Relatório de Estágio de Mestrado em Engenharia Informática - Computação Móvel

Upgrade na rede de Core de uma operadora de telecomunicações

Luís Filipe Calado Carvalho de Figueiredo

Relatório de estágio de Mestrado realizado sob a orientação do Doutor Paulo Jorge Gonçalves Loureiro, Professor Adjunto da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, 2011

Esta página foi intencionalmente deixada em branco

Resumo

A necessidade e exigência por parte dos consumidores ao nível das comunicações multimédia e entretenimento na Internet têm vindo a revelar-se cada vez maior. O que há uns anos se considerava primeira necessidade como por exemplo, consulta de conteúdos com informação apresentada em texto ou comunicação via e-mail, passou a ser substituído por conteúdos multimédia de vídeo em tempo real e imagens ou animações de resoluções gráficas elevadas ou ainda pela unificação dos sistemas de comunicação entre a voz e os dados.

O presente relatório de estágio foca as necessidades de uma operadora de comunicações por cabo denominada por Operadora A, no suporte aos serviços que actualmente comercializa. De acordo com a necessidade específica da Operadora A, é realizado o planeamento do projecto de melhoria da sua rede de *Core*, que irá servir de base para todos os trabalhos a efectuar dentro do âmbito do projecto.

Inicialmente é apresentada uma introdução teórica que pretende enquadrar as tecnologias usadas nos trabalhos efectuados, seguido da definição do problema e apresentação de soluções. Posteriormente é apresentada a descrição da componente prática do estágio referida como implementação. Caso a caso são definidos procedimentos de execução que auxiliam nos trabalhos e representam o planeamento do projecto.

Terminada a execução dos procedimentos, a rede de *Core* da operadora fica preparada para a implementação de funcionalidades futuras de suporte a serviços, satisfazendo as necessidades da operadora.

Em resumo, a rede de *Core* da operadora foi actualizada com incrementos de largura de banda, capacidade de processamento, memória e versão do sistema operativo.

Palavras-chave: Operadora de comunicações por cabo, rede de *Core*, *Upgrade* de *routers* de *Core*

Esta página foi intencionalmente deixada em branco

Abstract

The consumer's needs and demand for communication and multimedia entertainment on the Internet proved to be increasing. The basic needs changed, in the past e-mail and text based queries were heavily used to gather all sort of information, nowadays people prefer rich media, real time video, high resolution images and animations, unified data and voice communications.

This report will focus on the needs of a cable communications operator called Operadora A and the support services that currently provides. According to the specific needs of this operator, will be presented in this document, a project plan conducted to improve the *Core* network, which will guide all the work.

Initially we present a theoretical introduction that attempts to fit the technologies used in the carried out work, followed by the problem definition and solutions presentation. Then a description of the practical component referred as implementation is presented. After that, implementation procedures are defined, these procedures assist in the course of the work and represent the project planning.

Finally, after the procedure execution ends, the *Core* network is ready to provide new service support functionalities, satisfying the operator necessities with increased bandwidth, processing capacity, memory and operating system version.

Keywords: Communications cable operator, *Core* Network, *Core Routers* Upgrade

Esta página foi intencionalmente deixada em branco

Índice de Ilustrações

Esta página foi intencionalmente deixada em branco

Índice de Tabelas

Lista de siglas

BGP	Border Gateway Protocol
CM	Cable Modem
CMTS	Cable Modem Termination System
DA	Destination Address
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DPC	Dense Port Concentrator
DSL	Digital Subscriber Line
DSLAM	*Digital Subscriber Line Access Multiplexer*
EDGE	Enhanced Data rates for GSM Evolution
FPC	Flexible PIC Concentrator
HFC	Hybrid fibre-coaxial
HS	Host Subsystem
IBGP	Internal Border Gateway Protocol
IS-IS	Intermediate System-to-Intermediate System
LTE	3GPP Long Term Evolution
MIC	Modular Interface Card
MPC	Modular Port Concentrator
MPLS	MultiProtocol Label Switching
NSN	Nokia Siemens Networks
PE	Provider Edge Router
PEM	Power entry module
PIC	Physical Interface Card
RE	Routing Engine
SA	Source Address
SCB	System Control Board
SIB	Switch Interface Board
SPF	Shortest Path First
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ToD	Time of Day
VDC	virtual circuit descriptor
XFP	10-gigabit small form-factor pluggable transceiver

Esta página foi intencionalmente deixada em branco

Índice

Esta página foi intencionalmente deixada em branco

1. Introdução

A tendência de mercado das operadoras está focada no fornecimento de conteúdos ou serviços. Os tipos de serviços e principalmente a qualidade com que são disponibilizados vão definir as tendências e marcar a diferença entre a concorrência. É com base nestas necessidades que o presente relatório documenta um caso real de melhoramentos de parte de uma rede de *Core* de uma operadora de comunicações por cabo.

1.1 Apresentação da empresa

Perfil da empresa

A Nokia Siemens Networks (NSN) é uma das principais fornecedoras mundiais de estrutura para redes fixas e móveis que atende a uma variada carteira de clientes de diversos países com diferentes necessidades. A NSN é líder em serviços e é a primeira do mundo no fornecimento de serviços em Long Term Evolution (LTE). A empresa tem uma forte presença no mercado de fornecedores de serviços ou operadores de comunicações, apresentando um portfólio exclusivo de soluções para negócios com o objectivo de auxiliar os clientes a agregar maior valor em cada serviço de telecomunicações oferecido aos seus assinantes.

É estimado que diariamente um quarto da população mundial usa soluções e infra-estruturas de comunicação da NSN. Com base no trabalho da empresa, estima-se que em 2015 seja necessário existir uma infra-estrutura de suporte para mais de 5 biliões de dispositivos conectados em simultâneo. A NSN pretende fazer face a este desafio, apresentando soluções inovadoras.

Actualmente a NSN possui cerca de sessenta mil colaboradores em mais de cento e cinquenta países em todo o mundo.

O mercado

Um dos principais desafios da NSN passa por oferecer soluções inovadoras para todos os clientes a nível nacional, além de contribuir com o contínuo desenvolvimento das telecomunicações nos países em desenvolvimento.

A competitividade no mercado de telecomunicações faz surgir no nosso país grandes oportunidades para o crescimento e desenvolvimento dos serviços de comunicação, no entanto, como é um mercado bastante competitivo, leva a que as operadoras de comunicações, os clientes da NSN, se preocupem cada vez mais com a satisfação do consumidor final, procurando oferecer serviços de maior valor agregado, como pacotes de dados, voz e televisão zelando pela qualidade dos mesmos.

As três áreas em torno das quais a estrutura da empresa é alinhada são:

- **Soluções Empresariais:** Focada em ajudar os clientes a gerar novas receitas e distinguir-se da concorrência, proporcionando uma rápida disponibilização dos serviços ao consumidor final; melhorar a capacidade de facturação e cobrança; automatizar e simplificar processos; enfrentar os desafios da convergência do mercado para fornecer ao cliente uma experiência única.

- **Sistemas de Rede:** Voltada para as necessidades no endereçamento na camada de rede, tanto de infra-estrutura de redes fixas e móveis, os sistemas de transporte de dados e equipamentos ópticos de acesso de banda larga.

- **Serviços Globais:** Focada em ajudar os clientes a melhorar a eficiência operacional através de terciarização de actividades não essenciais; rápido suporte e gestão das suas redes com as ofertas de atendimento e suporte ao cliente garantindo a robusta e eficiente implementação de novas redes e actualização das já existentes.

Objectivos

Com o constante crescimento da necessidade de comunicações mais seguras, fiáveis e rápidas nas empresas, é indispensável que se desenvolvam tecnologias e apliquem novas técnicas para suportar este crescimento. Prevê-se que em 2015 seja necessário existir uma infra-estrutura de suporte para mais de 5 biliões de dispositivos conectados (Nokia Siemens Networks).

Com o objectivo de fornecer os mais altos níveis de qualidade, todo o planeamento de operação não assenta apenas no fornecimento de equipamento ou serviços, mas também na

assistência pós-venda. O objectivo é disponibilizar um apoio mais próximo e adequado à forma de trabalho de cada cliente conduzindo a um acréscimo na qualidade de utilização dos serviços não só aos utilizadores particulares como também às empresas. Tendo em conta que o principal objectivo não é fornecer suporte ao consumidor residencial, o fornecimento de suporte adequado às operadoras de comunicações, está indirectamente a aplicar um aumento progressivo na experiência de utilização dos serviços por parte dos consumidores finais.

Desafios

Como principais clientes as operadoras de telecomunicações, os desafios são enfrentados aumentando a eficiência e gerindo a pressão dos custos operacionais. Os operadores têm mantido a tendência de fornecer um serviço mais individualizado, chegando mais próximo do cliente, permitindo melhorar a sua experiência de utilização dos serviços e consequentemente, a satisfação do cliente leva a que o mesmo não troque de operadora (Nokia Siemens Networks).

A experiência em serviços de comunicações individualizados fornece uma grande mais-valia à qualidade do serviço prestado e aumenta consideravelmente a confiança do cliente na operadora. Para as operadoras conseguirem esta qualidade no serviço, têm de possuir um conjunto de serviços e produtos de suporte às suas infra-estruturas ao nível que a NSN fornece.

Futuro

O futuro dos serviços é fortemente baseado na capacidade das redes de comunicação. A tendência está no aumento da utilização e número de serviços de *cloud computing* como email, redes sociais, serviços corporativos e aplicações gerais de comunicação de voz e vídeo, já presentes actualmente em muitos servidores. O desenvolvimento das tecnologias em ambiente local permite uma experiência de utilização cada vez melhor. A transposição desta experiência para um ambiente de rede, como a utilização de *cloud computing* leva a que os desafios de manter a qualidade do serviço se tornem mais exigentes e complexos.

Um dos grandes desafios passa por fornecer esta experiência não só a países desenvolvidos como também aos países em desenvolvimento alargando o conceito *Internet of things.* O

conceito *Internet of things* consiste na interligação de dispositivos comuns usados no dia-a-dia de forma a poder haver uma gestão inteligente da sua utilização, criando e interligando tipos de redes diferentes. A tendência está em utilizar o conceito em cada vez mais objectos independentemente da sua função ou tamanho.

Para combater a complexidade deste tipo de comunicações mantendo a experiência de utilização elevada, deve ser realizada a gestão ao nível da segurança e autenticação de cliente mas ao mesmo tempo conseguir fornecer um serviço com um nível de personalização baseado na sua localização, contexto em que está inserido, dispositivo que está a usar, padrões de utilização ou outras preferências definíveis. Uma experiência de comunicações personalizadas constrói os melhores relacionamentos entre clientes e fornecedores de serviço. (Nokia Siemens Networks)

As soluções aplicadas a um caso em particular podem solucionar a questão, mas se forem pensadas apenas para essa situação, facilmente podem gerar problemas noutros pontos da infra-estrutura. Para evitar isso, a inovação nas soluções é constante e acompanha a infra-estrutura como um todo, pensando nas soluções tendo em conta toda a infra-estrutura de rede e não apenas no ponto onde surge o problema.

Responsabilidade

O âmbito da Responsabilidade Social Corporativa tem-se expandido nos últimos tempos. O objectivo da NSN em relação a este ponto é permanecer actualizada numa realidade em rápida alteração, que exige que as empresas sejam responsáveis marcando pela diferença. Como ponto de partida destacam-se as seguintes áreas abaixo.

- **Smart**

  Os desafios de procura de mercado não se vencem apenas adicionando largura de banda. Smart é trabalhar de forma mais inteligente para resolver um problema. As soluções inteligentes assumem diferentes utilizadores, aplicativos e dispositivos de forma a optimizar e automatizar uma rede para obter o máximo de seus activos. Fornece ainda a visão do cliente final que lhe permite tirar partido das novas oportunidades de negócios através da implementação de serviços diferenciados que irão atrair novos clientes e manter os seus actuais clientes leais. A inovação

constante leva à criação das redes inteligentes com dispositivos inteligentes. Tudo isto é possível com um foco em práticas de negócio sustentáveis, maximizando o impacto social e ambiental sem comprometer o desempenho.

- **Holística**

Estamos a passar por uma transformação que atravessa as tecnologias, fornecedores, redes e modelos de negócios. Para que as soluções da NSN sejam eficazes, não se pode assumir qualquer uma destas partes como garantidas, ou apresentar soluções para uma parte isoladamente. Deve-se olhar para todas as áreas em conjunto e para a além das infra-estruturas, de forma holística para resolver problemas do negócio dos clientes. O trabalho é realizado com base em parcerias consultivas para criar um ecossistema aberto abrangente de tecnologias e serviços.

Um cliente não pode correr riscos ao transformar as suas infra-estruturas e empresas. O cliente depende da NSN não apenas para cumprir as promessas de hoje, mas também para as de um futuro imprevisível. É essencial um parceiro com um histórico exemplar de entrega e adaptação permanente de serviços. A NSN é considerada líder em infra-estrutura móvel, em promoções comerciais de LTE e na nova geração de gestão de assinantes de dados.

Grupos de trabalho

A empresa divide-se em vários grupos que colaboram nas tarefas de forma a atingir os objectivos. De entre os grupos de trabalho destacam-se hierarquicamente o grupo de Vendas, Projecto e Planeamento e Suporte, considerados os que mais influenciam nas decisões do projecto. Como estagiário, o grupo de trabalho onde trabalhei foi o suporte. Parte das decisões presentes neste relatório não foram tomadas pela equipa do suporte porque pertenciam à responsabilidade de outras equipas, outras justificações ficaram comprometidas por falta de permissões de acesso à informação. A ilustração 1 mostra a hierarquia de funções da equipa de suporte.

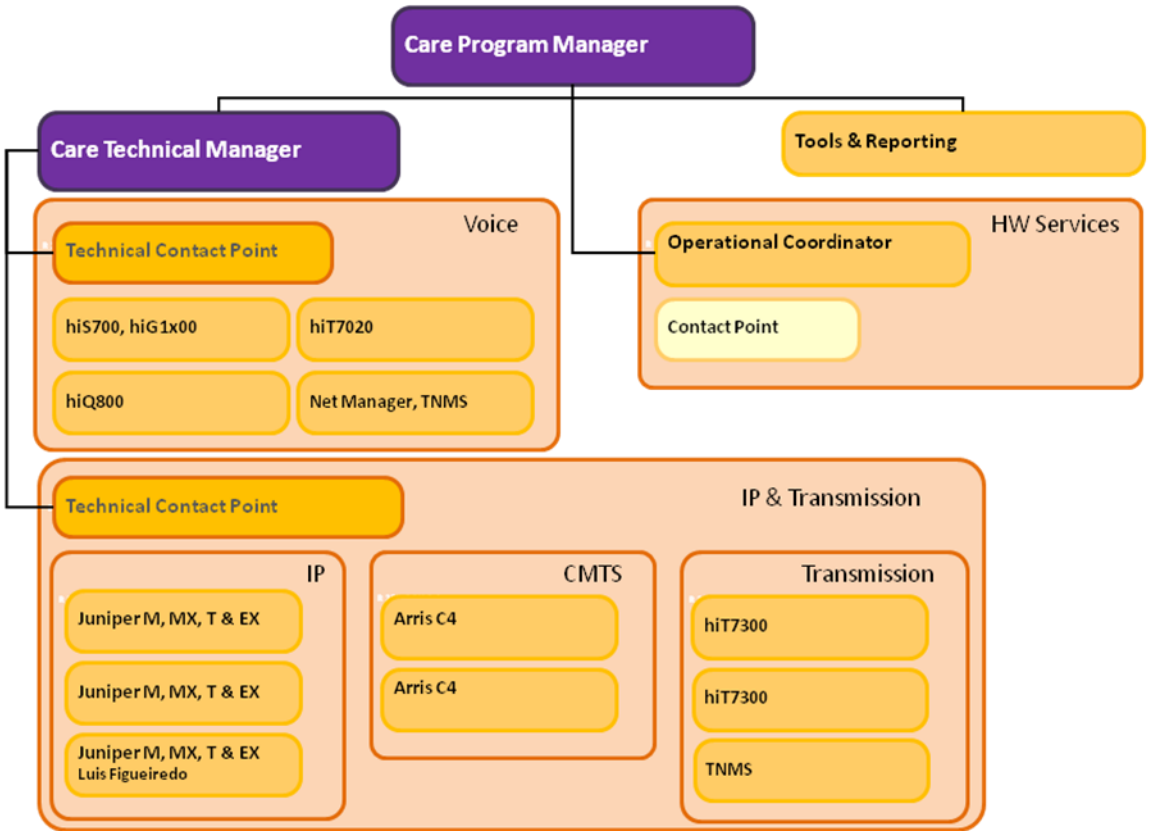

Ilustração 1 – Diagrama organizacional da equipa de suporte

Analisando a ilustração 1, destacam-se três grupos, *Voice*, *Hardware Services* e *IP transmission*. Dentro de cada grupo existe uma divisão por produto e por tecnologia. O grupo *Voice* fornece o suporte aos serviços de voz das redes por cabo. O grupo *Hardware services* fornece apoio a disponibilização e recolha de equipamentos ou componentes para reparação. O grupo *IP & Transmission* fornece todo o suporte as redes de dados fixas desde a transmissão à instalação/suporte dos equipamentos.

Dentro do serviço de suporte (*Care services*), ocupei a posição de técnico de suporte a equipamentos Juniper M, MX, T e EX *series* no grupo de IP.

1.2 Motivação

A elaboração do presente documento e a participação no estágio teve como motivação entrar no mercado de trabalho no ramo das redes de comunicação. A colaboração com uma empresa multinacional focada nas telecomunicações permite participar em projectos

cooperando com equipas diferenciadas e especializadas.

1.3 Cronograma

As tarefas realizadas durante o estágio estão mostradas na tabela 1. O planeamento foi realizado não só com base nas tarefas realizadas na empresa durante o estádio mas também com base nos requisitos e âmbito do curso de mestrado em Engenharia Informática – Computação Móvel.

Tarefa	2010			2011								
	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set
Reunião inicial	X											
Planeamento do Estágio	X											
Definição do tema e objectivos	X	X										
Formação	X	X										
Apresentação do projecto a realizar			X									
Homologação \ Testes			X									
Elaboração da documentação dos procedimentos e planeamento de intervenções			X	X								
Implementação – Intervenções				X	X							
Conclusão e fecho do projecto Apresentação da documentação final - Aceitação						X						
Análise dos dados recolhidos nos projectos							X	X				
Elaboração do documento do Relatório de estágio									X	X	X	
Reuniões finais											X	X

Tabela 1 - Cronograma de tarefas

As tarefas descritas na tabela 1 resumem os pontos de trabalho mais importantes de acordo com o tempo.

Reunião Inicial: Foi realizada uma reunião com o orientador onde foram introduzidas as linhas orientadoras e principais objectivos a atingir na realização do estágio. A reunião decorreu durante o mês de Outubro.

Planeamento do estágio: Com base nas linhas orientadoras definidas na reunião inicial, foi realizado um levantamento de tarefas e feito um planeamento do estágio. Definindo datas e prazos nesta etapa, auxilia no cumprimento dos requisitos.

Definição do tema: Dentro do âmbito do curso e preenchendo os requisitos exigidos para apresentação do relatório, o tema está inserido nas tecnologias de redes e comunicações. Durante dois meses foram analisados os detalhes importantes a incluir no estágio.

Formação: A introdução de conceitos e métodos de trabalho é essencial para um novo colaborador da empresa. Apesar de ter havido um acompanhamento na área constante ao longo do estágio, foi nos primeiros meses que se tornou mais necessário. Durante aproximadamente dois meses foi feito um acompanhamento aos colegas num ambiente de *trainning-on-Job*, onde foram mostrados métodos de trabalho e divulgados conteúdos importantes que permitiram ganhar autonomia rapidamente.

Apresentação do projecto: Depois da proposta do projecto ser apresentada e aceite pelo cliente, a NSN destacou colaboradores para trabalhar no projecto. Como destacado para acompanhar o projecto, foi redefinido o processo de estágio e reanalisados os requisitos de forma a garantir o enquadramento na realização do mesmo.

Homologação \ Teste: Esta etapa comprova em laboratório, a conformidade do trabalho que vai ser realizado na rede. São definidos aspectos a testar e é verificado o comportamento dos equipamentos com base no esperado. Foi estimado um período de um mês para a realização desta tarefa.

Documentos dos procedimentos: Depois de serem efectuados testes em laboratório, é realizado um procedimento para o trabalho que vai ser realizado. São acordadas datas, destacadas equipas de operação e elaborado um resumo das acções a efectuar por essas equipas nessas datas.

Elaboração do projecto – Intervenções: esta tarefa é definida como execução do projecto.

Conclusão e fecho do projecto \ Apresentação de documentos finais: Após a conclusão das intervenções e depois de efectuados testes de conformidade, são elaborados documentos de aceitação para o cliente aprovar o trabalho que foi realizado. Esta etapa

inclui a elaboração dos documentos e apresentação dos mesmos ao cliente.

Análise dos dados recolhidos nos projectos: Nesta fase é analisado todo o trabalho realizado ao longo do projecto e é feita uma recolha da informação enquadrada no estágio e mais importante para o documento de estágio.

Elaboração do Relatório de Estágio: Foi alocada uma janela de dois meses para a elaboração do relatório de estágio. A elaboração do relatório de estágio inclui a organização de informação recolhida ao longo da realização do projecto e as reuniões com o orientador.

Reuniões Finais: As reuniões finais com o orientador pretendem fazer a revisão do relatório de estágio e alinhar assegurar a entrega do documento dentro dos prazos.

1.4 Estrutura do relatório

Este relatório está dividido nos capítulos que passam a ser descritos de seguida:

- Capítulo 1 – Neste capítulo é realizada uma introdução ao tema do estágio, apresentada a empresa e condições em que é realizado. É ainda apresentado um cronograma do estágio que define as tarefas realizadas e a duração das mesmas.
- Capítulo 2 – Neste capítulo é apresentado uma proposta e planeamento do projecto realizado durante o estágio, a apresentação do cenário de rede de trabalho, as fases que o compõem, análise de riscos, definição de pressupostos e alocação de recursos.
- Capítulo3 – Este capítulo descreve os testes efectuados à proposta do projecto de forma a fundamentar o funcionamento da rede como planeado.
- Capítulo 4 – Este capítulo descreve a fase de implementação do projecto. A fase de implementação do projecto inclui a execução da proposta da solução, detalhando todas as tarefas e procedimentos para preparação dos trabalhos.
- Capítulo 5 – Este capítulo mostra com detalhe, a validação e aceitação do trabalho

realizado. No final da execução dos trabalhos são efectuados um conjunto de testes finais para comprovar o funcionamento da solução conforme o esperado e é apresentada a aprovação dos trabalhos por parte do cliente.

