PM

Migração da Tecnologia SDH para (IP) MPLS

PROJETO DE MESTRADO

Jorge Rodrigues Valente

MESTRADO EM ENGENHARIA ELETROTÉCNICA - TELECOMUNICAÇÕES

UNIVERSIDADE da MADEIRA

A Nossa Universidade

www.uma.pt

março | 2019

Migração da Tecnologia SDH para (IP) MPLS

PROJETO DE MESTRADO

Jorge Rodrigues Valente

MESTRADO EM ENGENHARIA ELETROTÉCNICA - TELECOMUNICAÇÕES

ORIENTADORA

Lina Maria Pestana Leão de Brito

CO-ORIENTADOR

Luís Armando de Aguiar Oliveira Gomes

Resumo

As redes de telecomunicações progrediram notavelmente nos últimos oito anos, o que permitiu a convergência de diferentes serviços suportados por uma única infraestrutura de rede. Após o sucesso no mercado de telecomunicações, a arquitetura *multi-protocol label switching* (MPLS) também está a revolucionar o mundo das empresas ligadas ao sector designadas por *utility*. Estas empresas procuram, essencialmente, fortalecer a segurança nas suas redes privadas (virtuais) que interligam as suas diferentes instalações.

A arquitetura MPLS permitiu que a Empresa de Eletricidade da Madeira (EEM) alcançasse os seus objetivos e os requisitos definidos inicialmente na implementação dos serviços na nova rede. A sua instalação foi projetada para ser de baixo custo e, além disso, dispor de: *(i)* uma elevada eficiência operacional; *(ii)* ser flexível; *(iii)* ser confiável; *(iv)* ser segura; *(v)* e possuir um nível de controlo sem precedentes. É uma solução que admite interoperabilidade entre diferentes protocolos numa plataforma baseada na comutação por rótulo, com elevado sucesso na capacidade de transportar voz com qualidade de serviço. A arquitetura MPLS simplifica e otimiza a troca de pacotes e fornece uma maior capacidade de gerir o tráfego e evitar congestionamentos.

Esta trabalho pretende explicar os procedimentos e as escolhas na implementação associados à migração de uma rede de arquitetura hierarquia digital plesiócrona/síncrona para uma arquitetura MPLS. Estas escolhas admitem integrar futuras soluções que o mercado venha a disponibilizar, no sentido de procurar a modernização das infraestruturas elétricas da EEM.

Palavras Chave:

Convergência de serviços, redes privadas, interoperabilidade, comutação por rótulo.

Abstract

Telecomunications networks have progressed remarkably in the past eight years, which has allowed the convergence of differents services supported by a single network infrastructure. Following the success in the telecom market, the *multi-protocol label switch*ing (MPLS) architecture is also revolutionizing the world of utility companies connected to this market. These companies are essentially looking to strengthen security in their (virtual) private networks that connect their facilities.

The MPLS architecture has allowed Empresa de Eletricidade da Madeira (EEM) to achieve its initially defined objectives and requirements in the implementation of the services in its new network. Its installation was intented to be low cost, while also allowing for: *(i)* an elevated operational efficiency; *(ii)* flexibility; *(iii)* reliability; *(iv)* security; *(v)* and an unprecedented level of control. It is a solution that allows for interoperability between different protocols on a labeled comutation based platform, with a high level of success in the transportation of voice with high quality of service. The MPLS architecture simplifies and optimizes the packet exchange and allows for superior traffick and congestion management.

This thesis will explain the procedures and implementation choices associated with the migration of a Plesiochronous/Sinchronous Digital Hierarchy architecture to an MPLS architecture. These choices and procedures allow for the integration of future network solutions in the forseable future, and permit the continued modernization of EEM's electrical infrastructure.

Keywords:

Convergence of services, private networks, elevated operational efficiency, flexibility, reliability, security, unprecedented control level, interoperability, labeled comutation.

Agradecimentos

Este documento é o culminar de uma aventura que começou em 2005, quando retomei os estudos, regressando ao secundário, após ter estado mais de onze anos afastado dos estudos.

Este documento foi realizado no âmbito da experiência adquirida no meu posto de trabalho, e queria por isso começar com os agradecimentos ao João Filipe Ferreira, que para além de ser meu superior hierárquico, é acima de tudo um amigo, que sempre me apoiou e me motivou nos estudos, pois entende que uma sociedade só se pode desenvolver com a riqueza obtida a partir do conhecimento. Quero também agradecer a todos os meus colegas de trabalho, do serviço de telecomunicações, que também contribuíram, à sua maneira, para que eu pudesse ter as condições que são exigidas num curso de engenharia. Agradeço todos, principalmente ao Fernando Cardoso e ao Rui Nóbrega pelo apoio e explicações.

Agradeço também os meus colegas de curso Carla Jardim, Fábio Ruben Mendonça, Filipe Santos, Ivo Valente, João Castro, Jorge Lopes, Rúben Sousa, Laura Moreira, Luciano Calaça, Miguel Teixeira, Natércia Sousa, Ricardo André Sousa, Rodolfo Henrique Rodrigues e Sofia Nóbrega.

Estou particularmente grato ao Carlos Gonçalves, colega de trabalhos de grupo de várias unidades curriculares.

Agradeço aos professores Dr.ª Lina Maria Pestana Leão de Brito e Dr. Luís Armando de Aguiar Oliveira Gomes pelos cuidados e interesse que demonstraram na leitura crítica, acompanhadas de sugestões, deste documento.

Estendo a minha gratidão aos diversos professores que tive a felicidade de conhecer no decorrer do meu percurso curricular, e sem prejuízo pelos nomes que omito, destaco o Dr. Joaquim Amândio Rodrigues Azevedo e o Dr. João Dionísio Simões Barros, pelas suas disponibilidades, escuta e competência. A sua experiência científica e conselhos sábios foram além de gratificantes, agradáveis, contribuindo significativamente para o fortalecimento da qualidade da minha formação e pelo gosto da engenharia.

Dedicatória

À minha mãe.

"Não conheço ninguém que conseguisse realizar o seu sonho, sem sacrificar feriados, sábados e domingos pelo menos uma centena de vezes. Terá que se dedicar, superar o cansaço, encontrar tempo, energia, deixar de lado o orgulho e o comodismo. O sucesso é construído à noite!

Durante o dia você faz o que todos fazem. Mas, para obter um resultado diferente da maioria, você tem que ser especial. Se fizer igual a todo o mundo, obterá os mesmos resultados. Não se compare à maioria, pois infelizmente ela não é modelo de sucesso. Se você quiser atingir uma meta especial, terá que estudar no horário em que os outros estão à frente da televisão, ou estão se divertindo. Terá de trabalhar enquanto os outros tomam banhos de sol à beira mar ou da piscina. A realização de um sonho depende de dedicação, há muita gente que espera que o sonho se realize por magia, mas toda magia é ilusão, e a ilusão não tira ninguém de onde está, em verdade a ilusão é combustível dos perdedores pois...

Quem quer fazer alguma coisa, encontra um meio.

Quem não quer fazer nada, encontra uma desculpa."

Roberto Shinyashiki

A idade certa para regressar aos estudos é a idade que se tem hoje.

Índice

Índice de figuras

Indices de tabelas

Lista de acrónimos

ABR	*Area Border Router*
AC	*Attachment Circuit*
ADM	*Add/Drop Multiplexer*
ADMS	*Advanced Distribution Management System*
AMI	*Advanced Metering Infrastructure*
AMR	*Automatic Meter Reading*
AMS	*Advanced Metering System*
APS	*Automatic Protection Switching*
ARP	*Address Resolution Protocol*
AS	*Autonomous System*
ASA	*Adaptive Security Appliance*
ASR	*Aggregation Services Router*
ATM	*Asynchronous Transfer Mode*
BDI	*Bridge Domain Interface*
BGP	*Border Gateway Protocol*
BPDU	*Bridge Protocol Data Unit*
BRI	*Basic Rate Interface*
CCTV	*Central Control Television*
CE	*Customer Equipment*
CES	*Circuit Emulation Service*
CESoPSN	*Circuit Emulation Service over Packet-Switched Network*
CGR	*Connected Grid Router*
CoS	*Class of service*
CPE	*Customer Premises Equipment (Demarcation Device)*
CRC	*Cyclic Redundancy Check*
CUCC	*Central Unit Cross connect*
CUD	*Central Unit Drop/Insert*
CVP	*Circuito Virtual Privativo*
DoS	*Denial of Service*
EDM	*Energy Data Management*
EEM	*Empresa de* Eletricidade *da Madeira*

EIA	*Eletronic Industry Association*
EGP	*Exterior Gateway Protocol*
EMI	*Electromagnetic interference*
EMS	*Element Management System*
EoS	*Ethernet over SONET*
EPL	*Ethernet Private Line*
EPLAN	*Ethernet Private LAN*
ESM	*Ethernet Switch Module*
ETSI	*European Telecommunications Standards Institute*
EUI	*Extended Unique Identifier*
EVC	*Ethernet Virtual Connection*
EVPL	*Ethernet Virtual Private Line*
EVPLAN	*Ethernet Virtual Private LAN*
FDDI	*Fiber Distributed Data Interface*
FDM	*Frequency Division Multiplexing*
FE	*Fast Ethernet*
FIB	*Forwarding Information Base*
FMX2R3	*Flexible Multiplexer Release 3*
FRR	*Fast Rerouter*
GFP	*Generic Framing Procedure*
GMPLS	*Generalized Multi-Protocol Label Switching (Optical over MPLS)*
GR	*Graceful Restart*
HO VC	*High Order Virtual Container*
HO VC SM	*High Order Virtual Container Switch Matrix*
IEC	*International Electrical Commission*
IED	*Intelligent Electronic Device*
IEEE	*Institute of Elétrical and Electronics Engineers*
IEM	*Interferencia Eletromagnética*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IP	*Internet Protocol*
IPBX	*(ou IP PBX) PBX with Internet Protocol*
IPLB	*IP Loop Back (IP virtual)*
ISDN	*Integrated Services Digital Network*

ISE	*Integrated Services Engineering*
ISI	*Intersymbol Interference*
ISIS	*Intermediate System to Intermediate System*
ISO	*International Standards Organization*
ISP	*Internet Service Provider*
ISPABX	*Integrated Services PABX*
ISR	*Integrated Services Router*
ITSP	*Internet Telephony Service Provider*
ITU-T	*International Telecommunication Union, Telecommunication Standardization*
L2TP	*Layer 2 Tunneling Protocol*
LAG	*Link Aggregation Group*
LAN	*Local Area Network*
LC	*Line Card*
LCAS	*Link Capacity Assignment Scheme*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
LER_i	*Label Edge Routers ingress node*
LER_e	*Label Edge Routers egress node*
LIB	*Label Information Base*
LFIB	*Label Forwarding Information Base*
LO VC	*Low Order Virtual Container*
LO VC SM	*Low Order Virtual Container Switch Matrix*
LSA	*Link-State Advertisement*
LSDB	*Link-State Datebase*
LSP	*Label Switched Path*
LSR	*Label Switch Router*
LTO	*Line Termination Optical Unit*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MP-BGP	*Multiprotocol Extensions for Border Gateway Protocol*
MP2MP	*Multipoint-to-Multipoint*
MPLS	*Multi-Protocol Label Switching*
MS-SPRing	*Multiplex Section Shared Protection Ring*
MSOH	*Multiplexer Section Overhead*

MSP	*Multiplex Section Protection*
MSPP	*Multi-Service Provisioning Platform*
MTU	*Maximum Transmission Unit*
MXS19C	*Multiplex Shelf 19-inch*
NAC	*Network Access Control*
NE	*Network Element*
NG-SDH	*Next Generation - Synchronous Digital Hierarchy*
NSF	*Nonstop Forwarding*
NT	*Network Termination (context RDIS)*
NTP	*Network Time Protocol*
OH	*Overhead*
OLC	*Optical Line Card*
OLT	*Optical Line Termination*
OSI	*Open Standard Interconnection*
OSPF	*Open Shortest Path First*
PABX	*Private Automatic Branch Exchange*
PBX	*Private Branch Exchange*
PCM	*Pulse Code Modulation*
PDH	*Plesiochronous Digital Hierarchy*
PDU	*Protocol Data Unit*
PE	*Provider Edges*
PMD	*Polarization Division Multiplexing*
POH	*Path Over Head*
POP	*Point-Of-Presence*
PPP	*Point-to-Point Protocol*
PRI	*Primary Rate Interface (porto de acesso primário)*
PSN	*Packet Switch Network*
PVID	*Port VLAN ID*
PW	*Pseudowire*
PWE3	*Pseudo Wire Emulation Edge to Edge*
QoS	*Quality of Service*
RAS	*Registration, Admission and Status*
RIB	*Routing Information Base*
RD	*Route Distinguisher*

RDIS	*Rede Digital com Integração de Serviços*
RR	*Route Reflector*
RT	*Route Target*
RTe	*Route Target Export*
RTi	*Route Target Import*
RTU	*Remote Terminal Unit*
RSOH	*Regenerator Section Overhead*
RSTP	*Rapid Spanning Tree Protocol*
SAToP	*Structure-Agnostic TDM over Packet*
SCADA	*Supervisory Control and Data Acquisition*
SDH	*Synchronous Digital Hierarchy*
SE	*Subestação*
SEPM	*Sistema Elétrico de Serviço Público da Madeira*
SFD	*Start Frame Delimiter*
SFP	*Small form-factor pluggable* (Transcetor, transmissor e recetor, de fibra ótica)
SIP	*Session Initiation Protocol*
SIPS	*System Integrity Protection Schemes*
SISA	*Supervision and Information System for Local and Remote Areas*
SLA	*Service Level Agreement*
SNCP	*Sub-Network Connection Protection*
SNUS	*Service Network Unit Shelf*
SOH	*Section Overhead*
SONET	*Synchronous Optical Networking*
SPT	*Serviço público de telecomunicações*
SSO	*Stateful Switchover*
STM	*Synchronous Transfer Mode*
STP	*Shelfed Twisted Pair*
SUE	*Supervision Unit*
TA	*Terminal Adapter, adaptador terminal (num contexto RDIS)*
TCP	*Transmission Control Protocol*
TDM	*Time Division Multiplexing*
TDP	*Tag Distribution Protocol*
TE	*Terminal Equipment (contexto RDIS)*
TFTP	*Trivial File Transfer Protocol*

TMX	*Terminal Multiplexer*
ToS	*Type of Service*
TPDU	*Transaction Protocol Data Unit*
TS	*Time slot*
TTL	*Time to Live*
TU	*Tributary Unit*
TUG	*Tributary Unit Group*
UCS	*Unified Computing System*
UDP	*User Datagram Protocol*
UTP	*Unshelfed Twisted Pair*
VC	*Virtual Container*
VCat	*Virtual Concatenation*
VLAN	*Virtual LAN*
VoD	*Video on Demand*
VoIP	*Voice over Internet Protocol*
VPLS	*Virtual Private LAN Service*
VPWS	*Virtual Private Wire Service*
VRF	*Virtual Routing Forwarding Table*
WAN	*Wide Area Network*
WDM	*Wavelength Division Multiplexing*
Wifi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*

1. Introdução

Neste capítulo serão abordados de forma breve a motivação, os objetivos e a estrutura deste documento.

