Escola de Comunicação, Arquitetura, Artes e Tecnologias da Informação

---

Licenciatura Informática de Gestão

3º Ano | 2º Semestre | 2013/204

Relatório Trabalho Final de Curso

Trabalho realizado sob a orientação de:

Professor José Faísca

Maio 2014

Discentes: **Miguel Ferrão| 2203147**

Agradecimentos

Desde do ano académico de 2006/2007, que este trabalho está por entregar. Muitas desculpas seriam aqui expostas, mas de facto a realidade de estar longe, de ter embarcado num projeto profissional e pessoal noutro continente, fez com que esta tarefa fosse deixada para segundo plano (mas não esquecida).

Ao longo destes anos os meus Pais e Esposa sempre serviram de "voz da consciência" para que finaliza-se de uma vez este desafio, de forma a poder seguir em frente tanto academicamente como profissionalmente.

Academicamente porque ao fim destes anos, e apesar de não ter a licenciatura acabada fui acumulando créditos em cursos dentro da área de TI e projetos de forma a consolidar os conhecimentos mas sem nunca poder obter graus extra.

Profissionalmente porque devido às características do pais onde me encontro a exigência de ter uma licenciatura serve de fator eliminatório para a autorização de residência, fator que somado á regra interna da empresa onde trabalho para progressão de carreira fez de sobremaneira voltar para finalizar este trabalho.

Assim, com tal os primeiros agradecimentos são para os meus Pais (Orestes e Deolinda) e para a minha Esposa (Isadora) que sempre me deram apoio e animo para chegar aqui.

Não posso deixar de agradecer claro está ao **Professor Pedro Malta** que ao longo destes anos sempre foi quem tentou apoiar mesmo remotamente, e claro está foi durante no meu tempo de estudante um professor de referência sempre disposto a ajudar os alunos, mesmo tento na altura ele próprio um enorme desafio Académico e profissional.

Quero também agradecer á **Professora Alexandra Campos** que sempre foi excelente na forma como me aconselhou e orientou nos passos a seguir para retomar esta tarefa. Lembro a paciência que teve ao telefone para comigo e interagiu com o meu Pai com informações e orientações, pois eu estou fora de Portugal.

Por fim ao **Professor José Faisca**, que me deu orientação necessária para o trabalho, mesmo a 10 mil km de distância e com as dificuldades inerentes de fusos, agenda e ligações Internet.

Índice

Resumo

Atualmente no mercado de Telecom existe um variado *portfólio* de serviços e tecnologias desenhado para que os clientes possam escolher consoante o orçamento, necessidades técnicas do negócio, dispersão geografia, Know-how dentro da empresa e a necessidade de flexibilização de serviços.

Neste contexto, o foco deste trabalho é apresentar um caso prático onde as duas tecnologias/serviços foram aplicadas, fazendo não só a explanação técnica, contida nos anexos, mas também uma apresentação de configurações usadas de forma a dar uma melhor ideias dos ambientes e necessidades. O cenário usado, é o de numa empresa multinacional que devido ao crescimento e necessidade de aprovisionar os seus escritórios em variadas geografias com as limitações técnicas inerentes.

Inicialmente é mostrado o ambiente original e que foi usado durante uma fase de maturação da empresa numa dada geografia, mas que com o crescimento e aumento de serviços de rede (Voz, dados e Video) e outras necessidades teve de fazer uma restruturação de forma que pudesse cumprir com os objetivos.

Assim teremos num primeiro momento a utilização de *VPN IPSEC* ponto a ponto, como tecnologia usada para ligações internacionais, sofrendo das limitações nativas de ligações de Internet relativamente fracas, passando para um cenário de ligações de maior debito e tecnologias variadas, mas com uma arquitetura diferente como é o MPLS.

Por motivos de confidencialidade o nome das empresas provedoras e cliente foram alteradas para nomes diferentes e que permitam uma generalidade de casos e uma fácil entendimento durante o desenho da demonstração.

Abstract

Today's Service Provides offer list is full, with solutions that can serve to a wide range of clients depending of the business requirements, like budget and geographical locations; and technical requirements like Know-how and Services (Voice, Data and Video).

Based on that, this document rather than act as a technical compilation and a compilation between two of those services, will give a real world approach of a multinational company that had to migrate from one starting solution (IPSEC VPN) to a bigger and more professional (MPLS VPN).

This migration was caused by the needs to grow and add more services (Voice, Data and Video) to the network.

The document will use a generic scenario, where the real names of the Services Provides and the Client will be changed to a more generic name to provide a prototype environment.

Introdução

Este trabalho vem no seguimento de uma apresentação feita em 2007 durante um evento organizado pela Cisco, na qual eu participei como orador e onde foram expostas duas tecnologias de VPN focando um pouco a sua configuração, protocolos, ambientes bem como suas vantagens e desvantagens.

Apesar da distância temporal, o tema não perde importância nem sequer motivo de ser apresentado, pois se nos mercados de Telecom que já possuem as soluções e tecnologias a um preço de fácil acesso, nos mercados emergentes como Moçambique, onde vivo e trabalho a necessidade de flexibilizar a oferta por parte dos Provedores de Serviço, e a vontade de usar serviços mas a um custo rentável, cria oportunidades para a sua utilização.