- Capítulo 6 – Fecha o documento com um balanço do estágio onde são tiradas conclusões acerca do trabalho realizado e dos conhecimentos adquiridos.

2. Rede de *Core* desactualizada da Operadora A

Os equipamentos e serviços que há uns anos eram necessários para suportar os clientes por parte das operadoras, hoje não são os mesmos e existe a tendência de permanecerem menos tempo no activo. Os conteúdos consultados diariamente na Internet e a quantidade de dispositivos e utilizadores conectados têm crescido de forma exponencial, o que tende a formar congestionamentos de tráfego nas redes das operadoras de comunicações e conduz ainda à escassez de endereços a nível mundial (Mika, 2008).

Várias soluções têm sido estudadas e técnicas para solucionar problemas têm sido progressivamente aplicadas como é o exemplo do IPV6. Consequentemente, as infra-estruturas de comunicação não acompanham esta evolução se não forem melhoradas de forma a garantir a qualidade do serviço prestado ao cliente. A falta de performance dos equipamentos para preencher as necessidades dos clientes tem de ser resolvida.

A segurança e privacidade, controlo de qualidade e controlo de acesso e conteúdos são componentes que têm vindo a mostrar cada vez mais a sua necessidade e consequentemente mostrado que requerem mais recursos de forma a cumprirem com os objectivos. Os requisitos a nível de hardware para estes componentes são elevados e tendem a aumentar devido ao aumento de conteúdos. Com estas necessidades, a mudança ao nível do hardware da rede de *Core* da Operadora A é essencial para permitir a adaptação às necessidades dos clientes e de igual forma proporcionar uma base sólida para o desenvolvimento de novas soluções e produtos. O aumento de clientes e serviços, leva à necessidade de melhorar a rede de *Core* incrementando a largura de banda de ligações e melhorando a capacidade de processamento dos equipamentos do *Core*.

Este capítulo descreve o processo de planeamento e apresentação do problema/necessidades do projecto. Foram reunidos os requisitos, definido o cenário de rede alvo para os trabalhos a efectuar e ainda foram definidas as linhas orientadoras para a elaboração do relatório.

De forma a enquadrar os trabalhos nas necessidades do cliente e no planeamento do projecto, são introduzidos neste capítulo alguns conceitos chave que auxiliam ainda na compreensão do contexto do trabalho.

2.1 Definição da rede da Operadora A

Nesta secção são descritos os elementos de rede abordados neste projecto e o enquadramento dos mesmos nos trabalhos efectuados. Inicialmente é ilustrado um diagrama lógico da rede seguido de uma breve descrição dos elementos que compõem a rede.

2.1.1 Topologia de rede da Operadora A

A ilustração 2 descreve os componentes principais que compõem a rede da Operadora A. A disposição dos elementos na rede da Operadora A não generaliza uma rede de operadora, no entanto, de forma simplificada, a rede da Operadora A segue a esquematização da ilustração 2.

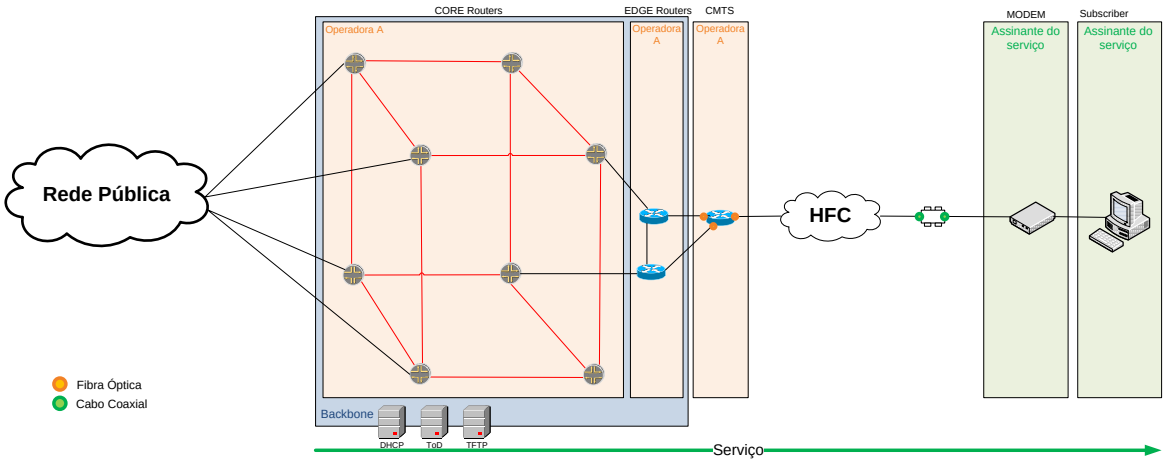

Ilustração 2 - Topologia de rede da Operadora A

O limite laranja identifica os equipamentos do lado da operadora. Existe a rede de *Core* que, para facilitar a leitura, pode ser representada sob a forma geométrica de um cubo e tem ligação para a *Public Network* que representa as ligações para gestão dos *service providers*. Ainda localizado dentro da operadora, existem os *Cable Modem Termination System* (CMTS) que são equipamentos que não são abordados neste projecto por não se enquadrarem no âmbito dos trabalhos.

Entre o limite laranja e o verde, denominado por HFC, estão localizadas as infra-estruturas

de rede pública de comunicações. Do lado do cliente está o *Cable Modem* (CM) que faz a interface entre o equipamento de acesso do cliente e a rede pública de acesso.

Após a análise da ilustração 2 é possível identificar alguns elementos nomeadamente os *Core* e *Edge routers*, CMTS e CM. Apesar de não estarem incluídos no diagrama, outros equipamentos como os *Route Reflector Routers* também fazem parte da rede de *Core* de uma operadora. De seguida são caracterizados todos estes equipamentos.

***Edge routers* – Fornecedor do serviço**

Habitualmente o *Edge router* aceita o tráfego do cliente, independentemente do tipo ou origem de fora da rede para dentro da rede. A sua função depois de recebido o tráfego é fazer a sua marcação e o policiamento, seja entre outro *Edge* ou *Core router*. Outra das funções principais dos *Edge routers* é fornecer segurança e controlo de admissão ao *Core*. Resumindo, os *Edge routers* injectam tráfego classificado no *Core* vindo do cliente e encaminham o tráfego do *Core* para o cliente.

***Core routers* – Fornecedor do serviço**

Os *Core routers* proporcionam o serviço de encaminhamento de pacotes entre outro *Core* router ou *Edge router*. A única gestão que é feita pelos *Core routers* é ao nível da congestão de tráfego. O principal objectivo é fazer o encaminhamento do tráfego entre *Edge routers* o mais rapidamente possível.

***Provider Edge routers* – Fornecedor do serviço**

O *Provider Edge router* é um equipamento situado numa área administrada por uma operadora e outras áreas administradas por outras operadoras. O seu objectivo é encaminhar tráfego para outras operadoras ou para *Autonomous Systems* (AS) de grandes empresas.

***Route Reflector routers* – Fornecedor do serviço**

O *Route Reflector* (RR) é um equipamento que serve para minimizar a quantidade de sessões *Internal Border Gateway Protocol* (IBGP) entre equipamentos dentro do mesmo AS. Na sua ausência as sessões são criadas em *full-mesh* permitindo aos equipamentos conhecer todas as rotas. O RR cria uma hierarquia dentro do IBGP que possibilita haver o

conceito de redistribuição de rotas deixando a cargo deste equipamento a função de "reflectir" as actualizações das rotas para todos os outros menos para quem a anunciou.

CMTSs – Fornecedor do serviço

O *Cable Modem Termination System* (CMTS) é um equipamento localizado no *hubsite* da operadora e é usado para fornecer serviços de dados de alta velocidade como Internet por cabo ou voz sobre IP para assinantes de cabo. O CMTS fornece as mesmas funções para cabo que o *Digital Subscriber Line Access Multiplexer* (DSLAM) para o sistema DSL.

HFC – Fornecedor do serviço

Hybrid Fiber-Coaxial network é uma rede de comunicações, habitualmente redes de cabo, que usam uma combinação de fibra óptica e cabo coaxial. A fibra fornece alta velocidade ao *backbone* enquanto o cabo coaxial liga os clientes ao *backbone*.

Modem - cliente

A ligação do cliente à rede pública é feita através de um *Cable Modem* (CM) propriedade da operadora localizado no cliente. A negociação dos parâmetros ou condições de ligação é realizada entre o CMTS e o CM. A título informativo, o processo de inicialização do CM é apresentado na ilustração 3.

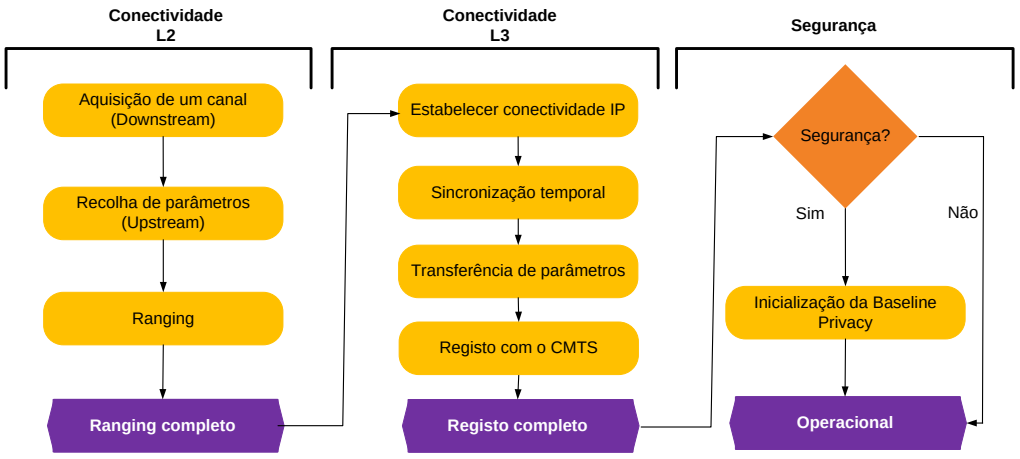

Ilustração 3 - Fluxograma de inicialização do cable modem (Excentis, 2007)

A ilustração 3 representa o fluxo de inicialização de um CM. De seguida é detalhada cada uma destas etapas.

Aquisição de um canal

A aquisição de um canal por parte do CM é baseada no *scanning* que o mesmo faz no *downstream* de ligação com o CMTS. O CMTS envia mensagens em *broadcast* que são recebidas pelo CM com as informações necessárias para completar a etapa.

Ranging

Em redes de *Hybrid Fiber-Coaxial* (HFC), os CM não estão à mesma distância física do CMTS, o que provoca diferentes intervalos de tempo entre a chegada de pacotes entre eles. Ambos os equipamentos necessitam de saber esse tempo. Este processo tem o nome de *Ranging* ou tempo de propagação. O *Ranging* fica completo quando o CM recebe no *Downstream* todos os parâmetros necessários.

Estabelecimento de parâmetros

Após a etapa de *ranging*, o CM estabelece conectividade Layer 3. Para isso podem ser necessários servidores como *Dynamic Host Configuration Protocol* (DHCP) para endereçamento, servidor *Time-of-Day* (ToD) para sincronização temporal e um *Trivial File Transfer Protocol* (TFTP) para estabelecimento de outros parâmetros.

O CM espera por receber um identificador (ID) com os dados de ligação que envia para o CMTS e lhe permite a partir desta etapa, enviar dados para a rede HFC.

Segurança

O *baseline-privacy* é um processo de encriptação de dados entre o CM e o CMTS para fornecer garantias de segurança nas ligações.

2.1.2 Cenário de rede afectado pelas intervenções

O cenário de rede afectado pelas várias componentes do projecto está representado na ilustração 4.

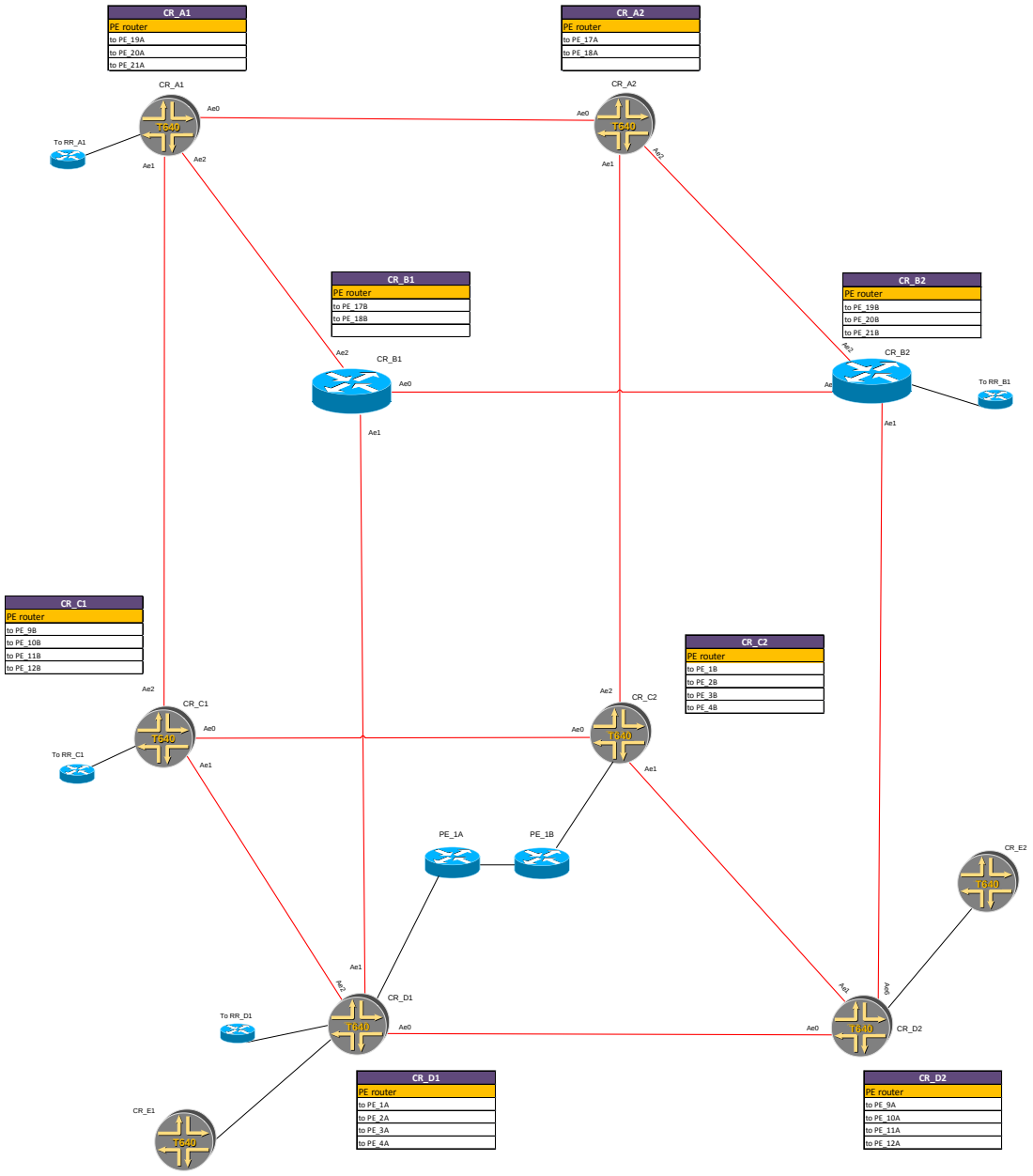

Ilustração 4 – Cenário físico reduzido da rede de produção

Através da análise da ilustração 4 é possível identificar os equipamentos afectados directa ou indirectamente. Tal como caracterizados anteriormente, os tipos de equipamentos existentes na rede são *Core Routers*, *Route Reflector Routers* e *Provider Edge Routers*. Os *Core Routers* são identificados por "CR_" seguido da localização e o número

correspondente à identificação individual. A localização deve-se ao facto dos equipamentos estarem geograficamente distanciados. As tabelas localizadas próximo dos *Core Routers* resumem os *Provider Edge Routers* que carecem de monitorização durante e após as intervenções.

2.1.3 Caracterização do equipamento

Os *Core Routers* alvo de intervenções, representados no diagrama da ilustração 4 são equipamentos Juniper T640 modulares e podem ter diversas configurações de acordo com as necessidades específicas da posição que ocupam na rede. A ilustração 5 mostra a disposição dos componentes no chassis. De seguida é feito um levantamento dos componentes base que constituem um *Router* Juniper T640.

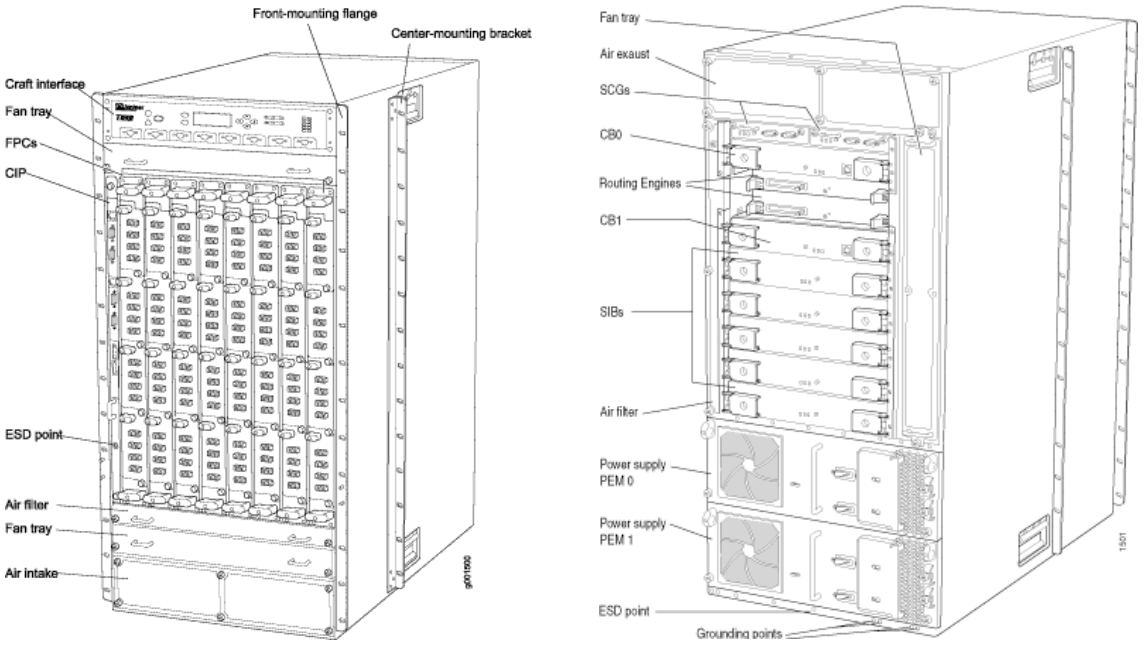

Ilustração 5 - Componentes de um router Juniper T640 (Juniper Networks, 2011)

Craft Interface – Conjunto de indicadores que permitem ver o estado do equipamento, identificar falhas e efectuar funções de controlo.

Flexible PIC Concentrator (FPC) – Concentrador de interfaces. As interfaces físicas, independentemente do tipo, são módulos que se ligam neste concentrador. Estes módulos têm o nome de *Physical Interface Card* (PIC).

No caso específico deste projecto, os equipamentos possuem PICs designadas por *Gigabit Ethernet PICs with SFP(Small Form-factor Physical Transceiver)* que permitem ligações de fibra óptica do tipo LC de 10Gbps.

Connector Interface Pannel (CIP) – Painel que contém as ligações físicas de gestão (consola) e as ligações físicas dos alarmes.

ESD point – Por se tratar de um equipamento electrónico, a sua manipulação faz-se acompanhar de uma pulseira electrostática para prevenção de descargas electrostáticas.

Routing Engines (RE) – Componente do router responsável por gerir todos os protocolos de encaminhamento bem como os processos de software de controlo de interfaces, dos componentes do chassis, da gestão do sistema e dos acessos dos utilizadores.

Uma RE é composta por:

- **CPU** – Unidade de processamento base. Executa o Junos OS (Sistema operativo da Juniper) de forma a manter as tabelas de encaminhamento e controlar os protocolos de encaminhamento.
- **SDRAM** – Fornece armazenamento para as tabelas de encaminhamento e para os processos da RE.
- **CompactFlash card** – Armazenamento principal dos ficheiros de configuração e das imagens de software.
- **Hard disk** – Armazenamento secundário para os ficheiros de *logs*, *dumps* de memória e reiniciar o sistema no caso da *CompactFlash* falhar.

Os equipamentos deste projecto possuem a *Routing Engine*, modelo RE-A-1600-2048 com as características presentes na tabela 2.

• 1.6 GHz Pentium IV processor with integrated 256 kb, Level 2 cache
• 2 GB DRAM, 1 GB compact flash drive for primary storage
• 40 GB Integrated Drive Electronics (IDE) hard drive for secondary storage, 128 MB PC card for tertiary storage
• 10/100ASE-T auto-sensing RJ-45 Ethernet port for out-of-band management
• Two RS-232 (DB9 connector) asynchronous serial ports for console and remote management

Tabela 2 - Especificações da Routing Engine RE-A-1600-2048

Control Board (CB) – Componente da *Host Subsystem* que fornece o controlo e funções

de monitorização dos elementos do router.

No caso específico deste projecto, os equipamentos afectados pela intervenção possuem CBs do tipo T *Series* com um barramento PCI de ligação às REs.

Switch Interface Board (SIB) – Fornece a funcionalidade de *switching* do *Packet Forwarding Engine* (PFE). O PFE processa os pacotes redireccionando-os entre as interfaces de saída e de entrada.

Small form-factor pluggable transceiver (SFP) – Fornece o suporte para ligações ópticas e de cobre. As SFPs são *hot-insertable* e *hot-removable*. Na ilustração 6 é mostrado um exemplo de uma SFP ligada na PIC.

Ilustração 6 - Exemplo de uma PIC com uma SFP para ligações ópticas

2.1.4 Caracterização da rede de *Core*

A rede de *Core* é constituída por *Core*, *Edge* e *Provide Edge routers*. A ligação entre eles varia de acordo com os elementos que interliga no entanto todos assentam em ligações de fibra-óptica e cabo coaxial e implementa mecanismos de redundância que passam a ser descritos de seguida.

