo numa rede que foi desenhada para fornecer dados numa forma de melhor esforço. Portanto, os principais parâmetros para a definição de QoS são:

- **Vazão:** é a quantidade de dados, isentos de erros, transferidos com sucesso entre dois pontos. Além dos limites físicos (tecnologia utilizada), a vazão é limitada pela

quantidade de fluxos que compartilham a utilização de determinados componentes da rede. (BRAVO 2008)

- **Atraso:** é o somatório de erros impostos pela rede e pelos equipamentos utilizados na comunicação. O atraso em redes de pacotes tem duas origens principais: primeiro, devido aos recursos compartilhados da rede; segundo, devido o processamento que ocorre em /cada nó de comutação (router) entre a origem e o destino.
- **Jitter:** é definido como sendo uma variação no atraso dos pacotes recebidos. Os pacotes são enviados num fluxo contínuo e espaçados de maneira uniforme. Devido ao congestionamento da rede, filas impróprias, ou erros de configuração, este fluxo constante pode tornar-se irregular, ou o intervalo entre cada pacote pode variar ao invés de permanecer constante (SILVA 2010).
- **Perda de pacotes:** Segundo SILVA 2010, um pacote é perdido quando, ao chegar a um nó de comutação (*router*), este equipamento está com a fila de chegada cheia, provavelmente devido a congestionamento. Não tendo onde armazenar mais pacotes, o *router* começa a descartar os pacotes que chegarem.

  Outro motivo que pode levar à perda do pacote é o seu tempo de vida. O tempo de vida do pacote diminui a cada salto por um nó. Um trajecto demasiado longo poderá consumir todo tempo de vida do pacote e o pacote se destruíra. (SILVA 2010)

a) Arquitecturas de QoS

A Internet fornece um serviço apenas do tipo melhor esforço (*best-effort*), no qual todos os pacotes que trafegam na rede são tratados de maneira uniforme para entregá-los ao destino. Quando há um congestionamento, os pacotes são descartados indiscriminadamente, não havendo garantia de que o serviço será realizado com sucesso, nem que haverá bom desempenho. (ODOM & CARNAVAUGH 2004)

Aplicações em tempo real, tais como tráfego de voz, vídeo e multimídia, necessitam de garantia de largura de banda e são aplicações sensíveis a atraso (*delay*), variação do atraso dos pacotes (*jitter*) e perda de pacotes. (LINS *et al* 2011)

Devido à crescente demanda por largura de banda para a transmissão de serviço como VoIP, vídeos e dados em simultâneo, e com diferenciação por classes de serviço, surgiu no mercado duas formas de prover QoS em redes IP:

- ***IntServ;***
- ***DiffServ***.

- **Serviços Integrados (*Intserv*)**

O objectivo desta arquitectura é obter a largura de banda e a latência necessárias para uma determinada aplicação. (DAVIDSON *et al.* 2007)

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 *et al.* 2012)

Nesta arquitectura a qualidade de serviço é garantida através de mecanismos de reserva de recursos na rede. Isso é tipicamente obtido através do protocolo RSVP (*Resource reSerVation Protocol*). (CHOWDHURY 2002)

A maior vantagem do Serviço Integrado é que previamente é feita uma alocação de banda, uma vez que cada *router* é consultado ao longo do caminho para fazer essa reserva, garantindo assim a entrega dos pacotes. Por outro lado, a sua principal desvantagem é o facto de não ser uma arquitectura escalável, pois a quantidade de informações de estado aumenta proporcionalmente com o número de fluxos, exigindo uma sobrecarga de processamento nos *routers*. (OLIVEIRA *et al*. 2012)

- **Serviços Diferenciados (*DiffServ*)**

A arquitectura de Serviços Diferenciados (*DiffServ*) foi introduzida como uma alternativa para a arquitectura *IntServ*, evitando problemas de escalabilidade e complexidade. A qualidade de serviço nesta arquitectura é garantida através de mecanismos de priorização de pacotes na rede, diferentemente da arquitectura *IntServ*, onde a qualidade de serviço é garantida através de reserva de recursos na rede (OLIVEIRA *et al.* 2012). Desta forma, dois novos tipos de classes especiais surgiram com o modelo diferenciado, de acordo com Oliveira *et al*. (2012):

- **Classe AF (*Assured Forwarding*):** consiste num conjunto de serviços, especificados em termos de largura de banda relativa disponível e políticas de descarte de pacotes. O serviço AF é composto por várias subclasses de serviço que possuem diferentes níveis de precedência em relação ao descarte de pacotes. É indicado para as aplicações que não são tão sensíveis ao atraso e requerem garantia de banda;

- **Classe EF (*Expedited Forwarding*):** oferece um serviço de redes com baixa perda, baixo atraso, baixo *jitter* e banda garantida. É indicado para aplicações de tempo real.

Para identificar a classe de um pacote, as redes *DiffServ* utilizam o campo DS (*Differentiated Service*) que inclui o DSCP (*Diferentiated Service Code Point)*, conhecido anteriormente como tipo de serviço (ToS - *Type of Service*), situado dentro do cabeçalho dos pacotes. Desta forma, quando um novo tráfego chega a uma rede *DiffServ*, este é primeiro classificado pelos *routers* de borda (PE), em seguida passa por um filtro de admissão, com o intuito de moldá-lo de acordo com a política de controlo associada com aquela classificação. (MATA 2002)

2.3.2 Escalabilidade

A escalabilidade refere-se à capacidade de crescimento que um projecto de rede pode suportar. Constitui o objectivo primário de quase todos projectos de rede, para que seja possível adicionar usuários, aplicações ou conexões a um ritmo consideravelmente veloz.

A necessidade de aumentar a capacidade da rede aos mais diversos níveis tem aumentado significativamente. Os parâmetros requeridos para suportar as quantidades de terminais, de fluxos, de utilizadores, de sessões e volume de tráfego têm um impacto determinante nas tecnologias utilizadas e na arquitectura adoptada nas redes, bem como na estrutura operacional dos operadores de telecomunicação. (EUSÉBIO 2010)

Segundo Boava (2011),

> "As VPN MPLS são consideradas os principais elementos da arquitectura de convergências das redes de nova geração e estão se tornando cada vez mais acessíveis para todos os usuários, principalmente em função da alta escalabilidade oferecida e pela fácil implementação, que são características próprias do modelo das VPN baseadas em MPLS. Entretanto, esse modelo trabalha directamente sobre as VRF's (*Virtual Routing and Forwarding*) do PE, que cresce rapidamente à medida que se aumenta a quantidade de *sites* das VPN's conectadas aos PE's".

2.3.3 Segurança

É um conjunto de princípios, técnicas, protocolos, regras e normas que visão garantir um melhor nível de confiabilidade. Tudo isso se tornou necessário com a grande troca de informação entre os sistemas informáticos e principalmente pela vulnerabilidade oferecida por esses sistemas.

Um dos requisitos de segurança mais importantes das VPN's é que o tráfego dos *sites* pertencente a uma determinada VPN fique separado do tráfego das outras VPNs, ou seja, a solução de rede não deve permitir que o tráfego de um usuário de uma determinada VPN seja visto, nem que invada o tráfego da outra VPN. (BOAVA 2011)

Outro requisito importante para um provedor que pretende oferecer o serviço VPN é permitir que o plano de endereçamento de um usuário de uma VPN possa ser utilizado por outra VPN, sem afectar as outras VPN's ou o núcleo da rede. (BOAVA 2011)

As VPN MPLS apresentam uma solução atractiva para os dois requisitos acima citados, sendo que nesta arquitectura usa-se o conceito de RD (*Route Distinguisher*), que "é um identificador único de 64 *bits* que é inserido em frente do IPv4, sendo portanto o único dentro do *backbone* MPLS. A combinação dos endereçamentos IPv4 e esses identificadores de rotas fazem com que as rotas IPv4 sejam únicas através da rede VPN MPLS". (OLIVEIRA *et al.* 2012)

Segundo Boava (2011),

> "Em um dado *router*, pode ser configurado um RD que define uma VRF em que os planos de endereços IPv4 possam ser usados em outra VRF, desde que esta seja configurada com RD distinto. Para as considerações de segurança, é importante entender que o RD faz com que as rotas das VPNs IPV4 sejam únicas no núcleo das VPNs MPLS. O RD é mais bem detalhado em IETF RFC 4364".

Outro conceito importante no que concerne à segurança da VPN MPLS é o RT (*Route Target)*, que segundo Oliveira *et al.* (2012),

> "É um atributo que indica uma colecção de VRF's pelo qual um roteador PE irá distribuir as rotas, ou seja, ele indica quais rotas devem ser importadas e exportadas pelo MP-BGP, permitindo assim que possa haver conversação entre diferentes VRF's e que também possam ser feitas restrições de importação e exportação de rotas".

CAPÍTULO III – MARCO CONTEXTUAL DA INVESTIGAÇÃO

Neste capítulo faz-se menção do que poderá ser observado a respeito da organização sobre aspectos relacionados com a sua visão, visão, seus valores, objectivos, sua estrutura, sua infra-estrutura tecnológica e o problema sobre base pela qual originou este caso de estudo de modo a se obter um enquadramento organizacional do trabalho.

3.1 A Organização

A Universidade Politécnica, designada abreviadamente por A POLITÉCNICA, é uma instituição privada de ensino superior, com a sua sede na cidade de Maputo.

A POLITÉCNICA oferece uma variedade de cursos, que abrangem todos os níveis do ensino superior e todas as áreas do conhecimento.

Vocacionada para três grandes domínios de investigação, nomeadamente: Ciências Empresariais, Ciências Sociais, Ciências Humanas e Tecnologias. A sua acção processa-se através de um conjunto diversificado de actividades, com permanente sentido de interdependência entre ensino/formação, investigação e prestação de serviços à comunidade.

3.1.1 Missão

A POLITÉCNICA tem como missão, contribuir para a elevação do nível educacional, técnico científico e cultural dos moçambicanos, perseguindo os mais altos padrões de qualidade do ensino ministrado aos seus estudantes e da formação dos seus docentes e investigadores, perspectivando uma abordagem teórico-prática e profissionalizante das matérias.

3.1.2 Objectivos

A POLITÉCNICA tem como objectivo reforçar o sentimento patriótico; intervir criticamente na análise e debate de questões de interesse público, a nível nacional e internacional; e contribuir para a eliminação das assimetrias no desenvolvimento nacional, nomeadamente, através da promoção do acesso dos cidadãos ao ensino e à formação.

3.1.3 Valores

Os valores fundamentais pelos quais se rege A POLITÉCNICA são o Humanismo, Rigor e Profissionalismo.