No seguimento dessa ideia a decisão de apresentar um caso pratico onde de facto os dois tipos de VPN são aplicados foi fácil. Não só porque precisava de um tema para este documento, mas porque participei na implementação e na sua gestão.

Tecnicamente duas soluções muito destintas e com cargas administrativas bem diferentes para cliente e para provedor.

Temos em confronto uma VPN que é dependente em todo do lado do cliente apenas usando a Internet como meio de transporte, com uma tecnologia que "ignora" o que cliente tem do lado do seu escritório, pois toda a carga de configuração é feita do lado do Provedor, que poderá (consoante o tipo de cliente) incluir na prestação de Serviço equipamento de conectividade *Router* ou *Switch*.

Ambas *VPN's* são usadas em muitos cenários por esse mundo fora, e por vezes poderemos ter uma mistura de ambientes que devido a limitações (orçamentárias ou técnicas) permitem uma maior flexibilidade.

O principal objetivo deste trabalho é dar exemplo da sua aplicação usando o exemplo real de necessidades do negócio que levaram a uma enorme implementação que envolveu Provedor e cliente.

Ambas as tecnologias que são explicadas em mais detalhe no **Anexo 1,** bem como alguns termos estão incluídos no glossário.

O projecto "*Rede global*"

Toda a parte técnica apresentada foi baseada numa implementação que teve a designação de "Rede Global". Essa implementação teve lugar nos vários locais onde a empresa onde trabalho, tem escritórios e tinha como objetivo criar uma base de Telecomunicações que permitem-se a centralização de serviços de rede.

Sendo uma multinacional, o ambiente estava sujeito às limitações de cada geografia. Sendo que tínhamos localizações no meio da floresta Amazónica/Africana, estepes da Mongólia até localizações em várias cidades, tais como São Paulo, Toronto ou Maputo. Todas essas localizações tinham formas mais ou menos avançadas de conexão com a casa Mãe e consoante a capacidade dessa conexão tinham acesso a mais ou menos serviços.

No caso concreto de Moçambique, a empresa iniciou com uma conexão aos escritórios globais localizados no Brasil e no Canadá através de VPN ISEC.

Essa topologia apesar de barata em termos de telecomunicações, pois usava as ligações de Internet disponíveis nas várias localizações limitava um pouco o crescimento dos sites e a implementação de serviços e ideias corporativas tais como telefonia IP e Voz sobre IP, *Email* centralizado, *Office Comunicator* e Portais Internos que por razões de Segurança e de negócio tinham de estar numa Intranet.

Tínhamos um desafio enorme, pois como se não bastassem as ideias corporativas, existiam também duas migrações enormes que tinham de ser feitas, uma relacionada com a estrutura de *Active Directory* (AD), que ira passar para um único domínio. E a outra que era a criação de centros de Video conferência em determinadas localizações para que existissem menos viagens e mais reuniões de equipas que estavam espalhadas.

Assim e com tudo isso em vista, e com várias fases de implementação começamos o projeto de "Rede Global".

O Problema de infraestrutura (Cenário inicial)

No início da implementação (2008) da empresa na geografia onde eu me encontrava os meus colegas que a iniciaram, tiveram uns desafios bem interessantes e mesmo aquando da minha entrada em 2010 o cenário não era muito melhor.

Moçambique é um Pais de assimetrias sociais e económicas muito vincadas, fazendo com que os negócios tenham um pouco de cautela nos investimentos. Para além da sua dimensão geográfica, a falta de infraestruturas e estabilidade surge como barreira (apesar de ter melhorado muito).

Inicialmente esse investimento era centrado na capital do Pais (Maputo), cidade que durante muito tempo sofreu de uma falta de investimento e de manutenção, por razões que não me cabem discutir, mas que causaram um atraso no pais.

Em termos de telecomunicações as ofertas eram poucas e sempre baseadas em tecnologias um pouco "fracas" em termos de capacidade e escalabilidade. A Internet era um negócio interessante, que fez com que surgissem nalgumas cidades alguns Provedores de Internet regionais, que utilizando tecnologias sem fios ofereciam aos clientes ligações de baixo débito e partilhadas, fazendo depois uso de uma ligação por eles contratada os operador local e monopolista. Outras empresas com pouco mais de força económica conseguiam já oferecer serviços um pouco mais profissionais (mais caros) tais como ligações sem fios de alto débito (WIMAX ou pré-Wimax), VSAT's.

Para complicar mais as coisas a empresa estava localizada em vários pontos, um dos quais nem sequer energia, logo qualquer ideia de criar fosse o que fosse no local era algo "titânico".

Assim no início a empresa começou a criar as infraestruturas base para a poder construir escritórios e iniciar o seu projeto de negócio. Ao mesmo tempo o TI ia conforme podia e com recursos possíveis criar o ambiente TI para que as pessoas pudessem trabalhar.

Para dar um exemplo de um dos desafios, numa das localizações tivemos de levar ligações ***E1*** *de voz e conexão* de 2 *Mbit* ponto a ponto no meio do mato (literalmente). O operador público era o único que podia executar essa tarefa com a instalação de uma ligação rádio usando PDH. O motivo era simples, passar fibra naquela região era caro e corríamos o risco de ficar sem postes, pois a população decerto que iria cortar a madeira. Fazer condutas também, porque a distancia e investimentos seriam elevados, e na altura não havia ainda um mapa certo da zona de exploração da mina o que poderia implicar passar fibra onde mais tarde iria ser retirado minério.