Host subsystem - O *Host subsystem* (HS) consiste no funcionamento de *Routing Engines* (RE) em conjunto numa *System Control Board* (SCB). Um *router* pode ter uma ou duas HS. Quando estão instaladas duas HS, uma opera como *master* enquanto a outra opera como *backup*. Se a *master* ou algum dos seus componentes falha, a *backup* começa a operar no seu lugar assumindo-se como *master*. Para operar, cada HS requer uma RE directamente ligada a uma SCB.

PEM Redundancy – O router Juniper T640 possui duas fontes de alimentação denominadas de PEM que partilham o fornecimento de energia do equipamento. Com duas fontes de alimentação os equipamentos conseguem garantir redundância ao nível de alimentação e caso uma falhe, a outra suporta todo o equipamento sem haver quebra de serviço.

A Operadora A implementa ainda balanceamento e redundância ao nível da ligação. Considerando a figura geométrica do cubo apresentado na ilustração 4 as arestas do cubo são compostas por agregados de interfaces. Os agregados de interfaces são uma técnica com dupla vantagem na sua utilização. A técnica consiste em unir duas ou mais interfaces de forma a balancear os dados a transmitir entre a origem e destino, aumentando a velocidade da transmissão, pois os dados são divididos pelo número de interfaces e da mesma forma caso uma das ligações falhe, as restantes asseguram a transmissão dos dados.

Todos os equipamentos do *Core* possuem interfaces de gestão de consola (apenas para acesso ao equipamento *on-site*) e de gestão remota com um IP e porto definidos pela Operadora A.

O encaminhamento entre elementos do *Core* é assegurado através do protocolo IS-IS com a particularidade de implementar um mecanismo de autenticação dos pacotes do tipo HELLO. A tabela 3 mostra um exemplo de configuração do protocolo IS-IS para as interfaces que compõem os agregados.

```
isis {
lsp-lifetime 65535;
level 1 disable;
level 2 wide-metrics-only;
interface ae0.0 {
   hello-padding adaptive;
   point-to-point;
   level 2 {
      metric 10;
      hello-authentication-key <OMITTED>; ## SECRET-DATA
      hello-authentication-type md5;
   }
}
interface ae1.0 {
   hello-padding adaptive;
   point-to-point;
   level 2 {
      metric 50;
      hello-authentication-key <OMITTED>; ## SECRET-DATA
      hello-authentication-type md5;
   }
}
interface ae2.0 {
   hello-padding adaptive;
   point-to-point;
```

```
    level 2 {
        metric 10;
        hello-authentication-key <OMITTED>; ## SECRET-DATA
        hello-authentication-type md5;
    }
}
```

Tabela 3 - Configuração do protocolo IS-IS nas interfaces

2.2 Identificação do problema

Actualmente os conteúdos disponibilizados pelos serviços que as operadoras de comunicações fornecem, requerem uma largura de banda muito maior da que a necessária há alguns anos atrás. A utilização de aplicações *real-time* ou televisão interactiva exigem larguras de banda elevadas para conseguirem garantir o serviço de boa qualidade. A largura de banda elevada na rede de *Core* das operadora requer equipamentos com performance elevada para conseguir gerir grandes quantidades de tráfego de rede. De forma a preencher estas necessidades, este projecto pretende descrever todo o processo de melhoramento de parte da rede de *Core* da Operadora A, instalando e substituindo equipamentos na rede. A instalação dos equipamentos passa por várias fases, entre elas a instalação com migração de serviço ou a definição e configuração das funções do equipamento na rede. Este projecto é constituído por várias etapas que não estão documentadas neste trabalho. As etapas contempladas neste documento são: testes de soluções em laboratório, planeamento e execução de intervenções relacionadas com instalação e configuração de equipamento no local. As etapas do projecto não contempladas neste documento, como a decisão da solução a apresentar, controlo de custos ou decisão dos testes e homologações a efectuar, apesar de fazerem parte do projecto, não são descritas porque foram realizadas por colegas de outros departamentos aos quais não existia permissões de acesso para poderem ser documentadas.

As necessidades principais que levam à implementação do projecto são:

- **Escalabilidade ao nível do hardware** – A capacidade de expansão ao nível de ligações em alguns equipamentos está próxima do limite máximo.
- **Implementação de novas funcionalidades –** Crescimento ao nível da rede em número de clientes e expansão para outras localidades.

- **Melhorar a performance ao nível do hardware** – De forma a permitir futuras implementações de serviços que necessitem de maior poder de processamento e de maior largura de banda.

- **Garantir continuidade no suporte dos equipamentos** – Todos os equipamentos têm um período de suporte garantido. Após esse período apesar de existir suporte, a garantia de resolução dos problemas é limitada e tendencialmente deixa de existir desenvolvimento de actualizações e correcção de *bugs*. Apesar de os equipamentos estarem sob suporte garantido, esta medida é tomada como preventiva de curto prazo.

- **Redução dos custos inerentes a escalabilidade** – Por se tratar de equipamento a sair de fabricação e estar a atingir os limites de expansão de potencialidades, torna-se cada vez mais dispendioso melhorar as capacidades do equipamento, mesmo sabendo que ainda cumpriria com as funcionalidades que implementa actualmente.

O levantamento das necessidades apresentadas anteriormente, apesar de fazerem parte do planeamento do projecto, é resultado da análise de outras equipas de trabalho. A sua inclusão neste projecto serve de enquadramento aos trabalhos efectuados e tomam-se como um pressuposto, baseando os resultados dos testes de aceitação apresentados neste documento nestes pressupostos.

2.3 Proposta de solução

Não estão documentadas neste relatório todas as etapas do projecto uma vez que o projecto integra intervenções idênticas mas em pontos da rede diferentes. Uma vez que ao nível de procedimentos as etapas apresentam uma estrutura semelhante, apenas são documentadas as intervenções referentes ao Site B e ao Site D apesar de serem apresentadas todas as fases do projecto referentes aos restantes sites, Site A e Site C.

De seguida são apresentadas as etapas que compõem o projecto e definidas as tarefas efectuadas em cada uma.

Site Survey

O *Site Survey* consiste na deslocação ao local onde vai ser realizada a intervenção para efectuar verificações de suporte ao planeamento e execução do projecto, nomeadamente:

-Condições físicas;

-Identificação das operações de troca e migração de hardware;

-Verificação das necessidades de etiquetagem, passagem de fibras extra;

-Verificação das interfaces de energia;

-Confirmação da disponibilidade dos recursos humanos;

Fases do projecto

Site A - Integração de equipamento novo na rede

- É da responsabilidade das equipas de operações da Operadora A, garantir a instalação do equipamento durante o dia anterior à intervenção.
- Preparação do equipamento e migração do serviço por parte da equipa NSN na janela de intervenção definida.

Site B - Integração de equipamento novo na rede

- É da responsabilidade das equipas de operações da Operadora A, garantir a instalação do equipamento durante o dia anterior à intervenção.
- Preparação do equipamento e migração do serviço por parte da equipa NSN na janela de intervenção a definida.

Site C - Troca de equipamento.

- A intervenção é realizada durante uma madrugada definida;
- As equipas da NSN e da Operadora A realizam a substituição do equipamento da mesma janela de intervenção.

Site D - Instalação de equipamento e migração de serviço

- É da responsabilidade das equipas de operações da Operadora A, garantir a instalação do equipamento durante o dia anterior à intervenção.
- Migração do serviço por parte da equipa NSN na janela de intervenção definida.

2.3.1 Caracterização do equipamento da proposta

Conforme referido na secção anterior, o projecto envolve várias etapas com intervenções idênticas com a diferença dos sites serem distintos. Neste documento apenas estão documentadas as intervenções referentes ao Site B e ao Site D. A intervenção referente a integração de equipamento novo na rede inclui dois tipos de equipamentos, o router Juniper T640 e o Juniper MX960.

Um dos principais objectivos deste projecto passa por renovar os *routers* que compõem o *Core*. Nas intervenções de integração de equipamento, o projecto envolve troca de *routers* Cisco por *routers* Juniper, o que implica neste caso específico, cada intervenção inclua um router Juniper T640 e um Juniper MX960. Posteriormente estão previstas substituições dos equipamentos Juniper T640 destas intervenções por equipamentos Juniper MX960. As vantagens na troca deste equipamento estão descritas de seguida.

O equipamento Juniper T640 foi caracterizado na secção anterior e não faz parte da solução final, não se assumindo que faça parte da proposta como objectivo principal, mas um passo intermédio ou solução “temporária” até se substituir definitivamente por um

Juniper MX960, os equipamentos propostos para as intervenções. Isto deve-se ao facto da operadora não ter adquirido todos os equipamentos Juniper MX960 ao mesmo tempo e ter extras de Juniper T640.

Nestas condições, apesar das intervenções presentes neste documento incluírem a solução intermédia usando os Juniper T640, apenas vamos considerar a proposta da solução final com os MX960 apenas. Tendo em conta as capacidades dos equipamentos Juniper T640 a substituir, as vantagens da proposta são:

Alta disponibilidade – O hardware dispõe de mecanismos que garantem redundância total, isto é, sistema de refrigeração, fontes de alimentação, REs e SCBs. O sistema operativo é modular incluindo várias implementações de acordo com as necessidades. Permite intervenções de hardware e software sem ser necessário reiniciar ou desligar o equipamento e consequentemente sem causar perturbação no tráfego que encaminha.

Alta performance – Funcionalidades de QoS. Performance multicast melhorada. Capacidade de processamento e memória aumentados.

Comparativamente aos equipamentos a substituir, pretende-se um acréscimo na capacidade de processamento, nomeadamente no processador e na quantidade de memória, como está descrito na tabela 4.

• 2.0 GHz Pentium IV processor • 4 GB DRAM, 1 GB compact flash drive for primary storage • 40 GB Integrated Drive Electronics (IDE) hard drive for secondary storage, 128 MB PC card for tertiary storage • 10/100/1000BASE-T auto-sensing RJ-45 Ethernet port for out-of-band management

Tabela 4 - Características da Routing Engine aplicada nos *routers* da proposta

Flexibilidade de serviços – Suporte para serviços Ethernet Layer 2 e Layer 3 em simultâneo, como por exemplo VPLS, IP/MPLS VPNs, Triple Play entre outros.

Não foram analisadas as necessidades futuras da rede em relação ao suporte a novos serviços, no entanto de acordo com os colegas do departamento que efectua essa análise, as necessidades incidem nos temas descritos na secção 2.2.

2.3.2 Análise de riscos

Para permitir uma redução nos riscos, foram realizadas pesquisas, análises e definido um conjunto de pressupostos que deverão ser levados em consideração. De seguida são descritos os riscos calculados por intervenção e resumidos os parâmetros de análise na tabela 5.

Migração no site C e D

Durante o período crítico da intervenção em que será substituído completamente o T640 pelo MX960, não está prevista qualquer indisponibilidade no serviço dado que o tráfego presente no CR_D2 irá ser baldeado para o CR_D1 e o tráfego de CR_C2 para o CR_C1.

Embora não esteja previsto qualquer impacto no serviço durante a intervenção, poderá ainda existir tráfego residual presente no CR_D2, a afectação neste tráfego será momentânea aquando do *shutdown* dos portos usados para encaminhamento do tráfego. Após esta operação, o tráfego residual, caso haja, irá cursar pelo CR_D1. O mesmo acontece para os elementos CR_C2 e CR_C1 do site C respectivamente.

Instalação no site A e B

Durante o período crítico da intervenção em que serão migrados os portos de *Core* do ER_B2 não está previsto qualquer indisponibilidade no serviço dado que o tráfego presente no ER_B2 irá ser à priori baldeado para o ER_B1.

Tal como na etapa de migração, embora não esteja previsto impacto no serviço, poderá de igual forma existir tráfego residual presente no ER_B2, a afectação neste tráfego será momentânea aquando do shutdown dos portos. Após esta operação este tráfego residual, caso haja, irá cursar pelo ER_B1.

A instalação dos equipamentos ER_A2 é semelhante à ER_B2 pelo que neste documento será descrito apenas para uma instalação pois os trabalhos e procedimentos serão análogos.

A tabela 5 resume o planeamento das intervenções em relação aos riscos. Define a descrição dos trabalhos, a data de execução, o risco e os impactos nos serviços.

Tópico	Descrição
Intervenção	Instalação de equipamento no site A e B
Classificação do risco	Risco Elevado
Duração	Quatro Intervenções, uma por site. De 15/11/10 a 07/12/10.
Descrição dos trabalhos	Retirar dois *Core Routers* Cisco ASR9000 do *Core* IP da Operadora A como elementos de *Core*. Integrar dois *Routers* Juniper MX960 e Juniper T640 na rede como elementos de *Core*. Migração do serviço relativo à operação de troca dos equipamentos.
Impactos no serviço	Não estão previstos impactos no serviço. Dado que a rede implementa mecanismos de redundância suficientes para suportar o tráfego habitual para o horário definido para a intervenção. É assumido que a intervenção é executada dentro de uma janela de intervenção definida de forma a poderem ser activados os mecanismos necessários para suportar o que foi anteriormente descrito.
Descrição do Risco	Dado que a migração vai ocorrer no *Core*, o risco é considerado elevado. Qualquer interrupção no *Core* vai afectar todos os serviços da Operadora A. É necessário um procedimento que previna o impacto no serviço e um plano de *rollback* para o caso em que seja detectado algum problema durante a intervenção e seja possível cancelar a intervenção sem causar falhas na rede.

Tabela 5 - Planeamento de riscos

2.3.3 Plano de actividades

O planeamento das actividades teve em consideração algumas questões que se acharam essenciais para que o projecto avançasse de acordo com o previsto. Na tabela 6 resumem-se estes aspectos.

Tópico	Descrição
Definição das obrigações por parte da NSN	Execução do procedimento previamente acordado
Definição das obrigações por parte da Operadora A	Providenciar acesso ao site. Presença de equipa de operações no site com e a equipa da NSN. Fazer a monitorização do serviço. Supervisionar as comunicações.

Categorização da actividade acordada com o cliente	Procedimento detalhado de execução acordado com o cliente, incluindo procedimento de rollback. Não está definido um procedimento de interrupção da intervenção.
Janelas de intervenção	Acordo dos dias de intervenção entre a NSN e a Operadora A. Janela de tempo para intervenção definida pela NSN. Janela de tempo para monitorização definida pela Operadora A.
Plano de Contingência	Acordo com o cliente sobre quem ficará responsável pelo suporte e intervenção. Acordo com o cliente sobre quem ficará responsável pelo suporte durante o dia seguinte.
Suporte Back-end	Todos os organismos necessários das diferentes Layers de suporte da NSN estão informados acerca desta intervenção.
Requisitos adicionais	Os sites onde vão ser efectuadas as intervenções têm de estar preparados ao nível de circuitos de comunicação alimentação e ar condicionado. Spares de substituição no site para o caso de falhas. Documentação técnica de suporte ao equipamento disponível. Suporte no dia seguinte à intervenção.
Testes	Testes realizados ao procedimento de execução em laboratório da NSN para garantir a sua conformidade. Análise da documentação técnica do equipamento. Testes realizados ao procedimento de rollback em laboratório da NSN para garantir um retrocesso da intervenção dentro da janela de intervenção sem causar perturbação na rede.

Tabela 6 - Planeamento de actividades

2.3.4 Considerações ao projecto

Dada a dimensão do projecto e das entidades envolvidas, a conclusão do mesmo só seria possível dentro do tempo planeado se o trabalho fosse dividido por equipas especializadas em cada tarefa. Esta secção pretende resumir as condições que foram impostas por parte das equipas da NSN e da Operadora A de forma a garantir o sucesso do projecto. São assumidos como pressupostos, os requisitos necessários a todos os níveis, quer sejam antes ou durante a intervenção. Depois de recebido do fabricante, o equipamento passa por uma fase de testes iniciais de *hardware*, onde é carregada uma configuração de teste. A esta fase dá-se o nome de *commissioning*.

2.3.5 Homologação do Hardware

Depois de passar por uma fase de testes e preparação, o *hardware* que vai ser usado é homologado ou não. Todo o *hardware* necessário ao projecto é testado antes de ser colocado em ambiente de produção. Desta forma é validada a homologação por parte do cliente e o equipamento pode avançar para a etapa seguinte, integração em ambiente de produção. Esta é uma tarefa a cargo da NSN.

2.3.6 Homologação do Software

Depois de passar por uma fase de testes e preparação, o *software* que vai ser usado é aprovado. Todo o *software* necessário ao projecto é testado antes de ser colocado em ambiente de produção. A homologação do software passa por várias etapas, *upgrade* e *downgrade* das versões propostas para suporte das funcionalidades e serviços a que o equipamento se propõe a fornecer. Da mesma forma que acontece com o *hardware*, o cliente tem de homologar o *software* para que este parta para utilização em produção. Esta é uma tarefa a cargo da NSN que se compromete a garantir a conformidade do *hardware* e *software* de acordo com o ambiente de rede onde vai ser colocado. No capítulo 4, referente aos testes, são definidos detalhes para esta componente do projecto.

2.3.7 Disponibilização do equipamento

Os equipamentos têm de estar disponíveis no site no dia anterior à intervenção. É assumido ainda que as fibras de ligação que atravessam bastidores são instaladas pela Operadora A antes das intervenções. No caso das migrações, podem ser mantidas fibras ou ser completamente substituídas devido a existência de terminações diferentes nos cabos. Esta tarefa é planeada entre as equipas de operações da NSN, da Operadora A e as equipas do fornecedor do equipamento. Com o auxílio das tabelas de mapeamento apresentadas posteriormente neste documento, as equipas de operações da Operadora A garantem a passagem das fibras de ligação dos equipamentos.

Alimentação e Ar-condicionado

Os equipamentos de ar-condicionado e alimentação têm de ser testados de forma a garantir

o suporte ao novo equipamento. Esta tarefa fica a cargo da Operadora A, no entanto foi apresentado pela NSN um resumo dos requisitos de alimentação do equipamento de forma a ser possível às operações, providenciarem o necessário. Tendo em consideração que o tipo de alimentação para os Juniper MX Series disponível nos sites é DC, de seguida são apresentados os requisitos recomendados pelo fabricante.

Como todos os equipamentos envolvidos neste projecto foram instalados / migrados em sites já devidamente preparados para receber novo equipamento, não foi necessário remodelar o sistema de refrigeração.

O router Juniper MX960 pode conter duas ou quatro fontes de alimentação (PEM) DC localizadas na parte traseira entre as posições PEM0 e PEM3 da esquerda para a direita. O chassis possui quatro fontes de alimentação normais e pode sofrer um upgrade para quatro fontes de alta capacidade que são colocadas nas posições anteriormente referidas. A redundância funciona aos pares entre a PEM0 e PEM2 e PEM1 e PEM3. O primeiro par fornece alimentação redundante para as DPC slot 6 a 11, aos slots SCB 1 a 2 e ainda ao sistema de refrigeração inferior enquanto que o segundo par oferece alimentação aos slots 0 a 5 das DPC, ao slot 0 da SCB e ao sistema de ventilação superior.

Quatro fontes de alimentação garantem redundância total, caso uma falhe, a redundante toma o seu lugar permitindo a continuidade do serviço sem interrupção.

Em relação às fontes de alimentação presentes no chassis, cada fonte de alimentação tem apenas uma entrada DC (-48 VDC e *return*) enquanto, as de alta capacidade possuem duas. No total este projecto requer oito ligações de entrada DC porque tem de garantir redundância total e suporte de alimentação para futuros upgrades. (Juniper Networks, 2011)

A alimentação e a redundância estão garantidas nos Juniper T640 a instalar por estes já terem funcionado noutros pontos da rede.

Requisitos de energia para o equipamento Juniper MX960

A tabela 7 mostra o detalhe dos componentes de alimentação instalados no chassis do equipamento.

Output

```
user@CR_B2-re0> show chassis hardware detail | no-more
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                ************      MX960
Midplane         REV 03   710-013698   ********          MX960 Backplane
FPM Board        REV 03   710-014974   ******            Front Panel Display
PDM              Rev 03   740-013110   ************      Power Distribution Module
PEM 0            Rev 08   740-013683   ************      DC Power Entry Module
PEM 1            Rev 08   740-013683   ************      DC Power Entry Module
PEM 2            Rev 08   740-013683   ************      DC Power Entry Module
PEM 3            Rev 08   740-013683   ************      DC Power Entry Module
```

Tabela 7 - Resumo do hardware de alimentação dos equipamentos Juniper MX960 do projecto

De acordo com o comando anterior, recolhido do equipamento na fase de *commissioning*, as fontes de alimentação presentes no equipamento são *standard* com 2800w de capacidade (58A). Desta forma, o fabricante recomenda providenciar no mínimo 116A a -48VDC nominal por par de fontes de alimentação *standard*.

Como não está previsto que o sistema funcione com uma carga de energia elevada por não entrar ao funcionamento com todas as funcionalidades activas, foram realizados cálculos de acordo como *hardware* a instalar de forma a garantir o correcto funcionamento do equipamento com o *hardware* e funcionalidades necessárias.

De acordo com o fabricante os valores de consumo para o componente base são:

Configuração da alimentação DC	Potência necessária (Watts)	Corrente necessária (Amps @ –48 VDC)
A configuração para alimentação DC redundant inclui quarto fonts de alimentação DC o *midplane*, a interface *craft*, e as *fan trays* a funcionar à velocidade normal.	400 W (approximado)	8.3 A (approximado)

Tabela 8 - Requisitos de energia DC base para um router Juniper MX960 (Juniper Networks, 2011)

O componente base inclui: *midplane*, *craft interface* e *fan trays* a funcionar à velocidade normal. De seguida é resumido na tabela 9 o consumo individual de energia de cada

componente de forma a ser possível calcular o consumo global do *hardware* efectivo que vai ser instalado.

Componente	Potência necessária (Watts)	Corrente necessária (Amps @ –48 VDC)
SCB	150 W	3.1 A
Routing Engine	90 W	1.9 A
Cooling system (full speed – normal speed)	600 W – 400 W = 200 W	4.2 A
High-capacity cooling system (Full speed - normal speed)	640 W - 400 W = 240 W	5.0 A
DPC—Generalized typical value	312 W	6.5 A
DPC—Generalized maximum value	365 W	7.6 A
FPC2 (without PICs)	110 W	2.3 A
FPC3 (without PICs)	180 W	3.8 A
MPC (fixed configuration)	440 W	9.17 A
MPC (without MICs)	294 W	6.13 A

Tabela 9 - Requisitos de energia dos componentes DC de um router Juniper MX960 (Juniper Networks, 2011)

De forma a calcular os valores previstos para o consumo de energia do equipamento a tabela 10 mostra um resumo do *hardware* instalado.