1.1 Motivação

A substituição da arquitetura tradicional pela arquitetura *multi-protocol label switching* (MPLS) veio permitir implementar uma solução com requisitos que parecem contraditórios: *(i)* reduzir custos aumentando a eficiência; e *(ii)* prestar mais serviços, sem afetar os serviços existentes. O MPLS tem os planos de dados e planos de controlo separados o que confere à arquitetura muito mais flexibilidplemeade no encaminhamento, num ambiente neutro (multiprotocolo). O MPLS apenas utiliza mais um protocolo, o *label distribution protocol* (LDP), os atributos da comunidade estendida do *border gateway protocol* (BGP): *route distinguisher* (RD) e *route target* (RT) e o mecanismo *virtual routing and forwarding* (VRF). A EEM optou por implementar a arquitetura MPLS para poder implementar serviços muito rapidamente, tanto VPN-L2 como VPN-L3, ou ainda utilizar o mecanismo de engenharia de tráfego. É de fácil integração, permite futuras expansões, e é acompanhada por uma redução custos. O MPLS permite criar estatitiscas, de atrasos e de congestionamento, utilizadas na análise da tendência do tráfego.

1.2 Objetivos

Como parte do seu programa de modernização da rede de telecomunicações, a EEM implementou uma solução que permitiu migrar da tecnologia em uso, *next generation synchronous digital hierarchy* (NG SDH), para uma rede de comutação por pacote, utilizando o MPLS, e a sua infraestrutura de fibra ótica nas ligações físicas.

Esta implementação permitiu suprir as necessidades exigidas numa arquitetura de rede baseada no transporte de pacotes IP. A solução disponibiliza uma rede multisserviços e multifornecedores, permitindo atender aos requisitos associados a todos os seus serviços de comunicação, com elevados níveis de qualidade, respeitando o binómio custo/eficiência.

Este documento tem por objetivo explicar os motivos e as opções tomadas nessa migração, que permite a EEM abraçar os novos desafios com mais tranquilidade, assegurando elevados níveis de disponibilidade, flexibilidade e capacidade de crescimento.

A solução implementada admite suportar não apenas os serviços atuais, mas também um conjunto de serviços adicionais que venham a ser implementadas no futuro, dando suporte às inovações técnicas relacionadas com novos sistemas: *(i) supervisory control and data acquisition – energy management systems* (SCADA EMS) / *supervisory control and data acquisition - avanced distribution management systems* (SCADA ADMS), bem como aos novos sistemas *advanced metering infrastructure* (AMI) / *automated meter reading* (AMR) / *energy data management* (EDM) para as *smart grids*; *(ii)* de comando local das subestações baseados em *local area networks (LAN)* e em protocolos de comunicação baseados pela tecnologia *Internet Protocol* (IP) utilizados nas *smart grids*; *(iii)* de suporte à introdução de novos dispositivos eletrónicos

inteligentes (*intelligent electronic device*, IED), i.e, sensores, unidades terminais remotas *(remote terminal unit*, RTU), etc., de uma forma independente nas referidas subestações, através de uma arquitetura distribuída; *(iv)* de suporte à supervisão comando e controlo da rede elétrica, independentemente do protocolo utilizado na comunicação, RTU e do centro de comando e controlo; *(v)* de suporte à utilização de redes/serviços de comunicação baseados na norma IEC-61850 e respetivas extensões; e *(vi)* de suporte ao tráfego corporativo, permitindo o acesso à rede corporativa da EEM, email e aplicações diversas de comunicação.

Os dispositivos que adotam a tecnologia *Smart Grid* dispõem de amplos recursos de comunicação que permitem a transmissão dos valores de medição dos parâmetros físicos, bem como monitorização dos transformadores ou outros dispositivos digitais associados a diversos elementos da rede elétrica de recolha de dados. O *smart grid* permite que aos operadores que supervisionam a rede elétrica de gerir e monitorizar milhões de dispositivos e sensores. Existem 3 conceitos associados à leitura dos contadores e dois associados ao SCADA que são os seguintes: *(i) advanced metering system* (AMS*); (ii) automated meter reading (AMR); (iii) advanced metering infrastructure (AMI); (iv)* O *SCADA energy management systems; (v)* SCADA *avanced distribution management systems.* O AMS é um medidor de consumo de gás e ou de eletricidade, com um endereço IP. Envia automaticamente essa informação digital, em tempo real, para o fornecedor de energia*.* O AMR é igual ao AMS, mas também recolhe informações para diagnóstico. As leituras em tempo real, combinados com uma análise mais aprofundada de outros dados recolhidos, oferecem um maior controlo sobre o consumo de eletricidade, água e gás. O AMI é igual ao AMR, mas também admite a comunicação bidirecional entre utilitários e clientes. Esta comunicação bidirecional permite ao fornecedor de serviço ligar ou desligar remotamente o serviço prestado*.* O SCADA EMS veio substituir o tradicional SCADA, com funções mais avançadas de monitorização e controlo. O SCADA *avanced distribution management systems* (ADMS) veio permitir a integração de outras formas de produção energia na rede (eólicas, fotovoltaicos, veículos elétricos, etc) *[1.2-1]*.

Com a tendência generalizada para a implementação de soluções que permitam a gestão da rede de energia até ao consumidor, a *International Electrotechnical Commission* (IEC) desenvolveu uma norma para a troca de dados entre dispositivos instalados nas subestações (IEC 61850) *[1.2-2]*. O protocolo de comunicação na rede local de comunicações residente nos sistemas de proteção, comando e controlo numéricos, utilizado no SCADA, é o protocolo normalizado IEC 60870-5-104, abreviado por 104, e utiliza o encapsulamento do protocolo *ethernet*.

Devido aos desafios internos, também designados por desafios operacionais, que condicionam o fornecimento de serviços públicos, a EEM teve necessidade de investir numa solução MPLS com benefícios a longo prazo. Este documento aborda os motivos que levaram à necessidade de migração, as opções tomadas, bem como a integração da nova rede lógica sobre a rede física existente. Esta migração ocorreu sem comprometer os requisitos essenciais da rede que já estava em funcionamento, tais como a largura de banda, a disponibilidade de serviço e a segurança. Associada a esta migração, foi também necessário aumentar a capacidade da rede de fibra ótica, por forma a permitir suportar o funcionamento das duas redes de telecomunicações (SDH e MPLS) em paralelo e potenciar outras vertentes como a implementação de uma *smart grid* e numa outra possível oportunidade de negócios.

À medida que as redes elétricas evoluem em direção a uma *smart grid*, esta evolução admite a integração de energia de fontes renováveis. O conceito de *smart grid* é a gestão de energia numa rede elértrica, agregandado várias tecnologias e permite, entre muitas outras coisas, otimizar os sistemas de monitorização da rede elétrica em tempo real que nos permita saber o estado da

rede eléctrica. É necessário alargar a instalação de diversos sensores ao máximo de outros elementos da compõe a rede elétrica. Esses sensores recolhem dados locais que são automaticamente transmitidos pela rede de telecomunicação por forma a permitir a tomada de decisões relacionado com a gestão da rede electrica. Este envio de dados, em tempo real, permite visualizar padrões de produção e de consumo, e tomar decisões que permitam melhorar a eficiência energética e garantido máxima segurança. Neste contexto entende-se "consumo" como sendo a potência consumida no cliente final e não nas subestações. O Centro de Despacho é responsável pela coordenação do funcionamento da rede de transporte e dos sistemas electroprodutores até as saídas de média tensão das subestações de distribuição, sendo de referênciar as seguintes: abastecimentos de energia aos pontos de entrega em média tensão, monitorização das atividades de produção dos centros electroprodutores e coordenação das indisponibilidades da rede de transporte e dos produtores sujeitos a despacho.

Numa primeira fase, a EEM apenas realizava a telecontagem dos consumos de energia, pois implementou uma infraestrutura de medição avançada (*advanced metering infrastructure*, AMI) e um sistema de gestão da sua rede de postos de transformação (*advanced distribution management system*, ADMS). A possibilidade de recolha de registos, e posterior análise, de todos os pontos de medição, irá permitir o tratamento de dados por forma a ajudar no planeamento da rede elétrica, tal como localizar as falhas com um elevado grau de precisão e evitar interrupções. Estes dois aspetos, AMI e ADMS, estão fora do âmbito deste documento, mas foram os impulsionadores da necessidade de migração da rede de telecomunicações.

1.3 Estrutura do documento

Este documento está estruturado em 5 capítulos por forma a organizar os temas abordados. Foram adicionados apêndices que esclarecem com mais aprofundamento alguns assuntos abordados nos capítulos 3 e 4, e utilizados na conclusão onde são feitas comparações das vantagens e desvantagens das diferentes soluções.

No capítulo 1 são apresentados a motivação e os objetivos deste documento.

No capítulo 2 é enquadrada a Empresa de Eletricidade da Madeira, tal como é apresentado o Sistema Elétrico de Serviço Público da Madeira (SEPM), o serviço de telecomunicações e as diferentes soluções adotadas.

No capítulo 3 é descrito o estado da arte, onde se compara a arquitetura *Internet Protocol* e MPLS. É fundamentada a necessidade de migrar, e como é construída a hierarquia da rede. São apresentados alguns esclarecimentos sobre o MPLS e de alguns recursos utilizados.

No capítulo 4 é descrita a metodologia aplicada na construção da rede "WAN SCADA" da EEM. Explicação das opções tomadas no encaminhamento e configurações dos *routers*. Explicação de quais os protocolos *interior gateway protocol* (IGP) utilizados, quais os mecanismos de recuperação em caso de avaria e quais as opções de anunciar os prefixos de rede. Necessidade de se terem configurado rotas explicitas recorrendo ao mecanismo engenharia de tráfego. Pequena abordagem à segurança da rede.

No capítulo 5 são apresentadas as conclusões deste trabalho e são apresentadas algumas sugestões para desenvolvimentos de trabalhos futuros.

2. Enquadramento

Neste capítulo será apresentada a Empresa de Eletricidade da Madeira (EEM), sendo descrito o Sistema Elétrico de Serviço Público da Madeira (SEPM) e a necessidade da EEM possuir uma rede de telecomunicações.

2.1 A Empresa de Eletricidade da Madeira

A EEM tem por objetivo fornecer energia elétrica à população da Região Autónoma da Madeira. A EEM, de capitais totalmente públicos, à data da publicação deste documento, está incumbida de produzir, transportar, distribuir e comercializar energia elétrica. Na qualidade de operadora da rede regional de transporte de eletricidade, a EEM está obrigada, contratualmente, a adequar o fornecimento de energia elétrica às necessidades, quer em quantidade e em regularidade, quer qualitativamente (segurança e capacidade), de todos os seus consumidores.

2.2 Sistema elétrico de serviço público da Madeira

O Sistema Elétrico de Serviço Público da Madeira (SEPM) foi concebido de modo a admitir o transporte da energia elétrica entre as unidades de produção e os consumidores de uma forma segura e fiável (contínua). A otimização da rede potenciou a possibilidade de distribuir e integrar diversas fontes de produção de energia. O SEPM é robusto, pois satisfaz a demanda dos consumidores e com qualidade, independentemente da hora do dia ou da sua localização. O SEPM caracteriza-se por uma enorme interação entre dispositivos ativos e passivos. O SEPM é um sistema não-linear, uma vez que as relações de tensão, corrente, e de potência dependem das características da rede. Os dispositivos ativos são grupos electroprodutores, disjuntores, proteções e cargas. Os dispositivos ativos passivos são as linhas, subestações e pontos de secionar. Todas estas características contribuem para definir o SEPM como um sistema complexo que, na ausência de uma solução que permita monitorizar e controlar os fluxos de energia, não pode ser operado com eficiência e de uma forma segura.

Essa monitorização consiste na medição, em tempo real, de todos os parâmetros elétricos do SEPM, e que são transmitidos para um Centro de Despacho. O Centro de Despacho é constituído por operadores experimentados na análise comportamental da rede, como as flutuações nas cargas ou como os riscos operacionais. Consideram-se riscos operacionais curto-circuito, desligamento inesperado de uma central, destruição de componentes/elementos de rede elétrica, etc.). Para auxiliar os operadores, os dados recebidos no Centro de Despacho são apresentados de forma gráfica, permitindo uma avaliação intuitiva e a tomada de decisões assertivas. Cabe ao programa *supervisory control and data acquisition* (SCADA) o processamento dos dados para estes serem apresentados de uma forma gráfica. O SCADA também admite o envio das ordens de controlo para o fecho ou abertura dos disjuntores ou das facas dos seccionadores, tal como a subida ou descida de tomadas dos transformadores em carga.

Para a caracterização do SEPM, foram instalados diversos tipos de relés de proteção eletrónica com processamento (*intelligent electronic device*, IED), em todos os nós da rede elétrica. Os IED

medem diversos parâmetros (medidas físicas) e dispõem de informação do estado dos elementos mecânicos, e daí uma rede elétrica ser caracterizada comumente como uma rede sensorizada.

A Figura 2.1 ilustra o esquemático dos dados apresentado aos operadores do Centro do Despacho, após processamento dos dados recebidos.

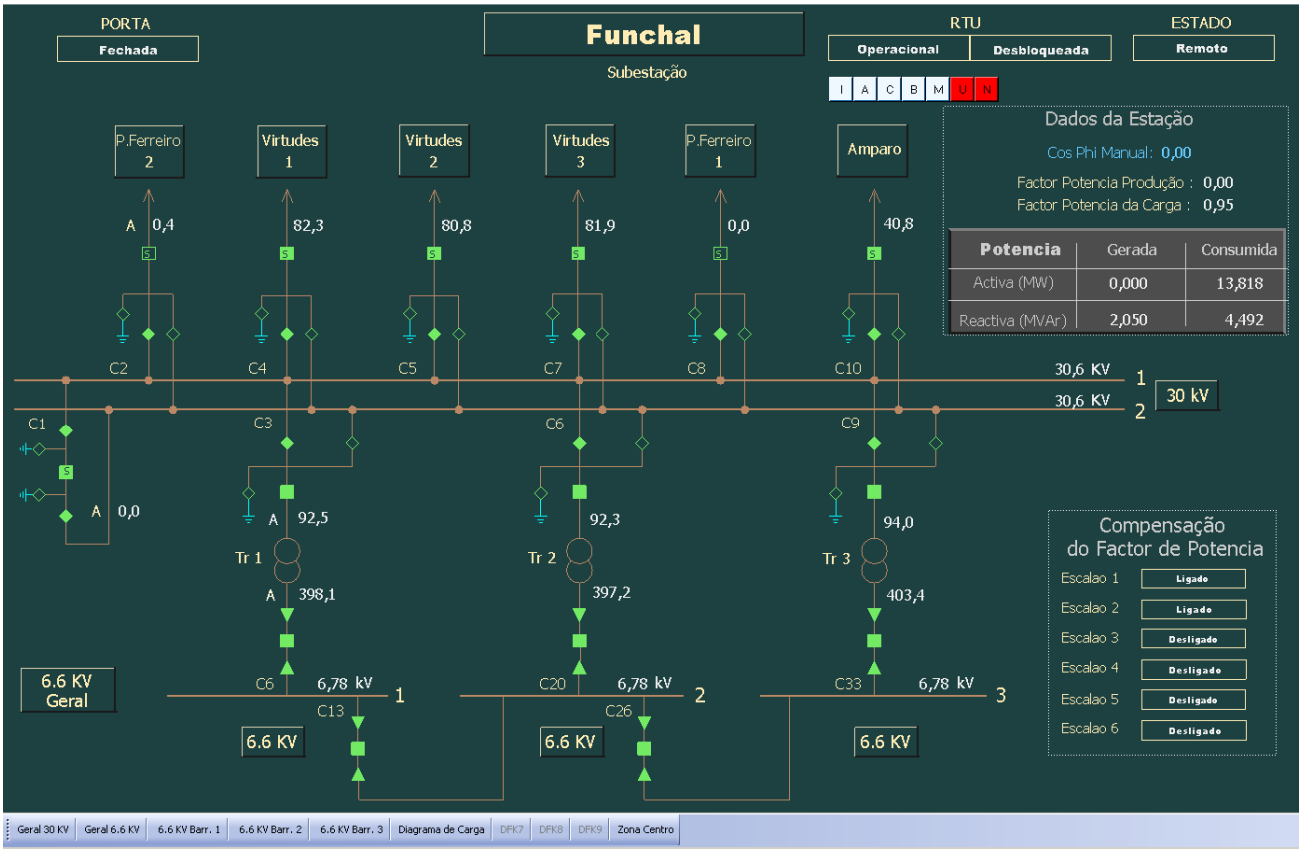

Figura 2.1 – Exemplo de algumas características elétricas da subestação do Funchal.