Com o correr do tempo e com as constantes falhas do único operador, optamos por contratar uma conexão de VSAT para que tivéssemos redundância entre o escritório na capital e a zona de exploração e de implantação da mina. Esse VSAT para além de ter pouca largura de banda era muito caro, mas teve de ficar ativo durante um tempo.

Ainda assim, com o tempo a situação foi melhorando, e com algum esforço tudo funcionou com a pouca largura de banda que existia entre os dois escritórios.

Com o decorrer do projeto, novos requisitos e demandas foram surgindo e a dimensão com que o projeto estava a ficar, mostrava que algumas melhorias eram precisas.

Na comunidade o impacto e dimensão do projeto da empresa teve também um reflexo nos provedores e empresas locais, que tiveram de se adaptar á dimensão e número de pessoas envolvidas. Por exemplo os dois provedores de comunicações móveis tiveram de montar mais torres de forma a cobrir a zona do projeto, pois não era só a nossa empresa que estava a crescer. A cidade de TETE e a Vila de Moatize, empresas de terceiros, instituições públicas que tiveram de aumentar a sua capacidade, era tudo um universo que iria usar a rede móvel e internet 3G.

Para nós, que estávamos envolvidos era muito engraçado ver o impacto e as mudanças que o projeto estava a ter na comunidade também. Pois numa cidade que não havia quase nada, e o que havia estava em mau estado, a entrada de pessoas novas motivou, hotéis, clinicas, oficinas, restaurantes, lojas de IT … apenas para dar exemplos.

Esse crescimento da empresa somado às necessidades e imposições da casa mãe foram também motivo de desafio para nós e para os operadores e prestadores de serviços. A necessidade de ligar os escritórios de “Africa” (como eram chamados os escritórios de Moçambique) com os centros de dados Globais foi o início de um processo de uniformização tecnológica que iria trazer serviços e padronizações globais aos nossos utilizadores.

Sem contar com os problemas técnicos e logísticos, um obstáculo que tivemos foi preço da largura de banda dedicada internacional em Moçambique, que era cara. Os acessos á internet eram muito fracos, causa disso era uma infraestrutura de telecomunicações e acessos locais de baixa capacidade bem como a falta de capacidade de ligação internacional. Assim inicialmente foi escolhida uma ligação de um 1 Mbit dedicados que nos iria permitir fazer uma VPN IPSEC para um concentrador de VPNS no Brazil (para quantificar, o valor de 1 Mbit rondava os 1000/1500 Euros)

Os requisitos iniciais eram básicos e não muito demandantes em largura de banda nem em qualidade de serviço, pois tínhamos de dar acesso a um conjunto de portais corporativos dentro de uma Intranet que se estava a criar. No entanto sabíamos que esta solução seria temporária e que a demanda de novos serviços iria aumentar.

Instalamos uma ligação de 1 Mbit simétrica e configuramos um túnel seguro que iria atuar como ligação ponto a ponto entre o escritório de Maputo e o centro de dados no Brasil.

No entanto o peso administrativo, e a falta de escalabilidade para novos serviços mostravam que a VPN IPSEC era uma solução com pouco futuro. Apesar de claro está ter permitido o aprovisionamento de alguns escritórios, mas que exigiam sempre intervenção, troca de chaves e certificados para autenticação.

Os problemas eram frequentes e surgiam quando a ligação de *Internet* falhava e os tuneis caiam e não retomavam a conexão, ou porque as chaves expiravam ou mesmo porque do outro lado alguém queria mudar o IP ou algum parâmetro. O mais complicado era quando os equipamentos eram de diferentes fabricantes ou com versões de sistema antigos. Em termos

de rede, o tempo provou que o 1Mbit não servia pois na verdade o aproveitamento da banda era menor.

Dado que a VPN era baseada em meio partilhado e atravessava vários provedores até chegar ao destino, a performance era também muito pobre. E nem mesmo o aumento de banda ajudou.

Apesar de tudo serviu para começar, para aprovisionar alguns escritórios que surgiam em Moçambique, Africa do Sul, Zâmbia e Malawi. Numa dada altura chegamos a ter IPSEC VPN e PPTP VPN (baseada em Microsoft ISA Server) pois alguns locais nem Router tinham e usar *Open Source* era proibido na empresa.

Exatamente por política de segurança, fomos forçados a usar IPSEC VPN nos locais que não tinha equipamento Cisco, e instalar o cliente Cisco para VPN nos portáteis e computadores para que pudéssemos estar dentro da política de segurança, e utilizar a ligação de Internet para ligar aos escritórios.

Essa mudança fez com que a ISA Server (que atuava como Firewall e VPN server) fosse retirado e trocado por uma Firewall ASA 5540 da Cisco que passou a fazer ligação á Internet. Nessa ASA iriam terminar as VPN iniciadas nos clientes remotos. Situação que se mantêm pois temos alguns utilizadores que precisam de ter acesso remoto é empresa.

Em resumo, o cenário da utilização da VPN IPSEC entre Moçambique e os centros de dados no Brasil funcionou até 2012, quando por razões de estratégia começamos a ter a necessidade de aprovisionar e permitir os novos serviços que demandavam largura de banda e qualidade de serviço, para além de variados pontos de acesso entre as várias localizações espalhadas pelo mundo.