Comandos

```
user@CR_B2-re0> show chassis hardware detail | no-more
Hardware inventory:
Item            Version  Part number  Serial number     Description
Chassis                                ************      MX960
Midplane        REV 03   710-013698   ************      MX960 Backplane
FPM Board       REV 03   710-014974   ************      Front Panel Display
PDM             Rev 03   740-013110   ************      Power Distribution Module
PEM 0           Rev 08   740-013683   ************      DC Power Entry Module
PEM 1           Rev 08   740-013683   ************      DC Power Entry Module
PEM 2           Rev 08   740-013683   ************      DC Power Entry Module
PEM 3           Rev 08   740-013683   ************      DC Power Entry Module
Routing Engine 0 REV 12   740-013063   ************      RE-S-2000
...
Routing Engine 1 REV 12   740-013063   ************      RE-S-2000
```

```
...
CB 0          REV 08   710-021523   ************     MX SCB
CB 1          REV 08   710-021523   ************     MX SCB
CB 2          REV 08   710-021523   ************     MX SCB
FPC 0         REV 16   750-031089   ************     MPC Type 2 3D
...
FPC 1         REV 16   750-031089   ************     MPC Type 2 3D
...
FPC 2         REV 16   750-031089   ************     MPC Type 2 3D
...
```

Tabela 10 - Recolha do hardware instalado no equipamento Juniper MX960 da intervenção

De acordo com o *hardware* instalado no chassis, apresentados na tabela 10, os cálculos para os requisitos de alimentação são dados por:

Consumo = Base system (8.3 A) + 3 SCBs (3.1 A) + 2 Routing Engines (1.9 A) + 3 FPC (9.17 A) = 48 A @ 48 VDC

Consumo = 48 * 48

Consumo = 2304 W DC

O valor real previsto dos consumos de energia do equipamento é de 2304 W. Este é o valor apresentado na proposta de instalação do equipamento e pretende servir de base para todos os testes que serão realizados quando a intervenção terminar. Posteriormente, na fase de testes, é comparado este valor ao recolhido do equipamento para comprovar a sua conformidade.

Requisitos de energia para o equipamento Juniper T640 DC

Como referido anteriormente, o equipamento Juniper T640 é um elemento alvo de uma intervenção intermédia, no entanto como se trata da rede de *Core*, tem de ser garantido com todo o rigor como se se tratasse da implementação final da solução.

Os *upgrades* à rede são essenciais e constantes, por isso, de forma a suportar um crescimento ao nível de hardware sem ter de alterar a infra-estrutura de alimentação, devem ser seguidas as seguintes recomendações do fabricante (Juniper Networks, 2011):

- 68 A @ –48 VDC (nominal) para cada entrada de energia das fonte de alimentação de 160-A DC de duas entradas.

De seguida é apresentada a tabela 11 com os valores individuais para cada componente de forma a calcular a energia necessária adequado ao *hardware* instalado.

Componente	Corrente necessária (Amps @ –48 VDC)
Base system, not including FPCs and PICs (includes five SIBs, one host subsystem, one SCG, cooling system, and craft interface), and two DC power supplies	16.9 A
SIB: Standard SIB, standard SIB version B, or T640-SIB	0.8 A
Enhanced FPC1 and Enhanced II FPC1	3.4 A
Enhanced Scaling FPC1	7.1 A
FPC2, Enhanced FPC2, and Enhanced II FPC2	3.4 A
Enhanced Scaling FPC2	7.5 A
FPC3, Enhanced FPC3, and Enhanced II FPC3	6.8 A
Enhanced Scaling FPC3	9.1 A
Type 4 FPC	8.2 A
T640 Enhanced Scaling FPC4-1P	7.0 A
Host subsystem (Routing Engine and T-CB)	2.6 A
SCG	0.2 A
Power supply	1.7 A
Cooling system (normal speed)	6.7 A
Cooling system (full speed)	22 A
Craft interface	0.2 A
PIC—Generalized typical value	0.625 A
PIC (Type 3)—Generalized maximum value	1.2 A
PIC (Type 4)—Generalized maximum value	3.3 A

Tabela 11 - Requisitos de energia por componentes do equipamento Juniper T640 (Juniper Networks, 2011)

De acordo com o *hardware* instalado no chassis, os cálculos para os requisitos de alimentação são dados por:

Consumo = Base System (16.9 A) + 5 Enhanced Scaling FPC3 (9.1 A) + 2 Routing engine (2.6 A) + 17 PICs (1.2 A) = 88 A @ –48 VDC

Consumo = 4224 W DC

O valor real de consumo do equipamento é de 4224 W. Tal como para o equipamento Juniper MX960, este é o valor apresentado na proposta de instalação do equipamento e vai servir de comparativo para os testes que serão realizados. Posteriormente neste documento, na secção 5.1, é comparado este valor ao recolhido do equipamento no final da intervenção de forma a poder comprovar a sua conformidade.

2.3.8 Recursos afectos à intervenção

Dos recursos necessários à intervenção, foram os recursos humanos que mais atenções mereceram devido à alocação a outros projectos. O equipamento necessário e de substituição no caso de falhas, foram garantidos por outras equipas de trabalho de outros departamentos. Esta componente do projecto foi assumida como garantida uma vez que apenas foram apresentados os requisitos e outro grupo de trabalho providenciou os equipamentos e condições necessárias.

Material a existir nos sites de intervenção:

- Devem existir no site REs, MPCs, MICs e XFPs de substituição, pelo menos, um de cada tipo dos afectos a esta intervenção [NSN].
- Patch cords instalados e devidamente acessíveis necessários de modo a acomodar todos os circuitos identificados à migração [OPERADORA A].
- A identificação dos patch cords deve ser de forma unívoca em ambas as pontas [OPERADORA A].
- Contactar a supervisão de forma a dar início e no final dos trabalhos [OPERADORA A].
- Chaves Philips [NSN].
- Cabos de consola para os equipamentos em questão [NSN].
- Pulseira electrostática. [NSN]

Recursos materiais

Como referido anteriormente neste documento, foi planeado incluir material suplente na intervenção para no caso de haver falhas de hardware ser mais fácil recuperar o estado do equipamento. A existência de um componente de substituição de cada tipo é considerado suficiente para garantir a execução da intervenção. Para todas as intervenções foi realizada uma lista de componentes de substituição (*spare part*) de acordo com as necessidades individuais. De seguida, na tabela 12 é mostrado um exemplo, para o caso particular da intervenção de integração do Juniper MX960.

Spares para a intervenção		
Quantidade	**Modelo**	**Descrição**
1	RE-S-2000-4096-S	Routing Engine
1	MX-MPC2-3D-R-B	Line Card
1	MIC-3D-4XGE-XFP	Modular Interface Card
1	XFP-10G-L-OC192-SR1	10Gbps Multi-modeTransceiver
1	XFP-10G-S	10Gbps Single-mode Transceiver

Tabela 12 – Exemplo de lista de *spare parts* para a intervenção (MX960)

Recursos humanos

Foi definido que teriam de existir equipas de suporte antes, durante e após a intervenção para cobrir o período de preparação, intervenção e monitorização respectivamente.

O suporte no site de intervenção no dia da intervenção é composta por:

- A equipa NSN é composta por dois técnicos.
- A equipa da Operadora A é composta por técnicos de operações, monitorização e suporte à intervenção no site. O número de pessoas é definido pela operadora A.

O suporte para monitorização da rede no dia seguinte à intervenção é realizado por uma equipada NSN e outra da Operadora A. A composição das equipas é definida por:

- A NSN disponibiliza um técnico para suporte no dia seguinte à intervenção.

- A Operadora A disponibiliza técnicos para monitorização no dia seguinte à intervenção, não estando definido a sua quantidade.

2.4 Síntese

Neste capítulo foram reunidos as necessidades da Operadora A enquanto fornecedor de serviços e foi proposta uma solução e realizado um planeamento para a execução do projecto. O planeamento do projecto inclui a análise de riscos, definição de pressupostos de execução e alocação de recursos.

O capítulo seguinte descreve a etapa de testes referentes à solução, que fornecem apoio à tomada das decisões da proposta. Os testes efectuados têm como base um cenário de laboratório baseado na rede de produção de forma a garantir a aproximação ideal ao caso real e poder assim comprovar o esperado. Adicionalmente, como existem trocas de equipamentos são realizados ainda testes de balanceamento e de *software*.

Esta página foi intencionalmente deixada em branco

3. Implementação laboratorial da solução

Constituindo uma componente essencial no projecto, a fase de testes consiste na implementação da rede de produção em ambiente de simulação e implementar as funcionalidades e configurações de forma a comprovar o funcionamento da proposta do projecto sem colocar em risco a rede de produção. Este capítulo descreve o planeamento destes testes e a apresentação do resultado dos mesmos.

3.1 Cenário de rede do laboratório

A definição do cenário de rede no laboratório teve como base a representação da rede de produção em ambiente independente. Foram configurados equipamentos à semelhança da rede real de forma a testar o encaminhamento, o balanceamento, a versão do sistema operativo e o hardware dos equipamentos. Para se conseguir representar o ambiente de laboratório teria de se utilizar um número equivalente de equipamentos físicos configurados da mesma forma que os do ambiente de rede real o que se tornaria impossível devido ao custo e espaço que ocuparia todo esse equipamento. Para tal usam-se técnicas como a virtualização para simular equipamentos físicos. Estes equipamentos virtuais são denominados de *logical systems.* Como não vão ser realizados teste de performance, apenas de funcionalidade, um equipamento físico pode criar/gerir um largo conjunto de outros virtuais. Como a performance não vai ser alvo de testes, desde que se consigam reproduzir os cenários, não é relevante o modelo dos equipamentos desde que preencham os requisitos ao nível das funcionalidades, daí terem sido usados dois *routers* Juniper M320 e um Juniper MX960. Com três equipamentos físicos disponíveis, foi definido o seguinte cenário de laboratório presente na tabela 13.

Equipamento Físico	Logical systems	Função na rede
M320_1	BR_LAB1	Border Router
	PE_18A	Provider Edge Router
	PE_18B	Provider Edge Router
	PE_23A	Provider Edge Router
	PE_23B	Provider Edge Router
	F1	
	F2	
M320_2	CR_A1	*Core* Router
	P1	
	P2	
	CR_B1	*Core* Router
	CR_C1	*Core* Router
	CR_D1	*Core* Router
MX960_1	C1	
	C2	
	CR_A2	*Core* Router
	CR_B2	*Core* Router
	CR_C2	*Core* Router
	CR_D2	*Core* Router

Tabela 13 - Caracterização do cenário de rede de laboratório

De forma a conectar os equipamentos necessários para a realização dos testes de acordo com a rede de produção, foram reservadas interfaces físicas para cada *logical system* e realizadas as ligações entre eles. A definição dos *logical systems* em cada um dos equipamentos físicos não obedeceu a nenhum critério específico. Como a rede de laboratório é usada por várias equipas de trabalho, este processo de definição assentou sobre a disponibilidade do equipamento para receber configurações, ou seja, foi um processo faseado dependente da utilização do equipamento por parte de outras equipas de trabalho.

A ilustração 7 representa o diagrama físico de rede de laboratório definido para os efeitos

anteriormente referidos.

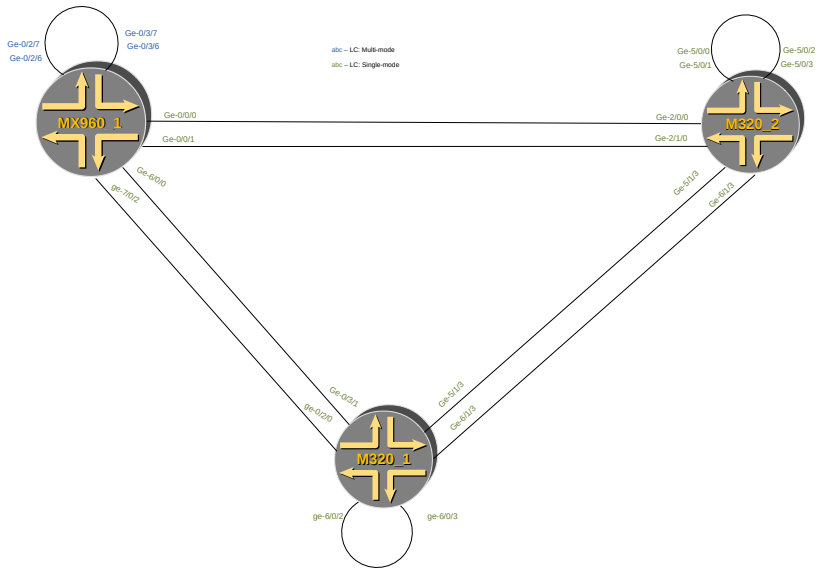

Ilustração 7 - Cenário físico de rede do laboratório

Tal como referido anteriormente, a composição do cenário de simulação teve como base a virtualização de equipamento pois só assim era possível representar todos os equipamentos físicos. A virtualização é uma funcionalidade que pode ser usada nos equipamentos de teste de forma a representar logicamente um equipamento físico. A configuração é realizada nos três equipamentos alvo de acordo com as necessidades individuais através de comandos de consola. Um *logical-system* configura-se através da sequência de comandos exemplo da tabela 14.

Comandos
##nomear o logical system set logical-systems name **##configurar a interface física** set interfaces fe-1/1/3 description "main router interface" **##configurar a interface do logical system** set logical-systems LS1 interfaces fe-1/1/3 unit 0 family inet address 10.11.2.2/24 **##submeter as configurações**

commit **User** - utilizador autenticado no router **Host** - nome do equipamento físico a que está associado o logical system **Name** – nome do logical system

Tabela 14 - Comandos necessários para a configuração de um logical system

A representação lógica da configuração de rede física anteriormente definida, que representa a rede de produção no final do projecto é mostrada na ilustração 8.

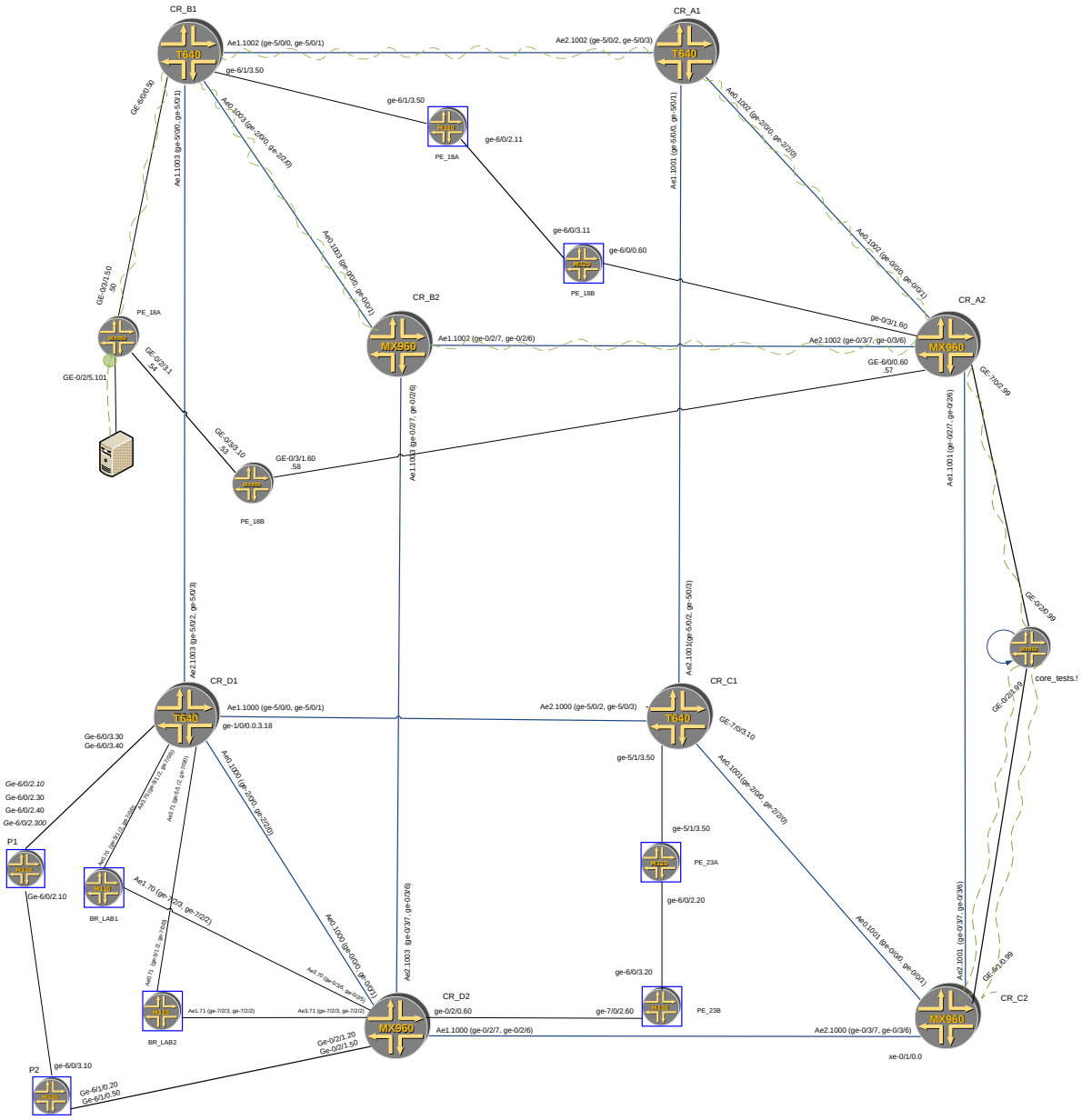

Ilustração 8 - Diagrama lógico de rede de laboratório

Após ser submetida a configuração e testada a conectividade entre os *logical systems*, foram definidos os testes. De seguida são caracterizados os testes, começando por definir o cenário de rede de produção seguido do cenário de rede simulado em laboratório.

3.2 Topologia da rede de produção

Como referido anteriormente neste documento, o cenário de laboratório pretende representar em ambiente de simulação o cenário da rede de produção final após as intervenções.

A ilustração 9 identifica o cenário de rede em produção e pretende mostrar quais os elementos de rede que fazem parte das intervenções bem como os adjacentes que podem ser afectados. À data, a rede de *Core* dispõe de oito equipamentos Juniper T640 como elementos do *Core* alvos de intervenção. Como referido no capítulo 4, duas das etapas do projecto prevêem a substituição de equipamentos e a migração de funções dos Juniper T640 para os Juniper MX960. O cenário de laboratório apresenta a topologia final da rede de produção.

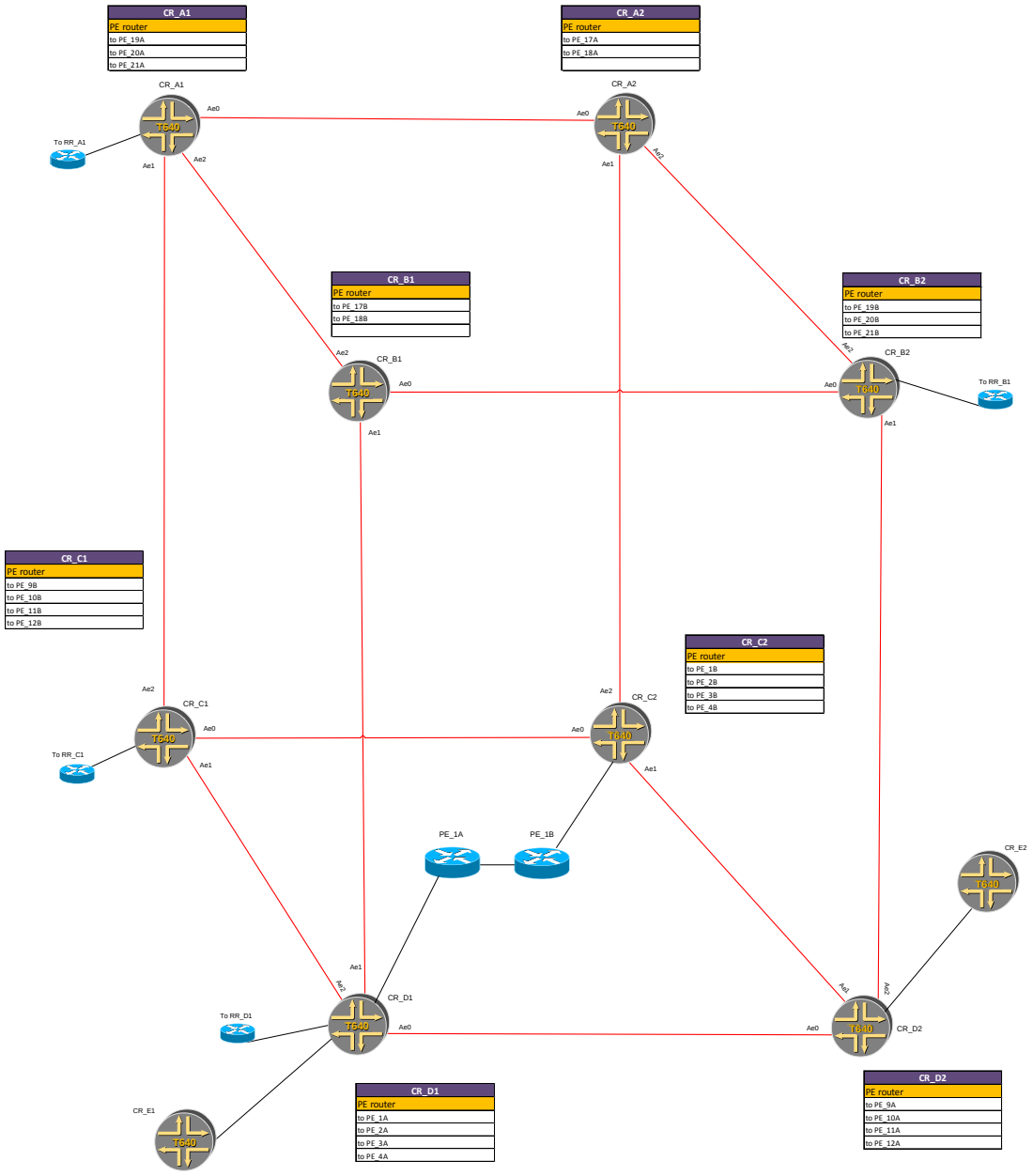

Ilustração 9 – Diagrama físico da rede de produção antes das intevenções

Através da análise da figura, identificam-se os elementos alvo das intervenções pelo nome CR_xx onde "CR" significa que se trata de um elemento do *Core* e "X" assinala a sua localização e a sua identificação individual. Os restantes equipamentos identificados como PEs são *routers* que podem ser afectados nas intervenções mas são monitorizados e

controlados pelas equipas da Operadora A, não fazendo parte das responsabilidades da NSN nos trabalhos.