3.1.4 Organograma da Universidade A Politécnica

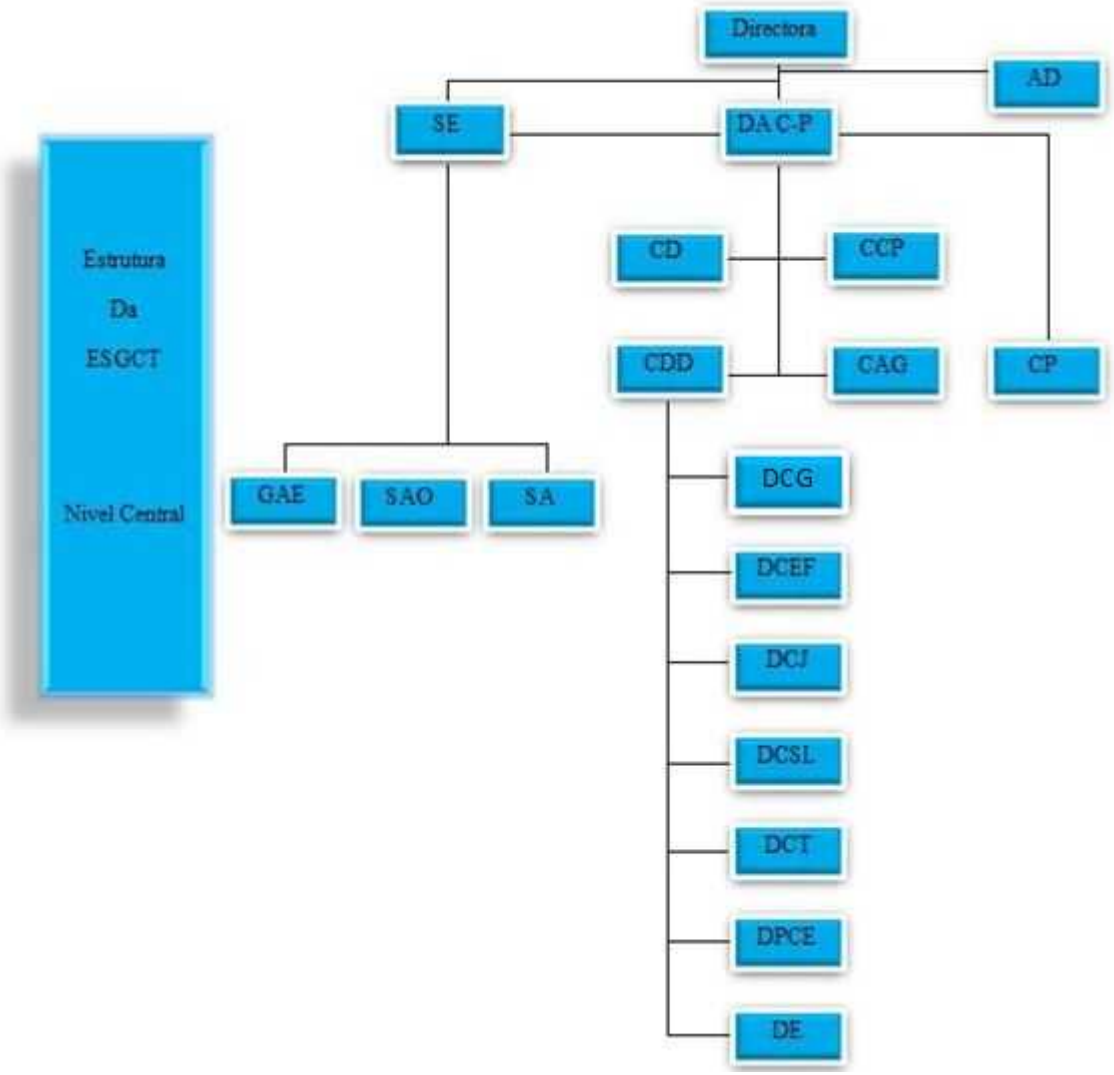

Figura 14 – Estrutura Orgânica da Universidade A Politécnica de Maputo. Fonte: (Universidade A Politécnica)

Legenda:

AD	Assistente de Direcção	**DCT**	Departamento de ciências Tecnológicas
CAG	Coordenador das Actividades de Graduações	**DE**	Departamento de Engenharia

CCP	Comissão Científico Pedagógica	**DCEF**	Departamento de Ciências Económicas e Financeiras
CD	Conselho de Direcção	**DCG**	Departamento de ciências de Gestão
CDD	Chefe de Departamentos	**DPCE**	Departamento de Psicologia e Ciências de Educação
CP	Curso Propedêutico	**GAE**	Gabinete de Apoio Estudantil
DA C-P	Director Adjunto Científico-Pedagógico	**SA**	Sector Académico
DCJ	Departamento de Ciências Jurídicas	**SAO**	Sector Administrativo
DCSL	Departamento de Ciências Sociais e de Linguagem	**SE**	Secretário da Escola

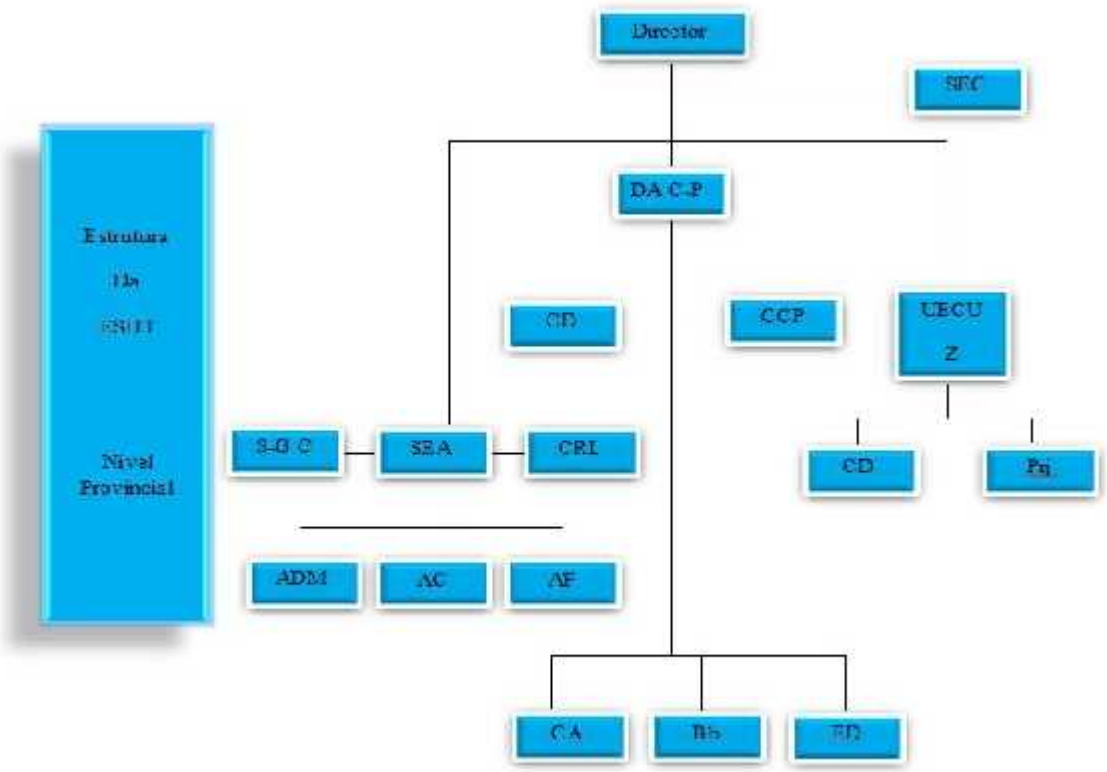

Figura 15 – Estrutura Orgânica da Universidade A Politécnica de Quelimane. Fonte: (Universidade A Politécnica)

Legenda:

AC	Área Académica	**CRL**	Centro de Recursos Laboratorial
ADM	Área Administrativa	**DA C-P**	Director Adjunto Científico Pedagógico
AF	Área Financeira	**ED**	Ensino a Distância
Bb	Biblioteca	**S-G C**	Secretário-geral do Campos
CA	Coordenadores das Áreas	**SEA**	Secretário Executivo e Académico
CD	Cultura e Desporto	**SEC**	Secretário
CDD	Conselho de Direcção	**Prj**	Projectos
CCP	Comissão Científica-Pedagógica	**UECU Z**	UECU Zambézia

CAPÍTULO IV – METODOLOGIA DE RESOLUÇÃO DO PROBLEMA E APRESENTAÇÃO DE RESULTADOS

Neste capítulo foi feita a descrição da proposta de desenvolvimento do cenário de virtualização. Em seguida, é apresentada uma descrição de estudo de caso na Universidade A Politécnica, descrevendo o objectivo, mostrando a descrição técnica, descrevendo deste modo o tipo de estudo e desenho de pesquisa e equipamento existente para a implementação da virtualização da rede na instituição.

O dimensionamento da rede VPN com base nas tecnologias MPLS apresenta-se como uma solução para as diversas barreiras que podem se encontrar na transmissão de dados, voz e vídeo. O projecto é desenvolvido na plataforma GNS3. Este programa de computador é empregado com eficiência na área de redes, onde, no caso do projecto será aplicado para a simulação e configuração do enlace proposto. O ambiente empregado nesta interface é o GUI (*Graphic User Interface*). Esta ferramenta de desenvolvimento proporciona um ambiente simples e amigável para o usuário.

4.1 Entrevista

Com base em uma entrevista semiestruturada (ver anexo I e II) e um estudo aprofundado da actual situação da Universidade em termos de comunicação com a delegação, foi possível a recolha de informação para melhor conhecimento dos meios de comunicação e tecnológicos existentes até o momento. Os resultados da entrevista foram usados para a construção do marco-contextual do presente trabalho, bem como na planificação da estratégia da solução proposta.

Esta colecta de informação (entrevista) deu-se através da interacção directa com s representantes de diversos departamentos a nível da Universidade, sendo os principais:

- Área Administrativa: representantes do departamento de Administração;
- Área Técnica: representantes da repartição de Informática

4.2 Especificação das aplicações a considerar no dimensionamento

A presente fase tem como principal objectivo de identificar as principais aplicações utilizadas na Universidade, com vista a que as classes de serviços (CoS) devem ser classificadas e agregadas.

As aplicações são identificadas pelas suas respectivas portas UDP/TCP. A seguir são apresentadas as principais aplicações utilizadas na Universidade bem como as aplicações previstas para o presente dimensionamento:

- Comunicação entre utilizadores da Universidade através do correio electrónico e partilha de ficheiros;
- Acesso a base de dados;
- Iterações remotas entre utilizadores e ou pessoal das TIC's e utilizadores;
- Transferência de ficheiros dentro da WAN;
- Serviços de voz sobre IP.

4.2.1 Divisão das aplicações em múltiplas classes de serviço

De modo a oferecer serviços diferenciados (DiffServ) de acordo com as aplicações do utilizador, os tráfegos devem ser agrupados m classes segundo os requisitos das aplicações.

Cada classe deve ser diferenciada pela rede de acordo com o serviço definido na configuração da QoS para essa classe. No presente dimensionamento são recomendadas 6 classes de serviços destacadas a seguir:

- **Padrão BE – Classe Dados Padrão *Best Effort* (BE) – Classe 0**
  Classe de serviço que corresponde ao tráfego de menor prioridade.

  Esta classe oferece basicamente conectividade sem nenhuma garantia, sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como trafego importantes. As transferências de ficheiros na WAN serão associadas a esta classe de serviço.

- **Classe Dados com prioridades – AF**
  Classe de serviço que provê uma priorização de trafego das aplicações críticas do usuário em relação a dados Melhor Esforço.

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

  Aplicações com mensagens de tamanho muito variado e que não exigem o atendimento imediato aos usuários.

  Todas as aplicações classificadas nesta classe terão prioridade em relação às aplicações do padrão – BE. À esta classe será associado a um serviço de correio electrónico (email).

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

  Aplicações não interactivas, com grande volume de dados importantes para os usuários da organização. Essas aplicações serão consideradas prioritárias em relação às aplicações não críticas e de melhor esforço. As futuras soluções em sistemas de gestão de base de dados integrados, tais como Oracle ou SQL *server*, serão associadas a esta classe de serviço.

- **AF3 – Gestão – Classe 3**

  Esta classe será reservada para aplicações de gestão de redes e de sistemas que necessitam de uma banda mínima para actividades de suporte técnico, mesmo em situações de congestionamento severo da rede. Esta classe terá prioridade em relação às anteriores. Aplicações para iteração remota que usam protocolos como SSH, bem como as de gestão da rede que usam protocolos como SNMP serão associadas a esta classe de serviço.