Tínhamos 3 Centros de dados onde estavam armazenados serviços corporativos (Correio eletrónico, portais e outras aplicações), várias salas de Video conferência, ligações de voz. Perante isto a solução atual de VPN IPSEC não encaixava, tínhamos de procurar melhores soluções.

Entrada da Rede GLOBAL

Assim e com o foco que tínhamos de mudar, foi criado um projeto para implementar mundialmente novas ligações com características que suprissem as novas necessidades.

Passado o período de desenho e de escolha de um fornecedor global, feito através da casa mãe, Moçambique foi escolhido como uma das localizações para iniciar a implementação. Durante a fase de desenho tinha sido decidido (sem ter sido alinhado com a equipa de telecomunicações local) que “Africa” iria ter uma ligação de fibra com banda de 8Mbits. No entanto nada estava mais desalinhado com a verdade. “Africa” não era apenas uma localização, mas várias. Duas delas importantes, com geografias distintas e limitações técnicas inerentes. Depois de algumas conversas, conseguimos alterar o que estava definido, e passamos a ter não apenas uma ligação de Fibra/radio em Maputo, mas também uma ligação de 4Mbits VSAT na Mina de Moatize. Os dois locais estavam conectados via uma ligação de 2 Mbit HDLC (ponto a ponto) que pode vezes falhava. Assim mantivemos essa ligação, mas

usando a ligação de VSAT como ligação para a rede global, criando também redundância de serviço.

Em termos de ligação física e tecnologias utilizadas, nada diferia do que alguns de nós estávamos habituados, o que diferia eram as configurações e a forma de que nós iriamos olhar para esse novo serviço. No meu caso pessoal tudo isto não era novo, pois um dos motivos de estar envolvido neste projeto foi exatamente o facto de já ter participado num evento semelhante.

O projeto levou o seu tempo, teve muitos intervenientes e cada um tinha o seu papel, e curiosamente que para nós que tínhamos durante dois anos sido o centro de responsabilidade e de controlo da rede da empresa, tínhamos a sensação de que iriamos ficar sem trabalho, mas o tempo mostrou que não.

Inicialmente a preparação dos locais onde as ligações iriam ser instaladas foi primordial. Em Moatize onde o VSAT iria ser instalado tivemos de garantir a parte física (base de cimento para a antena, energia e aterramento) e em Maputo tivemos de instalar um radio pois o circuito de fibra prometido não estava pronto devido a dificuldades do operador incumbente de entregar o lacete local.

De seguida o "arrumo" da rede e dos bastidores surgiu como necessidade pois iriamos ter mais equipamento para instalar pois apesar de uma ligação por local, iriamos ter também os equipamentos secundários para minimizar falhas.

Esses equipamentos seriam dois Routers Cisco que seriam por nós geridos e que iriam ser as fronteiras da nossa rede (***C****ustomer Router)* e dois Routers do provedor global que iriam servir entrada para a rede global (***C****ustomer* ***E****dge Router)*.

As configurações do nosso lado iriam ser feitas por nós. A ideia era ser "só ligar" a nossa rede á rede do provedor. O CE Router tinha toda a "inteligência" para criar a criação da MPLS VPN.

Foram-nos dadas/negociadas as classes de serviços que iram caracterizar o tráfego que iria passar dentro da rede do provedor, com essas classes nós preparamos o trafego de saída (da nossa rede) para que tivéssemos mais detalhe e aproveitamento da rede Global. Esse detalhe ia também criar as bases de classe do SLA, pois iriamos ter diferentes tempos de resposta/suporte e medidores quando tivéssemos um problema de rede.

Apesar de também ser possível fazer QOS (Quality of Service) numa VPN IPSEC não tiramos proveito nenhum pois apenas marcamos o trafego na entrada do túnel. Na verdade estamos a dizer qual é que vai entrar primeiro apenas.

No caso do QOS aplicado com MPLS VPN o controle é muito maior, pois para além da negociação com o Operador, a entrada de tráfego e a sua marcação poderá criar dois cenários distintos:

1. Uma única VPN por onde passam todo o tráfego marcado com as respetivas prioridades,

2. Criação de VPN por extirpe de tráfego, ou seja ter vários tuneis para os vários tipos de marcação feita.

O cenário mais aplicado pela maioria dos operadores é, por motivos de configuração e de controlo, o primeiro.

Com todas estas ferramentas este novo serviço de MPLS iria dar aos nossos utilizadores os novos serviços corporativos que outrora eram acedidos via VPN e alguns com vários métodos de acesso e de autenticação.

Apenas para dar exemplo:

- Novo serviço de correio eletrónico e de comunicação instantânea,
- Novo ERP,
- Novos Portais ou versões deles,
- Voz sobre IP,
- Video conferência.

Tudo iria passar dentro da VPN com marcações de tráfego e prioridades.

Para tudo funcionar foi atribuído por localidade/escritório um código e uma Range de IP derivada da Classe A para que pudéssemos usar nas redes locais. Na ideia original apenas iria haver uma saída por região, e uma região poderia ter mais que uma "localidade" (forma como no Brasil se referiam ao termo site/escritório). Essas "localidades" iria ser ligadas por conexões *WAN* nacional para que depois houvesse apenas a saída para a Rede Global. No caso de Moçambique, como mencionei, mudamos essa ideia e passamos a ter duas ligações á Rede Global.