3.3 Descrição dos testes

Antes das implementações dos projectos serem aplicadas na rede de produção têm de ser testadas em ambiente independente, num cenário de laboratório. Depois de configurar os equipamentos de laboratório de acordo com o cenário real são definidos alguns testes entre eles a validação da versão de software e balanceamento de carga entre os *links*. O balanceamento de tráfego foi testado com geradores dedicados, no entanto a configuração desse equipamento não fez parte do trabalho efectuado no estágio pelo que para justificar foram retirados apenas os *outputs* do equipamento em teste. Posteriormente são apresentados os resultados destes testes.

Os testes de laboratório incluem o teste à configuração. A configuração é definida pelas equipas de engenharia da Operadora A em conjunto com a NSN e testada pela NSN de forma a garantir a sua conformidade com o equipamento. Os testes foram realizados por etapas de acordo com:

- Testes da configuração
  - funcionalidades gerais
  - encaminhamento
  - balanceamento do tráfego
- Testes de software
  - Upgrade
  - Downgrade
- Testes de Hardware
  - Requisitos de alimentação

3.4 Resultados dos testes

Os testes da configuração referentes à definição das funcionalidades gerais e do encaminhamento foram testadas logo após a configuração do cenário de rede do laboratório. Como a configuração assenta sobre uma configuração base já estabelecida na rede noutros equipamentos de *Core*, apenas pequenos componentes da configuração foram testados pela NSN na etapa de *commissioning* do equipamento, os restantes testes ficaram a cargo da Operadora A.

3.4.1 Testes de configuração: Balanceamento de tráfego

Quando existem grandes quantidades de tráfego a circular numa rede, a tendência é haver congestão de tráfego. Para auxiliar nas comunicações a este nível, implementam-se mecanismos de balanceamento de tráfego. A topologia de rede da Operadora A, conforme descrito anteriormente, possui ligações agregadas de várias interfaces. A ilustração 10 mostra um exemplo de uma configuração de cenário onde pode ser necessário configurar o balanceamento entre dois agregados de duas interfaces.

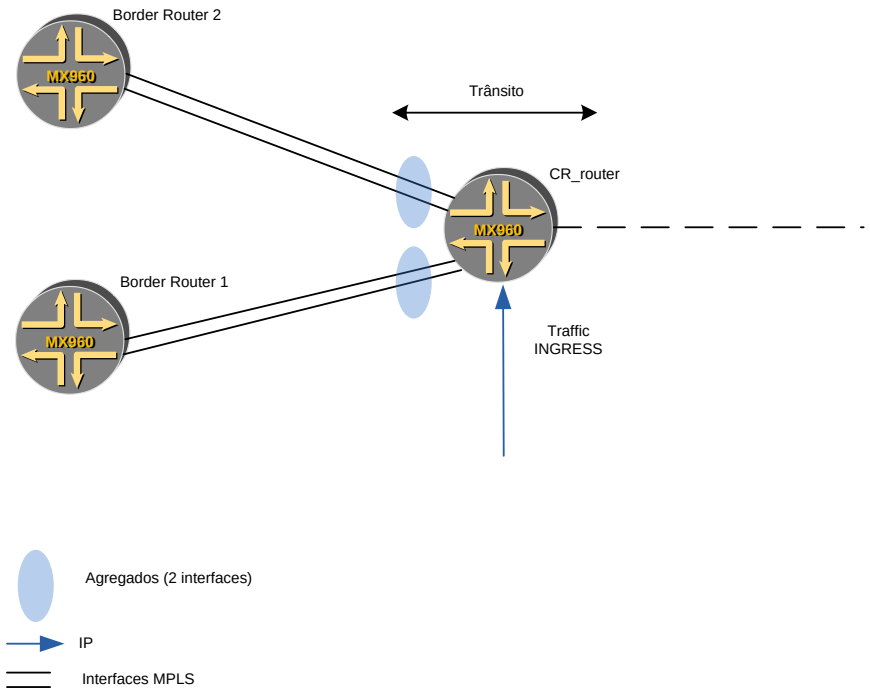

Ilustração 10 – Cenário exemplo de balanceamento de tráfego

A ilustração 11 apresenta um resumo do comportamento esperado da funcionalidade de balanceamento de tráfego.

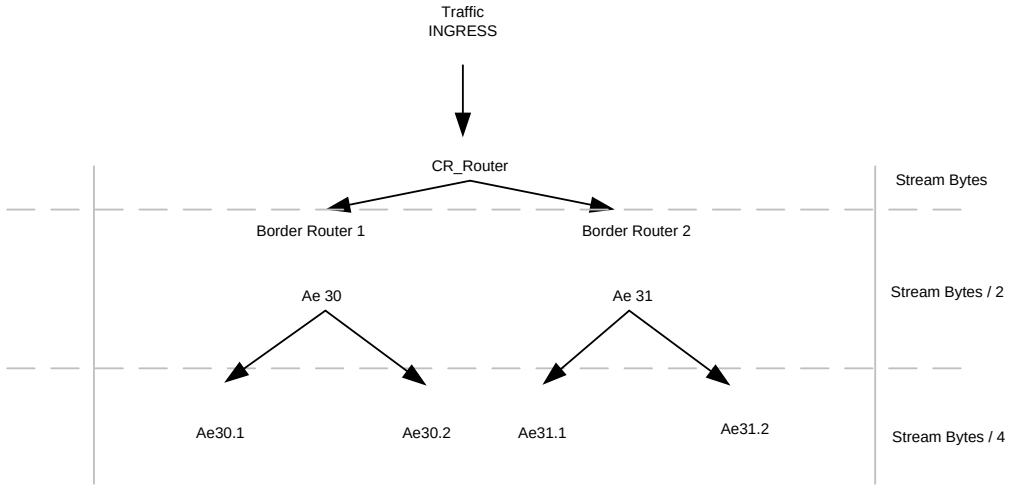

Ilustração 11 – Comportamento da funcionalidade de balanceamento de tráfego

Como é possível ver pela análise da ilustração 11, a entrada do tráfego é feita no router de *Core* (CR_Router) que depois tem a função de encaminhar o tráfego para dois *Border Routers* (Border Router 1 e Border Router 2) de forma balanceada. Considerando-se *Stream Bytes* a quantidade de dados que o CR_router recebe, na interface destino pretende-se receber um valor aproximado a *Stream Bytes* /4.

A pedido do cliente, foi necessário fazer testes de balanceamento. Os testes consistem em gerar 1000 *streams* com definição de *Source Address* e *Destination Address* usando o protocolo TCP para o transporte. Os equipamentos escolhidos como exemplo foram CR_B1 e P1 e as leituras dos resultados teriam de ser realizadas na interface do *Destination Address*. Foram também sendo feitos outros testes noutros pontos da rede à semelhança do mostrado. É esperado que exista balanceamento do tráfego entre os *links* e entre os agregados que compõem a ligação entre os equipamentos. Através do comando *show interfaces ae3 extensive* recolhem-se as estatísticas das interfaces que permitem comprovar o esperado. No capítulo 5 são mostrados os resultados.

3.4.2 Upgrade / Downgrade do software

Os testes de *upgrade / downgrade* do software são realizados depois do fecho da configuração. Com a configuração carregada no equipamento são efectuados testes com diferentes versões de *software* candidatas. A instalação de novas versões de *software* permite corrigir problemas detectados em versões anteriores assim como permite a implementação de novas funcionalidades futuramente.

Estes testes pretendem fazer o despiste de problemas relacionados com mudanças na configuração provocadas por essa troca de versões. Apenas são feitos testes de *upgrade / downgrade* de versões de *software* homologadas, isto é, certificadas pela Operadora A.

Para estes testes foi definido um procedimento presente no anexo B deste documento, que inclui de forma detalhada os passos necessários para efectuar a tarefa, bem como o procedimento de contingência. Como o objectivo geral é testar a aceitação da versão de software no equipamento e particularmente caso a caso, as configurações que são alteradas em cada um, o procedimento foi um trabalho elaborado a pensar na necessidade que existe actualmente em futuras intervenções de upgrade de equipamentos na rede.

3.5 Sintese

Neste capítulo foram realizados testes de laboratório necessários à implementação da solução que justificam a tomada de decisões para as soluções apresentadas.

O capítulo seguinte descreve as etapas que compõem a implementação da proposta na rede da Operadora A detalhando todos os procedimentos de execução das tarefas. A implementação é composta por etapas de integração e migração de elementos na rede de *Core*

4. Implementação da solução

A preparação das intervenções seguiu alguns critérios, entre eles a alocação de recursos, definição de datas e planeamento das acções a tomar para a execução das tarefas. Este capítulo pretende descrever todo o processo de execução das tarefas bem como o planeamento das acções e a elaboração dos procedimentos necessários. Como descrito no capítulo 3, apesar de o projecto envolver várias intervenções, não estão todas documentadas neste relatório, sendo que, a implementação de uma etapa demonstra o trabalho, efectuado para as outras.

4.1 Etapa 1 - Integração de elementos no *Core*

Esta etapa pretende descrever a fase do projecto que consiste na integração de novos elementos no *Core*. Os novos elementos a integrar no *Core* são os equipamentos Juniper T640 e Juniper MX960 conforme já descritos anteriormente. Estes equipamentos pretendem tomar o lugar de elementos do *Core* existentes e fazer esses existentes ocupar outro papel na rede, não estando incluído neste projecto a configuração dos mesmos.

4.1.1 Descrição do procedimento

Depois de serem definidas as necessidades do cliente, pretende-se descrever todos os passos necessários de forma a completar a intervenção com sucesso. De seguida é resumido na ilustração 12 todos os passos necessários para completar a tarefa de integração, posteriormente são definidas as tarefas e detalhados os pontos do procedimento.

É assumido que a intervenção correspondente ao CR_A2 e CR_A1 é realizada à semelhança da apresentada nesta secção, correspondente a CR_B2 e CR_B1, pelo que não será documentada neste documento apesar de ter feito parte do projecto.

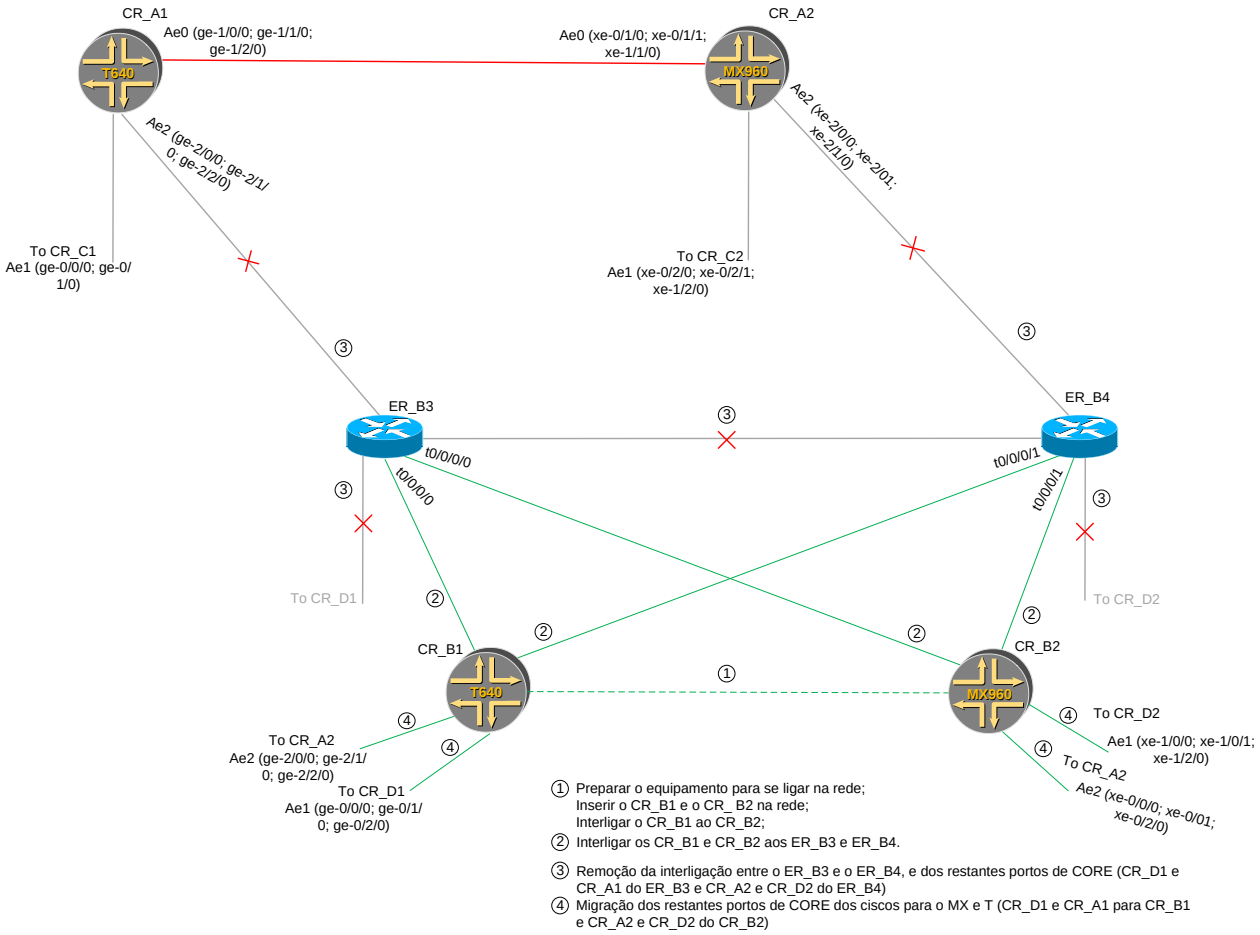

Ilustração 12 - Diagrama físico de rede alvo de intervenção

De forma a simplificar o planeamento da intervenção, o processo de integração foi dividido em quatro pontos. De seguida são explicadas com detalhe, cada uma das fases:

1. Preparação do equipamento ou *commissioning*, esta preparação do equipamento envolve duas partes. O *commissioning* e a instalação física do equipamento no bastidor destino. No ponto 4.1.2 é descrito todo o processo de preparação do equipamento.

2. Activação dos portos de *Core*. Depois da instalação física dos equipamentos, é feita uma ligação entre eles que mais tarde se vai transformar numa ligação de *Core*.

3. Remoção da interligação entre ER- B3 e ER-B4 e dos restantes portos de *Core* (CR_D1 e CR_A1 do ER_B3; CR_A2 e CR_D2 do ER_B4).

4. Migração dos restantes portos do *Core* dos equipamentos Cisco para o MX e T (CR_D1 e CR_A1 do CR_B1 e CR_A2 e CR_D2 do CR_B2).

O método de recolha de dados para efectuar os procedimentos foi baseado nas interfaces recolhidas da configuração de produção dos equipamentos que não pôde ser apresentada neste documento por razões de sigilo, desta forma as interfaces anunciadas que não apresentem correspondência nas tabelas de mapeamento devem ser consideradas como o que representam mesmo sem terem uma ligação lógica neste documento que o justifique.

4.1.2 Fase 1 – Preparação do equipamento

Commissioning

Todos os equipamentos envolvidos passaram por uma fase de preparação denominada *Commissioning*. Esta etapa consiste em fazer uma configuração inicial básica no equipamento e é semelhante a todos os *routers* envolvidos neste projecto.

A preparação do equipamento incluindo a configuração básica, depois de ser recebido do fabricante envolve as seguintes tarefas:

1. O equipamento é desembalado e instalam-se os componentes que compõem o chassis (fontes de alimentação, cartas, entre outros);
2. Ligar o equipamento à alimentação e fazer o *power up*;
3. Entrar no modo de configuração do equipamento;
4. Configurar a interface de configuração via Ethernet;
5. Activar o acesso à consola via *telnet*;
6. Criar acesso privilegiado (root) e definir a *password* para acesso privilegiado;
7. Testar os acessos;
8. Instalar \ actualizar o sistema operativo. Como o sistema implementa

redundância ao nível do processamento, este processo é feito para ambas as *Routing Engines*;

9. Carregar a configuração que vai ser usada em produção.

   Neste passo, é carregada a configuração testada em laboratório e aprovada pela Operadora A. Esta configuração apresenta tudo o que é necessário para o funcionamento a que se propõem, no entanto algumas funcionalidades entram na rede desactivadas, como por exemplo as interfaces e o encaminhamento com o protocolo IS-IS. Posteriormente, após verificações, são activadas progressivamente para completar todo o processo.

   À configuração inserida no equipamento nesta etapa pode ser necessário aplicar um *Delta* (ficheiro que assinala diferenças) que corresponde a pequenas correcções na configuração que possam surgir antes da intervenção e depois da etapa de *commissioning*.

Depois de ser realizado o procedimento de *commissioning* os equipamentos são instalados fisicamente no bastidor destino de instalação. A instalação física do equipamento é realizada de acordo com instruções do fabricante. Como a instalação é realizada pelas equipas de operações da Operadora A, a NSN apenas supervisiona e garante a conformidade com o exigido pelo fabricante. Nos anexos A e B são definidos os processos de instalação para cada equipamento.

Recolha do estado inicial

Esta fase também terá início durante o dia da intervenção, mais precisamente imediatamente antes da janela de intervenção e não causa qualquer indisponibilidade de serviço.

Nesta fase são recolhidos os parâmetros de configuração dos *routers* ao nível da redundância e protocolos e ainda os registos de log existentes nos equipamentos. As configurações de redundância (ligações e alimentação do equipamento) e ao nível protocolar (encaminhamento e funcionalidades gerais) são importantes de salvaguardar pois como as intervenções são realizadas na rede de produção é necessário recolher

padrões de tráfego a determinadas horas do dia para poder comprovar a conformidade dos trabalhos no final da intervenção. Os *logs* servem para analisar o histórico de actividades no equipamento para despiste de eventuais problemas.

No final da intervenção são recolhidos os mesmos parâmetros que irão ser comparados com os iniciais de forma a garantir o serviço.

Conforme descrito na secção 3.1, nesta fase não esteve prevista qualquer perturbação no serviço, porém, como iria haver uma modificação da arquitectura de rede e a intervenção seria no *Core*, deveria ser executada dentro de uma janela de intervenção.

4.1.3 Fase 2 – Activação dos portos de *Core* que interligam CR_B1 e CR_B2

Partindo do princípio que a configuração de produção está presente no *router* mas permanece por activar, nesta fase começa-se por activar os portos de *Core* entre o CR_B1 e CR_B2. Para tal, foi definido o seguinte procedimento:

1. Verificar a potência óptica dos portos que compõem o agregado 0 (ae0) de ambos os equipamentos. Com a verificação da potência óptica testa-se a conectividade entre interfaces.

Comandos
##########MX960 ##### ae0 show interfaces diagnostics optics xe-2/0/0 show interfaces diagnostics optics xe-2/0/1 show interfaces diagnostics optics xe-2/2/0 ######T640 ##### ae0 show interfaces diagnostics optics ge-1/0/0 show interfaces diagnostics optics ge-1/1/0 show interfaces diagnostics optics ge-1/2/0

Tabela 15 - Activação dos portos de *Core* – Verificação das potências ópticas

2. "*no shutdown*" entre os portos de *Core* CR_B1 e CR_B2 – Activação das interfaces que entram na configuração no modo desactivado.

Comandos
##########MX960
edit private
delete interfaces xe-2/0/0 disable
delete interfaces xe-2/0/1 disable
delete interfaces xe-2/2/0 disable
commit
exit
######T640
edit private
delete interfaces ge-1/0/0 disable
delete interfaces ge-1/1/0 disable
delete interfaces ge-1/2/0 disable
commit
exit

Tabela 16 – Activação dos portos de *Core* – Activação de interfaces

3. Verificar o encaminhamento nos equipamentos Juniper MX960, T640 e em elementos adjacentes da rede.

Comandos
##########MX960
show IS-IS adjacency | no-more
show IS-IS interface | no-more
show ldp session | no-more
show ldp interface | no-more
show ldp route | no-more
######T640
show IS-IS adjacency | no-more
show IS-IS interface | no-more

show ldp session | no-more show ldp interface | no-more show ldp route | no-more

Tabela 17 - Activação dos portos de *Core* –Encaminhamento de elementos adjacentes

No final da activação das interfaces, deve ser consultado o estado dos protocolos de encaminhamento e verificar que existe tráfego nas interfaces. No caso de afirmativo, esta fase fica concluída.

4.1.4 Fase 3 – Integração dos equipamentos CR_B1 e CR_B2 na rede

Nesta fase é efectuada a interligação dos portos entre os CR_B1 e CR_B2 aos ER_B3 e ER_B4. Esta fase envolve duas etapas, a migração dos portos de *Core* e integração de novos elementos no *Core.*

Migração dos portos de *Core* dos ER_B3 e ER_B4 para o CR_B1 e para o CR_B2

Esta fase inclui a migração dos portos de *Core* referentes aos CR_B1 e CR_B2 e é composta pelas seguintes etapas:

1. Efectuar a ligação do *patch* ao CR_B2 no porto xe-0/1/0 e xe-1/1/0.
2. Verificar a potência óptica de ambos os portos.

Comandos
#######MX960 show interfaces diagnostics optics xe-0/1/0 show interfaces diagnostics optics xe-1/1/0 ######T640 show interfaces diagnostics optics ge-0/3/0 show interfaces diagnostics optics ge-2/3/0

Tabela 18 – Interligação dos – Activação de interfaces

3. Efectuar "*no shutdown*" do porto xe-0/1/0.
4. Verificar *routing* no CR_B2 e em elementos adjacentes da rede.
5. Efectuar "*no shutdown*" do porto xe-1/1/0.
6. Verificar *routing* no CR_B2 e em elementos adjacentes da rede.