- **AF4 – Missão Crítica – Classe 4**

  Esta classe será reservada para as aplicações que exigem entrega garantida e tratamento prioritário. Essa classe terá prioridade em relação às anteriores. As aplicações de gestão ou processamento de transacções WWW serão associadas a esta classe de serviço.

- **Classe Tempo Real – EF – Classe 5**

  Aplicação sensíveis ao retardo (*delay*) e variações de retardo da rede (*jitter*), que exigem priorização de pacotes e reserva de banda são adequadas para essa classe. Essa classe terá prioridade em relação às anteriores. O serviço de VoIP é apropriado para essa classe.

Classe de serviço	Aplicações	Porta UDO/TCP
Padrão (BE) Classe 0	Transferências de ficheiros	21
Não Crítico (AF1) Classe 1	Correio Electrónico	25
Suporte a Negócio (AF2) Classe 2	SQL Service	156
	Oracle	1521 ou 1526
Gestão (AF3) Classe 3	SSH	22
Tempo Real (EF) Classe 5	Voz – RTP/RTCP	5004 ou 5005

Tabela 1. Especificação das classes de serviço e portas UDP/TCP para aplicações. Fonte: Autor

4.3 CODEC

Uma vez que se pretende que haja comunicação por voz sobre a VPN, é imprescindível o uso de CODEC.

O termo CODEC, significa codificador/descodificador, que consiste num algoritmo para a execução dos processos de quantificação e digitalização do sinal de áudio ou de vídeo, reduzindo a quantidade de bytes gerados e consequentemente diminuindo a largura de banda necessária para a transmissão ou espaço para o armazenamento. Existe actualmente uma variedade de CODEC's usados para as aplicações de voz de acordo com as necessidades. A seguir alguns CODEC's usados em aplicações de voz:

- O G.711 é um padrão de CODEC usado basicamente para a telefonia convencional (PSTN). Este padrão digitaliza a voz em 64 Kbps, sem compressão.
- O G.729 é um padrão usado para a operação de voz comprimida a 8 Kbps, sendo este um dos padrões mais comummente implementados em operações VoIP, por permitir a compressão da voz.

- O G.723.1 já foi o padrão de compressão recomendado. Opera em 6,3 Kbps e 5,3 Kbps. Embora este padrão ainda reduza o consumo de largura de banda, a voz é notavelmente mais pobre do que com o G.729, por isso não é muito usado para VoIP.

Codec e Taxa de Bits (Kbps)	**Tamanho da Amostra do Codec (Bytes)**	**Intervalo da Amostra do Codec (ms)**	**Mean Opinion Score (MOS)**	**Tamanho do Payload de Voz (Bytes)**	**Intervalo do Payload de Voz (ms)**
G.711 (64 Kbps)	80	10	41	160	20
G.729 (8 Kbps)	10	10	3.92	20	20
G.723.1 (6,3 Kbps)	24	30	3.9	24	30

Tabela 2. Codecs de voz que podem ser usados para dimensionarem a largura e banda VoIP.
Fonte: Cisco (2016)

Legenda:

- **Taxa de Bits (Kbps):** é o número de bits por segundo que precisam de ser transmitidos numa chamada de voz;
- ***Mean Opinion Score* (MOS):** é um sistema usado para classificar a qualidade de voz das conexões telefónicas. Com o MOS, um amplo intervalo de ouvintes classifica a qualidade de uma amostra de voz em uma escala de um (péssimo) a cisco (excelente);
- **Tamanho do *Payload* de Voz (Bytes):** representa o número de bytes (ou bits) que são preenchidos em um pacote.

Para o presente projecto foi usado o CODEC G. 729, por este consumir uma largura de banda acessível (8Kbps) e possuir um nível de MOS estável para uma chamada de voz com um grau de inteligibilidade aceitável.

O tamanho da amostra do CODEC é também um factor a ter em conta no dimensionamento da largura de banda, com influência directa no atraso da chamada VoIP. Ao aumentar o tamanho do *payload* de voz, a largura de banda diminui o atraso geral aumenta.

O CODEC G.729 usa um valor padrão de 20 bytes para o *payload* de voz, embora ainda se possa usar valores compreendidos entre a escala de 10 bytes a 230 bytes.

Com vista a minimizar os gastos em largura de banda, mas sem comprometer a qualidade da chamada (ex.: aumento do atraso geral), para o presente projecto serão usados 30 bytes como tamanho do *payload* de voz e 30 ms como intervalo do *payload* de voz.

4.4 Determinação da tecnologia de acesso

Uma das redes mais acessíveis e com maior abrangência é a rede telefónica, formada por pares de condutores eléctricos de cobre. Pelo facto de serem acessíveis, as linhas telefónicas têm sido foco de grandes estudos para disponibilizar acesso de dados em alta velocidade. O xDSL (*Digital Subscriber Line*), é visto como uma das formas mais modernas e acessíveis de prover acesso de dados, com base nas linhas telefónicas tradicionais.

A utilização do xDSL (*Digital Subscriber Line*) como forma de acesso das VPN-MPLS, representa uma redução significativa dos custos para a operadora e, consequentemente, dos preços do serviço para o usuário final. As formas de conexão DSL com a VPN-MPLS basicamente consistem em um PVC (*Private Virtual Circuit*) entre o cliente e o provedor do serviço.

Uma outra alternativa como solução para o acesso CE – PE para as VPN-MPLS, é o uso do *link* (hiperligação) dedicado via rádio, que consiste numa conexão directa entre dois pontos. A grande vantagem do *link* dedicado é que ele tem um aproveitamento de 100%, todo o tempo. Se for contratado um *link* dedicado de 1Mbps, haverá 1Mbps de banda disponível o tempo todo, embora se houver alguma falha nos equipamentos haverá um corte de conexão.

Os custos de implementação dessas tecnologias são, no entanto, muito diferentes entre si. Como consequência, é sugerido o modelo de atendimento descrito abaixo:

- A primeira alternativa é o atendimento via xDSL, caso seja possível atender os requisitos das aplicações dos usuários e haja disponibilidade de acesso na localidade onde o usuário se encontra (tanto em Maputo bem como em Quelimane);
- Caso não seja possível o atendimento por xDSL, a segunda alternativa visando o menor custo seria um *link* dedicado**,** do cliente até o PE mais próximo.

4.5 Orçamento proposto do projecto

Para o presente dimensionamento, foi seleccionada a empresa Teledata como provedora, para o fornecimento do serviço de VPN MPLS, por esta ser a entidade directamente relacionada à empresa pública TDM (Telecomunicações de Moçambique), que é a detentora do maior *backbone* por fibra óptica a nível nacional e provedora dos circuitos dedicados que serão instalados pela Teledata.

4.5.1 Proposta técnica

A ligação será estabelecida através de um circuito dedicado digital. A qualquer momento a Universidade A Politécnica poderá solicitar o *upgrade* ou *downgrade* do pacote/banda, caso não satisfaça ou está além das necessidades da instituição. No entanto, importa salientar que por cada alteração de banda do *link* primário é cobrada uma taxa de *Upgrade* ou *Downgrade* (pagamento único) cujo valor corresponde a 10.000,00 MT.

A proposta da Teledata é de fornecer a Universidade A Politécnica o serviço de conectividade de dados MPLS através de infra-estrutura de comunicações terrestre (circuitos alugados) com *backbone* em fibra óptica. O circuito a instalar entre a Sede da Universidade A Politécnica e a Teledata de Maputo servirá de **Colector** das ligações das subsequentes instalações.

4.5.2 Serviço de dados MPLS

O serviço de transmissão de dados é baseado na comunicação de pacotes, com utilização do protocolo de transmissão IP, disponibilizando através de circuitos alugados da TDM, com o *backbone* por fibra óptica e cobertura nacional. O serviço com mensalidade fixa inclui:

- 1 Opção de ligação com 1 Mbps para sede na cidade de Maputo e 512 Mbps para sucursal na cidade de Quelimane de banda/débito;
- 1 Opção de ligação com 512 Mbps para sede na cidade de Maputo e 256 Mbps para sucursal na cidade de Quelimane de banda/débito;

- Nível de entrega Layer 3;
- Endereçamento IP fixo privado;
- Conectividade permanente 24/24h;
- Tráfego ilimitado;
- Equipamento de roteamento e *firewall* (Mikrotik ou Router Cisco 1941 – ver Anexo IV) para terminação da ligação em cada local.

Figura 16 – Cisco 1941Series Integrated Services Routers. Fonte: (Cisco 2014)

4.5.3 Diagrama de rede

A seguir apresenta-se o diagrama de rede da solução proposta para interligar as instalações da Universidade A Politécnica em Maputo à sucursal na cidade de Quelimane.

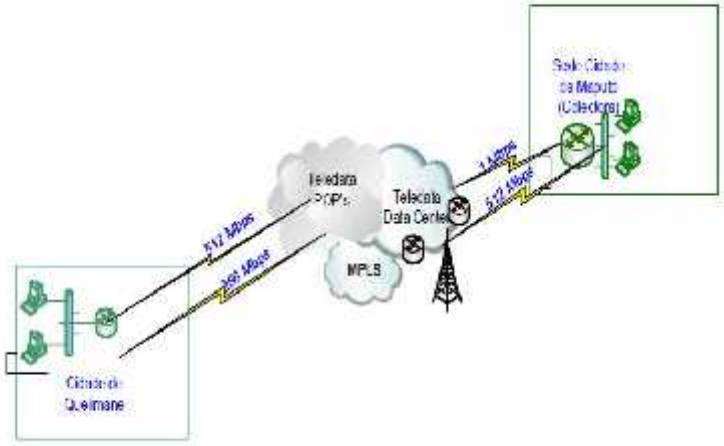

Figura 17 – Diagrama da VPN-MPLS proposta pela Teledata. Fonte (TELEDATA 2018)

4.5.4 Proposta comercial da teledata

Relativamente aos serviços de comunicação de dados, a solução proposta terá um preço composto por duas rubricas principais:

- Taxa de instalação (a pagar uma única vez);
- Mensalidades do serviço prestado.

Local	Débito	Serviço MPLS Ligação Primária	
	Opção	Tx de Instal. (MT)	Mensalidade (MT)
Syrex Lda (Sede) – Cidade de Maputo	2Mbps	6.872,00	8.490,00
Cidade de Quelimane	512 Mbps	20.000,00	48.540,00
Syrex Lda (Sede) Cidade de Maputo	1Mbps	6.872,00	5.220,00
Cidade de Quelimane	256 Mbps	20.000,00	42.320,00
Total			

Tabela 3 – Tabela de Preços para a Proposta de VPN-MPLS. Fonte: (TELEDATA 2018)

4.6 Simulação da VPN-MPLS

Devido à sua maior popularidade, à facilidade de *softwares* para emulação e ao facto de grande parte de provedores de serviços fazerem uso de equipamentos do fabricante *Cisco Systems* em seus *backbones*, todos os testes realizados foram exemplificados com base nos comandos e equipamentos deste fabricante.

Foi utilizado um ambiente de simulação para os testes através do *software* emulador GNS3 e imagens de roteadores e *switches* da Cisco IOS. Trata-se de um emulador gráfico que permite emular o *software* real de diferentes fabricantes de dispositivos de rede como Cisco, Mikrotic, Hp, Dell e Arista.