Ligação vista lado do Cliente e configurações feitas

Ao contrário do que anteriormente era feito, quando tínhamos IPSEC VPN, onde para ligar mais que um escritório criávamos um túnel específico e para cada um a necessidade de gerir tempos de espera (***Time Outs***), senhas de autenticação, algoritmos de cifra, endereços IP de vizinhos (***Peers Address***). No caso do MPLS a ideia era apenas "ligar e funcionar".

Nada mais simples … e funcional. Claro que para a nossa dimensão não seria apenas isso.

Não é que não funcionasse, pois na verdade a ideia base do serviço de ***VPN MPLS*** oferecido pelos provedores é exatamente atuar com transparência e flexibilidade, pois toda a carga está do lado da rede do provedor, é lá que são feitas as VPN. O Cliente terá apenas de ligar o seu equipamento á conexão física do provedor. Normalmente essa conexão é já Ethernet e simplifica as coisas. Mas por vezes o cliente não tem um Router, ou interface que suporte a ligação ao provedor (***RJ45, RJ48, RJ11, X.21*** ou fibra) e ai o operador entrega um ligação ***LAN***, mas que por detrás tem toda a panóplia de equipamento para permitir a parte física (**Layer 1**) e a parte de protocolo (**Layer 2**). Esse equipamento pode ser um modem ***VSAT***, ou algo que sirva de conversor (fibra para cobre, Fibra para Fibra, Radio para cobre).

No nosso caso para além do modem VSAT em Moatize e da uma Antena Radio em Maputo, íamos ter um equipamento que nos iria converter a ligação de fibra para vários E1 de VOZ, ligações Serial (V.35) e ligação RJ45 onde nos entregavam os circuitos.

Isto acontecia porque o operador global (OG) teve de pedir ao Operador local (OL) a criação de conexão entre os nossos escritórios e o seu POP. Dado que o *OL* já nos fornecia serviços, eles entregaram no mesmo equipamento o circuito de 4 Mbit. Posso dizer que no início foi um pouco complexo de gerir, pois era apenas um ponto de falha de meio físico, o que nos levou a perder umas noites de sono, pois só quando mudamos de um escritório para um novo é que conseguimos ter um pouco mais de fiabilidade.

Depois da parte física resolvida podemos então instalar os Routers.

Do nosso do iriamos ter apenas configuração de roteamento BGP, iriamos usar a range de endereços IP definida e tínhamos de injetar tráfego para a rede global segundo as classes de serviço (***CoS***) acordadas e desenhadas pela equipa de arquitetura.

Como protocolo de roteamento iriamos usar o protocolo ***BGP*** (***Border Gateway Protocol***) que apesar não sendo o mais leve é o que melhor e mais ferramentas tem para controlar rotas. E normalmente usado dentro das redes de operadores, mas também é usado para grandes implementações como a nossa.

Não sendo um protocolo fácil e de rápida explanação, tem a possibilidade de correr IPV4 e IPV6 e tem uma escalabilidade e estabilidade elevada. A sua capacidade de transportar rotas e de criar e gerir tabelas de roteamento servia os nossos propósitos, pois a empresa é muito grande, e iriamos passar a ter acesso a quase todas as redes de quase todos os escritórios de outras localizações.

Configuramos o protocolo nos nossos Routers anunciando as nossas redes locais. Ao mesmo tempo criamos políticas de propagação de rotas (***prefix-list***) para que não se estivesse a receber e a enviar informação detalhada e sim sumarizada.

Parte da de configuração de BGP onde são dadas a conhecer que rotas são anunciadas:

```
router bgp 65210
 no synchronization
 bgp router-id 10.47.254.5
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 network 10.47.254.5 mask 255.255.255.255
 network 172.25.16.0 mask 255.255.252.0
```

network 172.25.21.0 mask 255.255.255.0

network 172.25.22.0 mask 255.255.255.0

Como iriamos ter regras e vários tipos aplicações, a lista de identificação de tráfego de rede que iria ser marcado com as classes de serviço para podermos melhorar a performance e prioridade de fluxo dentro da rede do operador (***QoS***). Tudo isso foi feito com base nas ferramentas de configuração *Cisco* que correm já no sistema operativo dos *Routers*. Para que se conseguir cumprir com as premissas usamos uma lista de controlo que nos davam a possibilidade de configurar protocolo e porto. Tudo o resto que não está identificado como prioritário entra numa lista de baixa prioridade que poderá ser descartado, caso não exista largura de banda.

Parte da configuração de QOS onde foi atribuída largura de banda utilizada por classe previamente criada:

policy-map WAN_QOS_NESTED

class EF_VOICE

priority percent 10

set ip dscp ef

class AF4_VIDEO

priority percent 25

police rate percent 25

conform-action transmit

exceed-action drop

set ip dscp af41

class AF3_SIGNALING

bandwidth percent 10

queue-limit 64 packets

set ip dscp af31

class AF2_CRITICAL

bandwidth percent 20

queue-limit 128 packets

fair-queue

```
 set ip dscp af21
class class-default
  bandwidth percent 35
  queue-limit 256 packets
  fair-queue
   random-detect dscp-based
   random-detect dscp 0 150 256
   random-detect dscp 10 150 256
   random-detect dscp 12 50 100
policy-map WAN_QOS
 class class-default
  shape average percent 100
 service-policy WAN_QOS_NESTED
policy-map LAN_QOS
 class AF12_SCAVENGER
  set ip dscp af12
```

Ligação vista lado do operador (MPLS VPN)

Do lado do operador, apesar de não termos sido executantes, por motivos de relacionamento e de histórico fomos mantidos sempre a par do que estava a ser feito.