Como se pode constatar, a porta da subestação está fechada, os seccionadores associados às duas linhas do Palheiro Ferreiro estão abertos, mas não estão em manutenção, pois a linha não está "aterrada". O "aterrar" da linha significa ligar a linha ao barramento de Terra existente na subestação para escoar qualquer carga que surja pelo fato da linha ser desnudada, protegendo assim os técnicos que estão a exercer os trabalhos de manutenção. O fator de potência é de 95%, quando o ideal seria 98%, apesar de dois dos 6 escalões do equipamento que compensa o fator de potência estarem ligados. Os três transformadores estão ligados a rede SEPM, fornecendo assim carga aos seus respetivos barramentos do secundário. Os três barramentos de 6,6 kV estão interligados, daí as cargas serem as mesmas. Os valores não são iguais devido a desvios provocados pelos transformadores de intensidade (TI). Um TI é um dispositivo que mede a corrente elétrica, em amperes, transportada pelo traçado. O concentrador de dados local *(remote terminal unit slave*, RTU *slave*) está operacional e o controlo remoto pode ser exercido. Os níveis de tensão estão ligeiramente acima dos valores nominais para permitir a compensação das perdas provocadas pelas características dos cabos de potência.

Os IED para além de processarem os dados recolhidos também os enviam para uma RTU *slave* e, em paralelo, para o Centro de Despacho, utilizando um sistema de telecomunicações. Os registos são informações respeitantes às características dos elementos da rede elétrica que os IED

protegem, e são gravados em suporte digital tanto localmente como no Centro de Despacho. Os IED têm autonomia para enviar comandos aos elementos moveis associados ao SEPM, ou executam esses mesmos comandos a pedido do Centro de Despacho, como por exemplo: desligar o disjuntor a que está associado se forem detetados valores de parâmetros fora do estipulado na sua configuração. Estes dispositivos admitem configurações específicas para cada tipo de linha, uma vez que são programáveis e possibilitam um registo cronológico dos eventos em suporte digital.

2.3 Serviço de telecomunicações

Para responder aos desafios colocados pelas constantes evoluções de um sistema elétrico, é imprescindível uma rede de telecomunicações associada. A rede de telecomunicações existente na EEM, integrada no SEPM, oferece inteligência ao sistema elétrico, possibilitando a monitorização e o envio de comandos por controlo remoto. São partes constituintes de um sistema sensorizado de energia: *(i)* um sistema SCADA; *(ii)* o serviço "teleproteção"; e *(iii)* os dispositivos que recolhem informações e controlam o estado do SEPM.

A rede sensorizada, suportada por um sistema robusto e fiável de telecomunicações, possibilita uma maior eficiência e confiabilidade, contribuindo assim para a segurança e robustez do serviço prestado pelo SEPM. Com a associação dos IED a um sistema de telecomunicações, passou a existir a capacidade de recolha e transmissão de grandes quantidades de informação (medidas e estados dos componentes da rede elétrica). Em caso de falha do sistema de telecomunicação, a subestação tem autonomia para executar ações de segurança, pois a RTU *slave* é um autómato. Se falhar a RTU *slave*, o Centro de Despacho continua a poder controlar os IED instalados nas diferentes subestações, enviando comandos. O Centro de Despacho, com os dados recebidos de toda a infraestrutura elétrica do SEPM, fica capacitado para realizar a monitorização e o controlo remoto sobre todos os elementos mecânicos instalados no SEPM. A terminologia "infraestrutura elétrica" refere-se a subestações, postos de seccionamento, centrais de produção. Por forma a incrementar a qualidade da atuação das proteções, alguma dessa informação recolhida é também enviada para os dispositivos de proteção instalados nas infraestruturas elétricas vizinhas às da recolha. A informação recebida é depois comparada com as informações das proteções locais, permitindo a tomada de decisões assertivas e, quase instantâneas, de como deverão proceder face a uma anomalia no SEPM. Esta informação, que é critica, é gerada pelas teleproteções.

2.4 Problema da migração

Após dois anos de estudos, em abril de 2017 foi aprovado um projeto de modernização para a implementação de uma infraestrutura de telecomunicações baseada na arquitetura MPLS, para substituir a infraestrutura existente baseada na arquitetura hierarquia digital plesiócrona /síncrona (SDH/PDH). Esta modernização foi realizada por etapas de modo a permitir a coabitação de ambas as tecnologias, e assim continuará, em paralelo, até à validação da nova tecnologia adotada. A gestão das duas redes pode gerar conflitos e sobreposição de serviços, daí

a necessidade de uma planificação listada. A rede de fibra ótica da EEM veio garantir o sucesso da migração, pois permitiu a interligação de todas as instalações que compõe a infraestrutura do SEPM.

2.5 Arquitetura da rede de telecomunicações baseada no rádio

O projeto da automatização do SEPM, iniciado em 1985, veio permitir que o serviço de fornecimento de energia tivesse maior fiabilidade e qualidade. Com efeito, com a automatização e consequentemente com a aquisição dos parâmetros que caracterizam cada nó do SEPM, veio a ser possível uma melhoria no tempo de resposta em caso de perturbações e/ou avarias.

Esta automatização foi suportada por um sistema de telecomunicações vocacionado para a transmissão de dados. Em 1985, e por falta de investimentos do único operador de telecomunicações existente na altura, este não oferecia um serviço homogéneo em toda a RAM tendo sido descurada as localidades menos densamente povoadas. Infelizmente, as centrais hídricas agregadas ao SEPM estavam localizadas precisamente nessas zonas e a possibilidade de transmitir dados para o Centro de Despacho era deficiente ou mesmo inexistente. Ou seja, nessas localidades, o operador de telecomunicações não dispunha de tecnologia que permitisse a transmissão de dados e, quando existia, não era fiável nem confiável. Também havia uma elevada latência em repor situações anómalas, principalmente em caso de destruição das infraestruturas provocadas por derrocadas ou incêndios, não compatível com as necessidades da EEM. Face a esta situação, foi decidido a integração de um sistema de transmissão via rádio, para oferecer mais segurança e disponibilidade de serviço no projeto de automação.

Além disso, a utilização dessa tecnologia estava sujeita a vários constrangimentos, tais como o facto de só permitir comunicações por conferência (por ser analógico) e estar sujeito a perturbações alheias à EEM, tais como incêndios nos terrenos circundantes (os fumos interferiam na qualidade do sinal, ou quando havia muita precipitação). Quando a RTU *slave* introduzia muito ruído, bloqueava o canal ao qual estavam várias RTU agregadas em série, e a infraestrutura do sistema de rádio implementado não possibilitava redundância. Para piorar a situação, o fabricante descontinuou o desenvolvimento do sistema de rádio, não garantindo assim peças de substituição.

Refira se que as antenas recebiam em modo de difusão e transmitiam para a antena vizinha num feixe, até chegar ao Centro de Despacho.

2.6 Arquitetura da rede de telecomunicações baseada no PDH

A implementação nas subestações de novas soluções *intelligent electronic device* (IED), com processamento digital, veio exigir meios técnicos de transmissão que a opção do rádio analógico não oferecia. Em 2003, teve início a construção de uma nova rede de telecomunicações, baseada na tecnologia PDH suportada por uma rede física construída em fibra ótica.

O acesso múltiplo por divisão de tempo (*time-division multiple access*, TDMA) é uma técnica que admite a transmissão de múltiplos fluxos de tráfego num único canal ou faixa de frequência. Um

fluxo de informação é uma sequência de pacotes relacionados e que recebem idêntico tratamento em cada nó até chegarem ao seu destino final. É utilizado uma unidade de divisão de tempo da largura de banda (*time slot*, TS), de forma a permitir distribuir a largura de banda entre os diferentes utilizadores. Esta tecnologia necessita de sincronismos.

Na definição do modo de trama E1, a EEM optou pelo PCM31. Ou seja, das 32 TS de capacidade da trama E1, o multiplexador tinha ao seu dispor 31 TS para tráfego útil, sendo que a que sobrava era para o alinhamento da trama (pois não existe sincronização). Este assunto é abordado no "*Apêndice 2 – Arquitetura Hierarquia Digital Plesiócrona*".

2.7 Arquitetura da rede de telecomunicações baseada no (NG) SDH

Em 2006, numa primeira fase (de duas), a EEM implementou a tecnologia NG SDH através da instalação de 5 equipamentos do fabricante Siemens, modelo SURPASS hiT 7050 *Flat Pack* 1. Esta tecnologia veio permitir: *(i)* uma redução de número de fibras óticas; *(ii)* maior capacidade de transporte; *(iii)* transporte de tráfego *ethernet*; e *(iv)* redundância na rede de telecomunicações. O transporte de tráfego *ethernet* veio potenciar o serviço de acesso remoto às proteções individuais de cada cela existente nas subestações. A "cela" é o compartimento individual de cada sistema trifásico de cabos de potência numa subestação, onde estão instalados os diversos dispositivos de medida e proteção. Numa segunda fase, foram instalados outros dois modelos do mesmo fabricante, mas com capacidades diferentes: SURPASS hiT 7020 e SURPASS hiT 7060. Este assunto é abordado no "*Apêndice 4 – Arquitetura NG SDH*".

2.8 Conclusão

A EEM tem a responsabilidade de produzir, transportar, distribuir e vender a energia elétrica consumida na RAM. O serviço é prestado sobre o SEPM e o serviço prestado está classificado como serviço público. Para assegurar o cumprimento da tarefa, e para incrementar a segurança do SEPM, a EEM criou o serviço de telecomunicações para transportar toda a informação relacionada com os parâmetros que caracterizam cada nó da rede. Os parâmetros são essencialmente os valores de tensão, corrente, fator de potência e estados dos elementos mecânicos. Cabe ao Centro de Despacho otimizar a gestão, em tempo real, oferecendo ganhos de eficiência no transporte da energia e disponibilidade de serviço. Mediante a análise dos parâmetros, o Centro de Despacho pode enviar, se for necessário, comandos remotos, de abertura ou fecho de dispositivos (disjuntores, seccionadores), de subida ou descida de tomadas dos transformadores. Além disso, os relés de proteção dispõem de capacidade de processamento da informação lida pelos sensores que lhe estão acopladas e de interagir com os disjuntores de corte. Essas informações são também enviadas ao Centro de Despacho pela rede de telecomunicação instalada paralelamente à rede elétrica.

Pelos motivos já expostos, torna-se evidente a necessidade da EEM dispor de uma rede de telecomunicações moderna e que dê suporte ao SEPM.

3. Estado da arte

O MPLS oferece uma melhoria muito significativa nessa velocidade de encaminhamento dos pacotes IP, pois a decisão é tomada analisando um rótulo adicionado na camada 2 e meio do modelo OSI. Na arquitetura IP, as tabelas de encaminhamento (*routing information base*, RIB) tendem a crescer de forma exponencial, resultando num demorado processo de tomada decisão no encaminhamento. A otimização dos recursos é conseguida pela utilização do mecanismo de engenharia de tráfego, principalmente pelas tomadas de decisão baseadas pelo congestionamento da rede. Sobre o MPLS é implementado uma arquitetura IP que permite garantir que a rede seja escalável e resiliente. Os protocolos de encaminhamento interior padrão (*interior gateway protocol*, IGP), do tipo *link-state,* descobrem unicamente o caminho de menor custo (*shortest path routes*), sem atender ao estado de carga de cada troço da rede. A utilização de um protocolo IGP para construir a topologia da rede é fundamental para que a rede seja dinâmica. No processo de construção da tabela de encaminhamento, o protocolo IGP proporciona o transporte de pacotes contendo objetos descritores (*link-state advertisement*, LSA), com a informação necessária as atualizações das tabelas de encaminhamento dos *routers* vizinhos *[3]*.

3.1 Alguns conceitos utilizados no MPLS

Para uma melhor compreensão da arquitetura MPLS, são aqui descritos alguns conceitos que permitem uma melhor compreensão do MPLS.

Pacotes *link-state advertisement*

Os pacotes dos objetos descritores (*link-state advertisement*, LSA) são pacotes com informações, designadas por objetos descritores, trocadas entre *routers* vizinhos, em *multicast*, o campo "*Time to Live*" (TTL) existente no cabeçalho do pacote IP igual a um, para atualizações da topologia da rede.

Encaminhamento por classes equivalentes

O encaminhamento por classes equivalentes (*forward equivalence class*, FEC) é a representação de um fluxo no transporte, fazendo com que todos os pacotes IP (do mesmo fluxo) sejam alvo do mesmo procedimento durante o encaminhamento. Tomando como exemplo, todo o tráfego com o mesmo valor de precedência IP (*IP precedence*), do campo "ToS" do cabeçalho, pode ser utilizado para definir o FEC. É semelhante ao *per-hop behavior* do modelo *diffServ*, e, ao contrário do encaminhamento IP convencional, no MPLS só se analisa o primeiro pacote IP do fluxo que entra no domínio MPLS, ao qual é-lhe atribuído um FEC *[3.1-1]*.

MPLS *label distribution protocol*

Um conceito fundamental no MPLS é que dois *routers*, que comutam por rótulo *(label switching routers*, LSR), devem concordar com o significado dos rótulos utilizados para encaminhar o tráfego entre eles. Esse entendimento comum é alcançado utilizando um conjunto de procedimentos, denominado por protocolo de distribuição de rótulos (*label distribution protocol*, LDP), que permite ao *router* LSR informar os seus *routers* vizinhos dos seus rótulos para um determinado fluxo de tráfego *[3.1-2]*.