No cenário representado na figura 18, foi configurado VPN-MPLS para enviar pacotes de dados e de voz do cliente (Universidade A Politécnica) sobre a rede de provedor. Os protocolos OSPF e BGP foram configurados no domínio do prestador de serviços (routers PE1, LSR-MPLS, LSR-MPLS2, PE2). O ponto motivacional para o uso do OSPF no *backbone* foi o facto de que o OSPF usa *multicast* de IP para enviar actualizações de *link-state*. Isto garante menor processamento nos *routers* que não estão a estudar os pacotes OSPF. Além disto, as

actualizações são enviadas nos casos em que mudanças ocorrem, ao invés de periodicamente, o que garante melhor utilização da banda.

No cliente, foi configurado o protocolo EIGRP por ser um protocolo proprietário da Cisco, por isso é 100% compatível com os seus equipamentos. Outro ponto motivacional foi o facto de que o EIGRP combina as características dos protocolos de roteamento baseados em Vector de Distância com as características dos mais recentes protocolos baseados no algoritmo de Estado de Enlace. Ele também proporciona economia de tráfego por limitar a troca de informações de roteamento.

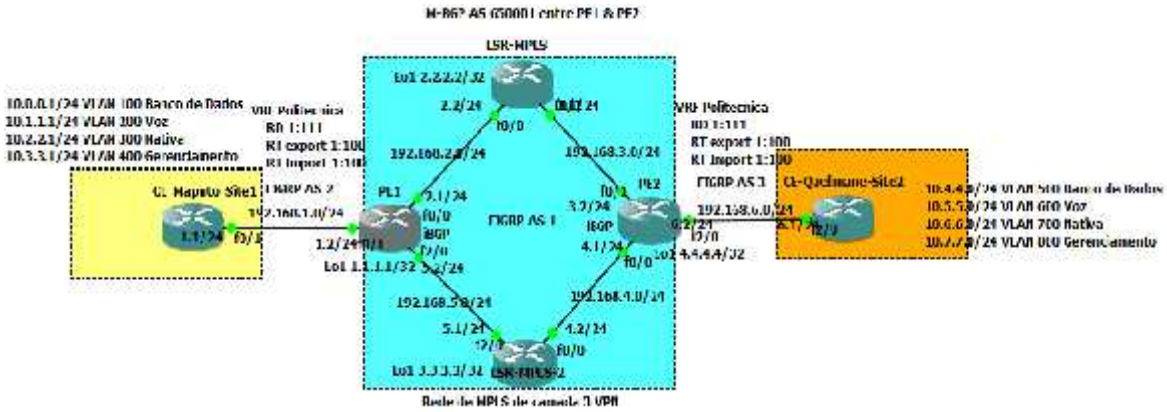

Figura 18 – Arquitectura da Rede VPN-MPLS. Fonte: (Autor)

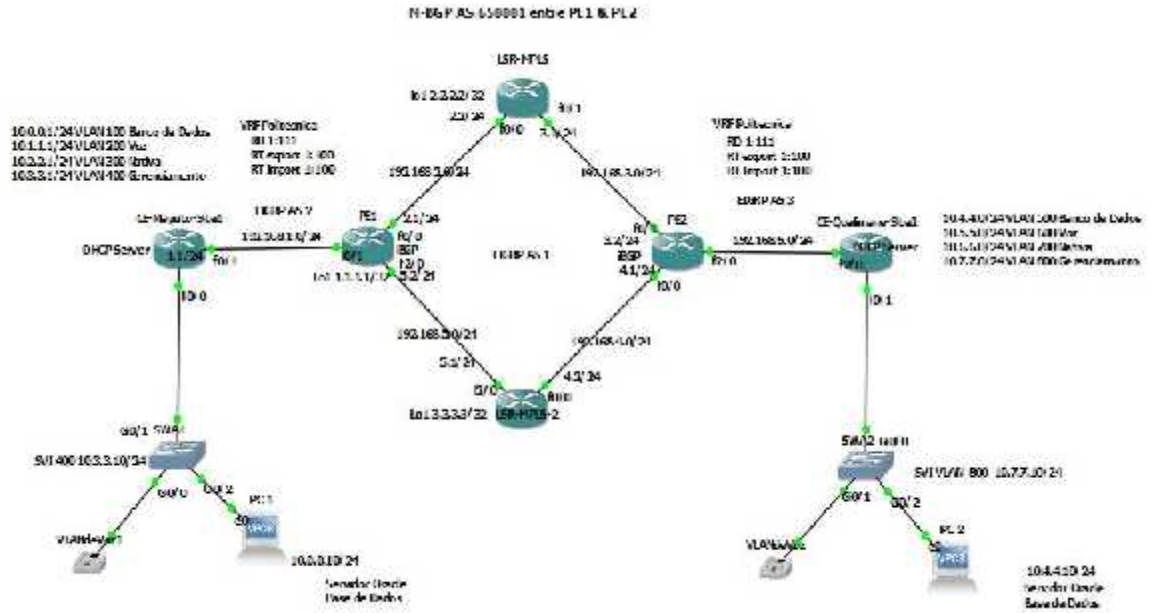

Figura 19 – Arquitectura da Rede VPN-MPLS. Fonte: (Autor)

Para questões de simulação da VPN-MPLS e teste de Conectividade, optou-se por usar o ***router* Cisco 3725 Série**, com os IOS: C3725-ADVENTERPRISEK9-M.image, por ser um *router Enterprise*, anunciado como *High-Performance Services Aggregation* fornecem serviço para Telefones IP sendo uma solução aplicável para pequenas, medias e grandes empresas.
A seguira escolha do equipamento e IOS para a simulação:

```
PE2-Quelimane#show version
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 12:08 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14, RELEASE SOFTWAR
E (fc2)
```

O cabo proposto para implementação é o cabo de fibra óptica padrão **SMF IEEE 10GBASE-LR** que pode transmitir até 10Gbps numa distância até 10Km necessário para garantir a conexão física dos 2 *sites* até a junta do provedor ODF que irá permitir a comunicação com o provedor de serviço.

4.6.1 Endereçamento IPv4

Quanto ao endereçamento IP na rede privada de MPLS, será usado endereçamento IP privado IPv4.

Endereçamento IP na rede WAN:

- **Classe c 192.168.1.0/24** conexão entre **CE-Maputo** e **PE1-Maputo;**
- **Classe c 192.168.6.0/24** conexão entre **CE-Quelimane** e **PE2-Quelimane;**
- **Conexão entre os routers PE- P na rede Core MPLS Backbone;**
- **Classe c 192.168.2.0/24** conexão entre **PE1-** e **LSR-MPLS**;
- **Classe c 192.168.5.0/24** conexão entre **LSR-MPLS** 2 e **PE1;**
- **Classe c 192.168.3.0/24** conexão entre **LSR-MPLS** e **PE2;**
- **Classe c 192.168.4.0/24** conexão entre **LSR-MPLS 2** e **PE2.**

4.6.2 Escopo do projecto de instalação e configuração no ambiente real

1. Fazer a instalação dos roteadores na rack;
2. Fazer a instalação dos módulos SFP para fibra óptica;
3. Conectar o cabo console aos roteadores;
4. Fazer a cablagem dos cabos de fibra e UTP cat5e para a LAN de Maputo e Quelimane;
5. Configurar os roteadores e switches;
6. Testar a conectividade entre os *sites*;
7. Fazer a verificação da configuração;
8. Copiar a configuração em execução para a NVRAN e para o servidor TFTP.

4.6.3 Simulação no GNS3, escopo de configuração:

1. Fazer o diagrama lógico;
2. Conectar os cabos como ilustra o diagrama;
3. Fazer a configuração básica;
4. Configurar os endereços de IP;
5. Activar as interfaces;
6. Testar a conectividade ponto a ponto;
7. Activar o CEF e verificar a FIB;
8. Configurar MPLS-LDP em todos os roteadores PE e P;
9. Configurar a EIGRP AS l na rede Core interna MPLS Teledata IGP;
10. Configurar as VRF nos roteadores PE na rede MPLS;
11. Associar as VRF as interfaces conectadas aos CE-Maputo e CE-Quelimane
12. Fazer a configuração do protocolo de roteamento M-BGP nos roteadores PE1 e PE2;
13. Verificar a operação de BGP;
14. Verificar a operação do MPLS LDP;
15. Verificar os rótulos de MPLS associado as rota de BGP na LFIB;
16. Configurar EIGRP AS 2 entre CE-Maputo e PE1;
17. Configurar EIGRP AS 3 entre CE-Quelimane e PE2;
18. Configurar o M-BGP *Address Family* VPNv4;
19. Associar ao EIGRP AS 2 e AS 3 a VRF Politécnica;
20. Configurar a redistribuição de rotas entre EIGRP AS 2 e AS 3 e M-BGP nos roteadores PE1 e PE2;

21. Testar a conectividade entre os roteadores CE-Maputo e CE-Quelimane;
22. Configurar os roteadores para serviços de voz sobre IP;
23. Configurar a política de QoS;
24. Implementar segurança com ACL.

4.6.4 Configuração da VPN-MPLS

Configuração básica do roteador CE-Quelimane.