Claro que os segredos técnicos do negócio nunca foram revelados, mas o facto de o operador saber que do nosso lado havia alguém que sabia o que devia ser feito, e ter sido indicado como ponto focal, fez com que eles tivessem um pouco mais de cuidado e detalhe na implementação.

Essa implementação foi feita globalmente e de forma igual para toda a rede da empresa, não houve truques nem exceções.

O objetivo era criar ligações multiponto que permitissem melhor interação entre as localidades.

Como tecnologia de ***Core*** o ***MPLS*** é usado de uma forma que permita uma melhor utilização da rede de transporte. Atualmente os ***Cores*** dos operadores são IP, logo nada melhor que otimizar e criar novos serviços sobre essa rede.

Se formos analisar, como era feito o roteamento dos pacotes numa rede IP, iremos ver que todo o pacote tem um cabeçalho onde tem de entre outros campos o endereço de origem e endereço de destino.

Logo cada vez que um equipamento de roteamento tem de encaminhar um pacote, no mínimo terá de verificar esses dois campos, o que é uma carga de trabalhos. Se pensarmos que esse processo implica verificar endereços, e verificar na tabela de rotas (*Routing table*) se esse endereço está acessível e por onde –(***Next hop***). Pode parecer pouco, mas quando se trata de milhares de pacotes, cria uma carga adicional. Mais se somarmos políticas de QOS que também estão publicadas nos campos de cabeçalho do pacote, que também terá de ser avaliadas sempre no envio do pacote. Com a introdução de MPLS nas redes de operador, estas ficaram um pouco mais rápidas e mais inteligentes, para poderem oferecer mais serviços aos clientes.

Sendo um ***standard*** definido na sua génese o MPLS é configurado por cima da rede IP, e ativando muitos operadores usam apenas as ***Layer 2 VPN***, que é uma implementação mais simples e que faz uso de um conjunto de Bits (***Labels***) para encaminhando de pacotes.

O que o protocolo vai fazer é depois de ativo nos equipamentos as rotas irão ser identificadas com uma ***Label*** de entrada, ***Label*** de saída e respetivo interface de saída. Assim é criada uma tabela com essa informação para que o roteamento seja feito de uma forma mais expedita. Fazendo a analogia com uma tecnologia de nível 2 (***Data link***) o MPLS usa as ***labels*** um pouco como o ***Frame Relay*** usava os ***DLCI*** .

Dado que o ***MPLS*** corre sobre redes IP, um protocolo de roteamento que entenda o mecanismo de ***labels*** deverá ser escolhido para que possa haver mais rapidez e convergência de roteamento.

Esta ***Layer 2 VPN*** permite já aos operadores melhorar a sua rede e evoluir para outros serviços tais como os que na minha empresa utilizamos ou seja Layer 3 VPN e QoS.

A ***Layer 3 VPN*** tem como principal objetivo criar “tuneis” baseados em IP e permitir que ao invés dos clientes terem múltiplas ligações para vários locais ter minados no seu equipamento, como acontecia com a ***VPN*** de ***IPSEC*** com os seus múltiplos tuneis. Para que isso possa acontecer, o operador cria nos ***Routers*** agregadores de conexões de clientes que dentro do Ponto de presença (***POP***) condições para iniciar a ***Layer 3 VPN***.

Esse Router dá pela identificação de ***PE Router*** (***Provider Edge Router***) e é nele que está a configuração base dessas ***VPN***s.

No caso que serve para este documento esse ***PE*** ficaria dentro das nossas instalações, por uma questão de capacitação e de estratégia do operador. Segundo eles, seria mais fácil para eles trocarem os equipamentos ou a tecnologia de acesso (cabos, modens ou antenas) sem afetarem o serviço prestado.

Assim nesses equipamentos de ***PE*** para além da ligação física a nossa rede, iria haver a ligação á rede de ***Core*** do operador. Em termos de configuração da ***VPN de MPLS*** houve parâmetros que tiveram de ser configurados. Já foi dito que tivemos de configuram BGP nos nossos Routers, logo do lado do operador também foi configurado BGP, neste caso Multiprotocolo BGP (***MP-BGP***). Mas vamos por partes.

Para que tudo funcione o operador tem de criar uma forma de receber as rotas do cliente e não as misturarem com outras rotas de outros clientes ou mesmo com as suas. Assim tem de criar uma VRF (***Virtual Routing and Forwading***) que não é mais que uma sub tabela de roteamento que irá guardar as rotas das redes do cliente ao qual para além de um Nome iremos atribuir um identificador chamado ***Route Distinguisher*** (***RD***) que será anexado ás rotas IP para criar unicidade e esconder também as rotas. Esse ***RD*** é representado por dois campos. Um com a identificação do ***ASN*** (Numero identificador do site ou ***AS***) e outro onde teremos uma identificação usada dentro da rede do operador como se de um índex se tratasse.

Por exemplo:

Se dois clientes usam as mesmas redes IP isso não seria possível, pois poderia levar a uma confusão sobre que cliente seria. Assim criamos um número único dentro da rede de operador (como se fosse um código postal) e passamos a identificar cada um dos clientes com isso.