Tabelas

Os protocolos de encaminhamento IGP, como os *open shortest path first* (OSPF) e *intermediate system to intermediate system* (IS-IS), permitem que os *routers* vizinhos troquem informações entre si, por forma a ficarem a conhecer a topologia da rede a que pertencem (*autonomous system*, AS). Essas informações são utilizadas pelos *routers* na construção da sua primeira tabela com o de estados de ligação (*link-state database*, LSDB). A partir desta primeira tabela (LSDB), o *router* constrói e mantém atualizada, a tabela de encaminhamento (*routing information base*, RIB) que relaciona o prefixo de rede IPv4 com o porto de saída do pacote IP.

No entanto, quando o pacote IP chega ao *router*, o que o *router* analisa é o campo “IP de destino” do cabeçalho associado ao pacote IP. Assim, no preenchimento do porto de saída, o *router* consulta uma outra tabela criada, a tabela *address resolution protocol* (ARP), que correlaciona o endereço virtual (IP) com o endereço físico (MAC) permitindo, assim, a interligação da camada 2 e da 3, do modelo OSI. O endereço MAC que o *router* utiliza na sua consulta à tabela ARP é o endereço MAC do porto do *router* vizinho a que está associado o seu porto de saída.

No contexto MPLS, para além de existirem estas tabelas, há necessidade de mais outras três para permitir realização da comutação por rótulo. A construção dessas tabelas depende de uma sequência de procedimentos: *(i)* criação de um rótulo na *label information base* (LIB); *(ii)* envio dessa mesma tabela LIB para os *routers* MPLS adjacentes; *(ii)* construção, e atualizações, da tabela *label forwarding information base* (LFIB). Todas estas tabelas estão ilustradas na Figura 3.1 *[3.1-3]*.

- Tabela *routing information base*

A partir da topologia da rede, guardada na tabela *link-state date base* (LSDB), o *router* cria a tabela de encaminhamento (*routing information base*, RIB), que é constituída por uma lista com todos os destinos conhecidos. Além dos destinos conhecidos também dispõe de informação sobre os melhores próximos saltos para dar continuidade ao encaminhamento (*next hop*) a serem utilizados para alcançá-lo.

- Tabela *label information base*

A tabela *label information base* (LIB) apresenta informações que correlacionam os rótulos, de significado local, com os portos do *router* utilizados na comutação por rótulo. E para a sua construção são utilizados dois protocolos de sinalização: o *resource reservation protocol* (RSVP) e o *label distribution protocol* (LDP). O RSVP permite a sinalização e negociação por forma a garantir um caminho, e o LDP é responsável pela distribuição dos rótulos necessários à comutação, assunto abordado no ponto "*Distribuição de rótulos*" na seção “*11.1 - Tipos de*

protocolos" do apêndice 6. Existe uma relação entre as tabelas LIB e RIB que permite construir outras duas tabelas: FIB e a LFIB, que serão utilizadas pelo MPLS para comutar os pacotes MPLS entre os portos de entrada e o porto de saída.

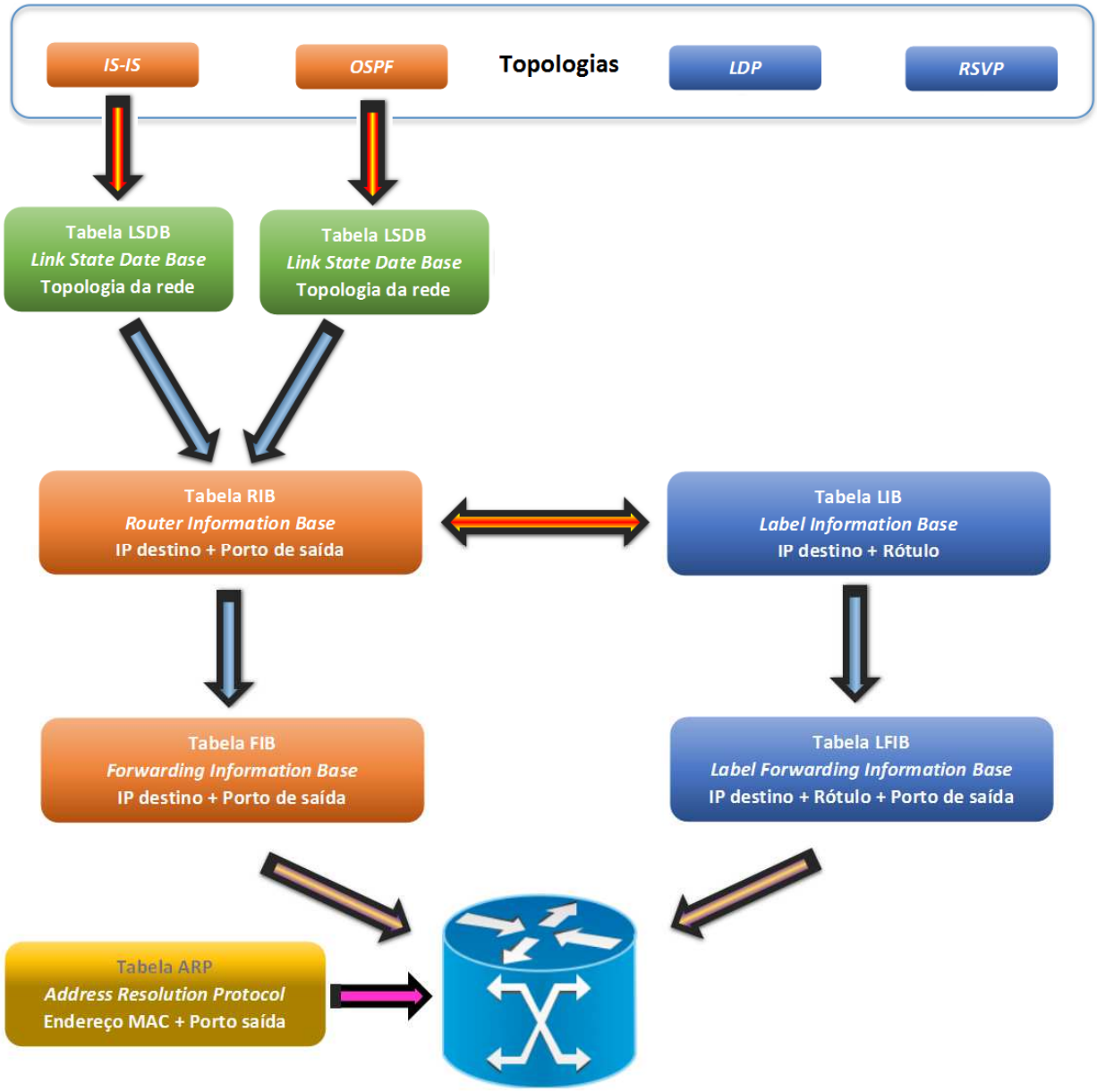

Figura 3.1 – As várias tabelas que o *router* (MPLS) consulta para comutar o tráfego.

- Tabela *forwarding information base*

Recorrendo ao mecanismo de otimização, são selecionados os melhores caminhos da tabela RIB e estes são inseridos na tabela *forwarding information base* (FIB). A tabela FIB é um agente que interage com o plano de dados (do *router*). Na tabela FIB, além dos destinos dos melhores próximos saltos, para dar continuidade ao encaminhamento, há também informação sobre o porto (*interface*) específico que deve ser utilizado. Se essa informação não existir na tabela FIB, o pacote MPLS é descartado.

- Tabela *label forwarding information base*

A tabela *label forwarding information base* (LFIB), é um agente que interage com o plano de dados dos *routers*. A tabela LFIB, é construída a partir das diversas tabelas LIB recebidas dos *routers* adjacentes, transportadas pelo protocolo de sinalização *label distribution protocol* (LDP), e correlacionada com a tabela FIB. Para que o domínio MPLS possa construir uma malha completa de circuitos emulado (*label switched path*, LSP), as tabelas LFIB precisam de ser preenchidas dinamicamente com os melhores próximos saltos (*next hop*).

A Figura 3.2 ilustra a relação entre o plano de controlo e o de dados no processo de atribuição de rótulos aos pacotes MPLS. O protocolo de encaminhamento OSPF é responsável pela descoberta do caminho mais curto para permitir entregar os pacotes IP com destino ao IP 10.0.0.0/8. O LDP informa o *router* que os pacotes IP que acedam pelo lado esquerdo devem possuir o rótulo 17, e pelo lado direito o rótulo 16. Os *routers* vizinhos recebem essa informação (LIB) através da receção dos pacotes IP transportados pelo LDP. Os *routers* atualizam as suas tabelas LFIB.

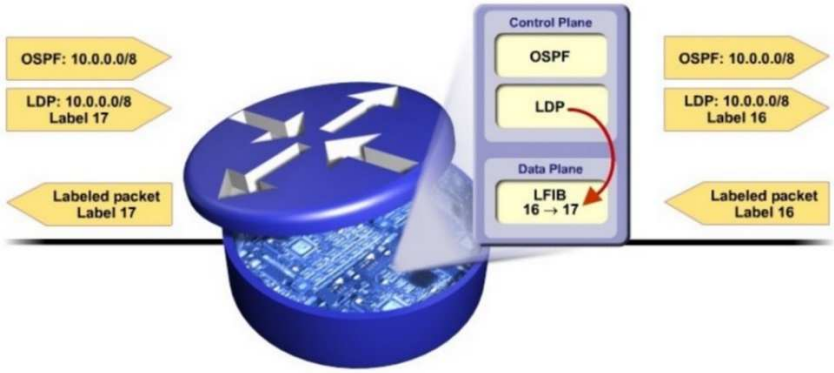

Figura 3.2 – Construção da tabela LFIB *[3.1-4]*.

Attachment circuit

As VPN MPLS só têm significado dentro do *backbone* MPLS, mas necessitam de ter uma ligação física com o CE. Essa ligação física é designada em inglês por *attachement circuit* (AC), e permite a troca de tráfego segmentado de forma lógica. Ou seja, o AC é na realidade um *uplink* de vários serviços, pois proporciona o transporte a vários serviços, de clientes diferentes existente no mesmo *router* CE. Na segmentação do tráfego é adicionado um rótulo (*tag*).

Ethernet flow point

Uma instância de serviço de ponto de fluxo *ethernet* (*ethernet flow point*, EFP) é uma *interface* lógica que interliga um domínio de comutação (*bridge domain,* BD) a um porto físico ou a um grupo *etherchannel*.

Ethernet virtual connection

Uma *ethernet virtual connection* (EVC) é uma associação entre duas ou mais *interfaces* de rede do utilizador que identificam um caminho ponto a ponto ou multiponto a multiponto dentro da rede do provedor de serviços. Um domínio de transmissão EVC é determinado por um *bridge domain* e os EFP que estão ligados a ele. É possível ligar vários EFP da mesma *interface* física ao mesmo *bridge domain*, e cada EFP pode ter seus próprios critérios de correspondência. Um pacote só é recebido se é compatível com os critérios de correspondência EFP na *interface bridge domain* (BDI). Se não houver EFP correspondentes, o pacote é descartado.

3.2 Arquitetura MPLS

Uma das principais vantagens do MPLS, comparada com o "simples" encaminhamento por IP, prende-se com o seu procedimento no encaminhamento de pacotes.

Arquitetura *Internet Protocol*

O encaminhamento de pacotes IP numa arquitetura *Internet Protocol* (IP), está dependente da análise do cabeçalho associado ao pacote IP, análise essa que é sucessivamente repetida em cada *router* por onde passe o pacote IP. A análise só é possível após o desencapsulamento (desmultiplexação) do pacote IP recebido para alcançar o cabeçalho onde consta a informação do IP de destino do pacote. O algoritmo de encaminhamento em execução no *router*, utiliza essa informação (IP de destino do pacote IP) na consulta da tabela de encaminhamento, que contém a informação do porto de saída do pacote IP. Também contém a informação do endereço MAC do porto do *router* vizinho associado a esse porto de saída para poder comutar o pacote IP. Esse endereço MAC vai substituir o endereço MAC de destino existente no cabeçalho do pacote IP quando este chegou ao *router*. Depois da substituição, o pacote IP é reconstruído por multiplexagem, procedimento conhecido por encapsulamento. Após o encapsulamento, o pacote IP é armazenado na fila de espera até que haja uma oportunidade para ser enviado para o nó seguinte. Este procedimento é cíclico, para cada pacote IP, e ocorre em todos os nós da rede, terminando quando o pacote IP chega ao seu destino. Se o IP de destino não for identificado pelo *router*, o pacote IP é descartado. O protocolo de encaminhamento IGP, do tipo *link-state,* procura o caminho mais curto, sem atender ao estado de carga de cada troço da rede, o que, por vezes, leva a que sejam escolhidos caminhos congestionados em detrimento de caminhos mais longos, mas nos quais existem os recursos que satisfaçam o encaminhamento. O conceito subjacente ao MPLS vem, de alguma forma, colmatar esta deficiência, permitindo encontrar caminhos que têm efetivamente os recursos necessários ao transporte dos fluxos de tráfego. O *router* também divide todos os possíveis pacotes IP numa série de classes de encaminhamento para admitir o encaminhamento por classes equivalentes (*forwarding equivalence classe*, FEC).

Arquitetura MPLS

A arquitetura MPLS permite maximizar o rendimento das múltiplas aplicações existentes sem qualquer impacto sobre o respetivo desempenho. A atribuição de uma determinada classe de encaminhamento ao fluxo associado ao primeiro pacote IP, é feita apenas uma vez e à entrada da rede. É utilizado o valor da FEC no cálculo do rótulo MPLS que é adicionado a todos os pacotes IP. O pacote IP ao receber um rótulo MPLS é transformado num pacote MPLS, fazendo com que

o pacote MPLS seja comutado em todos os *routers* por onde passe o pacote MPLS sem necessidade de processar o cabeçalho do pacote IP.

Os rótulos dos pacotes MPLS servem de índice de procura na tabela FIB, que contém a informação necessária para determinar qual é o próximo elemento de rede de destino do pacote MPLS e qual deverá ser o novo rótulo a adicionar ao pacote MPLS. Este conceito traz uma série de vantagens relativamente às redes IP convencionais. Destaca-se a possibilidade de o pacote MPLS poder indicar o *router* através do qual ingressou na rede e, consequentemente, as decisões de encaminhamento poderem ser baseadas nessa informação. Uma outra característica de relevo do MPLS tem a ver com o facto dos rótulos MPLS, para além de transportarem informações útil ao encaminhamento, permitem inferir informação relacionada com a classe de serviço. Na arquitetura IP tal é mais complexo, uma vez é necessário desmultiplexar todo o cabeçalho.

Mecanismo *traffic engineering*

O protocolo de encaminhamento OSPF ao determinar o caminho mais curto determinado pelo seu algoritmo, para que o pacote IP chegue ao seu destino, pode não ser a melhor opção e podem existir caminhos alternativas subutilizados. Pois, nas redes com topologia de malha completa, existem ligações suscetíveis de estarem subutilizadas. O MPLS disponibiliza um mecanismo de engenharia de tráfego (*traffic engineering*, TE), designado por MPLS-TE, que garante uma melhor eficiência na utilização dos recursos disponíveis ao providenciar rotas que suportem requisitos específicos das aplicações ou serviços sujeitos as exigentes restrições de qualidade de serviço *[3.2-1]*.