1. Configuração em execução em CE-Quelimane-Site2

```
CE-Quelimane-Site2#
CE-Quelimane-Site2#Configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CE-Quelimane-Site2(config)#!
CE-Quelimane-Site2(config)#!
CE-Quelimane-Site2(config)#!
CE-Quelimane-Site2(config)#Hostname CE-Quelimane
CE-Quelimane(config)#!
CE-Quelimane(config)#no IP domain lookup
CE-Quelimane(config)#!
CE-Quelimane(config)#IP domain-name apolitecnica.ac.mz
CE-Quelimane(config)#!
CE-Quelimane(config)#! configuracao de SSH
CE-Quelimane(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: CE-Quelimane.apolitecnica.ac.mz

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non exportable...
*Mar  1 00:19:57.975: %SYS-3-CPUHOG: Task is running for (2024)msecs, more than (
000)msecs (0/0),process = crypto sw pk proc.
-Traceback= 0x62F0AAA4 0x62FD71A0 0x62FD7CDC 0x62FD540C 0x62FD606C 0x62D1E20C 0x6
2D1E270 [OK]

CE-Quelimane(config)#!
CE-Quelimane(config)#ip ssh version 2

*Mar  1 00:20:04.623: %SYS-3-CPUHOG: Task is running for (2024)msecs, more than (
000)msecs (0/0),process = crypto sw pk proc.
 Traceback= 0x62B26198 0x62F8AAA1 0x62FB71A0 0x62FB7CBC 0x62FB51AC 0x62FB686C 0x6
2D1E20C 0x62D1E270
CE-Quelimane(config)#ip ssh authentication-retries 3
CE-Quelimane(config)#IP ssh time-out 110
CE-Quelimane(config)#!
CE-Quelimane(config)#username admin privilege 15 secret cisco1234
```

```
CE-Ouelimane(config)#username admin privilege 15 secret cisco12345

*Mar  1 00:20:06.179: %SSH-5-ENABLED: SSH 1.99 has been enabled
CE-Ouelimane(config)#!
CE-Ouelimane(config)#service password-encryption
CE-Ouelimane(config)#!
CE-Ouelimane(config)#enable secret cisco12345
CE-Ouelimane(config)#!
CE-Ouelimane(config)#no ip domain lookup
CE-Ouelimane(config)#ip cef
CE-Ouelimane(config)#!
CE-Ouelimane(config)#!
CE-Ouelimane(config)#cdp run
CE-Ouelimane(config)#!
CE-Ouelimane(config)#!
CE-Ouelimane(config)#interface FastEthernet2/0
CE-Ouelimane(config-if)# description link to PE2 Ouelimane MPLS Core BACKBONE
CE-Ouelimane(config-if)# ip address 192.168.6.1 255.255.255.0
CE-Ouelimane(config-if)# no shutdown
CE-Ouelimane(config-if)# cdp enable
CE-Ouelimane(config-if)# exit
CE-Ouelimane(config)#!
CE-Ouelimane(config)#interface FastEthernet0/1
CE-Ouelimane(config-if)# description interface de tronco para as VLANS
CE-Ouelimane(config-if)# no shutdown
CE-Ouelimane(config-if)# cdp enable
CE-Ouelimane(config-if)# exit
CE-Ouelimane(config)#!
CE-Ouelimane(config)#Criacao para roteamento entre VLANS router on stick
CE-Ouelimane(config)#interface FastEthernet0/1.500
CE-Ouelimane(config-subif)# encapsulation dot1Q 500
CE-Ouelimane(config-subif)# IP address 10.4.4.1 255.255.255.0
CE-Ouelimane(config-subif)#  description Banco de Dados
CE-Ouelimane(config-subif)#  no shutdown
CE-Ouelimane(config-subif)#  exit
CE-Ouelimane(config)#!
CE-Ouelimane(config)#interface FastEthernet0/1.600
CE-Ouelimane(config-subif)# encapsulation dot1Q 600
CE-Ouelimane(config-subif)# IP address 10.5.5.1 255.255.255.0
CE-Ouelimane(config-subif)#  description Vlan de Voz
CE-Ouelimane(config-subif)#  no shutdown
CE-Ouelimane(config-subif)#  exit
CE-Ouelimane(config)# '
```

```
CE-Quelimane(config)#interface FastEthernet0/1.700
CE-Quelimane(config-subif)# encapsulation dot1Q 700 native
CE-Quelimane(config-subif)#
*Mar  1 00:20:12.487: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to
up
*Mar  1 00:20:13.407: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
up
*Mar  1 00:20:13.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
2/0, changed state to up IP address 10.6.6.1 255.255.255.0
CE-Quelimane(config-subif)#  description Vlan Nativa
CE-Quelimane(config-subif)#  no shutdown
CE-Quelimane(config-subif)#  exit
CE-Quelimane(config)#!
CE-Quelimane(config)#interface FastEthernet0/1.800
CE-Quelimane(config-subif)# encapsulation dot1Q 800
CE-Quelimane(config-subif)# IP address 10.7.7.1 255.255.255.0
CE-Quelimane(config-subif)#  description Vlan de Gerenciamento
CE-Quelimane(config-subif)#  no shutdown
CE-Quelimane(config-subif)#  exit
CE-Quelimane(config)#!
CE-Quelimane(config)#Banner motd & ACESSO NAO AUTORIZADO &
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#line con 0
CE-Quelimane(config-line)# exec-timeout 5 0
CE-Quelimane(config-line)#password cisco12345
CE-Quelimane(config-line)# logging synchronous
CE-Quelimane(config-line)# login
CE-Quelimane(config-line)# exit
CE-Quelimane(config)# !
CE-Quelimane(config)#line aux 0
CE-Quelimane(config-line)# exec-timeout 5 0
CE-Quelimane(config-line)# privilege level 15
CE-Quelimane(config-line)# password cisco12345
CE-Quelimane(config-line)# exit
CE-Quelimane(config)# !
CE-Quelimane(config)#line vty 0 4
CE-Quelimane(config-line)#
*Mar  1 00:20:14.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
0/1, changed state to upTransport input ssh
CE-Quelimane(config-line)# login local
CE-Quelimane(config-line)# exit
```

2. Verificação do estado das interfaces e teste da conectividade entre CE-Quelimane e PE2

```
CE-Quelimane(config-line)# exit
CE-Quelimane(config)# !
CE-Quelimane(config)#line vty 5 15
CE-Quelimane(config-line)#Transport input ssh
CE-Quelimane(config-line)# login local
CE-Quelimane(config-line)# exit
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#!
CE-Quelimane(config)#end
CE-Quelimane#! Teste de conectividade
CE-Quelimane#ping 192.168.6.2 Source FastEthernet2/0 repeat 100
*Mar  1 00:20:16.719: %SYS-5-CONFIG_I: Configured from console by console
CE-Quelimane#ping 192.168.6.2 Source FastEthernet2/0 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.6.1
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 36/67/216 ms
CE-Quelimane#show ip interface brief | include up
FastEthernet0/1            unassigned      YES unset  up                    up

FastEthernet0/1.500        10.4.4.1        YES manual up                    up

FastEthernet0/1.600        10.5.5.1        YES manual up                    up

FastEthernet0/1.700        10.6.6.1        YES manual up                    up

FastEthernet0/1.800        10.7.7.1        YES manual up                    up

FastEthernet2/0            192.168.6.1     YES manual up                    up
```

3. Verificar o estado das interfaces e teste de conectividade entre CE-Maputo e PE1

```
CE-Maputo#show ip interface brief | include up
FastEthernet0/0            unassigned      YES NVRAM  up                    up

FastEthernet0/0.100        10.0.0.1        YES NVRAM  up                    up

FastEthernet0/0.200        10.1.1.1        YES NVRAM  up                    up

FastEthernet0/0.300        10.2.2.1        YES NVRAM  up                    up

FastEthernet0/0.400        10.3.3.1        YES NVRAM  up                    up

FastEthernet0/1            192.168.1.1     YES NVRAM  up                    up

CE-Maputo#
CE-Maputo#! Teste de conectividade
CE-Maputo#ping 192.168.1.2 Source FastEthernet0/1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 4/10/24 ms
CE-Maputo#
```

Nota: A conectividade ponto-a-ponto foi testada sem nenhuma perda.

4. Configuração do protocolo EIGRP no PE1

```
PE1-Maputo(config)#router eigrp 1
PE1-Maputo(config-router)#eigrp router-id 1.1.1.1
PE1-Maputo(config-router)#network 1.1.1.1 0.0.0.0
PE1-Maputo(config-router)#network 192.168.2.0 0.0.0.255
PE1-Maputo(config-router)#network 192.168.5.0 0.0.0.255
PE1-Maputo(config-router)#no auto summary
PE1-Maputo(config-router)#exit
PE1-Maputo(config)#
*Mar  1 00:48:10.011: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.2.2 (Fast
EthernetO/O) is up: new adjacency
PE1-Maputo(config)#
*Mar  1 00:48:37.015: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.2.2 (Fast
Ethernet0/0) is resync: peer graceful restart
PE1-Maputo(config)#
```

5. Análise da configuração de EIGRP AS 1

```
PE1-Maputo#show ip eigrp interface
IP-EIGRP interfaces for process 1

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa2/0              1        0/0       425       0/1          2112          0
Fa0/0              1        0/0        30       0/2           124          0
Lo1                0        0/0         0       0/1             0          0
PE1-Maputo#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.2.2             Fa0/0             10 00:10:21   30    200  0  16
0   192.168.5.1             Fa2/0             14 00:14:49  425   2550  0  21
PE1-Maputo#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(1.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2.2.2.2/32, 1 successors, FD is 409600
        via 192.168.2.2 (409600/128256), FastEthernet0/0
P 1.1.1.1/32, 1 successors, FD is 128256
        via Connected, Loopback1
P 4.4.4.4/32, 1 successors, FD is 412160
        via 192.168.5.1 (412160/409600), FastEthernet2/0
        via 192.168.2.2 (435200/409600), FastEthernet0/0
P 3.3.3.3/32, 1 successors, FD is 156160
        via 192.168.5.1 (156160/128256), FastEthernet2/0
P 192.168.2.0/24, 1 successors, FD is 281600
        via Connected, FastEthernet0/0
P 192.168.3.0/24, 1 successors, FD is 307200
        via 192.168.2.2 (307200/281600), FastEthernet0/0
P 192.168.4.0/24, 1 successors, FD is 284160
        via 192.168.5.1 (284160/281600), FastEthernet2/0
P 192.168.5.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet2/0
PE1-Maputo#
```

6. Análise da tabela de roteamento e redes aprendidas de EIGRP AS 1

```
PE1-Maputo#show ip route eigrp
     2.0.0.0/32 is subnetted, 1 subnets
D       2.2.2.2 [90/409600] via 192.168.2.2, 00:07:09, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
D       3.3.3.3 [90/156160] via 192.168.5.1, 00:16:38, FastEthernet2/0
     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/412160] via 192.168.5.1, 00:11:54, FastEthernet2/0
D    192.168.4.0/24 [90/284160] via 192.168.5.1, 00:11:54, FastEthernet2/0
D    192.168.3.0/24 [90/307200] via 192.168.2.2, 00:11:57, FastEthernet0/0
PE1-Maputo#
```

7. Teste de conectividade entre PE1 para interface de *loopback*

```
PE1-Maputo#ping 2.2.2.2 source 1.1.1.1 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 16/28/44 ms
PE1-Maputo#ping 3.3.3.3 source 1.1.1.1 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 12/26/44 ms
PE1-Maputo#ping 4.4.4.4 source 1.1.1.1 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 16/57/88 ms
PE1-Maputo#
```

8. Configuração de MPLS e LDP entre os roteadores PE e P.

Com a infra-estrutura IP configurada e com todos os roteadores tendo conectividade com todas as redes do provedor de serviço a próxima fase é configurar o MPLS nos equipamentos.

É possível criar os LSP's estaticamente, assim como com as rotas, porém, não é prático. Para realizar esta configuração de maneira dinâmica, é possível utilizar o protocolo LDP.

De forma a poder trocar informações de label's para construir os LSP's, um roteador deve fazer a descoberta dos outros elementos na rede, em sua forma mais básica, o LDP faz essa descoberta através do envio de pacotes de *Hello* para o endereço de ***multicast* 224.0.0.2** usando a porta UDP 646 em todas as interfaces com o protocolo habilitado.

Para habilitar o LDP, basta configurar ***mpls label protocol* ldp** globalmente e habilitar ***mpls ip*** globalmente e nas interfaces.

A documentação do fabricante também indica ser necessário a configuração do Cisco ***Express Forwarding* (CEF)** globalmente, através do **comando IP CEF**. Esta funcionalidade já estava configurada por padrão no equipamento utilizado para esta simulação.

9. Verificação do CEF com pipe

```
PE1-Maputo#show run | include ip cef
ip cef
PE1-Maputo#
```

10. Configuração de MPLS e LDP no PE1

```
PE1-Maputo#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1-Maputo(config)#mpls label protocol ldp
PE1-Maputo(config)#mpls ip
PE1-Maputo(config)#interface Fa0/0
PE1-Maputo(config-if)#mpls ip
PE1-Maputo(config-if)#
*Mar  1 01:07:38.367: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (1) is UP
PE1-Maputo(config-if)#interface Fa2/0
PE1-Maputo(config-if)#mpls ip
PE1-Maputo(config-if)#

PE1-Maputo#
*Mar  1 01:16:27.855: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (2) is UP
PE1-Maputo#
```

11. Verificação dos parâmetros configurados para LDP

É possível verificar os valores dos parâmetros configurados para a LDP através do comando ***show mpls ldp parameters***

```
PE1-Maputo#show mpls ldp parameters
Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
Downstream on Demand Path Vector Limit: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
PE1-Maputo#
```

12. Operação do LDP

Para saber se os valores estão a enviar e receber o pacote *hello* do LDP pode-se executar o comando ***showw mpls ldp discovery detail***

```
PE1-Maputo#show mpls ldp discovery detail
 Local LDP Identifier:
    1.1.1.1:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/0 (ldp): xmit/recv
            Enabled: Interface config
            Hello interval: 5000 ms; Transport IP addr: 1.1.1.1
            LDP Id: 2.2.2.2:0
              Src IP addr: 192.168.2.2; Transport IP addr: 2.2.2.2
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Reachable via 2.2.2.2/32
        FastEthernet2/0 (ldp): xmit/recv
            Enabled: Interface config
            Hello interval: 5000 ms; Transport IP addr: 1.1.1.1
            LDP Id: 3.3.3.3:0
              Src IP addr: 192.168.5.1; Transport IP addr: 3.3.3.3
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Reachable via 3.3.3.3/32
PE1-Maputo#
```

```
PE1-Maputo#show mpls ldp discovery
 Local LDP Identifier:
    1.1.1.1:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/0 (ldp): xmit/recv
            LDP Id: 2.2.2.2:0
        FastEthernet2/0 (ldp): xmit/recv
            LDP Id: 3.3.3.3:0
PE1-Maputo#
```