Cliente A com a Rede IP 10.0.0/8 o **RD** seria **100:1**

Cliente B com a Rede IP 10.0.0.0/8 o **RD** seria **200:1**

O operador iria ver as rotas dentro da sua rede da seguinte forma (RD:Enderoço_IP):

Cliente A 100:1:10.0.0.0 e Cliente B 200:1:10.0.0.0

Ainda no ***Router*** do operador iria ser criada a VFR e a atribuição ao interface físico que liga cada cliente. Será preciso também criar uma forma de dar a entender que rotas alvo (Route-target) de propagação ou **exportação** e as rotas que em dada VRF são instaladas ou **importadas** para a tabela de roteamento local da seguinte forma:

Ip vrf CLIENTE_A

Rd 100:1

Route-target import 100:1

Route-target export 100:1

Ip vrf CLIENTE_B

Rd 200:1

Route-target import 200:1

Route-target Export 200:1

Nota:*Neste exemplo a ideia é que cada cliente exporte e importe todas as rotas dele, e que todos os locais possam aceder uns aos outros (Full-MESH), na demostração irá ser mostrado este exemplo. No entanto é possível criar VPN onde determinados locais acedam apenas a um ou dois. Para isso teríamos de ter um RD por local e importar ou exportar esses RD. Daria mais trabalho, mas é de facto mais seguro e escalável.*

Essas VRF iriam ser então atribuídas aos interfaces que liga aos clientes com o comando ***ip vrf forwarding NOME_DA_VRF***

```
interface Ethernet1/3
    ip vrf forwarding CLIENTE_A
    ip address 10.0.13.3 255.255.255.0
interface Ethernet1/4
    ip vrf forwarding CLIENTE_B
    ip address 10.0.14.3 255.255.255.0
```

Ao criarmos este mecanismo fazemos com que as rotas de cada cliente sejam escondidas de outros clientes, e que todos os escritórios do cliente A possam ser identificados com o mesmo ***RD*** (para casos simples).

No entanto ainda estamos a meio caminho da tal VPN de MPLS, pois falta agora configurar a propagação de rotas. Essa propagação será também com o protocolo de roteamento neste caso com o ***MP-BGP***.

A configuração é um pouco mais complexa e longa para aqui ser descrita. Mas antes disso por se chama ***MP-BGP***?

Inicialmente o protocolo ***BGP*** foi criado para aceitar ***IP*** versão 4, depois com as várias versões e com a entrada de novos tipos de endereços (tal como ***IPV6***, ***VPNv4*** – que é utilizado no ***MPLS*** com protocolo ***IPV4***) foi assim denominado e aceite pelos fabricantes de equipamentos de rede como um Standard (**RFC – 47560**).

Nessa configuração do protocolo **BGP**, podemos optar por apenas utiliza-lo para propagação de rotas de VPNv4 (RD:Endereço_IP), ou usá-lo também para transportar rotas de outros protocolos supra citados. Depois desta configuração a VPN fica ativa e permite criar topologias de ponto a ponto, ponto-multiponto ou mesmo de todos com todos (o chamado ***full-mesh***), tal como temos na empresa.

Nos casos que a segurança é extrema podemos usar ***IPSEC*** para cifrar o trafego que corre dentro da rede, ou mesmo criar regras de cifra entre a saída da nossa rede (CE) e a entrada da rede do operador (PE).

Também podemos tirar proveito do ***QoS*** e o operador fazer políticas de ***QoS*** para que o tráfego do cliente tenha prioridade dentro da ***VPN***, da mesma forma como numa ligação ponto a ponto. Por fim numa rede ***MPLS*** podemos também usar o **Traffic Engineering** (***TE***) que é uma ferramenta do ***MPLS*** que permite a criação de tuneis com parâmetros determinados e que cria automaticamente um caminho para esse túnel conforme as condições das redes.

Comparando ***TE*** com ***QoS*** é como ter uma faixa de ***BUS*** na cidade onde é sabido que os autocarros podem circular lá sempre, estejam cheios ou não, esteja o trânsito congestionado ou não. Ou então ter um policia sinaleiro em cada cruzamento que determina se os autocarros passam ou não na frente uns dos outros.

No caso da empresa onde estou, foi negociado que numa primeira fase iriamos ter o QOS com MPLS.

Descrição de configurações e exemplos

No anexo 3 e 4 estão dois documento que são muitos usados como exemplos explicativos do protocolo MPLS que são usados como base de formação.

No anexo 5 e 6 estão dois documentos que mostram como se pode configurar IPSEC Ponto a Ponto e servem de exemplo de como era feito na empresa.

Todos os documentos são em inglês e irão ser referenciados na bibliografia.

Testes á implementação e melhorias

Durante a implementação fomos testando os serviços, mas o melhor exemplo de que tudo funcionou, apesar não poder demostrar aqui foi que no dia a seguir a implementação os utilizadores notaram logo uma melhoria de performance, para além de poderem aceder a aplicações.

Com o correr do tempo introduzimos o serviço de voz entre todos os locais da empresa, apesar de limitado a um número de chamadas, mas que funcionou perfeitamente. Mais tarde iniciamos um projeto para implementar a vídeo-conferência, que foi um sucesso.