Comandos
#######MX960 edit private delete interfaces xe-0/1/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more show ldp session | no-more show ldp interface | no-more show ldp route | no-more edit private delete interfaces xe-1/1/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more show ldp session | no-more show ldp interface | no-more show ldp route | no-more

Tabela 19 - Comandos para migração dos portos de *Core* do Router Juniper MX960

7. Efectuar ligação do patch ao CR_B1 no porto ge-0/3/0 e ge-2/3/0.
8. Verificar a potência óptica de ambos os portos.
9. Efectuar "no shutdown" do porto ge-0/3/0.
10. Verificar *routing* no CR_B1 e em elementos adjacentes da rede.
11. Efectuar "no shutdown" do porto ge-2/3/0.
12. Verificar *routing* no CR_B1 e em elementos adjacentes da rede.

Comandos
######T640 edit private delete interfaces ge-0/3/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more show ldp session | no-more show ldp interface | no-more show ldp route | no-more edit private delete interfaces ge-2/3/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more show ldp session | no-more show ldp interface | no-more show ldp route | no-more

Tabela 20 - Comandos para migração dos portos de *Core* do Router T640

Integração dos novos elementos no *Core*

Esta etapa pretende descrever o processo para remover as ligações dos ER_B3 e ER_B4 ao *Core* e ligá-los no CR_B1 e CR_B2. Os comandos de execução da tarefa são semelhantes aos executados na fase 3, pelo que na tabela 21 apenas são resumidos os comandos a executar de acordo com os pontos-chave recolhidos de seguida e não é detalhado o seu significado.

1. Shutdown das portas de interligação para CR_A2 em ER_B4 [OPERADORA A].
2. Migrar a ligação do *patch* ao CR_B2 nos portos ae2 (para CR_A2) [OPERADORA A/NSN].
3. Verificar a potência óptica de ambos os portos ae2 [NSN].

4. Verificar *routing* no CR_B1 e em elementos adjacentes da rede [OPERADORA A/NSN].
5. Shutdown das portas de interligação para CR_D2 em ER_B4 [OPERADORA A].
6. Migrar a ligação do patch ao MX960 nos portos ae1 (para CR_D2) [OPERADORA A/NSN].
7. Verificar a potência óptica de ambos os portos ae1 [NSN].
8. Verificar *routing* no CR_B2 e em elementos adjacentes da rede [OPERADORA A/NSN].
9. *Shutdown* das portas de interligação para CR_A1 em ER_B3 [OPERADORA A].
10. Migrar a ligação do patch ao CR_B1 nos portos ae2 (para CE_A1) [OPERADORA A/NSN].
11. Verificar a potência óptica de ambos os portos ae2 [NSN].
12. Verificar *routing* no CR_B1 e em elementos adjacentes da rede [OPERADORA A/NSN].
13. *Shutdown* das portas de interligação para CR_D2 em ER_B4 [OPERADORA A].
14. Migrar a ligação do *patch* ao CR_B1 nos portos ae1 (para CR_D1) [OPERADORA A/NSN].
15. Verificar a potência óptica de ambos os portos ae1 [NSN].
16. Verificar *routing* no CR_B1 e em elementos adjacentes da rede [OPERADORA A/NSN].

Comandos
ae2 show interfaces diagnostics optics xe-0/0/0 edit private delete interfaces xe-0/0/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more show ldp session | no-more show ldp interface | no-more show ldp route | no-more

```
##### ae1
show interfaces diagnostics optics xe-1/0/0

edit private
delete interfaces xe-1/0/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more
show ldp session | no-more
show ldp interface | no-more
show ldp route | no-more

##### ae2
show interfaces diagnostics optics ge-2/0/0

edit private
delete interfaces ge-2/0/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more
show ldp session | no-more
show ldp interface | no-more
show ldp route | no-more

##### ae1
show interfaces diagnostics optics ge-0/0/0

edit private
delete interfaces ge-0/0/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more
show ldp session | no-more
show ldp interface | no-more
```

show ldp route | no-more

Tabela 21 - Comandos para integração de novos elementos no *Core*

4.1.5 Fase 4 – Migração dos portos do RR e dos PEs

Nesta etapa são removidas as ligações dos equipamentos ER_B3 e ER_B4 dos PEs e adicionadas aos equipamentos CR_B1 e CR_B2. De seguida é apresentado o procedimento definido para completar a tarefa.

1. Desligar as portas de interligação entre RR_A1 e ER_B2 **[OPERADORA A].**
2. Migrar a ligação do *patch* ao CR_B2 nos portos xe-2/1/1 (to SR_A1) **[OPERADORA A/NSN]**.
3. Verificar a potência óptica de ambos os portos xe-2/1/1 **[NSN]**.
4. Verificar *routing* no CR_B2 e em elementos adjacentes da rede que estiverem ligados ao RR **[OPERADORA A/NSN]**.
5. Desligar as portas de interligação entre RR_B1 e ER_B1 **[OPERADORA A].**
6. Migrar a ligação do *patch* ao T640 no porto ge-7/0/0 (to RMD1RRIP001) **[OPERADORA A/NSN]**.
7. Verificar a potência óptica de ambos os portos ge-7/0/0 **[NSN]**.
8. Verificar *routing* no MX960 e em elementos adjacentes da rede que estiverem ligados ao RR **[OPERADORA A/NSN]**.

Comandos
show interfaces diagnostics optics xe-2/1/1
edit private delete interfaces xe-2/1/1 disable commit exit
show IS-IS adjacency | no-more show IS-IS interface | no-more
show interfaces diagnostics optics ge-7/0/0

```
edit private
delete interfaces ge-7/0/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more
```

Tabela 22 - Migração do Route Reflector e dos Provider Edge *Routers*

4.1.6 Fase 5– Alteração dos fluxos de tráfego

O *Overload bit* é um identificador no IS-IS LSP usado para informar a rede de que um router anunciante não está disponível para encaminhar tráfego. Inicialmente foi introduzido para sinalizar sobrecarga ou anunciar à rede a redução dos recursos disponíveis em determinado *router*.

Usualmente este *bit* é activado quando se pretende isolar um *router* específico na rede para efectuar trabalhos de manutenção como substituição de equipamento, resolução de problemas relacionados com caminhos de rede entre outros. É muito útil aquando da instalação de um novo equipamento na rede antes de o colocar como encaminhador de tráfego ou prevenir que os *Route Reflectors* sejam usados na *routing path*.

O comando *set protocols IS-IS overload* no *router* alvo da intervenção desencadeia na rede a informação de que o equipamento não está preparado para encaminhar tráfego, ou por outras palavras, pede aos outros *routers* que não façam conta com ele como *transit hop* nos cálculos para o algoritmo *Shortest Path First* (SPF) que usa para definir as rotas.
Nesta fase, depois de desactivar o overload no IS-IS, espera-se a convergência do tráfego.

Desta forma, o restauro dos fluxos de tráfego é realizado da seguinte forma:

Comandos
delete protocolos IS-IS overload show | compare commit exit

Tabela 23 - Comandos para restauro dos fluxos de tráfego

Os *sites* B e C utilizam o protocolo IS-IS para encaminhamento e propagação de rotas, por isso a reconvergência do tráfego consegue-se desactivando a funcionalidade *overload* como referido anteriormente, no entanto para o site D para além de activar/desactivar o *overload bit*, correspondente ao encaminhamento do tráfego em geral, teve de ser activado/desactivado o protocolo BGP referente ao tráfego de propagação de rotas.

4.1.7 Fase 6– Migração dos PEs

O processo de migração dos PEs é análogo a todos os equipamentos, pelo que apenas é documentada a configuração para alguns PEs e os restantes terão uma configuração equivalente. Neste caso são migrados os PEs ligados nas interfaces Xe-1/3/0 do CR_B2 e das interfaces ge-2/0/0, ge-2/1/0 e ge-2/2/0.

Comandos
#####MX show interfaces diagnostics optics xe-1/3/0 edit private delete interfaces xe-1/3/0 disable commit exit show IS-IS adjacency | no-more show IS-IS interface | no-more #####T show interfaces diagnostics optics ge-2/0/0 show interfaces diagnostics optics ge-2/1/0 show interfaces diagnostics optics ge-2/2/0

```
edit private
delete interfaces ge-2/0/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more

edit private
delete interfaces ge-2/1/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more


edit private
delete interfaces ge-2/2/0 disable
commit
exit

show IS-IS adjacency | no-more
show IS-IS interface | no-more
```

Tabela 24 - Comandos para migração dos Provider Edge *Routers*

4.2 Etapa 2 - Migração de elementos no *Core*

A etapa de migração de equipamentos teve lugar em dois nós do *Core*. O procedimento de migração é análogo para ambos os nós. Desta forma vai ser apresentado um modelo genérico do procedimento e das tarefas efectuadas que é aplicado a ambas as intervenções. Os elementos de *Core* a migrar são CR_D2 e CR_C2.

4.2.1 Descrição do procedimento de migração

Para efectuar o procedimento foi necessário analisar as tarefas e verificar a duração de cada

uma, de acordo com as configurações a efectuar no equipamento. O procedimento envolve várias etapas que completam a intervenção com sucesso se forem realizadas pela ordem e dentro do tempo planeados. O cálculo da duração de cada etapa foi baseada na configuração a realizar no equipamento em comparação com projectos semelhantes realizados anteriormente. Na tabela 25 são resumidas as fases da intervenção e apresentados os valores de tempo usados para calcular as durações da actividade.

Planeamento da intervenção

Etapa	Descrição	Duração prevista
Fase 1	Verificação do estado inicial	60 mins
Fase 2	Alteração dos fluxos de tráfego	15 mins
Fase 3	Migração do Serviço	120 mins
Fase 4	Activação dos portos de ligação	25 mins
Fase 5	Restauro dos fluxos de tráfego	20 mins
Fase 6	Verificação do estado final	60 mins
Tempo necessário estimado para efectuar a intervenção com sucesso		5horas
Tempo alocado para rollback		2horas
Janela de Intervenção		00:00h – 07:00h

Tabela 25 - Planeamento da etapa de migração de elementos de *Core*

A janela de intervenção foi definida num dia acordado entre a Operadora A e a NSN e a sua duração teve por base no tempo estimado para a intervenção mais o tempo alocado para efectuar o *rollback* no caso em que a intervenção tenha de ser abortada. De seguida são definidas as etapas do procedimento numa ordem que deve ser respeitada de forma a completar a intervenção com sucesso.

4.2.2 Esquemas e ligações do equipamento

Os esquemas de ligações dos equipamentos tiveram como base a configuração das funcionalidades a implementar, as ligações a efectuar para tal e ainda o *hardware*

adquirido. De seguida na ilustração 13, é apresentado o mapeamento efectuado entre o equipamento antigo e o novo de forma a manter todas as ligações necessárias dado que se trata de uma tarefa de migração.

Ilustração 13 – Mapeamento físico de interfaces para a intervenção de CR_D2

Como referido na secção 3.1, é assumido que esta preparação de ligações é efectuada pela Operadora A antes da janela de intervenção.

A tabela 26 resume, por interface, qual o identificador a usar em cada fibra, de forma depois facilitar a ligação no equipamento novo. Esta tabela foi apresentada à Operadora A

de forma a auxiliar os trabalhos de migração das ligações.

T640	MX960	Identificador	Descrição
ge-0/0/0	xe-0/1/0	A0	To CR_D1 ge-0/0/0
ge-0/1/0	xe-0/1/1	A1	To CR_D1 ge-0/1/0
ge-0/2/0	xe-0/0/0	A2	To BR_D1 TG-0/1/0/0
ge-0/3/0	xe-0/0/1	A3	To BR_D1 TG-0/1/0/1
ge-1/0/0	xe-1/0/0	B0	To BR_D2 TG-0/1/0/0
ge-1/1/0	xe-1/0/1	B1	To BR_D2 TG-0/1/0/1
ge-1/2/0	xe-3/0/0	B2	To CR_C2 ge-0/0/0
ge-1/3/0	xe-3/0/1	B3	To CR_C2 ge-0/1/0
ge-2/0/0	xe-2/3/1	C0	To CR_E2 ge-0/3/0
ge-2/1/0	xe-3/3/0	C1	To CR_E2 ge-1/3/0
ge-2/2/0	xe-3/3/1	C2	To CR_E2 ge-2/2/0
ge-2/3/0	xe-2/3/0	C3	To PE_1
ge-3/0/0	xe-3/1/1	D0	To PE_2
ge-3/1/0	xe-2/1/1	D1	To PE_3
ge-3/2/0	xe-2/1/0	D2	To PE_4
ge-3/3/0	xe-1/3/1	D3	To PE_5
ge-4/0/0	xe-2/0/0	E0	To ER_B2
ge-4/1/0	xe-1/3/0	E1	To PE_6
ge-4/2/0	xe-3/1/0	E2	To ER_D2
ge-4/3/0	xe-1/1/1	E3	To PE_7
ge-7/0/0	xe-1/1/0	H0	To RR_D1 ge-0/0/1

Tabela 26 - Tabela do mapeamento de interfaces da intervenção de migração de CR_D2

4.2.3 Fase 1 – Verificação do estado inicial

Esta fase também terá início durante o dia da intervenção, uma hora antes da janela de intervenção e não causa qualquer indisponibilidade de serviço. Nesta fase são ainda recolhidos os parâmetros de configuração dos *routers* ao nível da redundância e protocolos e ainda os registos de *log* existentes nos equipamentos.

No final da intervenção são recolhidos os mesmos parâmetros que irão ser comparados com os iniciais de forma a garantir o serviço.

Conforme descrito no secção 3.1, nesta fase não esteve prevista qualquer perturbação no serviço, porém, como iria haver uma modificação da arquitectura de rede e a intervenção seria no *Core*, deveria ser executada dentro de uma janela de intervenção.

A verificação do estado inicial passa por:

- Teste de conectividade à consola do equipamento alvo de intervenção.
- Verificação da etiquetagem das FPCs/PICs para facilitar num possível *rollback*.

De seguida são descritos os passos do procedimento para efectuar esta fase.

Procedimento:	Recolha do estado inicial do T640 1. Alarmística; 2. Estado do *hardware*; 3. Estado dos processos e ocupação da memória;

Comandos
request support information | no-more
show log messages | no-more
show log chassisd | no-more
request routing-engine login other-routing-engine
show log messages | no-more
show log chassisd | no-more
exit
show chassis hardware detail | no-more
show interface terse | no-more
show interface descriptions | no-more
show chassis routing-engine | no-more
show chassis alarms | no-more
show system processes extensive | no-more

Tabela 27 - Comandos para recolha do estado inicial do equipamento a migrar

Milestone 1 - Avançar com o procedimento apenas se todas as verificações se encontrarem em conformidade, caso contrário avançar para a secção *Procedimento de Contingência* definido no ponto 4.2.9 deste documento.

Procedimento:	Efectuar verificação e *backup* da configuração actual do T640

Comandos
show configuration | no-more

Tabela 28 - Comandos para recolha e verificação da configuração do equipamento a migrar

É assumido que os equipamentos já possuem a configuração necessária à intervenção previamente carregada na etapa de *commissioning*, pelo que este comando serve para confirmação dessa configuração.

Procedimento:	Recolha do estado do serviço do T640 1. Verificação do estado do serviço (*routing*, MPLS e *bandwidth* das interfaces);

Comandos
show interfaces detail | no-more
show IS-IS adjacency | no-more
show IS-IS interface | no-more
show ldp session | no-more
show ldp interface | no-more
show ldp route | no-more
show bgp summary | no-more
show bgp neighbor 212.xxx.xxx.xxx | no-more
show bgp neighbor 212. xxx.xxx.xxx | no-more
show bgp neighbor 212. xxx.xxx.xxx | no-more
show bgp neighbor 212. xxx.xxx.xxx | no-more
show bgp neighbor 10. xxx.xxx.xxx | no-more
show route summary | no-more

Tabela 29- Recolha do estado ao nível protocolar do equipamento a migrar

Procedimento:	Verificar os estados das potências ópticas das interfaces do T640 para comparação posterior.

Comandos
show interfaces diagnostics optics ge-0/0/0 | no-more
show interfaces diagnostics optics ge-0/1/0 | no-more
show interfaces diagnostics optics ge-0/2/0 | no-more
show interfaces diagnostics optics ge-0/3/0 | no-more

show interfaces diagnostics optics ge-1/0/0 | no-more
show interfaces diagnostics optics ge-1/1/0 | no-more
show interfaces diagnostics optics ge-1/2/0 | no-more
show interfaces diagnostics optics ge-1/3/0 | no-more
show interfaces diagnostics optics ge-2/0/0 | no-more
show interfaces diagnostics optics ge-2/1/0 | no-more
show interfaces diagnostics optics ge-2/2/0 | no-more
show interfaces diagnostics optics ge-2/3/0 | no-more
show interfaces diagnostics optics ge-3/0/0 | no-more
show interfaces diagnostics optics ge-3/1/0 | no-more
show interfaces diagnostics optics ge-3/2/0 | no-more
show interfaces diagnostics optics ge-3/3/0 | no-more
show interfaces diagnostics optics ge-4/0/0 | no-more
show interfaces diagnostics optics ge-4/1/0 | no-more
show interfaces diagnostics optics ge-4/2/0 | no-more
show interfaces diagnostics optics ge-4/3/0 | no-more
show interfaces diagnostics optics ge-7/0/0 | no-more

Tabela 30 - Comandos para verificação do estado das potências ópticas

4.2.4 Fase 2 – Alteração dos fluxos de tráfego

Como referido na etapa 1 da implementação, a alteração dos fluxos de tráfego é realizado através da desactivação do *overload bit* no protocolo IS-IS.

A alteração dos fluxos de tráfego é realizada da seguinte forma:

Procedimento:	1. Activar o *overload bit* no protocolo IS-IS. 2. Verificar que o tráfego nas interfaces decresce para valores negligenciáveis. ***Nota:*** *Esta acção pode implicar a perda de conectividade remota ao equipamento alvo de intervenção. Por isso torna-se necessário ter uma forma de acesso de consola ao equipamento).*
Comandos	
edit private set protocols IS-IS overload exit show interfaces detail | no-more	

Tabela 31- Comando para alteração dos fluxos de tráfego

Nesta etapa, verifica-se nas plataformas de monitoria e serviço de que o tráfego é agora suportado por outros elementos de rede. Esta tarefa é da responsabilidade da Operadora A.

4.2.5 Fase 3 – Migração do Serviço

Embora não esteja previsto qualquer impacto no serviço dado que o tráfego já se encontra a cursar no **CR_D1** poderá existir algum tráfego residual ainda a cursar no **CR_D2**.

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à slot 0. 2. Efectuar o *shutdown* da FPC0. 3. Verificar de que o *hardware* ficou offline

Comandos
edit private set interfaces ge-0/0/0 disable set interfaces ge-0/1/0 disable set interfaces ge-0/2/0 disable set interfaces ge-0/3/0 disable commit exit request chassis pic fpc-slot 0 pic-slot 0 offline request chassis pic fpc-slot 0 pic-slot 1 offline request chassis pic fpc-slot 0 pic-slot 2 offline request chassis pic fpc-slot 0 pic-slot 3 offline request chassis fpc slot 0 offline show chassis fpc detail 0 show chassis fpc pic-status 0

Tabela 32 - Comandos para migração do serviço - Desactivação da slot 0

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à slot 1. 2. Efectuar o *shutdown* da FPC1. 3. Verificar de que o *hardware* ficou *offline*

Comandos
edit private set interfaces ge-1/0/0 disable set interfaces ge-1/1/0 disable set interfaces ge-1/2/0 disable set interfaces ge-1/3/0 disable

commit exit request chassis pic fpc-slot 1 pic-slot 0 offline request chassis pic fpc-slot 1 pic-slot 1 offline request chassis pic fpc-slot 1 pic-slot 2 offline request chassis pic fpc-slot 1 pic-slot 3 offline request chassis fpc slot 1 offline show chassis fpc detail 1 show chassis fpc pic-status 1

Tabela 33 - Comandos para migração do serviço - Desactivação da slot 1

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à *slot* 2. 2. Efectuar o *shutdown* da FPC2. 3. Verificar de que o *hardware* ficou *offline*

Comandos
set interfaces ge-2/0/0 disable set interfaces ge-2/1/0 disable set interfaces ge-2/2/0 disable set interfaces ge-2/3/0 disable commit exit request chassis pic fpc-slot 2 pic-slot 0 offline request chassis pic fpc-slot 2 pic-slot 1 offline request chassis pic fpc-slot 2 pic-slot 2 offline request chassis pic fpc-slot 2 pic-slot 3 offline request chassis fpc slot 2 offline show chassis fpc detail 2 show chassis fpc pic-status 2

Tabela 34 - Comandos para migração do serviço - Desactivação da slot 2

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à *slot* 3. 2. Efectuar o *shutdown* da FPC3. 3. Verificar de que o hardware ficou *offline*

Comandos
set interfaces ge-3/0/0 disable set interfaces ge-3/1/0 disable set interfaces ge-3/2/0 disable set interfaces ge-3/3/0 disable commit exit

request chassis pic fpc-slot 3 pic-slot 0 offline
request chassis pic fpc-slot 3 pic-slot 1 offline
request chassis pic fpc-slot 3 pic-slot 2 offline
request chassis pic fpc-slot 3 pic-slot 3 offline
request chassis fpc slot 3 offline
show chassis fpc detail 3
show chassis fpc pic-status 3

Tabela 35 - Comandos para migração do serviço - Desactivação da slot 3

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à *slot* 4. 2. Efectuar o *shutdown* da FPC3. 3. Verificar de que o *hardware* ficou *offline*

Comandos
set interfaces ge-4/0/0 disable
set interfaces ge-4/2/0 disable
set interfaces ge-4/3/0 disable
commit
exit
request chassis pic fpc-slot 4 pic-slot 0 offline
request chassis pic fpc-slot 4 pic-slot 1 offline
request chassis pic fpc-slot 4 pic-slot 2 offline
request chassis pic fpc-slot 4 pic-slot 3 offline
request chassis fpc slot 4 offline
show chassis fpc detail 4
show chassis fpc pic-status 4

Tabela 36 - Comandos para migração do serviço - Desactivação da slot 4

Procedimento:	1. Efectuar o *shutdown* dos portos afectados referentes à *slot* 7. 2. Efectuar o *shutdown* da FPC7. 3. Verificar de que o *hardware* ficou *offline*

Comandos
edit private
set interfaces ge-7/0/0 disable
commit
exit
request chassis pic fpc-slot 7 pic-slot 0 offline
request chassis fpc slot 7 offline
show chassis fpc detail 7
show chassis fpc pic-status 7

Tabela 37 - Comandos para migração do serviço - Desactivação da slot 7

Nesta etapa é realizada a substituição do equipamento. As fibras são todas previamente identificadas, depois desconectadas do T640 e este é removido do bastidor. Terminada esta etapa, o MX960 é inserido no bastidor e são conectadas as fibras nas portas de acordo com o mapeamento da tabela 26 e com o auxílio da ilustração 8.