13. Interfaces de MPLS

```
PE1-Maputo#
PE1-Maputo#show mpls interfaces
Interface              IP            Tunnel   Operational
FastEthernet0/0        Yes (ldp)     No       Yes
FastEthernet2/0        Yes (ldp)     No       Yes
PE1-Maputo#
```

```
PE1_Maputo#show mpls interfaces detail
Interface FastEthernet0/0:
        IP labeling enabled (ldp):
          Interface config
        LSP Tunnel labeling not enabled
        BGP tagging not enabled
        Tagging operational
        Fast Switching Vectors:
          IP to MPLS Fast Switching Vector
          MPLS Turbo Vector
        MTU = 1500
Interface FastEthernet2/0:
        IP labeling enabled (ldp):
          Interface config
        LSP Tunnel labeling not enabled
        BGP tagging not enabled
        Tagging operational
        Fast Switching Vectors:
          IP to MPLS Fast Switching Vector
          MPLS Turbo Vector
        MTU = 1500
PE1_Maputo#
```

14. Verificação dos roteadores vizinhos através do LDP

```
PE1-Maputo#show mpls ldp neighbor
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 3.3.3.3.43057 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 69/57; Downstream
        Up time: 00:50:15
        LDP discovery sources:
          FastEthernet2/0, Src IP addr: 192.168.5.1
        Addresses bound to peer LDP Ident:
          192.168.4.2     192.168.5.1     3.3.3.3
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.18662 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 48/42; Downstream
        Up time: 00:31:38
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.2.2
        Addresses bound to peer LDP Ident:
          192.168.2.2     192.168.3.1     2.2.2.2
PE1-Maputo#
```

Nota: A vantagem do comando ***show mpls ip binding*** é que também mostra qual rótulo de todas possíveis ligações remotas são usadas para encaminhar o tráfego que indica o rótulo de saída na **LFIB**.

15. Verificação dos rótulos associados as rotas

```
PE1-Maputo#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     2.2.2.2/32       0          Fa0/0       192.168.2.2
17     Pop tag     3.3.3.3/32       0          Fa2/0       192.168.5.1
18     18          4.4.4.4/32       0          Fa2/0       192.168.5.1
19     Pop tag     192.168.4.0/24   0          Fa2/0       192.168.5.1
20     Pop tag     192.168.3.0/24   0          Fa0/0       192.168.2.2
```

16. Configuração da VRF nos roteadores PE1 e PE2

Nome da VRF	**PE1-Maputo**	**PE2-Quelimane**
Politécnica		
Politécnica		
Route distinguisher RD	**1:111**	**1:111**
Route Target		
CE-Maputo Both	**1:100**	**1:100**
CE-Quelimane Both	**1:100**	**1:100**
Interfaces de implementação		
CE-Maputo	**Fa0/1**	
CE-Quelimane		**Fa2/0**

Tabela 4 - Detalhe da VRF.

Fonte: (Autor)

- VRF no PE1

```
PE1-Maputo(config)#!
PE1-Maputo(config)#ip vrf Politecnica
PE1 Maputo(config vrf)#rd 1:111
PE1 Maputo(config vrf)#route target import 1:100
PE1-Maputo(config-vrf)#route-target export 1:100
PE1-Maputo(config-vrf)#exit
PE1-Maputo(config)#interface Fa0/1
PE1-Maputo(config-if)#ip vrf forwarding Politecnica
% Interface FastEthernet0/1 IP address 192.168.1.2 removed due to enabling VRF Pol
itecnica
PE1-Maputo(config-if)#!
PE1-Maputo(config-if)#!
PE1-Maputo(config-if)#!
PE1 Maputo(config if)#IP address 192.168.1.2 255.255.255.0

PE1-Maputo#ping vrf Politecnica 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/38/64 ms
PE1-Maputo#ping vrf Politecnica 192.168.1.1 repeat 10

Type escape sequence to abort.
Sending 10, 100 byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 20/35/68 ms
PE1-Maputo#
```

- VRF no PE2

```
Password:
Password:
PE2-Quelimane#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE2-Quelimane(config)#!
PE2-Quelimane(config)#ip vrf Politecnica
PE2-Quelimane(config-vrf)#rd 1:111
PE2 Quelimane(config vrf)#route target import 1:100
PE2 Quelimane(config vrf)#route target export 1:100
PE2 Quelimane(config vrf)#exit
PE2-Quelimane(config)#interface Fa2/0
PE2-Quelimane(config-if)#ip vrf forwarding Politecnica
% Interface FastEthernet2/0 IP address 192.168.6.2 removed due to enabling VRF Pol
itecnica
PE2-Quelimane(config-if)#!
PE2-Quelimane(config-if)#!
PE2-Quelimane(config-if)#!
PE2-Quelimane(config-if)#ip address 192.168.6.2 255.255.255.0
PE2-Quelimane(config-if)#exit
PE2-Quelimane(config)#do ping vrf Politecnica 192.160.6.1 repeat 10

Type escape sequence to abort.
Sending 10, 100 byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
.!!!!!!!!!
Success rate is 90 percent (9/10), round-trip min/avg/max = 4/43/116 ms
PE2-Quelimane(config)#
```

17. Configuração do EIGRP no PE1

```
PE1-Maputo#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1-Maputo(config)#router eigrp 65001
PE1-Maputo(config-router)#address-family ipv4 vrf Politecnica
PE1-Maputo(config-router-af)#autonomous-system 2
PE1-Maputo(config-router-af)#network 192.168.1.0 0.0.0.255
PE1-Maputo(config-router-af)#
*Mar  1 03:01:51.959: %DUAL-5-NBRCHANGE: IP-EIGRP(1) 2: Neighbor 192.168.1.1 (Fast
Ethernet0/1) is up: new adjacency
PE1-Maputo(config-router-af)#
PE1-Maputo(config-router-af)#no auto-summary
PE1-Maputo(config-router-af)#
*Mar  1 03:02:07.107: %DUAL-5-NBRCHANGE: IP-EIGRP(1) 2: Neighbor 192.168.1.1 (Fast
Ethernet0/1) is resync: summary configured
```

18. Configuração do EIGRP no PE2

```
PE2-Quelimane#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE2-Quelimane(config)#router eigrp 65001
PE2-Quelimane(config-router)#address-family ipv4 vrf Politecnica
PE2-Quelimane(config-router-af)#autonomous-system 3
PE2-Quelimane(config-router-af)#network 192.168.6.0 0.0.0.255
PE2-Quelimane(config-router-af)#
*Mar  1 03:33:41.843: %DUAL-5-NBRCHANGE: IP-EIGRP(1) 3: Neighbor 192.168.6.1 (Fast
Ethernet2/0) is up: new adjacency
PE2-Quelimane(config-router-af)#no auto-summary
PE2-Quelimane(config-router-af)#
*Mar  1 03:33:51.295: %DUAL-5-NBRCHANGE: IP-EIGRP(1) 3: Neighbor 192.168.6.1 (Fast
Ethernet2/0) is resync: summary configured
PE2-Quelimane(config-router-af)#exit
PE2-Quelimane(config-router)#
PE2-Quelimane(config-router)#
```

19. Análise das redes aprendidas entre CE e PE na VRF

```
PE2-Quelimane(config-router)#do show ip eigrp vrf Politecnica neighbor
IP-EIGRP neighbors for process 3
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.6.1             Fa2/0             7 00:01:29   66   396  0  4
PE2-Quelimane(config-router)#
```

```
PE2-Quelimane#show ip route vrf Politecnica eigrp
     10.0.0.0/24 is subnetted, 4 subnets
D       10.7.7.0 [90/261120] via 192.168.6.1, 00:02:33, FastEthernet2/0
D       10.6.6.0 [90/261120] via 192.168.6.1, 00:02:33, FastEthernet2/0
D       10.5.5.0 [90/261120] via 192.168.6.1, 00:02:33, FastEthernet2/0
D       10.4.4.0 [90/261120] via 192.168.6.1, 00:02:33, FastEthernet2/0
PE2-Quelimane#
```

20. Teste de conectividade entre a VRF e as subinterfaces associadas às VLAN's

```
PE2-Quelimane#ping vrf Politecnica 10.7.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/60/104 ms
PE2-Quelimane#ping vrf Politecnica 10.6.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/45/60 ms
PE2-Quelimane#ping vrf Politecnica 10.5.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/35/52 ms
PE2-Quelimane#
```

21. Configuração de redistribuição de rotas entre EIGRP AS 3 e iBGP no roteador PE2

```
PE2-Quelimane#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
PE2-Quelimane(config)#router bgp 65001
PE2-Quelimane(config-router)#address-family ipv4 vrf Politecnica
PE2-Quelimane(config-router-af)#redistribute eigrp 3
PE2-Quelimane(config-router-af)#exit
PE2-Quelimane(config-router)#router eigrp 65001
PE2-Quelimane(config-router)#address-family ipv4 vrf Politecnica
PE2-Quelimane(config-router-af)#$e bgp 65001 metric 10000 1000 255 1 1500
PE2-Quelimane(config-router-af)#do show ip route vrf Politecnica
```

22. Configuração de redistribuição de rotas entre EIGRP AS 3 e iBGP no roteador PE1

```
PE1-Maputo(config)#router bgp 65001
PE1-Maputo(config-router)#address-family ipv4 vrf Politecnica
PE1-Maputo(config-router-af)#
*Mar  1 04:25:48.262: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.5.1 (Fast
Ethernet2/0) is down: holding time expired
*Mar  1 04:25:48.378: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.5.1 (Fast
Ethernet2/0) is up: new adjacency
PE1-Maputo(config-router-af)#redistribute eigrp 2
PE1-Maputo(config-router-af)#exit
PE1-Maputo(config-router)#router eigrp 65001
PE1-Maputo(config-router)#address-family ipv4 vrf Politecnica
PE1-Maputo(config-router-af)#redistribute bgp 65001 metric 5000 500 255 1 1500
PE1-Maputo(config-router-af)#
```

23. Análise da secção estabelecida de GBP sendo que BGP usa o ***handshak*** triplo para estabelecer a secção com pares de BGP usando TCP porta 179

```
PE1-Maputo#show tcp brief
TCB        Local Address               Foreign Address             (state)
650C2BE4   1.1.1.1.646                 3.3.3.3.43057               ESTAB
650C2230   1.1.1.1.646                 2.2.2.2.18662               ESTAB
6751E38C   1.1.1.1.179                 4.4.4.4.34584               ESTAB
PE1-Maputo#
```

24. Análise dos vizinhos de BGP

```
PE1-Maputo#show ip bgp neighbors
BGP neighbor is 4.4.4.4,  remote AS 65001, internal link
  BGP version 4, remote router ID 4.4.4.4
  BGP state = Established, up for 00:20:28
  Last read 00:00:18, last write 00:00:27, hold time is 180, keepalive interval is
 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  2          2
    Notifications:          0          0
    Updates:                3          4
    Keepalives:            35         35
    Route Refresh:          0          0
```