No estabelecimento de um caminho explícito, o administrador não permite que seja o protocolo de encaminhamento IGP a escolher o melhor caminho, maximizando a eficiência na gestão de recursos da rede. Este mecanismo, MPLS-TE, permite a compartilha de carga por vários caminhos (*label switched path traffic engineering*, LSP-TE) ao definir rotas diferentes para um fluxo específico, respeitando a qualidade de serviço e evitando pontos de elevado congestionamento. Este mecanismo atende a requisitos de alta disponibilidade e segurança de serviços, incluindo o mecanismo de reencaminhamento rápido (*fast rerouter,* FRR), permitindo que o *router* escolha rapidamente outro segmento constituinte do caminho quando um nó desliga ou falha. Esta elevada velocidade de recuperação impede perda de pacotes IP.

3.3 *Routers* MPLS

O *router* é um dispositivo de encaminhamento de pacotes de dados com vários tipos de adaptadores de rede e é identificado na rede por um IP estático IPv4 (IP *loopback* IPv4, IPLB) para gestão. Utiliza protocolos e tabelas de encaminhamento, que lhe permite descobrir qual deve ser o caminho que um determinado pacote IP deve seguir para chegar ao seu destino.

O MPLS utiliza três tipos *routers*: *(i) provider router* (P); *(ii) provider edge router peer* (PE); e *(iii) customer edge router* (CPE). O *provider routers* (P) é o *router* que permite construir a rede de transporte MPLS, e, normalmente, não dispõe de ligações com o *router* CPE. O *provider edge router* (PE) permite a divulgação dos prefixos de rede VPN-IPv4 entre *routers* PE *peers*,

recorrendo ao MP-BGP. O *router* CPE é a designação utilizada no MPLS, é "CE" na arquitetura IP, e oferece conetividade à rede do cliente no acesso ao *router* PE.

Os *routers*, utilizados no MPLS, também têm outra designação conforme a sua função: *label switching router* (LSR) e *label edge router* (LER). O *label switching router* (LSR) é um *router* de rede de transporte *(backbone)* que participa na construção de uma malha completa de circuitos virtuais emulados (*label switched path*, LSP). Estes *routers* recebem um pacote rotulado (pacotes MPLS), e baseiam-se na tabela LFIB para reencaminhar esses pacotes. A partir de um rótulo de entrada (rótulo local), é deduzido qual é o porto (*outgoing interface*) e o rótulo de saída (*outgoing tag*) para encaminhar os pacotes MPLS. O *label edge router* (LER), ou *router edge LSR*, é o *router* instalado na extremidade do domínio MPLS. Existem duas designações diferentes para o *router* LER, em função do seu papel no *backbone*: *(i)* no acesso ao domínio MPLS, designado por *router* LSR *ingress node*; e *(ii)* na saída do domínio MPLS, designado por LER *egress mode*. O *router* LER *ingress node* analisa o primeiro pacote IP do fluxo, calcula e adiciona o rótulo MPLS. O *router* LER *egress mode* é responsável por retirar o rótulo MPLS. Qualquer *router* LER pode ser *ingress* ou *egress*, pois esta designação refere-se à função que desempenha relativamente ao reencaminhamento do tráfego. Estes *routers* permitem fazer a transição entre outras redes e para o efeito dispõem de *interfaces* tradicionais (*legacy*).

Topologia *Hub and spoke*

A topologia em estrela *(hub and spoke)* é utilizada para ligações ponto-a-ponto. O objetivo é concentrar todo o acesso dos sites remotos (*spokes*) num único ponto (*hub*). Assim, ao nível do encaminhamento, o *hub* conhece todos os prefixos de rede e os *spokes* conhecem apenas os seus prefixos de rede.

Elemento de rede *route reflector*

O elemento de rede *route reflector* garante a construção de rede em malha completa lógica. O tráfego útil, para poder ser trocado na rede, necessita que haja o anúncio dos prefixos de rede VPNv4 entre os *routers* associados a VPN-L3. Esse anúncio só é possível se existir sessões entre todos os elementos do sistema autónomo (condição obrigatória para ser utilizado o protocolo de encaminhamento BGP). Ao criar-se todas as secções necessárias obtém-se uma rede de malha completa. Como é extremamente complexo criar uma topologia malha completa, é reconhecido nos *guide line* do fabricante como boa prática instalar na rede de telecomunicações dispositivos designados por *route reflector* para anunciar os prefixos de rede VPN-IPv4. No anuncio desses prefixos de rede é utilizado o protocolo de encaminhamento MP-BGP e uma rede do tipo de topologia *hub and spoke*. Assim, os dispositivos de rede apenas tem sessões com o *route reflector* para distribuir as informações relativas aos prefixos de rede.

3.4 Planos lógicos da arquitetura IP MPLS

A Figura 3.3 ilustra os três planos lógicos e os protocolos presentes no MPLS: *(i)* plano de controlo; *(ii)* plano de dados; e *(iii)* plano de gestão. O plano de gestão está fora do âmbito deste documento, logo não será abordado. A Figura 3.4 ilustra os dois planos lógicos. As mensagens de informação trocados entre os *routers* (LSR) adjacentes e de rótulos ocorre no plano de controlo.

Os pacotes de dados das aplicações ocorrem no plano de dados. O plano de dados contém o mecanismo de transmissão dos dados e é completamente independente da parte de sinalização. Possibilita, com base nas tabelas de comutação por rótulos (LFIB), encaminhar os pacotes rotulados no domínio MPLS *[3.4-1]*.

Figura 3.3 – Arquitetura lógica da arquitetura MPLS.

O plano de controlo é responsável pela gestão e manutenção dos rótulos e utiliza um dos protocolos de encaminhamento interior padrão para conhecer a topologia da rede em que o *router* está instalado. O protocolo de sinalização *resource reservation protocol* (RSVP), especialmente desenvolvidos para o MPLS, solicita reserva de recursos para garantir o transporte do tráfego.

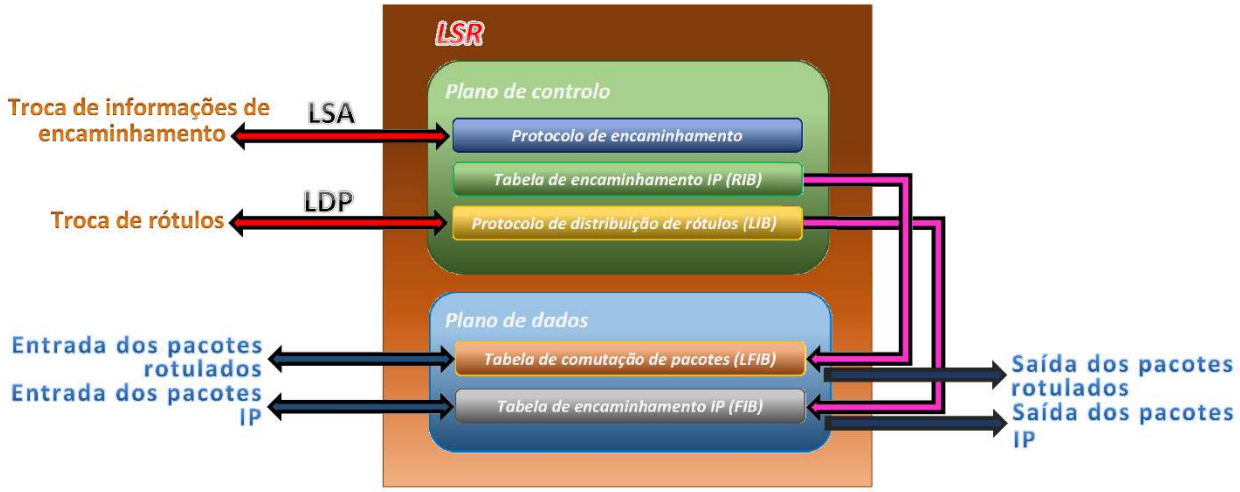

Figura 3.4 – Planos lógicos da arquitetura MPLS.

A Figura 3.5 ilustra o que acontece ao primeiro pacote IP, do fluxo enviado pela aplicação, ao chegar ao *router* LSR, *router* que garante o acesso ao domínio MPLS. O primeiro pacote IP é desmultiplexado para permitir a leitura do IP de destino do pacote IP contido no cabeçalho. Na descoberta do caminho que permita a entrega do pacote IP ao seu destino final, o protocolo IGP vai trocando de pacotes com objetos descritores (LSA) com os *routers* vizinhos. Um requisito para poder iniciar a transmissão é que, depois da descoberta do caminho, o protocolo de sinalização RSVP solicita aos *routers* que participam no encaminhamento do fluxo. Com a garantia da construção da rota que garante a entrega do fluxo, uma malha completa de circuitos emulados (*label switched path*, LSP), é calculado, em todos os *routers* que participam no encaminhamento,

o respectivo rótulo. O *label distribution protocol* (LDP) troca tabelas LIB entre os *routers* que participam, para poderem atualizar as suas tabelas LFIB.

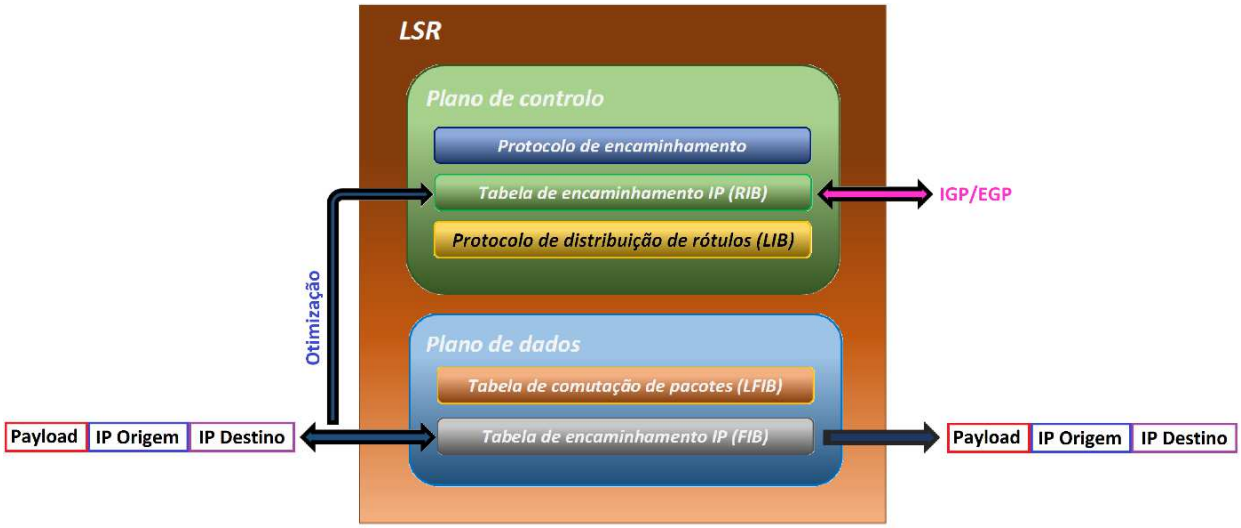

Figura 3.5 – Protocolo de encaminhamento para a descoberta do caminho para o destino.

A tabela FIB é criada a partir da otimização dos caminhos existentes na tabela encaminhamento (no processamento da tabela LFIB e RIB).

A Figura 3.6 ilustra o protocolo de sinalização RSVP/LDP do MPLS. Após a descoberta do caminho, o protocolo de sinalização RSVP solicita requisitos com todos os *routers* que participam no encaminhamento do fluxo. Ao garantir a construção de uma malha completa de circuitos emulados (*label switched path*, LSP), é calculado, em todos os *routers* que participam na construção de uma malha completa de circuitos emulados, o respectivo rótulo. No cálculo do rótulo, é utilizado no encaminhamento por classes equivalentes (*forwarding equivalence classe*, FEC). O *label distribution protocol* (LDP) troca tabelas LIB, com informação dos rótulos calculados individualmente por cada *router* para o mesmo fluxo, entre os *routers* que participam.

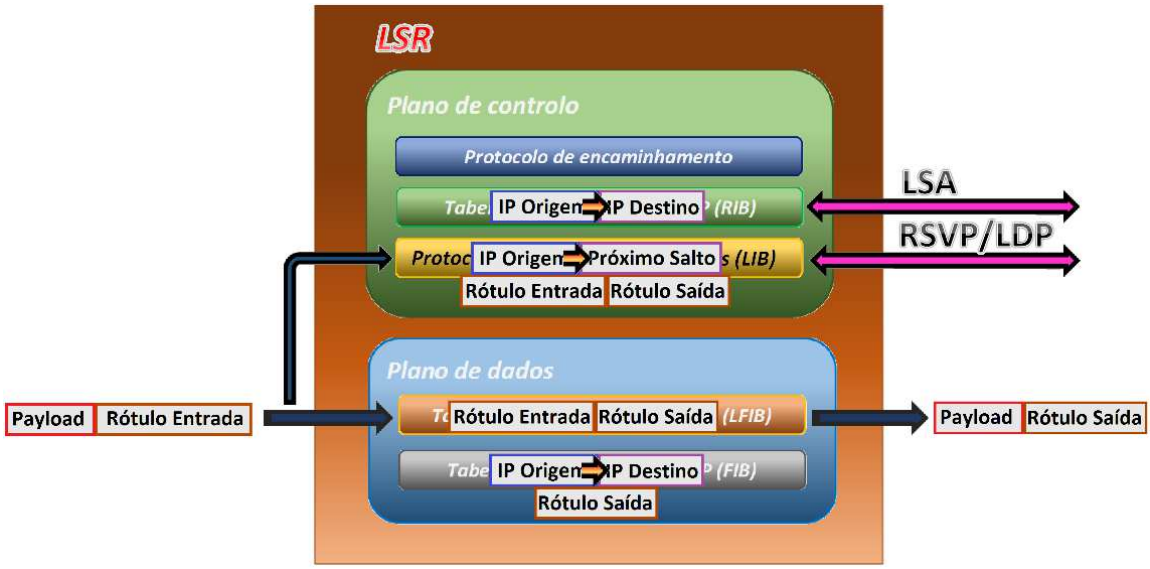

Figura 3.6 – Protocolo de distribuição de rótulos.

3.5 Hierarquia

A tendência emergente às comunicações nas subestações modernas passa por uma aposta numa infraestrutura de comunicação baseada em *ethernet*/IP. É cada vez mais comum encontrar-se um ambiente *ethernet* nas subestações, pois a construção de redes *ethernet* é cada vez menos dispendiosa. A hierarquia é um conceito muito geral, mas no contexto das redes de telecomunicações, caracteriza o sentido dos fluxos de tráfego numa rede. Isso implica que os fluxos crescem exponencialmente ao passar por pontos de agregação (nós) e tendem a seguir uma direção ou padrão específico (normalmente seguem em direção aos *datacenters*). Esta é uma consequência direta do tipo de aplicativo cliente-servidor. Isso implica um crescimento exponencial do fluxo em cada passagem por pontos de agregação (nós), e tendem a seguir uma direção ou padrão específico (normalmente seguem em direção aos *datacenters*). Esta é uma consequência direta do tipo de aplicativo cliente-servidor. As redes devem de ser implementa em três camadas hierárquicas: *(i) core*; *(ii)* agregação; e *(iii)* acesso. Este conceito, de organização por níveis de hierarquias, permite distribuir os elementos de rede considerando as funções que estes desempenham na rede de forma ideal. Assim, os elementos de rede dentro do mesmo nível hierárquico têm propriedades semelhantes e comportam-se de modo previsível. Com a ajuda desta classificação é possível definir a largura de banda necessária em cada ligação, ou, a capacidade do *backplane* necessário do dispositivo de rede. O *backplane* é o circuito impresso onde é ligado os componentes, como o barramento comum, as *interfaces* de expansão *(slots)*. A hierarquia é a base para muitos outros recursos da rede, pois possibilita a modularidade, a escalabilidade, a previsibilidade e a tolerância a falhas.