Nesta etapa são ainda contactadas as equipas de supervisão da operadora A de forma a poderem monitorizar a rede ou parte afectada pela intervenção e garantir que os outros equipamentos suportam o tráfego como esperado.

4.2.6 Fase 4 – Activação dos portos de ligação

Procedimento:	Verificar os estados das potências ópticas das interfaces para comparação posterior.

Comandos
show interfaces diagnostics optics xe-0/1/0
show interfaces diagnostics optics xe-0/1/1
show interfaces diagnostics optics xe-0/0/0
show interfaces diagnostics optics xe-0/0/1
show interfaces diagnostics optics xe-1/0/0
show interfaces diagnostics optics xe-1/0/1
show interfaces diagnostics optics xe-3/0/0
show interfaces diagnostics optics xe-3/0/1
show interfaces diagnostics optics xe-2/3/1
show interfaces diagnostics optics xe-3/3/0
show interfaces diagnostics optics xe-3/3/1
show interfaces diagnostics optics xe-2/3/0
show interfaces diagnostics optics xe-3/1/1
show interfaces diagnostics optics xe-2/1/1
show interfaces diagnostics optics xe-2/1/0
show interfaces diagnostics optics xe-1/3/1
show interfaces diagnostics optics xe-2/0/0
show interfaces diagnostics optics xe-1/3/0
show interfaces diagnostics optics xe-3/1/0
show interfaces diagnostics optics xe-1/1/1
show interfaces diagnostics optics xe-1/1/0

Tabela 38 - Comandos para recolha do estado das potências ópticas das interfaces

Após serem conectadas as fibras e antes de activar os portos de ligação, deve ser efectuada a comparação de todas as potências ópticas com as anteriormente retiradas, de forma a garantir que não existem falhas na comunicação por problemas relacionadas com o link físico.

Milestone 2 - Avançar com o procedimento apenas se todas as verificações se encontrarem em conformidade, caso contrário avançar para a secção 4.2.9 - Procedimento de Contingência.

Procedimento:	1. Efectuar o "*no shutdown*" gradual dos portos. Inicialmente a ligação ao *Route Reflector* e posteriormente as ligações aos *Border Routers*. De seguida activar os portos de *Core* e no fim os *Provider Edge Routers*. 2. Verificar para os *links* agregados e a largura de banda disponível.

Comandos

```
# Ligação ao RR
edit private
delete interfaces xe-1/1/0 disable
exit
show IS-IS adjacency | no-more
show ldp session | no-more
show bgp summary | no-more

# Ligações aos BORDERS
edit private
delete interfaces xe-0/0/0 disable
delete interfaces xe-0/0/1 disable
run show interfaces ae3 extensive
delete interfaces xe-1/0/0 disable
delete interfaces xe-1/0/1 disable
run show interfaces ae4 extensive
exit
show IS-IS adjacency | no-more
show ldp session | no-more

# Ligações ao CORE
edit private
```

```
delete interfaces xe-0/1/0 disable
delete interfaces xe-0/1/1 disable
run show interfaces ae0 extensive
delete interfaces xe-3/0/0 disable
delete interfaces xe-3/0/1 disable
run show interfaces ae1 extensive
delete interfaces xe-2/0/0 disable
run show interfaces ae6 extensive
delete interfaces xe-2/3/1 disable
delete interfaces xe-3/3/0 disable
delete interfaces xe-3/3/1 disable
run show interfaces ae5 extensive
exit
show IS-IS adjacency | no-more
show ldp session | no-more
show bgp summary | no-more

# Ligações aos PEs
edit private
delete interfaces xe-2/3/0 disable
delete interfaces xe-3/1/1 disable
delete interfaces xe-2/1/1 disable
delete interfaces xe-2/1/0 disable
delete interfaces xe-1/3/1 disable
delete interfaces xe-3/1/1 disable
delete interfaces xe-1/1/1 disable
exit
show IS-IS adjacency | no-more
show ldp session | no-more
```

Tabela 39 - Comandos para activação dos portos no novo equipamento

4.2.7 Fase 5 – Restauro dos fluxos de tráfego

O restauro dos fluxos de tráfego passa por desactivar o *overload* bit no protocolo IS-IS. Como explicado anteriormente, o *overload bit* isola o *router* dos caminhos de encaminhamento de tráfego. Nesta etapa, permanecendo ainda isolado, pretende-se dar a conhecer à rede que o *router* já se encontra disponível para encaminhar tráfego.

Procedimento:	1. Desactivar o *overload bit* no protocolo IS-IS. 2. Verificar que o tráfego nas interfaces está a aumentar.

Comandos
edit private
delete protocols IS-IS overload
exit
show interfaces detail | no-more

Tabela 40 - Comandos para restaurar os fluxos de tráfego

Depois de restaurados os fluxos de tráfego, nesta etapa é realizada a verificação do serviço nas plataformas de monitorização e serviço da Operadora A de que o tráfego é agora suportado por outros elementos de rede. Esta é uma tarefa a cargo da Operadora A.

4.2.8 Fase 6 – Verificação do estado final

Esta fase descreve os procedimentos para a verificação final essencial para garantir o sucesso da intervenção.

Procedimento:	Recolha do estado do equipamento alvo: 1. Alarmística; 2. Estado do *hardware*; 3. Estado dos processos e ocupações de memória; ***Nota:*** *Qualquer situação anómala deve ser previamente reportada*

Comandos
request support information | no-more
show log messages | no-more
show log chassisd | no-more
request routing-engine login other-routing-engine
show log messages | no-more
show log chassisd | no-more
exit
show chassis hardware detail | no-more
show interface terse | no-more

show interface descriptions | no-more
show chassis routing-engine | no-more
show chassis alarms | no-more
show system processes extensive | no-more

Tabela 41 - Comandos para verificação do estado final do equipamento

Procedimento:	Efectuar *backup* da configuração actual do equipamento alvo de intervenção;
Comandos	
show configuration | no-more	

Tabela 42 - Comando para recolha da configuração final do equipamento

Procedimento:	Recolha do estado protocolar final do equipamento afectado: 1. Estado do serviço (*routing*, MPLS e *bandwidth* das interfaces); ***Nota:*** *Qualquer situação anómala deve ser previamente reportada*
Comandos	
show interfaces detail | no-more	
show IS-IS adjacency | no-more	
show IS-IS interface | no-more	
show ldp session | no-more	
show ldp interface | no-more	
show ldp route | no-more	
show bgp summary | no-more	
show bgp neighbor 212.113.186.9 | no-more	
show bgp neighbor 212.113.186.10 | no-more	
show bgp neighbor 10.255.48.94 | no-more	
show route summary | no-more	

Tabela 43 - Comandos para recolha e configuração do estado final ao nível protocolar

Nesta etapa, avançar com o procedimento apenas se todas as verificações se encontrarem em conformidade, caso contrário avançar para o capítulo do Procedimento de Contingência definido no ponto 4.2.9 deste documento para a *milestone* respectiva.

Concluída a recolha do estado dos serviços, foram comparados os *outputs* com os retirados anteriormente. Se estiver de acordo com o esperado, a NSN garante a conformidade da

instalação. A verificação do serviço no equipamento foi realizada essencialmente pela NSN no entanto, as verificações finais em termos de serviço da operadora ficaram a cargo das suas próprias equipas. Estas verificações finais ditam a aceitação do projecto.

4.2.9 Procedimento de contingência

Esta secção descreve o conjunto de operações a executar de modo a efectuar o *rollback* da intervenção. Como referido anteriormente neste documento, existe um período dentro da janela de intervenção reservado para *rollback* e um limite máximo para decidir se é necessário realizá-lo. As operações a executar são descritas por:

Rollback Milestone 1

- Apurar a origem do problema detectado no MX960.

Rollback Milestone 2

- Determinar a origem do problema do MX960, caso seja identificado algum problema com o *patching* efectuar o despiste necessário à troca.
- Efectuar shutdown aos portos do MX960.
- Caso o problema persista executar *Rollback Milestone* 1.

Rollback Milestone 3

- Determinar a origem do problema do MX960, caso seja identificado algum problema com o *patching* efectuar o despiste necessário à troca.
- Caso não seja possível continuar com a intervenção:
    - Efectuar *shutdown* aos portos migrados.
    - Migrar os patchs cords para os equipamentos anteriores.
    - Efectuar "*no shutdown*" em todos os portos em que anteriormente foi efectuado *shutdown*.
    - Verificar *routing*, MPLS.
    - *Rollback Milestone 2.*

4.3 Síntese

Neste capítulo foram abordados os procedimentos de integração e migração de elementos no *Core* como implementação da solução, detalhando passo a passo, as tarefas a executar de acordo com a proposta de solução.

O capítulo seguinte descreve a etapa de aceitação e validação dos trabalhos dando-os por concluídos e as conclusões acerca da conformidade do trabalho efectuado com o planeado.

Esta página foi intencionalmente deixada em branco

5. Validação dos trabalhos

A validação dos trabalhos ou aceitação é a etapa de aprovação que a NSN tem no final do projecto por parte do cliente para os trabalhos efectuados. A aceitação envolve várias etapas desde a aceitação física à aceitação lógica.

A aceitação ao nível protocolar, ou lógica, consiste nos testes e monitorização efectuados no final da intervenção e no dia seguinte, quando o tráfego de rede atingir os níveis considerados normais, comprovando assim o funcionamento esperado da rede. A ilustração 14 mostra o cenário de rede final após todas as intervenções.

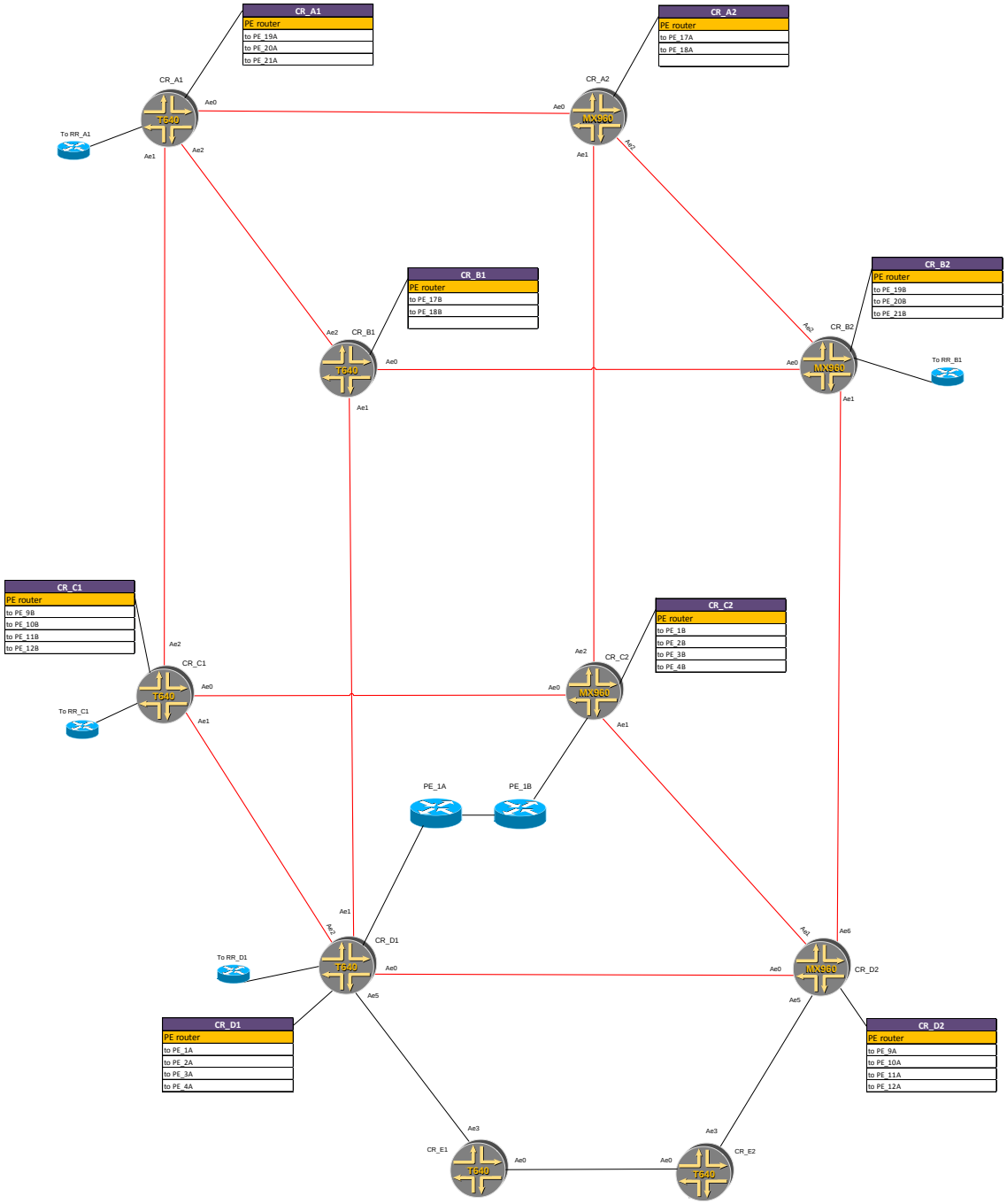

Ilustração 14 - Diagrama físico de rede após as intervenções

Depois da intervenção pretende-se confirmar a normalização dos fluxos de tráfego. Desta forma, foram recolhidas estatísticas que o comprovam. Estes dados foram recolhidos pela equipa de supervisão da Operadora A para garantir que a intervenção fosse controlada e para que os riscos se tornassem mais reduzidos.

Durante a intervenção a rede foi monitorizada pela Operadora A que ia descrevendo à equipa de intervenção on-*site* da NSN o estado da mesma. A aceitação passa por conseguir garantir que após a intervenção foram mantidos os valores para os fluxos de tráfego. A garantia destas condições é dada pela Operadora A.

A ilustração 15 apresenta o histórico dos fluxos de tráfego correspondente às horas que antecederam a intervenção, neste caso a intervenção referente a CR_D2. Os restantes equipamentos envolvidos nas intervenções seguiram um processo idêntico pelo que não são apresentados.

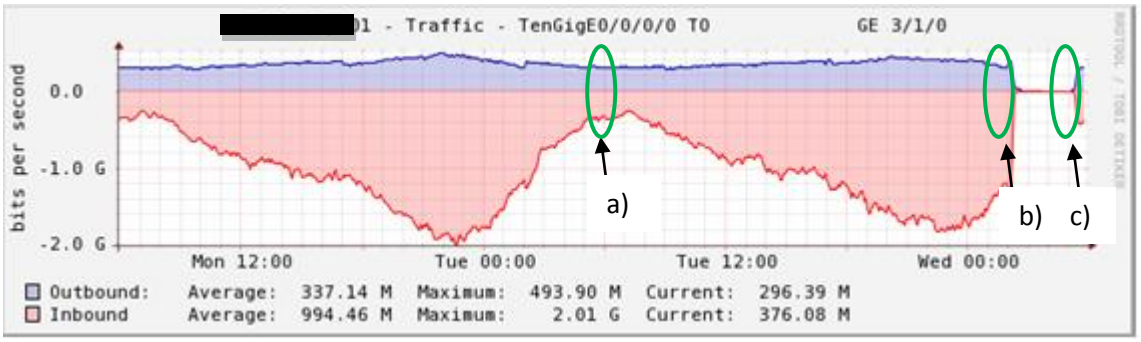

Ilustração 15 - Fluxos de tráfego durante a intervenção referente ao equipamento CR_D2

a) Recolha dos padrões de fluxo de tráfego período do dia equivalente ao período alocado para a intervenção. Esta recolha deve servir de base para posterior comparação com c).

b) Quebra de serviço provocada na intervenção, seguida do período em que não existe serviço. Este período está integrado na janela de intervenção e termina na etapa de restauro dos fluxos de tráfego.

c) Após activar o serviço, foram recolhidos dados correspondentes aos fluxos de tráfego no momento para comparar com os recolhidos anteriormente no ponto a) e comprovar assim que os fluxos de tráfego estavam normalizados.

Aceitação física

A aceitação a nível físico passa por validar a instalação física dos equipamentos no bastidor. Depois de seguir as indicações do fabricante (resumidas no anexo A) em relação à disposição do equipamento no bastidor e feitas as ligações, foram reunidos os cabos de

fibra óptica de forma a passassem pelos locais correctos de modo a acondicionar convenientemente o equipamento no bastidor. De seguida são mostradas figuras exemplo da configuração final do equipamento no bastidor.

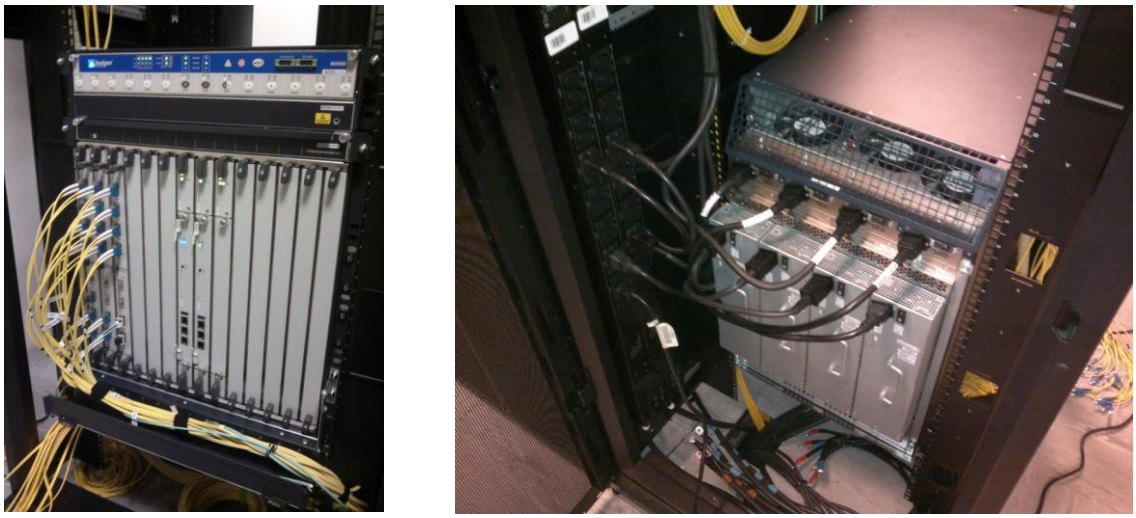

Ilustração 16 - Fotos do equipamento CR_B1 no final da intervenção

5.1 Testes de hardware

Nesta secção vão ser resumidos os resultados dos testes de hardware efectuados após a execução dos trabalhos. Todos os componentes são instalados de acordo com a proposta de solução apresentado e nesta etapa são testadas as soluções para comprovar a sua conformidade.

5.1.1 Verificação do hardware

No final de cada intervenção, são recolhidos os detalhes do *hardware* do equipamento. O processo é o mesmo para cada equipamento migrado ou instalado pelo que apenas é apresentado um exemplo de uma recolha, neste caso do CR_D2 e os demais envolvidos no projecto são semelhantes. Todos os inventários de *hardware* foram reunidos e apresentados à Operadora A nos documentos de aceitação. Nestes inventários pretende-se comprovar a

instalação dos equipamentos e componentes adquiridos. Na tabela 44, relativamente aos Juniper MX960 é possível verificar que os componentes instalados e consequentemente os consumos de energia correspondem ao proposto.

Inventário do hardware

```
{master}
user@cr_d2-re0> show chassis hardware detail | no-more
Hardware inventory:
Item          Version  Part number  Serial number     Description
Chassis                                                MX960
Midplane      REV 03   710-013698                      MX960 Backplane
FPM Board     REV 03   710-014974                      Front Panel Display
PDM           Rev 03   740-013110                      Power Distribution Module
PEM 0         Rev 05   740-027760                      PS 4.1kW; 200-240V AC in
PEM 1         Rev 05   740-027760                      PS 4.1kW; 200-240V AC in
PEM 2         Rev 05   740-027760                      PS 4.1kW; 200-240V AC in
PEM 3         Rev 05   740-027760                      PS 4.1kW; 200-240V AC in
Routing Engine 0 REV 12   740-013063                  RE-S-2000
  ad0     999 MB  SILICONSYSTEMS INC 1GB                    Compact Flash
  ad2   38154 MB  ST940817SM                         Hard Disk
Routing Engine 1 REV 12   740-013063                  RE-S-2000
  ad0     999 MB  SILICONSYSTEMS INC 1GB                    Compact Flash
  ad2   38154 MB  ST940817SM                         Hard Disk
CB 0          REV 07   710-021523                     MX SCB
CB 1          REV 07   710-021523                     MX SCB
CB 2          REV 08   710-021523                     MX SCB
FPC 0         REV 16   750-031089                     MPC Type 2 3D
  CPU         REV 06   711-030884                     MPC PMB 2G
  MIC 0       REV 24   750-028387                     3D 4x 10GE  XFP
    PIC 0               BUILTIN     BUILTIN       2x 10GE  XFP
      Xcvr 0  REV 02   740-014279                     XFP-10G-LR
      Xcvr 1  REV 02   740-014279                     XFP-10G-LR
    PIC 1               BUILTIN     BUILTIN       2x 10GE  XFP
      Xcvr 0  REV 02   740-014279                     XFP-10G-LR
      Xcvr 1  REV 02   740-014279                     XFP-10G-LR
  MIC 1       REV 24   750-028387                3D 4x 10GE  XFP
    PIC 2               BUILTIN     BUILTIN       2x 10GE  XFP
      Xcvr 1  REV 02   740-014279                     XFP-10G-LR
    PIC 3               BUILTIN     BUILTIN       2x 10GE  XFP
      Xcvr 0  REV 02   740-014279                     XFP-10G-LR
      Xcvr 1  REV 02   740-014279                     XFP-10G-LR
FPC 1         REV 16   750-031089                MPC Type 2 3D
  CPU         REV 06   711-030884                MPC PMB 2G
  MIC 0       REV 24   750-028387                3D 4x 10GE  XFP
    PIC 0               BUILTIN     BUILTIN       2x 10GE  XFP
      Xcvr 0  REV 02   740-014279                     XFP-10G-LR
```

```
    Xcvr 1      REV 02   740-014279                          XFP-10G-LR
  PIC 1                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 03   740-014289                          XFP-10G-SR
    Xcvr 1      REV 02   740-014279                          XFP-10G-LR
  MIC 1         REV 24   750-028387                    3D 4x 10GE  XFP
  PIC 2                  BUILTIN      BUILTIN        2x 10GE  XFP
  PIC 3                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279                          XFP-10G-LR
    Xcvr 1      REV 02   740-014279                          XFP-10G-LR
FPC 2           REV 16   750-031089          MPC Type 2 3D
 CPU            REV 06   711-030884          MPC PMB 2G
 MIC 0          REV 24   750-028387          3D 4x 10GE  XFP
  PIC 0                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279          XFP-10G-LR
  PIC 1                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279                          XFP-10G-LR
    Xcvr 1      REV 02   740-014279                          XFP-10G-LR
 MIC 1          REV 24   750-028387          3D 4x 10GE  XFP
  PIC 2                  BUILTIN      BUILTIN        2x 10GE  XFP
  PIC 3                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279          XFP-10G-LR
    Xcvr 1      REV 02   740-014279          XFP-10G-LR
FPC 3           REV 16   750-031089          MPC Type 2 3D
 CPU            REV 06   711-030884          MPC PMB 2G
 MIC 0          REV 24   750-028387          3D 4x 10GE  XFP
  PIC 0                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279                          XFP-10G-LR
    Xcvr 1      REV 02   740-014279                          XFP-10G-LR
  PIC 1                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279          XFP-10G-LR
    Xcvr 1      REV 02   740-014279          XFP-10G-LR
 MIC 1          REV 24   750-028387                    3D 4x 10GE  XFP
  PIC 2                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 1      REV 03   740-014289          XFP-10G-SR
  PIC 3                  BUILTIN      BUILTIN        2x 10GE  XFP
    Xcvr 0      REV 02   740-014279          XFP-10G-LR
    Xcvr 1      REV 02   740-014279          XFP-10G-LR
Fan Tray 0      REV 06   740-031521          Enhanced Fan Tray
Fan Tray 1      REV 06   740-031521          Enhanced Fan Tray
```

Tabela 44 -Recolha da configuração de hardware final

O comando anterior recolhe um relatório do *hardware* instalado no equipamento CR_D2. Foi realizado um documento de Aceitação para todos os equipamentos instalados e recolhido o comando anterior para todos eles. Como a descrição dos componentes é semelhante em todos variando apenas os elementos instalados de acordo com as necessidades de cada site, apenas é apresentado de um que servirá de exemplo.