25. Análise da tabela de roteamento no PE1 e as redes aprendidas na VRF Politécnica

```
PE1-Maputo#show ip route vrf Politecnica

Routing Table: Politecnica
Codes: C   connected, S   static, R   RIP, M   mobile, B   BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1   OSPF external type 1, E2   OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o   ODR, P   periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 8 subnets
D       10.7.7.0 [200/261120] via 4.4.4.4, 00:31:39
B       10.6.6.0 [200/261120] via 4.4.4.4, 00:31:39
B       10.5.5.0 [200/261120] via 4.4.4.4, 00:31:39
B       10.4.4.0 [200/261120] via 4.4.4.4, 00:31:39
D       10.3.3.0 [90/284160] via 192.168.1.1, 02:10:09, FastEthernet0/1
D       10.2.2.0 [90/284160] via 192.168.1.1, 02:10:09, FastEthernet0/1
D       10.1.1.0 [90/284160] via 192.168.1.1, 02:10:09, FastEthernet0/1
D       10.0.0.0 [90/284160] via 192.168.1.1, 02:10:11, FastEthernet0/1
B    192.168.6.0/24 [200/0] via 4.4.4.4, 00:31:41
C    192.168.1.0/24 is directly connected, FastEthernet0/1
PE1-Maputo#
```

26. Teste de conectividade entre CE-Maputo e CE-Quelimane usando VLAN 400 cmo Origem

```
CE-Maputo#ping 10.7.7.1 source 10.3.3.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 10.7.7.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 72/134/252 ms
CE-Maputo#ping 10.6.6.1 source 10.3.3.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 10.6.6.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 76/122/140 ms
CE-Maputo#ping 10.5.5.1 source 10.3.3.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 10.5.5.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 68/122/160 ms
CE-Maputo#ping 10.5.5.1 source 10.3.3.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 10.5.5.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 92/169/376 ms
CE-Maputo#
```

27. Teste de conectividade entre CE-Maputo e CE-Quelimane através do *traceroute*

```
CE-Maputo#traceroute 10.4.4.1

Type escape sequence to abort.
Tracing the route to 10.4.4.1

  1 192.168.1.2 44 msec 112 msec 88 msec
  2 192.168.5.1 [MPLS: Labels 18/24 Exp 0] 216 msec 228 msec 188 msec
  3 192.168.6.2 [MPLS: Label 24 Exp 0] 144 msec 144 msec 144 msec
  4 192.168.6.1 216 msec 224 msec 156 msec
CE-Maputo#
```

4.6.5 Voz sobre IP

- Primeira etapa o telefone obtém energia do *switch* através da porta *ethernet* com o uso da tecnologia PoE (*Power Over Ethernet*) neste caso é necessário que o *switch* tenha a capacidade de suportar essa funcionalidade, por padrão essa função já vem activa nos switches do cisco;
- O telefone IP carrega a configuração local;
- O *switch* permite informar o telefone IP sobre a VLAN de voz através do CDP ou LLDP;
- O Telefone IP necessita de um IP para se comunicar com outros telefones IP na rede esse IP pode ser estático ou dinâmico. Endereçamento IP estático é ideal para rede infra-estrutura pequena. Redes corporativas geralmente têm diversos dispositivos se torna um problema fazer a gestão de atribuição de IP, neste caso o servidor DHCP poder ser usado para satisfazer essas necessidades nesse projecto, o servidor DHCP será simulado integrado no roteador de modo a permitir atribuição de IP de forma dinâmica para telefones sobre IP e utilizadores finais;
- O Telefone voz sobre IP faz o download da configuração no servidor TFTP instruído através do DHCP option 150;
- O telefone IP se regista ao Cisco *Unified communication manager* CUCM.

4.7.6.1 Configuração da infra-estrutura de tráfego de voz

1. Configuração de servidor DHCP no roteador

```
CE-Maputo#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CE-Maputo(config)#ip dhcp excluded-address 10.1.1.1 10.1.1.10
CE-Maputo(config)#IP DHCP pool voz
CE-Maputo(dhcp-config)#network 10.1.1.1 /24
CE-Maputo(dhcp-config)#default-router 10.1.1.1
CE-Maputo(dhcp-config)#dns-server 8.8.8.8
CE-Maputo(dhcp-config)#domain-name apolitecnica.ac.mz
CE-Maputo(dhcp-config)#option 150 ip 10.1.1.1
CE-Maputo(dhcp-config)#exit
CE-Maputo(config)#
CE-Maputo(config)#
```

2. Configuração de servidor NTP no roteador

```
CE-Maputo(config)#clock timezone Harare 02 00
CE-Maputo(config)#
*Mar  1 00:17:55.931: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:17
:55 Harare Fri Mar 1 2002 to 02:17:55 Harare Fri Mar 1 2002, configured from conso
le by console.
CE-Maputo(config)#clock summer-time Harare recurring
CE-Maputo(config)#
*Mar  1 00:19:03.875: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:19
:03 Harare Fri Mar 1 2002 to 02:19:03 Harare Fri Mar 1 2002, configured from conso
le by console.
CE-Maputo(config)#end
CE-Maputo#clo
*Mar  1 00:19:18.335: %SYS-5-CONFIG_I: Configured from console by console
CE-Maputo#clock set 01:30:00 1 August 2018
CE-Maputo#
*Jul 31 22:30:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:21
:31 Harare Fri Mar 1 2002 to 01:30:00 Harare Wed Aug 1 2018, configured from conso
le by console.
CE-Maputo#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CE-Maputo(config)#ntp master 1
CE-Maputo(config)#
```


3. Configuração básica do *switch* e das VLAN'S

```
SWA1(config)#VLAN 100
SWA1(config-vlan)#name Banco de Dados
SWA1(config-vlan)#exit
SWA1(config)#VLAN 200
SWA1(config-vlan)#name Voz
SWA1(config-vlan)#exit
SWA1(config)#VLAN 300
SWA1(config-vlan)#Name Nativa
SWA1(config-vlan)#exit
SWA1(config)#VLAN 400
SWA1(config-vlan)#Name Gerenciamento
SWA1(config-vlan)#exit
SWA1(config)#!
```

4. Associação das VLAN’s às interfaces de tronco, acesso e voz

```
SWA1(config)#interface G0/1
SWA1(config-if)#Switchport trunk encapsulation dot1q
SWA1(config-if)#switchport mode trunk
SWA1(config-if)#Switchport trunk allowed vlan 100,200,300,400
SWA1(config-if)#exit
SWA1(config)#interface G0/0
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport voice vlan 200
SWA1(config-if)#exit
SWA1(config)#interface G0/2
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 100
SWA1(config-if)#exit
```

```
SWA1#show run | begin interface GigabitEthernet0/0
interface GigabitEthernet0/0
 switchport mode access
 switchport voice vlan 200
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 100,200,300,400
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 300
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 switchport access vlan 100
 switchport mode access
 media-type rj45
```

5. Verificação da VLAN

```
SWA1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/3, Gi1/0, Gi1/1
                                                Gi1/2, Gi1/3, Gi2/0, Gi2/1
                                                Gi2/2, Gi2/3, Gi3/0, Gi3/1
                                                Gi3/2, Gi3/3
100  Banco de Dados                   active    Gi0/2
200  Voz                              active    Gi0/0
300  Nativa                           active
400  Gerenciamento                    active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SWA1#
```

6. Verificação do Tronco

```
SWA1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/1       on               802.1q         trunking      300

Port        Vlans allowed on trunk
Gi0/1       100,200,300,400

Port        Vlans allowed and active in management domain
Gi0/1       100,200,300,400

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       100,200,300,400
SWA1#
```

7. Verificação do Servidor DHCP

```
CE-Maputo#show ip dhcp pool

Pool voz :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.1.1.1             10.1.1.1         - 10.1.1.254       0
CE-Maputo#
```

8. Configuração de serviços de telefone IP no CE-Maputo e configuração para realização de chamada para telefone 5061 localizado em Quelimane

```
dial-peer voice 5061 voip
 description WAN calls
 destination-pattern 50[0-9]
 session target ipv4:192.168.6.1
!
!
!
!
telephony-service
 no auto-reg-ephone
 max-ephones 2
 max-dn 5
 ip source-address 10.1.1.1 port 2000
 max-conferences 8 gain -6
 transfer-system full-consult
!
!
ephone-dn  1  dual-line
 number 5060
!
!
ephone  1
 device-security-mode none
 mac-address 0200.4C4F.4F50
 button  1:1
!
```

CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES

O presente projecto foi realizado com o propósito de dimensionar uma rede privada virtual utilizando a tecnologia MPLS, permitindo assim a comunicação entre a sede da Universidade A Politécnica em Maputo e a sua delegação na cidade de Quelimane, onde foi possível tirar as seguintes conclusões:

- O MPLS é uma tecnologia que provê uma das melhores soluções de VPN com diferenciação de classes de serviços, o que a torna numa solução atractiva para empresas que desejam comunicar pontos geograficamente distantes, com garantia de disponibilidade, elevadas taxas de transmissão, facilidade de instalação e segurança;
- Observando-se a situação actual da Universidade A Politécnica em termos de comunicação, a tecnologia MPLS é vista como a melhor solução para prover comunicação entre a sede e as suas delegações, visto que, as VPN MPLS garantem mecanismos acessíveis de escalabilidade;
- No dimensionamento realizado foi possível garantir priorização de banda para as aplicações consideradas como sendo de maior nível de prioridade, através do mecanismo de diferenciação de classes de serviços disponível na solução VPN MPLS com QoS.
- Com auxílio do simulador GNS3, foi possível simular a configuração de uma rede MPLS, bem como a configuração da VPN que consistiu na criação da VRF nos *routers* PE e associação das suas respectivas interfaces à mesma. Com a configuração da VRF foi possível comprovar a segurança da VPN MPLS, visto que com o conceito de *Route Distingisher* e *Route Target*, torna-se impossível que os tráfegos de uma VPN sejam recebidos em outra VPN partilhando os mesmos equipamentos PE. A escalabilidade da VPN MPLS é de fácil e rápida implementação, pois consiste apenas na associação de uma nova interface a VRF já existente. As configurações de QoS podem ser feitas tanto a nível da rede do cliente bem como na rede do provedor, sendo que na presente simulação as configurações foram feitas nos *routers* do cliente para permitir uma melhor gestão e controle dos mecanismos de priorização de trafego, utilizando planos de classificação e priorização de tráfegos privados.