Modularidade

A modularidade significa que a rede é constituída por blocos funcionais de construção distintos, cada um com um conjunto preciso de características e comportamentos. A sua principal vantagem é a de permitir fazer alterações na rede. Os blocos podem ser adicionados e/ou removidos sem se precisar de um projeto novo para a nova topologia da rede. O endereçamento também é muito fácil. A modularidade também significa isolamento, pois os blocos são separados e interagem através de caminhos específicos, facilitando o controlo e a segurança. Os blocos são independentes uns dos outros, logo as alterações num determinado bloco não afetam os outros blocos.

Escalabilidade

A escalabilidade permite que uma rede cresça consideravelmente sem fazer mudanças drásticas ou precisar de um projeto novo para a nova topologia da rede.

Previsibilidade

No planeamento da nova rede foi considerado um fator de previsibilidade que lhe está associado. A compreensão do comportamento dos diferentes tráfegos, que são transportados pela rede, ajuda os administradores de sistemas a operarem na rede. Assim, a rede está construída para que os fluxos de tráfego sejam facilmente identificáveis, os seus atrasos sejam previsíveis (dentro de limites aceitáveis) e os caminhos de recurso em caso de falha sejam facilmente identificáveis.

Tolerância a falhas

Este aspeto é intrínseco à própria definição do termo "rede", que geralmente implica um certo grau de organização. Uma rede inteligente depende desta propriedade para fornecer rotas redundantes de um nó para o outro, o que implica a capacidade resistir a falhas. Ao se utilizar uma hierarquia, não é necessário fornecer redundância entre cada dois pontos, pois a rede não precisa ser uma malha completa, em vez disso, é possível identificar nós críticos onde é importante implementar redundância.

3.6 Comutação e MPLS

O princípio básico do ATM consiste na comutação de pequenos pacotes de dados (53 octetos, 5 para o cabeçalho e 48 para dados de informação) chamados de células. Em geral, quando uma célula chega à um comutador ATM, o cabeçalho da célula será utilizado como o ponto de entrada (índice) na tabela de comutação para saber automaticamente qual é o porto de saída. O ATM também oferece suporte à qualidade do serviço, permitindo priorizar fluxos de acordo com seu tipo (voz, dados, etc.).

O MPLS permite uma melhor eficiência na utilização dos recursos, quando comparado com a arquitetura IP, no encaminhamento dos pacotes IP, pois combina os conceitos de encaminhamento da camada 3 e a comutação da camada 2, daí a designação por vezes utilizada de “IP MPLS”. O seu princípio básico consiste em aproveitar o encaminhamento por IP mas usando o mecanismo de comutação utilizado no ATM, o que proporciona o melhor dos dois mundos: a flexibilidade e robustez da arquitetura IP e a qualidade de serviço da arquitetura ATM.

O princípio básico do MPLS consiste na: *(i)* seleção de caminho; *(ii)* sinalização; *(iii)* distribuição dos rótulos; e *(iv)* comutação de pacotes. Assim, após descoberta do caminho, e antes de iniciar a transmissão de dados, é necessário primeiro reservar recursos. Na seleção de caminho é calculado o caminho que os pacotes IP devem seguir na rede, desde da sua entrada (*ingress node*) no domínio MPLS até à sua saída (*egress node*). Daí a necessidade de se utilizar os protocolos de encaminhamento tradicionais, mas adaptados (com extensões). Depois da descoberta do caminho, é necessário reservar recursos recorrendo ao protocolo de sinalização *resource reservation protocol* (RSVP). Após este passo, cada *router*, calcula independentemente uns dos outros o respetivo rótulo, baseado no FEC. Como esse rótulo tem um significado local, essa informação é transmitida aos *routers* vizinhos recorrendo à tabela LIB pelo protocolo LDP.

Label switched path

Os *routers* envolvidos no transporte do fluxo necessitam de construir um (circuito) *label switched path* (LSP), que garanta a entrega do fluxo no seu respetivo destino.

Conforme ilustrado na Figura 3.7, o *router* “LER-1”, ao receber o pacote IP, com o endereço de IP de destino 192.168.1.0. Quando o primeiro pacote IP chega ao *router* “LER-1”, é iniciado o cálculo na procura dos caminhos que garantem a entrega do fluxo a que pertence o pacote IP. Após essa descoberta, o *router* “LER-1” envia uma mensagem RSVP a todos os *routers* que participam no encaminhamento a solicitar recursos que garantem o encaminhamento por classes

equivalentes (*forward equivalence class*, FEC) do fluxo. Com a garantia de cativação de recursos necessários ao FEC dada por esses *routers*, é construído um circuito virtual unidirecional. Inicialmente, esta metodologia é semelhante ao encaminhamento IP tradicional, e o controlo é dito distribuído ou descentralizado, pois cada *router* decide independentemente da decisão do *router* vizinho que participa na construção do LSP. Este caminho virtual unidirecional é constituído por diversos pequenos traçados *label switched path* (LSP). Esses LSP transportam pacotes de mensagens contendo informações dos rótulos locais (LIB) que cada *router* calcula para o mesmo fluxo. Só depois de terminar as trocas de mensagens LDP é que os fluxos de dados úteis podem ser transportados, garantindo assim uma eficiência superior à comutação, quando comparado com o encaminhamento IP tradicional. O pacote IP recebe o rótulo e será encaminhado até ao *router* "LER-2" utilizando um traçado previamente calculado.

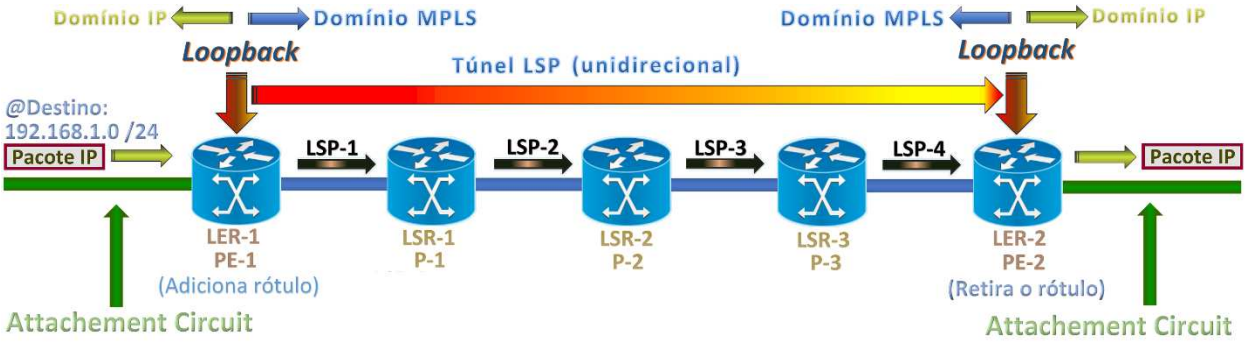

Figura 3.7 – Túnel LSP (unidirecional).

- *Label Switched Path* com encaminhamento explícito

Pode haver necessidade de forçar que um determinado fluxo que entre num determinado *router* LER lhe veja ser negada a possibilidade de ter um caminho obtido pelo algoritmo de encaminhamento dinâmico tradicional e siga por um caminho específico.

O MPLS propõe duas soluções para a implementação de um caminho, também designada por "túnel LSP". O fluxo é transparente aos nós (*router* LSR) que participam no traçado e o encaminhamento pode ser totalmente automatizado, ou parcialmente explícito. O encaminhamento explícito é definido pelo administrador de rede, ao ativar o mecanismo *explicitly routed label switched path* (ER-LSP). O ER-LSP é uma extensão do LSP e é implementado pelo protocolo de sinalização LDP-TE, um recurso do mecanismo de engenharia de tráfego. O ER-LSP consiste em especificar uma lista de nós que serão responsáveis pelo transporte de um determinado fluxo de tráfego, por forma a garantir a qualidade de serviço desejada e considerando as restrições associadas à rota. Os protocolos de encaminhamento explícitos são adaptações de outros protocolos. O *constraint routing - label distribution protocol* (CR-LDP) é uma extensão do LDP, e o protocolo de sinalização RSVP-TE é uma extensão do RSVP.

Geração de rótulo

A criação do rótulo está relacionada com uma política que permite diferenciar o encaminhamento por classes equivalentes *(forwarding equivalence classe*, FEC). A decisão de encaminhamento está dependente do ponto de entrada no *backbone* MPLS, designado por *router label edge router ingress* (LER_i). Tanto o *router* LER_i, como todos os outros *routers* que

participam na construção do caminho, calculam os respetivos rótulos, e de forma distribuída (independente uns dos outros). Para a realização do cálculo, que tem por objetivo determinar o rótulo a adicionar ao pacote IP, é utilizado o encaminhamento por classes equivalentes. O principal parâmetro avaliado no pacote IP é o conteúdo do campo "IP de destino" do cabeçalho, podendo, além disso, ser os campos "IP de origem" ou "IP *Precedence*". Esse rótulo calculado é sempre adicionado ao pacote antes de comutar para o porto de saída. O encaminhamento do pacote MPLS termina quando este chega ao *router* LER *egress*. O *router* LER *egress* retira o último rótulo ao pacote MPLS, comutando-o para o porto de saída como um pacote IP. Este rótulo possibilita que todos os pacotes MPLS, do mesmo fluxo, sigam a mesma regra de encaminhamento. É este procedimento que permite a técnica de comutação por rótulos.

O formato do cabeçalho MPLS (*shim header*) tem um comprimento de 32 bits, conforme ilustrado na Figura 3.8.

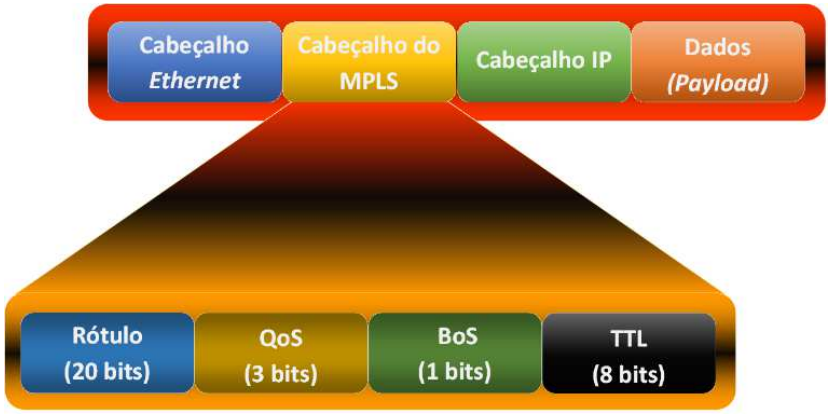

Figura 3.8 – Cabeçalho MPLS (*shim header*).

Desses 32 bits, 20 são para o rótulo calculado e com um significado local de um encaminhamento por classes equivalentes. O *shim header* é colocado entre o cabeçalho da camada 2 e 3 do modelo OSI, conforme ilustrado na Figura 3.8, o campo de 3 bits define a qualidade de serviço. É possível sobrepor vários rótulos consecutivos no pacote MPLS, permitindo combinar várias associações de serviço, como para o caso de ser um pacote MPLS VPN ou encaminhamento explícito. É, por isso, necessário um campo "S" (ou *bottom-of-stack*, BoS), de 1 bit, para indicar que se chegou ao último rótulo. O último campo é o campo "*Time to Live*" (TTL) de 8 bit e tem o mesmo propósito no pacote IP.

Comutação por encaminhamento

Na arquitetura IP o processamento é mais complexo e os algoritmos utilizados pelos IGP descobrem unicamente o caminho de menor custo (*shortest path routes*), no sentido lato, sem atender ao estado de congestionamento de cada troço da rede. Esse encaminhamento é mais complexo, pois o processo de desmultiplexagem do cabeçalho para chegar ao campo onde está o endereço IP de destino, do pacote IP, é mais elaborado e o caminho de menor custo não possibilita explorar a existência de percursos alternativos. A arquitetura IP também não dispõe de mecanismos de engenharia de tráfego, não permitindo assim providenciar rotas que suportem os requisitos específicos das aplicações ou dos serviços sujeitos a exigentes restrições da qualidade de serviço.

Comutação por rótulo

Esta metodologia, de comutação por rótulo, permite o encaminhamento dos fluxos de tráfego sem necessidade de consultar o respetivo endereço IP de destino, resultando numa entrega do pacote IP com baixa latência.

Utilizando a Figura 3.9 como exemplo, quando o *router* LER *ingress* ("LER-1") recebe o primeiro pacote IP do fluxo, o rótulo é calculado, com base no encaminhamento por classes equivalentes. Neste exemplo, o IP de destino 192.168.1.0 foi o único critério para a realização do cálculo. Para o encaminhamento até ao *router* LER *egress* ("LER-2") foi calculado o rótulo "5". O *router* "LSR-1" recebe o pacote MPLS, a partir do seu porto "0", e é lido "5" no campo "rótulo" do *shim header*. Com este dado é realizada uma consulta à tabela dos rótulos (LFIB) para reconhecer o pacote MPLS. Depois de o reconhecer, o *router* "LSR-1" consulta a tabela LFIB para saber que novo rótulo ("8") deverá ser colocado no *shim header*, com o anterior, que era "5", e o pacote MPLS deve ser comutado para o porto de saída "1". Este processo, de verificação, cálculo do rótulo e a sua troca, é repetido em todos os *routers* associados ao *label switched path* (LSP), até que o pacote MPLS chegue ao *router* "LER-2". Os *routers* LSR só trocam rótulos e encaminham os pacotes MPLS utilizando a informação do rótulo. O *router* "LER-2" retira o (último) rótulo e converte o pacote MPLS num pacote IP, e comuta-o para o respetivo porto *[3.6-1]*.