Apesar de tudo, e como a empresa está a crescer, novos requisitos surgem. Temos em mãos um aumento de largura de banda, que não irá alterar em nada do nosso lado, mas apenas do lado do operador pois vamos ter ***TE*** e um outro projeto que serve para melhorar a rede interna WAN e LAN para que possamos poupar um pouco mais de dinheiro e deixar de usar duas ligações á rede Global e passar a usar uma apenas. Esse projeto passa por configurar entre os escritórios de Moçambique uma rede MPLS regional para que possamos ter melhores serviços internos e mais fiabilidade de rede. Essa rede irá ser feita com base na infra – estrutura contratada a um operador que ficará responsável apenas pela parte física e nos iremos gerir toda a parte de MPLS e serviços.

Conclusões

Sendo um projeto Global teve algumas situações muito interessantes quer do ponto de vista técnico como de gestão.

Os custos envolvidos, a discrepância de condições técnicas e a urgência foram fatores que levaram a que o projeto tenha tido um impacto muito positivo dentro da empresa.

Se pensarmos apenas em custos, ter uma VPN IPSEC era muito mais barato. No entanto não é uma solução empresarial escalável. Ao passarmos para MPLS e usarmos a VPN via MPLS, tivemos logo uma melhoria de serviço notória. Claro que os custos são imensos estamos a falar em 50 mil Euros mensais, mas passamos a centralizar mais, desde a gestão e monitorização da rede, aplicações e serviços que outrora estavam espalhados por vários locais. A segurança foi outro ponto que teve um incremento de qualidade pois agora já não tínhamos várias senhas de acesso, e não usávamos formas diferentes de acesso.

Não é, claro está, um serviço que possa ser aplicado a todos os perfis de empresa, mas é claramente e com a evolução da oferta dos operadores uma mais-valia para empresas que desejam ter uma topologia de mais que um escritório, ou que por razões de estratégia optaram por usar um operador que usa o MPLS para dar serviços como internet, ou serviços de hospedagem.

Bibliografia usada na produção do relatório

- CCIE Playground Blog - *MPLS*, 2012. Escrito por **Piotr Wojciechowski**, disponível no endereço <http://ccieplayground.wordpress.com/category/mpls/> acedido em Julho de 2014
- MPLS Tutorial, 2012. Escrito por ***Sudeep Goya***, disponível no endereço <http://mplstutorial.com/> acedido em Julho de 2014
- Cisco support site – Cisco, vários documentos de vários autores, disponível no endereço <http://www.cisco.com/cisco/web/support/index.html#product > acedido em Julho de 2014

Anexos

Anexo 1 – Descrição técnica

Anexo 2 – Apresentação em *Power Point*

Anexo 3 – Configuração Básica de MPLS

Anexo 4 - Configuração de uma VPN L3 de MPLS

Anexo 5 – Configuração de uma VPN IPSEC entre dois Routers

Anexo 6 – Configuração de uma VPN IPSEC entre Firewall e um Router

Glossário básico

Active directory (AD): Estrutura de diretório criada para os Windows Servers 2000 e versões posteriores onde são guardados objetos que contemplam grupos de utilizadores, utilizadores, impressoras, pastas, permissões e serviços.

Autonomous System Number (ASN): Número atribuído a um conjunto de redes dentro de uma mesma unidade administrativa. Tem como objetivo identificar na internet operadores e empresas que estão diretamente ligadas á internet possuem endereços IP públicos. O intervalo 1 a 64511 são números públicos e 64512 a 65534 são privados e podem ser usados dentro de redes fechadas como as redes de MPLS.

Data link connection identifier (DLCI): endereço identificador das frames em Frame Relay. E usado pelo equipamento de comutação de frame relay para encaminhar as frames.

Frame Relay: Tecnologia de comunicação de dados que atua na camada 2 do modelo OSI. Actua dividindo a informação que circula na rede em frames e forma um circuito virtual (VC) através do caminho de ponta a ponta. E considerado como se de uma rede virtual privada fosse.

Multi protocol Label Switching (MPLS): tecnologia de transporte que é usada atualmente nas redes IP utilizando etiquetas identificadoras

Local área Network (LAN): Rede Local de dados, normalmente usada numa empresa

Plesiochronous Digital Hierarchy (PDH): Em Português "Hierarquia Digital Plesiocrona" é uma tecnologia de transmissão que utiliza a divisão de canais e a sua multiplexação para poder transmitir dados. Através de agrupamento de canais de 64 Kbps conseguimos por níveis atingir velocidades de E1 a E5 (2048 Mbps a 565,148 Mbps).

Quality of Service (QOS): Conjunto de regras e políticas que são utilizadas para classificar tráfego de rede para que exista otimização na transmissão de dados. Existem várias ferramentas e vários tipos de QoS que podem ser aplicados a várias situações.

Traffic Engineering (TE): método de aprovisionamento utilizado dentro das redes de transporte utilizado para poder oferecer aos clientes melhores condições de transmissão dentro da rede.

Virtual Private Network (VPN): Rede privada virtual em Português, tipo de ligação que cria um túnel seguro (cifrado) ou não e que permite ligar dois pontos ou mais através de um meio de transmissão que poderá ser comprometido.

Very Small aperture Terminal(VSAT): estação terrestre que é utilizada para transmissão de dados através de satélites.

Wide area Network (WAN): Rede de dados normalmente com abrangência regional