5.1.2 Alimentação MX

Como calculado na secção 2.3 deste documento, o valor recomendado para alimentação do equipamento é 2304 W DC.

Na tabela 45 é recolhido um relatório do equipamento para verificação da conformidade dos valores.

Comandos
user@cr_b2-re0> show chassis environment pem PEM 0 status: State Online Temperature OK DC Input: OK DC Output Voltage(V) Current(A) Power(W) Load(%) 55 3 165 5 Voltage: 48.0 V input 55000 mV PEM 1 status: State Online Temperature OK DC Input: OK DC Output Voltage(V) Current(A) Power(W) Load(%) 55 9 495 17 Voltage: 48.0 V input 55500 mV PEM 2 status: State Online Temperature OK DC Input: OK DC Output Voltage(V) Current(A) Power(W) Load(%) 55 3 165 5 Voltage: 48.0 V input 55500 mV PEM 3 status: State Online Temperature OK DC Input: OK DC Output Voltage(V) Current(A) Power(W) Load(%)

55 6 330 11

Voltage:

48.0 V input 55500 mV

#individualmente por cada fonte de alimentação é possível verificar a carga actual com o seguinte comando

{master}

user@cr_b2-re0> show chassis power

PEM 0:

State: Online

DC input: OK (1 feed expected, 1 feed connected)

DC input: 48.0 V input (55000 mV)

Capacity: 2800 W (maximum 2800 W)

DC output: 165 W (zone 0, 3 A at 55 V, 5% of capacity)

PEM 1:

State: Online

DC input: OK (1 feed expected, 1 feed connected)

DC input: 48.0 V input (55500 mV)

Capacity: 2800 W (maximum 2800 W)

DC output: 440 W (zone 1, 8 A at 55 V, 15% of capacity)

PEM 2:

State: Online

DC input: OK (1 feed expected, 1 feed connected)

DC input: 48.0 V input (55500 mV)

Capacity: 2800 W (maximum 2800 W)

DC output: 110 W (zone 0, 2 A at 55 V, 3% of capacity)

PEM 3:

State: Online

DC input: OK (1 feed expected, 1 feed connected)

DC input: 48.0 V input (55500 mV)

Capacity: 2800 W (maximum 2800 W)

DC output: 330 W (zone 1, 6 A at 55 V, 11% of capacity)

System:

Zone 0:

Capacity: 2800 W (maximum 2800 W)

Allocated power: 710 W (2090 W remaining)

Actual usage: 275 W

```
Zone 1:
   Capacity:        2800 W (maximum 2800 W)
   Allocated power:  1604 W (1196 W remaining)
   Actual usage:     770 W
Total system capacity: 5600 W (maximum 5600 W)
Total remaining power: 3286 W
```

Tabela 45 - Estado das alimentações do equipamento Juniper MX960 em ambiente de produção

Como é possível verificar no *output* recolhido, por cada fonte de alimentação, a carga exigida a cada fonte de alimentação (PME) é consideravelmente inferior à capacidade individual de cada uma. A capacidade máxima do equipamento é fixada em 5600 W, sendo que a energia total em uso é de 3286 W, a restante são cerca de 2314 W equivalente ao previsto de 2304 W calculado na proposta apresentada no capítulo 2.

5.2 Testes de balanceamento

Para efectuar os testes pedidos pelo cliente, a NSN teve de se certificar de que as configurações correspondentes à funcionalidade de balanceamento de tráfego estão correctamente configuradas. A configuração submetida é a indicada na tabela 46.

```
forwarding-options {
        load-balance {
                indexed-next-hop; # Balanceamento do tráfego em links agregados para o mesmo next-hop
        }
```

Tabela 46 – Configurações de balanceamento de tráfego

Descrição do teste: Balanceamento de tráfego entre P1 e CR_B1

Número de flows: 1000
Source: P1
Destination: CR_B1

Considerando-se o diagrama da ilustração 8 lidentifica-se o agregado 3 como a interligação entre os equipamentos deste teste. Através do comando *show interfaces ae3 extensive* recolhem-se os resultados. Para uma maior fiabilidade dos dados recolhidos optou-se por limpar os registos estatísticos do equipamento através do comando *clear interfaces statistics*

all.

Através do output recolhido, mostrado na tabela 47, é possível verificar a largura de banda do *link* usado, correspondente a 1Gbps.

Output
clear interfaces statistics all user@M320_2-RE0> show interfaces ae3 extensive Physical interface: ae3, Enabled, Physical link is Up Interface index: 131, SNMP ifIndex: 207, Generation: 132 Link-level type: Ethernet, MTU: 1580, Speed: 20000mbps, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0 Device flags : Present Running Interface flags: SNMP-Traps Internal: 0x4000 Current address: [redacted], Hardware address: [redacted] Last flapped : 2010-11-03 19:21:32 WET (22:57:56 ago) Statistics last cleared: 2010-11-04 18:19:17 WET (00:00:11 ago) Traffic statistics: Input bytes : 5889 6096 bps Output bytes : 771904200 972350008 bps Input packets: 37 0 pps Output packets: 522316 82236 pps

Tabela 47 - Recolha dos outputs do teste

Os resultados do balanceamento comprovam o funcionamento do balanceamento entre duas interfaces (ge-2/0/0 e ge-2/1/0) e entre dois agregados (Ae3.30 e Ae3.31). A tabela 48 resume os resultados para o teste em questão.

Output
Logical interface ae3.30 (Index 120) (SNMP ifIndex 354) (Generation 391) Description: BR_LAB1 ae3.30 Flags: SNMP-Traps 0x4000 VLAN-Tag [0x8100.30] Encapsulation: ENET2 Statistics Packets pps Bytes bps Bundle: Input : 9 0 1143 304 Output: 261121 41116 385925938 486166400

```
    Link:
      ge-2/0/0.30
        Input :          9        0        1143        304
        Output:      131087     20641    193735686   244062648
      ge-2/1/0.30
        Input :          0        0           0          0
        Output:      130034     20475    192190252   242103752
...
  Logical interface ae3.31 (Index 211) (SNMP ifIndex 355) (Generation 392)
    Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.31 ]  Encapsulation: ENET2
    Statistics        Packets        pps        Bytes          bps
    Bundle:
        Input :          10        0        1819        2896
        Output:      261152     41117    385971168   486178168
    Link:
      ge-2/0/0.31
        Input :          10        0        1819        2896
        Output:      130574     20558    192976884   243086144
      ge-2/1/0.31
        Input :          0        0           0          0
        Output:      130578     20559    192994284   243092024
```

Tabela 48 – Recolha dos outputs do teste

Como é possível verificar pela análise da tabela 48, as estatísticas mostram um tráfego com cerca de 9,73 Gbps que é repartido em dois agregados com 4,86Gbps e 2,43Gbps por interface como esperado.

5.3 Síntese

Este capítulo resume com detalhe, a aprovação do trabalho realizado. No final da execução dos trabalhos são efectuados um conjunto de testes finais a pedido do cliente para comprovar o funcionamento da solução conforme planeado e são elaborados documentos para é apresentada a aprovação dos trabalhos por parte do cliente.

No capítulo seguinte é feita uma conclusão acerca do trabalho efectuado e do contributo do estágio para formação e reforço de conhecimentos.

Esta página foi intencionalmente deixada em branco

6. Conclusão

O período de estágio de 9 meses teve como objectivo a integração no mercado de trabalho e a obtenção de conhecimentos considerados essenciais para solidificar novas técnicas de trabalho. O suporte realizado às operadoras de telecomunicações permite lidar com situações e tecnologias que não estão ao alcance do nível académico. O envolvimento directo em projectos de integrações de equipamentos novos na rede e migrações de serviço, permite compreender conceitos chave e explorar soluções para os problemas actualmente existentes nas redes de *Core* das operadoras. O contacto com novas tecnologias e metodologias, proporcionada por uma empresa como a NSN foi muito importante neste aspecto. As metodologias utilizadas pelos colegas de trabalho, foram adquiridas ao longo dos tempos e só se conseguiram com anos de experiência, o que faz com que, nestas condições, este estágio contribua fortemente para a introdução fundamental de suporte às exigências do mercado que se revela muito competitivo. A distinção da concorrência consegue-se sobretudo apostando no desenvolvimento de novos métodos de optimização do trabalho. O contacto directo com um fabricante específico não contribuiu apenas para reforçar os conhecimentos de determinadas tecnologias, mas também para apostar em questões como conquista de oportunidades de negócio e desenvolvimento de estratégias para marcar a diferença.

O estágio foi muito enriquecedor de conhecimentos não só do ponto de vista teórico, mas também da componente prática. Foi possível lidar fisicamente com os equipamentos, realizando configurações e planeamento de soluções assim como o bom grupo de trabalho que se revelou essencial para a conclusão dos projectos com sucesso, pondo à prova e reforçando a componente das *soft-skills*.

Esta página foi intencionalmente deixada em branco

7. Bibliografia

Excentis. (2007). Introduction to EURO-DOCSIS. In *Training - Introduction to EURO-DOCSIS* (S. Part 3: Ranging and Registering, pag. 5). Ghent, Belgium.

Juniper Networks. (25. Fevereiro 2011). *MX960 DC Power Supply*. Abgerufen am 20. Setembro 2011 von Juniper Networks - Support - Technical Documentation: http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/power-supply-mx960-dc.html

Juniper Networks. (18. Maio 2011). *Power Consumption for a DC-Powered MX960 Router*. Abgerufen am 20. Setembro 2011 von Juniper Networks - Support - Technical Documentadion: http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/specifications/mx960-power-components-dc.html

Juniper Networks. (27. Julho 2011). *T640 Chassis Description.* Abgerufen am 20. Setembro 2011 von Juniper Networks - Support - Technical Documentation: http://juniperpodcast.com/techpubs/en_US/release-independent/junos/topics/concept/chassis-t640-description.html

Juniper Networks. (27. Julho 2011). *T640 DC Power System Requirements.* Abgerufen am 20. Setembro 2011 von Juniper Networks - Support - Technical Documentation: http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/specifications/dc-power-t640-requirements.html

Mika, N. (14. Maio 2008). *Reuters - Tecnologia*. Abgerufen am 20. Setembro 2011 von Reuters: http://tecnologia.uol.com.br/ultnot/reuters/2008/05/14/ult3949u3711.jhtm

Nokia Siemens Networks. (kein Datum). *Mission and Vision - Nokkia Siemens Networks*. Abgerufen am 20. Setembro 2011 von http://www.nokiasiemensnetworks.com: http://www.nokiasiemensnetworks.com/about-us/company/mission-and-vision

Anexos

Anexo A

T640 Site Preparation Checklist

The checklist in Table 1 summarizes the tasks you need to perform when preparing a site for router installation.

Table 1: Site Preparation Checklist

Item or Task	Performed By Date
Environment	
Verify that environmental factors such as temperature and humidity do not exceed router tolerances.	☐
Power	
Measure distance between external power sources and router installation site.	☐
Locate sites for connection of system grounding.	☐
Calculate the power consumption and requirements.	☐
Rack	
Verify that your rack meets the minimum requirements for the installation of the router.	☐
Plan rack location, including required space clearances.	☐
If a rack is used, secure rack to floor and building structure.	☐
Cables	
Acquire cables and connectors:	☐
Determine the number of cables needed based on your planned configuration.	☐
Review the maximum distance allowed for each cable. Choose the length of cable based on the distance between the hardware components being connected.	☐
Plan the cable routing and management.	☐

Anexo B

Nokia Siemens Networks

Procedimento de upgrade

Procedimento upgrade 9.4R3.5 para 10.4R4.7

1. Introdução

2. Análise de Risco

3. Controlo de Versões

4. Equipa e Janela de intervenção

5. Requisitos

6. Procedimento de upgrade

1. Introdução

No âmbito do suporte em curso e de acordo com as necessidades da Operadora surge a necessidade de se efectuar o upgrade do Juniper M Series da presente versão 9.4R3.5, equipamento pertencente ao *CORE*, este documento descreve o procedimento de upgrade do M120 anteriormente indicado.

A Operadora deverá contactar a supervisão de forma a dar início e final dos trabalhos.

2. Análise de Risco

Durante o período crítico da intervenção em que será afectado o upgrade, não está previsto qualquer indisponibilidade no serviço dado que o tráfego cursante no EQUIPAMENTO A irá ser à priori baldeado para o EQUIPAMENTO B.

Embora não esteja previsto impacto, poderá ainda existir tráfego residual cursante no EQUIPAMENTO A, a afectação neste tráfego será momentânea aquando do reload do mesmo. Após esta operação este tráfego residual, caso haja, irá cursar pelo EQUIPAMENTO A.

3. Controlo de Versões

Versão	Data	Descrição	Autor
v1.0	13-Dezembro-2010	Primeira versão do documento.	(NSN)

4. Equipa e Janela de intervenção

Equipa Nome	Contacto	Empresa
A definir	A definir	
A definir	A definir	

Janela Inicio	Fim
A definir	A definir

5. Requisitos

Como requisito para a intervenção será necessário:

- O acesso por consola a ambas REs do equipamento. [Operadora].
- RE de spares disponíveis para a troca [Operadora].

6. Procedimento de upgrade

FASE – 1 – Recolha do estado inicial do router

- Esta fase terá inicio 60 minutos antes da janela de intervenção e não causa qualquer

indisponibilidade de serviço

Procedimento:	Nesta etapa, proceder à recolha do estado inicial do router. Esta recolha é realizada através dos comandos abaixo descritos.
Duração Prevista:	30 min (dependendo do tamanho do ficheiro de configuração)

Comando

`request support information | no-more`
`show log messages | no-more`
`show log chassisd | no-more`
`show system storage`
 	
`request routing-engine login other-routing-engine`
`show log messages | no-more`
`show log chassisd | no-more`
`show system storage`
`show system switchover`
`exit`
 	
`show chassis hardware | no-more`
`show mpls lsp terse | no-more`
`show interface terse | no-more`
`show interface descriptions | no-more`
`show chassis routing-engine | no-more`
 	
`show system processes extensive | no-more`

FASE – 2 – Recolha de informação protocolar para posterior comparação

Procedimento:	Nesta etapa, proceder à recolha de informação do router. Esta recolha é realizada através dos comandos abaixo descritos.
Duração Prevista:	10 min (dependendo do tamanho do ficheiro de configuração)

Comando

`show interfaces descriptions | no-more`
`show interfaces terse | no-more`
`show ospf neighbor | no-more`
`show pim neighbors | no-more`
`show dvmrp neighbors | no-more`
`show bgp summary | no-more`
`show route summary | no-more`

FASE – 3 – Cópia do software para o router

Procedimento:	Nesta etapa, copiar as versões de software necessárias para o upgrade para cada uma das *routing engines*. ***Nota:*** *Os comandos a baixo assumem que a master RE é a RE0*
Duração Prevista:	10 min

Comando	
{master} > file list /var/tmp	***Procurar a versão:*** jinstall-10.0R4.7-domestic-signed.tgz jinstall-10.4R4.5-domestic-signed.tgz
{master} > file list re1:/var/tmp	***Procurar a versão:*** jinstall-10.0R4.7-domestic-signed.tgz jinstall-10.4R4.5-domestic-signed.tgz
Visto que nenhuma das versões se deve encontrar nas REs correr os comandos a baixo:	
{master} > file copy file copy ftp://wse-emergency[redacted]outgoing/jinstall-10.0R4.7-domestic-signed.tgz /var/tmp/jinstall-10.0R4.7-domestic-signed.tgz {master} > file copy file copy ftp://wse-emergency[redacted]outgoing/jinstall-10.4R4.5-domestic-signed.tgz /var/tmp/jinstall-10.4R4.5-domestic-signed.tgz	Cópia das versões de software para a *master* RE.
{master} > file copy file copy var/tmp/jinstall-10.0R4.7-domestic-signed.tgz re1:/var/tmp/jinstall-10.4R4.5-domestic-signed.tgz {master} > file copy file copy /var/tmp/jinstall-10.4R4.5-domestic-signed.tgz re1:/var/tmp/jinstall-10.4R4.5-domestic-signed.tgz	Cópia das versões de software para a *backup* RE.

FASE – 4 – Backup da configuração

Procedimento:	Neste passo vamos guardar a configuração de forma a poder confirmar que a mesma se mantém inalterável com o processo de upgrade.
Duração Prevista:	10 min

Comando	Notas
{master} > show configuration | no-more	Gravar o output com num ficheiro à parte.

FASE – 5 – Desactivar GRES e commit synchronize

Procedimento:	Nesta etapa, vamos desactivar o GRES e o '*commit synchronize*'
Duração Prevista:	10 min

Comando	Notas
{master} # show chassis redundancy {master} # show system commit	Se o *GRES* ou o *commit synchronize* se encontrar desactivo, não executar os passos seguintes.
{master} # deactivate chassis redundancy	Desactivar o *GRES*.
{master} # deactivate system commit synchronize	Desactivar o *commit synchronize*
{master} # show | compare	
{master} # commit synchronize	
{master} # exit	

FASE – 6– Upgrade da RE de backup

	Nesta etapa, vamos fazer upgrade à RE de *backup* para a versão de software 10.0R4.7.
Duração Prevista:	35 min

Comando	Notas
{master} > request routing-engine login other-routing-engine	
{backup} > request system snapshot	
{backup} > request system software add /var/tmp/jinstall-10.0R4.7-domestic-signed.tgz validate	
{backup} > request system reboot	O reboot demora cerca de 10min
{master} > request routing-engine login other-routing-engine	
{backup} > show version	Verificar que a versão está correcta.
{backup} > request system software add /var/tmp/jinstall-10.4R4.5-domestic-signed.tgz validate	
{backup} > request system reboot	
{master} > request routing-engine login other-routing-engine	
{backup} > show version	Verificar que a versão está correcta.

FASE – 7 – Verificação da configuração

Procedimento:	Neste passo vamos confirmar que não houve alterações de configuração durante o processo de upgrade.
Duração Prevista:	10 min

Comando	Notas
{backup} > show configuration | no-more	Comparar o output com a configuração recolhida inicialmente.

FASE – 8 – Comutação da RE's Activo <-> Backup

Procedimento:	Nesta etapa, comutar o serviço para a RE que já tem a nova versão.
Duração Prevista:	10 min

Comando	Notas
QUEBRA DE SERVIÇO	
{master} > request chassis routing-engine master switch	

FASE – 9 – Verificação de serviço

Procedimento:	Nesta etapa, proceder à recolha de informação do router. Esta recolha é realizada através dos comandos abaixo descritos.
Duração Prevista:	10 min (dependendo do tamanho do ficheiro de configuração)

Comando
show interfaces descriptions | no-more show interfaces terse | no-more show ospf neighbor | no-more show pim neighbors | no-more show dvmrp neighbors | no-more show bgp summary | no-more show route summary | no-more

FASE – 10 – Upgrade da outra RE

Procedimento:	Nesta etapa vamos fazer o upgrade de outra RE (agora em backup).
Duração Prevista:	35 min

Comando	Notas
{master} > request routing-engine login other-routing-engine	
{backup} > request system snapshot	
{backup} > request system software add /var/tmp/jinstall-10.0R4.7-domestic-signed.tgz validate	
{backup} > request system reboot	O reboot demora cerca de 10min
{master} > request routing-engine login other-routing-engine	
{backup} > show version	Verificar que a versão está correcta.
{backup} > request system software add /var/tmp/jinstall-10.4R4.5-domestic-signed.tgz validate	
{backup} > request system reboot	
{master} > request routing-engine login other-routing-engine	
{backup} > show version	Verificar que a versão está correcta.

FASE – 11 – Activar GRES e commit synchronize

Procedimento:	Nesta etapa, reactivar o GRES e o '*commit synchronize*'.
Duração Prevista:	10 min (dependendo do tamanho do ficheiro de configuração)

Comando	
{master} > edit private	
{master} # activate chassis redundancy	
{master} # activate system commit synchronize	
{master} # show | compare	
{master} # commit	
{master} # exit	
{master} > request routing-engine login other-routing-engine {backup} > show system switchover	Verificação da correcta activação do GRES.