Tendo em conta o estudo realizado e as conclusões tiradas, para o presente projecto, recomenda-se:

- O dimensionamento de uma VPN-MPLS interligando as restantes delegações da Universidade à sede, com um plano de gestão de toda rede a partir da sede em Maputo;
- A realização de um estudo sobre como implementar a tecnologia VoIP (voz sobre IP) sobre a VPN-MPLS;
- A realização de um estudo sobre como dimensionar e implementar o serviço de videoconferência sobre IP, na VPN-MPLS da Universidade A Politécnica.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Collins, Daniel. (2004) *Carrier Grade Voice over IP*. 2nd Edition: McGraw-Hill Networking. Acedido a 13 de Abril de 2017. http://www.voiceip.com.ua/lit/Carrier%20Grade%20Voice%20Over%20IP.pdf.
2. Celestino, Pedro. (2005) *Redes Virtuais Privadas*. São Paulo – Bras
3. Chowdhury, Dhiman D. (2002). *Projetos Avançados de Redes IP*. 1ª Ed. Rio de Janeiro: Campus.
4. Cisco. (2014) *Cisco 1941 Series Integrated Services Router.* Acedido a 3 de Julho de 2018. https://www.cisco.com/c/en/us/products/routers/1941-integrated-services-routerisr/index.html.
5. Cisco. (2016) *Voz sobre IP – Consumo de largura de banda por chamada.* Acedido a 5 de Julho de 2018. Https://www.cisco.com/c/pt_br/support/docs/voice/voice-quality/7934-bwidth-consume.html.
6. Davidson, Jonathan, J. Peters, M. Bhatia, S. Kalindindi e S. Mukherjee. (2007) *Voice over IP Fundamentals*. 2ª Ed. Indianápolis: Cisco Press.
7. Eusébio, Francisco. (2010) *Redes de Telecomunicações*. 1ª edição Lisboa: Edições Silabo, Lda.
8. Filippetti, Marcos A. (2002) *CCNA 3.0 – Guia Completo de Estudo*. Florianópolis: Visual Books.
9. Itinstock. (2013) Cisco 3700 Series Cisco 3725 *Multiservice Access Router.* Acedido a 15 de Novembro de 2018. Https://www.itinstock.com/cisco-3700-series-cisco-3725-multiservice-access-router-11962-p.asp.
10. Kurose, James and Keith Ross. (2010) *Computer Networking: a top down approach featuring the Internet*. 4ª ed. Boston: Addison-Wesley.
11. Lewis, Cris. (1999) *Cisco TCP/IP Routing Professional Reference*. Nova Iorque: McGraw-Hill.
12. Miranda, Ivana Cardial. (2002) *VPN - Virtual Private Network*. Acedido a 22 de Fevereiro de 2017. https://www.gta.ufrj.br/seminarios/semin2002_1/Ivana/.
13. Marleta, Marcelo H. (2007) *Projecto de uma VPN (Rede Privada Virtual) baseada em computação reconfigurável e aplicada a robôs móveis.*
14. Mata, René Sousa. (2002) *Dimensionamento de Enlaces em Redes com Integração de Serviços*. São Paulo;

15. Odom, Wendell e Michael Cavanaugh. (2004) *IP Telephony Self-Study Cisco DQOS*. Indianápolis: Cisco Press.
16. Rosen, E., R. Callon, A. Viswanathan. (2001) *Multiprotocol label switching architecture*. RFC 3031. Acedido a 12 de Setembro de 2016. https://tools.ietf.org/html/rfc3031.
17. Santos, Renato Cesconetto. (2003) *Um estudo do Uso da Tecnologia MPLS emBackbones no Brasil*. Florianópolis, Brasil. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/85199/192602.pdf?sequence=1.
18. Sites. Cisco 3725 Original Layout: *Router Modification.* Acedido a 15 de Novembro de 2018. Https://sites.google.com/site/routermodification/home/step-by-step.
19. TALARI Networks. *A Brief History of MPLS*. Acedido ao 28 de Maio de 2018. https://www.talari.com/blog/brief-history-mpls/.
20. Tanenbaum, Andrew S. *Redes de computadores*: Editora Campus.

BIBLIOGRAFIA

1. Boava, Adão. (2004) Estratégia de Projeto de VPNs MPLS com Qualidade de Serviço. Dissertação de Mestrado, Universidade Estadual de Campinas.
2. Boava, Adão. (2011) Contribuição e Avaliação das Arquitecturas para as VPN's Convergentes com Escalabilidade, Segurança e Qualidade de Serviço. Tese de Doutoramento, Universidade Estadual de Campinas.
3. Cabrera, Yicel Frias. (2015) *Redes de Telecomunicação: Multiprotocol Label Switching (MPLS).* Maputo: Instituto Superior de Transportes e Comunicações.
4. Celestino, Pedro. 2005. *Redes Virtuais Privadas*. São Paulo –Brasil.
5. Lins, R. D., D. Barbosa e V. Nascimento. (2011) *VoIP – Conceitos e Aplicações*. 1ª ed. Rio de Janeiro: Brasport.
6. Mendes, Eloy Tavares. (2011) *Avaliação dos Serviços Voip em Links de Baixa Capacidade com Tráfego Compartilhado de Dados*. Niterói;
7. Nakamura, Juliana Akeme. (2009*) Evolução das Redes de Telecomunicação e o Multiprotocol Label Switching (MPLS).* São Carlos.
8. Oliveira, J. M., R. D. Lins e R. Mendonça. (2012) *Redes MPLS: Fundamentos e Aplicações*. Rio de Janeiro: BRASPORT.
9. Silva, L.S. (2002) *Virtual Privat Network – VPN*. Novatec.
10. Silva, Roberto Correia. (2010) *Optimização do sistema de comunicação da Aon Subsaariana implementando tecnologia Voz sobre IP sobre a WAN existente*. Maputo: Instituto Superior de Transportes e Comunicações.
11. Vapi, P. & Bernardes M. & Boavida, F. (2009) *ADMINISTRAÇÃO DE REDES INFORMÁTICAS*. Lisboa:FCA

ANEXOS

ANEXO I – Entrevista à equipe de Administração

ANEXO II – Entrevista à equipe representante da repartição de informática

ANEXO III – Proposta Técnica da Teledata para o fornecimento do serviço VPN-MPLS

ANEXO IV – Custo e Especificações Técnicas do *Router* Cisco 3725 Series

Anexo I – Entrevista à equipe de Administração

1. Como é que esta organizada a Universidade Politécnica de Maputo?
2. Como é que esta organizada a Universidade Politécnica de Quelimane?

Anexo II – Entrevista à equipe representante da repartição de Informática

1. Como é que esta organizada a rede da Universidade Politécnica de Maputo?
2. Como é que esta organizada a Universidade Politécnica de Quelimane?
3. A gestão da rede está centralizada?
4. Quais são os principais constrangimentos enfrentados a nível das TIC's?
5. Existe uma rede pela qual permite a partilha de dados?

ANEXO III - PROPOSTA TÉCNICA DA TELEDATA PARA O FORNECIMENTO DO SERVIÇO VPN-MPLS

1. Descrição dos Equipamentos a Instalar

Segue abaixo as características dos equipamentos de roteamento a fornecer Router Cisco a instalar em cada local:

P/N	*Descrição*	*Qtd*
Cisco 1941	Modular Router w/2xGE, 2 WAN slots. 256 FL/512 DR	1
CAB-ACE	Power Cord Europe	1
CAB-ETH_S_RJ45	Yellow Cable for Ethernet, Straght-throught. RJ-45, 6 feet	1
WIC-1T	1-Port Serial WAN Interface Card	1
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	1

Tabela 5 – Características do *Router* Cisco 1941.
Fonte: (AUTOR)

2. Alimentação Eléctrica

É da responsabilidade da Universidade Politécnica dotar as instalações de energia eléctrica, o consumo de corrente eléctrica dos equipamentos da Teledata a instalar por site corresponde a

650W (220v AC), devendo ser alimentado num ponto de energia “limpa” e estável. Assim é crucial que a Universidade Politécnica preveja uma UPS de 1KVA do tipo *online*.

Em caso de inexistência deste requisito, a Universidade Politécnica responsabilizar-se-á pela reparação do equipamento de comunicações que avarie por oscilação de corrente, mesmo que o equipamento esteja dentro da garantia.

3. Qualidade de Serviços – Acordos de Níveis de Serviço (SLA)

No acto da assinatura do contrato será igualmente assinando um acordo sobre a Qualidade de Serviço a prestar (SLA), com o comprometimento de envio mensal de um relatório com os indicadores de QoS e, em caso de necessidade, propostas de melhorias e *upgrades*.

3.1. Padrões de Desempenho e Qualidade

A Teledata compromete-se a prestar Serviços de Dados, com base nos seguintes parâmetros de qualidade:

- Disponibilidade do Serviço;
- Prazo de entrega do Serviço.

O período de observação a ser considerado para efeito de cálculo dos parâmetros acima referidos será de 1 (um) mês, ou seja, será considerado o período compreendido entre o primeiro e o ultimo dia do mês em que o Serviço foi prestado ao cliente.

Caso não sejam atingidos os índices estabelecidos, a Teledata estará sujeita ao pagamento das penalidades estabelecidas no presente SAL, cujos percentuais incidirão sobre o valor mensal do Serviço contratado pelo Cliente, sem impostos e contribuições.

No que se refere à disponibilidade, em situação de avaria, a Teledata efectuará o seu maior esforço na sua reparação, garantindo uma disponibilidade média mensal de 98.0% (noventa e oito por cento), excepto se a avaria for devida a motivos de força maior.

O índice de disponibilidade, compreende os serviços, os equipamentos e os meios fornecidos pela Teledata nos respectivos endereços do cliente (fim a fim).

O índice de disponibilidade corresponde a cada um dos acessos contratados para o fornecimento de serviço e a penalidade, em caso de incumprimento, será aplicada única e exclusivamente à mensalidade do acesso penalizado.

ANEXO IV – CUSTO E ESPECIFICAÇÕES TÉCNICAS DO *ROUTER* CISCO 3725 SERIES

Router Cisco	Preço (USD)	Câmbio do dia (22/05/17)	Preço (MZN)
3725 Series	2.836,36	61,45	174.294,32

Tabela 6 – Custo do *Router* Cisco 3725 Series.

Fonte: (AUTOR)

Figura 20 – Custo do *Router* Cisco 3725 Series.

Fonte: (ITINISTOCK 2013)

Figura 21 – Cisco 3700 Series *multiservice-access-router Interfaces*.

Fonte: (SITES n.d.)

Especificações Técnicas do *router* cisco 3725 Series

I

GENERAL /	
Flash Memory	32 MB (installed) / 128 MB (max)
Enclosure Type	Rack-mountable - modular - 2U
Manufacturer	Cisco
CAMERA /	
Installed Size	32 MB
NETWORKING /	
Form Factor	rack-mountable
Type	router
Connectivity Technology	wired
Data Link Protocol	ATM, Ethernet, Fast Ethernet, HSSI, ISDN, X.25
Features	manageable, modular design
POWER DEVICE /	
Nominal Voltage	AC 120/230 V
Frequency Required	50/60 Hz
Type	internal power supply
INTERFACE PROVIDED /	
Type	management, network, serial
Interface	Ethernet 10Base-T/100Base-TX, auxiliary, console
Qty	1, 2

II

PROCESSOR /	
Type	RM7061A
Installed Qty	1
Manufacturer	PMC-Sierra
Clock Speed	240 MHz

POWER /	
Installed Qty	1 (Installed) / 2 (max)
Max Supported Qty	2

MISCELLANEOUS /	
Rack Mounting Kit	optional
Height (Rack Units)	2 m

CHASSIS /	
Installed Devices / Modules Qty	1
Supported Devices / Modules Qty	8

MEMORY /	
Form Factor	CompactFlash Card

RAM /	
Installed Size	256 MB
Max Supported Size	256 MB
Technology	SDRAM

III

IP TELEPHONY /	
VoIP Protocols	H.323, MGCP, SIP v2
Voice Codecs	G.723, G.726, G.728, G.729, G.729a
VoIP	Yes

FLASH MEMORY /	
Max Supported Size	128 MB

SOFTWARE / SYSTEM REQUIREMENTS /	
Type	Cisco IOS

ENVIRONMENTAL PARAMETERS /	
Min Operating Temperature	32 °F
Max Operating Temperature	104 °F
Humidity Range Operating	5 - 95%

HEADER /	
Brand	Cisco
Product Line	Cisco
Model	3725
Packaged Quantity	1
Compatibility	PC

EXPANSION BAYS /	
Type	none

IV

EXPANSION SLOTS /	
Type	memory
Total Qty	1, 2, 8
Free Qty	0, 7

SLOT REQUIRED /	
Type	none

DIMENSIONS & WEIGHT /	
Width	17.1 in
Depth	15 in
Height	3.5 in
Weight	14.11 lbs

OS PROVIDED /	
Type	Cisco IOS

GENERAL /	
Manufacturer	Cisco