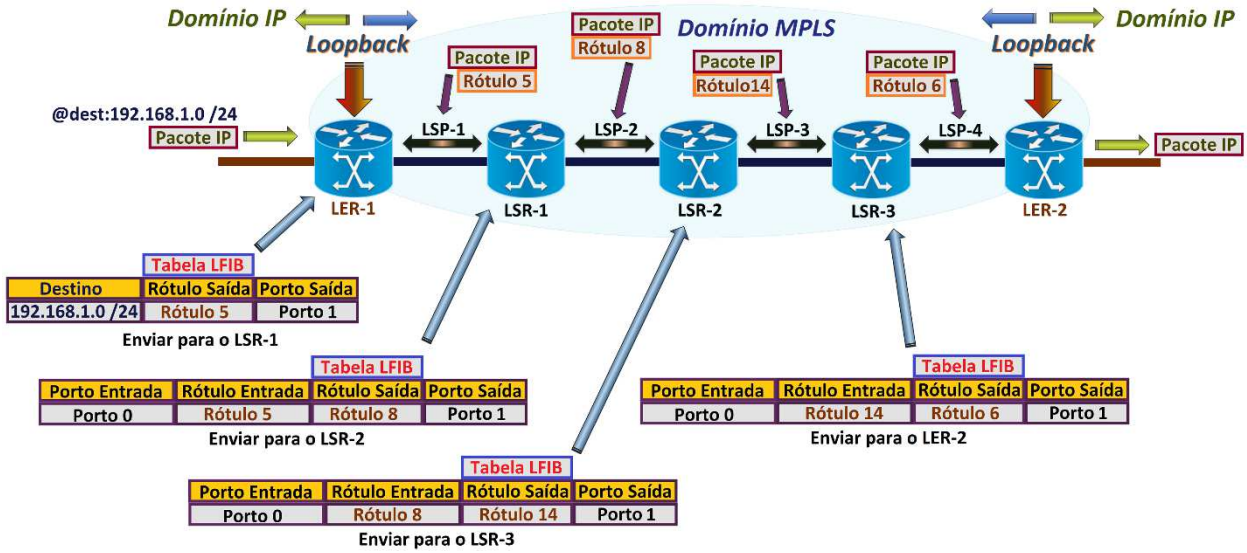

Figura 3.9 – Comutação do pacote MPLS e as trocas de rótulos nos *routers* LSR.

3.7 Endereço de IP

Cada *router* constituinte da rede, para poder ser identificado na rede pelo protocolo de encaminhamento interior padrão *(interior gateway protocol, IGP)*, dispõe de um identificador designado por *router ID*. Cada um dos *routers* deve ser configurado com uma *interface* virtual à que se lhe atribui um endereço de IP *loopback* IPv4 /32 (IPLB). Este IP virtual estático é um identificador atribuído ao "*router ID*" do *router* e a máscara /32 é uma das suas caraterísticas, pois só existe um único elemento dessa rede. O identificador IPLB permite ao administrador da rede aceder, por qualquer porto ativo ligado à rede, ao *router* enquanto este estiver operacional.

Se o serviço estiver associado ao porto físico, e se este falhar, falha o acesso ao dispositivo, logo falha a gestão. Um identificador IPLB permite, assim, dar mais alguma margem de operação ao administrador da rede. Não é necessário atribuir IP a todos os portos, pois ao se atribuir o IPLB ao dispositivo, é possível monitorizar todos os portos associados. Esta solução resolve dúvidas que possam surgir ao administrador de rede, pois é possível alcançar o IPLB por diversos traçados, conforme ilustra a Figura 3.10.

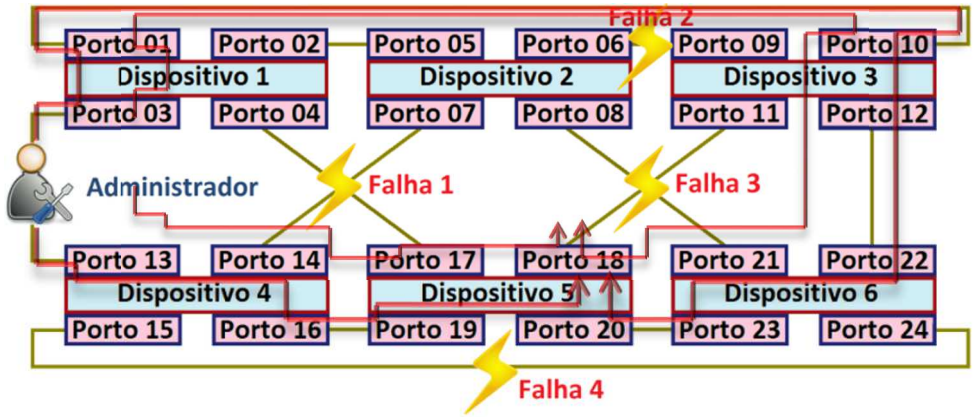

Figura 3.10 – Acesso aos portos numa rede com falhas.

Assim, se o porto 18 tiver uma anomalia, recorrendo ao IP virtual do "*Dispositivo 5*", o administrador de rede consegue obter alguma informação acerca do porto 18. Se na tabela de encaminhamento, para alcançar o porto 18, estiver a rota a partir do porto 4 do "*Dispositivo 1*", ou 7 do "*Dispositivo 2*", não seria possível ao administrador de rede obter informações do porto 18. Como o acesso ao IPLB do "*Dispositivo 5*" pode ser realizado pelos portos ainda ativos, recorrendo ao traçado assinalado a vermelho, a tarefa fica simplificada para o administrador.

O "*router ID*" é utilizado pelo protocolo de encaminhamento interior padrão para a troca, entre *routers*, de pacotes com informações conhecidas como pacotes de objetos descritores. É com base na recolha e processamento dessas informações que o *router* constrói a tabela com a topologia da rede (*link-state database*, LSDB). É possível existirem *subinterfaces* do identificador IPLB para diferentes fins, até à um número máximo de 65535.

3.8 Mecanismo *carrier-delay timer*

O mecanismo *carrier-delay timer* permite evitar re-convergência da rede caso não haja necessidade. O protocolo de encaminhamento BGP não necessita deste mecanismo, pois os elementos de rede estão todos ligados numa topologia de malha completa, utilizando sessões TCP, não necessitando de realizar o cálculo da re-convergência. Se uma ligação falhar e voltar a reestabelecer-se antes que o temporizador de atraso expire, o tempo de espera definido pelo administrador de rede para o envio de pacotes de objetos descritores, informando que o elemento de rede está no estado "*down*", não é tido em conta pelo algoritmo de vigilância (do IGP) responsável. Na realidade o evento nem sequer é detetado pelo dispositivo. Além disso, se for utilizado um valor de temporizador de atraso com um intervalo de tempo maior, para o envio de pacotes de objetos descritores, resulta num envio reduzido de eventos acerca do estado da

ligação, o que corresponde a um benefício em relação à estabilidade da rede. Assim, é necessário ponderar esse aumento, pois um temporizador de atraso com um intervalo de tempo grande pode prejudicar ao se ter um maior tempo de *blackholing*, e não se pretende que isso aconteça. O termo inglês "*backholing*" é utilizado quando ocorre uma indefinição do estado do porto e que pode resultar no descarte do pacote.

Quando não se configuram os temporizadores de atraso, os protocolos da camada superior (à física) são imediatamente notificados quando há falhas na ligação física, não sendo necessária nenhuma configuração adicional. Além disso, para evitar dúvidas quanto às configurações padrão, é considerada uma boa pratica definir tempo instantâneo nos dispositivos de *core*, nos de agregação e nos de acesso, e apenas nas *interfaces* 1 e 10 Gbps.

O atraso da portadora é configurável pelo gestor de rede. É o hiato de tempo criado entre a descoberta de uma transição do estado da ligação e a atualização do estado da *interface*. Ou seja, é o intervalo de tempo entre cada envio de pacotes de objetos descritores. O Exemplo de código 1 é reconhecido nos *guide line* do fabricante como boa prática para definir os tempos aceites na flutuação do porto.

```
interface TenGigabitEthernet <x/x/x>
 carrier-delay up msec 0
 carrier-delay down msec 0
```

Exemplo de código 1 – Configuração do atraso de portadora de *interface* de ligação desprotegida.

Note-se que se temporizador "*carrier-delay up msec 0*" for superior a zero, haverá eventos que não seriam detectados. E como é uma ligação de *core*, não se pretende que haja flutuação no porto ótico.

3.9 Auto negociação

O porto *gigabit ethernet* possui um procedimento de negociação automática (IEEE 802.3z), da camada 2, que é mais demorado, em comparação com *fast ethernet* de 10/100 Mbps, e é utilizado para trocar parâmetros de controlo de fluxo, informações de falhas e informações se o porto for *duplex*.

Deteção de falhas baseada em pacotes LSA "*Hello*"

O ajuste do intervalo da mensagem *"hello"* para detetar falhas não é utilizado, por demorar muito tempo. Para uma convergência rápida, o mecanismo *bidirectional forwarding detection* (BFD) oferece uma abordagem mais elegante, mais rápida e escalável.

Bidirectional Forwarding Detection

O mecanismo de deteção de falhas BFD permite fornecer um melhor tempo ao mecanismo IP FRR na deteção de falhas. Este método de deteção de falhas na ligação é utilizado como gatilho para permitir ao IP FRR agir de forma célere, garantindo bons tempos na convergência.

Ao se implementar este recurso, é importante considerar todas as alternativas e estar ciente que é necessário considerar os possíveis *trade-offs* (o termo inglês "*trade-off"* é utilizado para definir uma situação em que há conflito de escolha, e pretende-se resolver um problema, mas acarreta outro, obrigando uma escolha). A alternativa mais próxima ao BFD é o uso de mecanismos de deteção de falhas modificados, desenvolvidos pelos diferentes fabricantes. Existem várias vantagens na implementação do mecanismo BFD para reduzir o tempo na deteção de falhas na ligação (mensagens "*hello*"). Apesar dos temporizadores de deteção de falhas na ligação, do protocolo *open shortest path first* (OSPF), possam resultar num mínimo de um a dois segundos, há melhorias de tempo de recuperação com a utilização do mecanismo BFD, como: *(i)* permite reduzir o tempo de falha a menos de um segundo; *(ii)* não está associado a nenhum protocolo de encaminhamento específico, pode ser utilizado como um mecanismo genérico e consiste na deteção de falhas em qualquer IGP; *(iii)* é executado pelo plano de dados, o que permite reduzir o esforço de processamento comparando com os tempos reduzidos do OSPF, associados ao plano de controlo.

3.10 Convergência rápida

As falhas de ligação, ou do nó, numa rede de transporte de alto débito, e que liga os nós de rede de uma operadora de telecomunicações à grande distância *(*designado por *backbone),* causam perdas de pacotes até ao instante em que a rede se adapte à nova topologia de rede, recorrendo à convergência. Estas perdas de pacotes impactam diretamente na disponibilidade afetando o acordo de nível de serviço (*service-level agreement*, SLA). Para avaliar o seu significado, é possível calcular a quantidade de tempo de inatividade correspondente a diferentes compromissos de disponibilidade da rede avaliada em 99,999% (também designado por "cinco nove"), o que equivale a um tempo de inatividade inferior a menos de 1 segundo por dia. Outra forma de ilustrar o significado deste tempo de inatividade é considerar o impacto nos aplicativos e utilizadores finais. Nas chamadas de telefonia sobre rede IP (*Voice over Internet Protocol*, VoIP), os utilizadores finais percebem falhas na chamada na presença de perdas de alguns pacotes IP. Por exemplo, com uma amostra a cada 20 milissegundos, uma perda de ligação num intervalo de 100 a 150 milissegundos é percetível ao ouvido humano. Além disso, se a perda de conetividade for entre 1 a 2 segundos, a chamada pode ser descartada. Consequentemente, as redes que suportam serviços VoIP de alta qualidade são projetadas para realizar a convergência de rede, após falha na ligação ou nó, em menos de 1 segundo.

O tempo necessário para uma rede IP re-convergir depende do tamanho da rede, do protocolo IGP utilizado e da sua configuração específica. Para cumprir os objetivos de alta disponibilidade do nível de serviço (*service-level agreement*, SLA), é importante que o protocolo de encaminhamento seja ajustado para permitir uma convergência rápida. Um componente-chave da convergência do protocolo IGP é o ajuste dos temporizadores, que determinam a frequência com que os eventos principais do protocolo de encaminhamento podem ocorrer. Historicamente, isso resultou num *trade-off* entre convergências rápidas e a estabilidade do

protocolo de encaminhamento em que: *(i)* os temporizadores curtos resultaram em convergência rápida, mas com um maior potencial para gerar instabilidade; e *(ii)* os temporizadores mais longos resultaram numa maior estabilidade, mas uma convergência mais lenta. No ponto (i), considera-se gerar instabilidade ao facto de poder existir flutuação num porto e o re-estabelecimento é mais rápido que a re-convergência. O resultado pragmático desse *trade-off* foi que os temporizadores do protocolo IGP são geralmente configurados de forma conservadora e a convergência de rede IP é tipicamente de algumas dezenas de segundos. Em momentos de instabilidade da rede (por exemplo, causada devido a um porto com um estado de atividade flutuante – *up/down*), os temporizadores IGP aumentarão para acelerar a taxa de resposta aos eventos da rede. Este esquema garante uma convergência rápida quando a rede é estável e uma sobrecarga do protocolo de encaminhamento moderada (por exemplo, utilização de ciclos de CPU) quando a rede está instável.

A otimização, na configuração rápida, produz uma redução dos tempos de convergência de IGP dos (habituais) 10 segundos, para tempos com valores inferiores ao segundo. Os parâmetros de configuração da convergência rápida *(fast convergence*, FC) no OSPF implementados na rede "WAN SCADA" são considerados como sendo as melhores práticas, pois já foram implementados em várias grandes redes de provedores de serviço, e os parâmetros ideais foram obtidos a partir de muitos testes. A convergência rápida envolve os seguintes eventos principais: *(i)* deteção de falhas; e *(ii)* desvio exponencial.

Deteção de falhas

A deteção de falhas de ligação deve fornecer duas propriedades: velocidade e confiabilidade. Enquanto uma falha deve ser detetada o mais rápido possível, o sistema também deve evitar que um porto com um estado de atividade flutuante (*up/down* rápidas) cause um *churn* de encaminhamento.

3.11 Conceito VPN

O princípio de funcionamento de uma rede privada virtual (*virtual private network*, VPN), é o de oferecer uma infraestrutura partilhada e com os mesmos benefícios que uma infraestrutura privada. São circuitos bidirecionais ("túneis"), que garantem a segregação de fluxo entre diferentes clientes, pois foram desenvolvidos mecanismos a que essa comunicação só seja possível entre clientes VPN.

As VPN MPLS simplificam muito a implementação do serviço em comparação com as VPN IP tradicionais. Quando o número de rotas e clientes aumentam, as VPN MPLS podem suportar facilmente a carga, proporcionando ao mesmo tempo um bom nível de confidencialidade. Estas também podem transportar os endereços IP não-exclusivos. Ou seja, pode-se utilizar qualquer IP privado de um cliente, e o prestador de serviço nem sequer precisa de saber qual é, pois não precisa de saber o IP para realizar o encaminhamento. O encaminhamento no MPLS é realizado pela comutação de rótulos. As VPN MPLS são mais fáceis de gerir e expandir do que as VPN convencionais. Quando um novo *site* é adicionado a uma VPN MPLS, apenas é necessário configurar o *router* PE que fornece serviços ao site. O mecanismo VRF é uma extremidade lógica de uma VPN configurado num *router* PE. A tabela de encaminhamento global é preenchida com

prefixos de rede com a utilização do protocolo OSPF, enquanto os prefixos de rede VPN-IPv4 dos VRF são preenchidos com a utilização do protocolo MP-BGP.

Rede virtual privada na camada 2

Uma rede de telecomunicações permite criar circuitos seguros, sobre uma rede insegura, para possibilitar comunicações entre duas (ou mais) entidades, recorrendo a VPN da camada 2 ou 3.

A arquitetura *Ethernet* permite a interligação de redes locais baseada no envio de pacotes IP. A VPN da camada 2 (VPN-L2) permite o transporte e amplia o domínio *ethernet*. Nos últimos anos, o padrão *ethernet* tem sofrido evoluções de forma muito significativa no que se refere ao débito gerado, com uma capacidade de crescimento expressivo de 2 Mbps a 10 Gbps. Cria uma ligação virtual transparente e dispõe de dois tipos: *(i) virtual private wire service* (VPWS); e *(ii) virtual private LAN service* (VPLS). A Figura 3.11 ilustra as VPN-L2.

Figura 3.11 – Vários tipo de VPN-L2 que podem ser construídas.

Na área 1, está representado o serviço *virtual private wire service* (VPWS), do tipo *tunnelling protocol L2 version 3* (L2TPv3). O serviço utiliza um circuito construído sobre um *backbone* IP e recorre ao modelo *overlay*. Ao se prestar um serviço bidirecional multiponto, tende a ficar muito complexa a criação de todos os circuitos virtuais bidirecionais necessários. Pode-se implementar o serviço IPSec.

Na área 2, está representado o serviço VPWS, do tipo *any transport over MPLS* (AToM). O serviço utiliza um circuito construído sobre um *backbone* MPLS. Só após a criação desse circuito é que

se pode utilizar o serviço *pseudowire emulation edge-to-edge* (PWE3) para criar o circuito virtual bidirecional entre dois *routers* CPE. Um circuito virtual suporta os PWE3 que se pretendam implementar, mas não suporta o serviço IPSec. É pouco escalável pois é necessário um *pseudowire* por cada circuito virtual (ponto a ponto). Para contornar esta desvantagem foi desenvolvido o VPLS.

Na área 3, está representado o *virtual private LAN service* (VPLS), o serviço utiliza um túnel circuito construído sobre um *backbone* MPLS, e utiliza o mecanismo PWE3 para criar o circuito virtual bidirecional. Permite que *sites* dispersos geograficamente compartilhem o mesmo domínio de transmissão *ethernet*. O acesso é realizado recorrendo ao serviço *pseudowire emulation* (PWES).

Na área 4, está representado o serviço *IP-only LAN service* (IPLS), a VPN da camada 2, que é uma solução semelhante ao serviço VPLS mas que entretanto foi abandonada. A intenção original era fornecer uma solução alternativa à VPLS.

- Serviço *Pseudowire emulation edge-to-edge*

No MPLS, utiliza-se o serviço *pseudowire emulation edge-to-edge* (PWE3), padronizada pelo RFC3985, e abreviado por *pseudowire* (PW), ilustrados na Figura 3.12. Este serviço é um circuito virtual bidirecional não IP, e proporciona o estabelecimento de uma (ou várias) VPN-L2. Como o tráfego é transparente ao serviço PW, não encaminha pacotes, mas sim comuta-os.

O serviço PW termina em instâncias VSI, configuradas nos PE *peers*, onde existe a função *ethernet bridge* e oferece, num domínio de partilha, dois tipos de serviços aos clientes, representados na Figura 3.11: *(i) virtual private wire service* (VPWS); e *(ii) virtual private LAN service* (VPLS). Na configuração das extremidades da PW utilizam-se os *IP loopback* dos *routers* PE *peer*, conforme ilustrado na Figura 3.12. É também por configuração que o PW é associado ao *attachment circuit* correspondente. Para permitir que dois *routers* do cliente ("CE-1" com o "CE-4" e o "CE-2" com o "CE-5") comuniquem entre si, é configurado duas VPN-L2 nos dois *routers* PE *peer* ("PE-1" e "PE-4") para poder ser utilizado dois serviços PW. No entanto, para que o tráfego possa alcançar os CE de destino é necessário configurar o *pseudowire emulation servisse* (PWES).

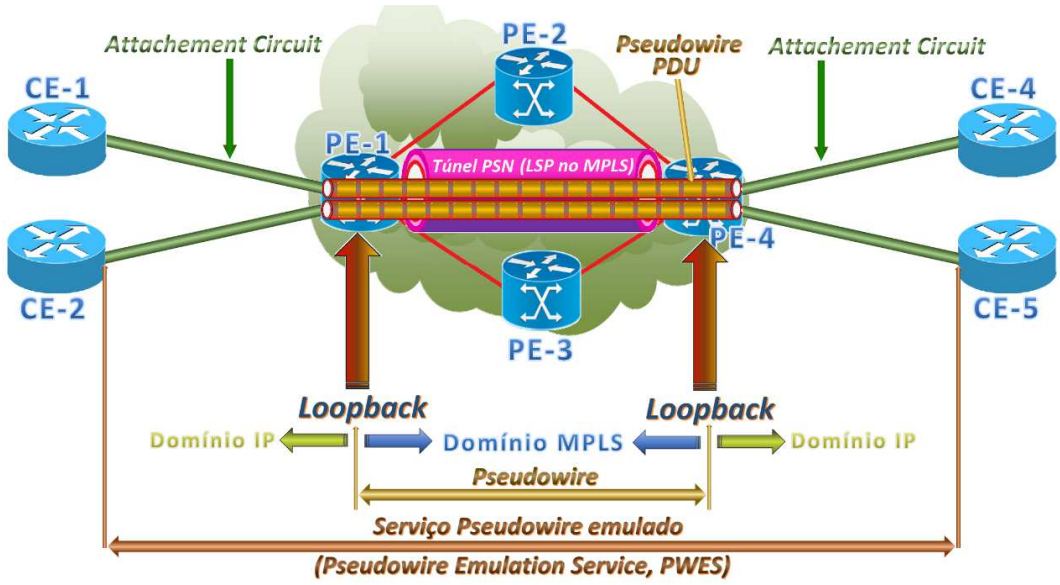

Figura 3.12 – Arquitetura de um serviço que provendencia uma ligação PWES.

- Serviço *Pseudowire emulation service*

O serviço *pseudowire emulation service* (PWES) consiste basicamente num circuito de comunicação transparente entre dois *routers* CE e permite perpetuar a tecnologia *legacy*, ao mesmo tempo que se otimizam os custos no transporte de dados.

Esta capacidade de estender o domínio da tecnologia de comutação por pacotes, é a principal vantagem do PW ao proporcionar a convergência de diversos serviços, conforme ilustrado na Figura 3.13. O PW viabiliza o transporte de vários serviços num único formato e sobre uma rede de comutação de pacotes (PSN). Cabe aos *routers* PE das duas extremidades do PW realizarem o encapsulamento e a descapsulação necessários da mensagem PW-PDU e gerarem todas as outras funções necessárias para garantir o serviço PW. Assim, os dados nativos (*legacy*) do cliente ao chegarem ao *router* PE, utilizando o *attachment circuit*, são encapsulados numa mensagem PW-PDU, para poderem ser transportados através do circuito do PSN. No sentido inverso ocorre o desencapsulamento.

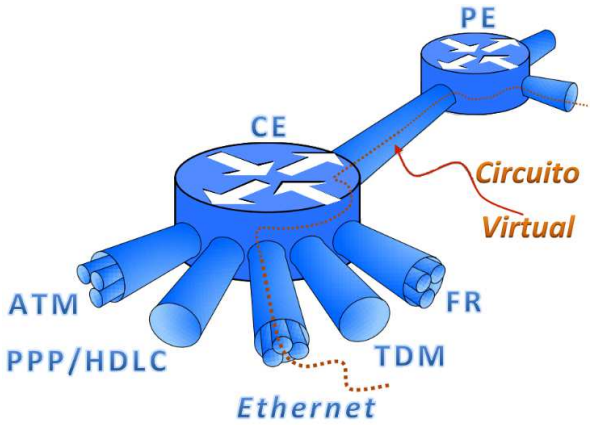

Figura 3.13 – Serviços *legacy* são transportados utilizando o serviço PWES.

Técnica *split horizon*

O conceito de virtualização de comutador de ponte *(bridge domain*, BD) baseia-se na comutação de tráfego *ethernet* não diferenciando os portos físicos e virtuais. Os portos físicos estão associados ao *attachment circuit* (AC) e os portos virtuais estão associados aos *pseudowires* (PW). O tráfego recebido nunca será reenviado para o AC, ou PW, que o recebeu. O *router* recebe tráfego de vários VRF num único porto, e utiliza a *interface bridge domain* (BDI) para separar o tráfego e comutá-lo ente o mesmo domínio de *broadcast*. O BDI só é utilizado na comutação para o lado do *router* CE, e nunca no domínio MPLS (circuitos virtuais).

O *split horizon* é uma técnica de resolução na presença *loops* no encaminhamento e acelera a convergência da rede. O princípio desta técnica consiste em não transmitir falsas informações de encaminhamento para o lugar de onde elas vêm. Ou seja, o *split horizon* bloqueia o anúncio de informações de encaminhamento para a *interface* de origem. Assim, e tendo como exemplo a Figura 3.14, os pacotes de *broadcast* trazidos pelo AC "1" serão replicados para todos os PW e do AC "2". Quando o tráfego chega num PW, por padrão, os pacotes de *broadcast* nunca são enviados para os outros PW que partilham o mesmo grupo *split horizon*. Os pacotes de *broadcast* só são enviados aos AC.

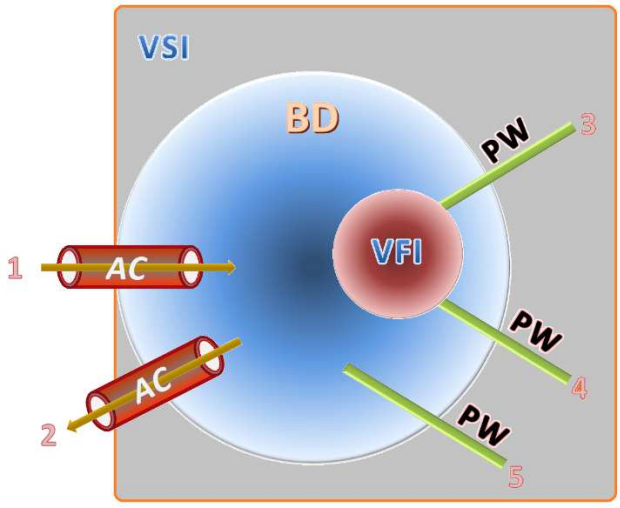

Figura 3.14 – O *Split Horizon* é uma técnica de resolução contra *loops*.

Virtual private wire service

O *virtual private wire service* (VPWS) proporciona o transporte na camada 2 do tráfego TDM, ATM, *frame relay* e *ethernet*. O método de transmissão TDM considera o *circuit emulation service over PSN* (CESoPSN) e o *structure agnostic TDM over packet* (SAToP).

Para implementar o VPWS é necessário configurar: *(i)* os portos do *router* CE utilizados na conexão ao domínio MPLS, e deve ser adicionado um rótulo VLAN, e retira-lo quando chega ao CE de destino; *(ii)* na entrada do domínio MPLS os portos dos *routers* PE ligados aos CE estabelecem a correspondência entre as EFP (VLAN) e os PW; e *(iii)* na saída do domínio MPLS, o *router* PE estabelece a correspondência entre os PW e as respetivas VLAN *[3.11-1]*.

Nota-se que na configuração dos portos é uma exigência que os portos físicos de acesso sejam totalmente dedicados em ambos os *routers* CE.

- Protocolo CESoPSN e SAToP

O serviço de emulação de circuito sobre a rede com comutação de pacotes (*circuit emulation service over packet switched network*, CESoPSN) e a estrutura agnóstica TDM sobre pacotes (*structure-agnostic time division multiplexing over packet, SAToP*) define o serviço TDM ponto-a-ponto. Uma estrutura agnóstica significa que o transporte é realizado sem avaliar o *overhead* (OH). O CESoPSN é um serviço estruturado que permite o mapeamento dos dados úteis num intervalo de tempo específico (X.21), enquanto o SAToP oferece um serviço não estruturado (E1).

O *structure-agnostic TDM over packet* (SAToP) encapsula fluxos de bits utilizando a multiplexação por divisão de tempo e constrói uma *pseudowire* (PW) sobre uma rede pública de comutação. O protocolo ignora qualquer estrutura do SDH (*structure-agnostic*) que pode ser imposta pelo fluxo, em particular a estrutura imposta pelo enquadramento TDM padrão. Ou seja, constrói um novo pacote constituído pelo pacote SDH adicionando um cabeçalho SAToP, e cria uma *pseudowire*. O protocolo utilizado para a emulação desses serviços (SAToP) não depende do método com que os circuitos de ligação (*attachment circuits*, camada física) entregam os pacotes aos dispositivos de borda (*router* PE). Utilizando o protocolo SAToP, a *interface* que recebe os

pacotes considera que está a receber um fluxo de bits em contínuo. A formatação de dados como um pacote TDM adicionando um cabeçalho SAToP *[3.11-2]*.

O *circuit emulation service over packet-switched network* (CESoPSN) encapsula fluxos de bits de multiplexação por divisão de tempo para transportar pacotes de dados de 64kbps.

- Serviço *any transport over MPLS*

O serviço *any transport over MPLS* (AToM), foi originalmente desenvolvido para transportar pacotes *frame relay* e ATM no MPLS, pois providencia o equivalente a uma linha virtual alugada (*virtual leased line*, VLL), numa conetividade designada de "ligação ponto a ponto" num domínio partilhado.

Virtual private LAN service

Uma rede construída com um *backbone* IP suporta circuitos que permitem implementar um serviço *ethernet* MP2MP (multiponto a multiponto), mas gera uma série de problemas inerentes a este tipo de solução, nomeadamente o fato de suportar poucos clientes das áreas metropolitanas. Tal facto deve-se a que a maioria dos provedores de serviço de (*Metro*) *Ethernet* construiu as suas infraestruturas com base em comutadores *ethernet*, resultando em vários fatores limitativos: *(i)* o número máximo de ID VLAN (de transporte, *QinQ*) é de 4096. É necessário um ID VLAN por cliente e, como os ID VLAN têm um significado global dentro da rede do operador *ethernet*, devem de ser exclusivos; *(ii)* para a diferenciação dos pacotes, este oferece poucas ou nenhumas soluções de qualidade de serviço; e *(iii)* a utilização do serviço *spanning tree* (STP), para tratar a resiliência das ligações, não é ideal em termos de partilha da carga e tempo de convergência. Por esta razão, uma abordagem que passa por uma implementação de serviços *Ethernet* MP2MP em várias redes metropolitanas, sem mudança de tecnologia, não é hoje em dia realista *[3.11-3]*.

Assim, em 2011, surgiu um serviço designado por *virtual private LAN service* (VPLS), construído num *backbone* MPLS, que resolve estes inconvenientes da infraestrutura baseada em comutadores *ethernet*. O VPLS permite estender o domínio de comutação por pacotes entre diversos locais distanciados fisicamente, numa conetividade designada de "ligação *any-to-any*" ou MP2MP. Este serviço disponibiliza conetividade *ethernet*, utilizando o IP, assim como mecanismos de túneis para fornecer conetividade entre vários locais (MP2MP), podendo por isso ser utilizado em infraestruturas metropolitanas. A utilização do protocolo de encaminhamento MPLS, em substituição do serviço *Ethernet*, e o recurso aos rótulos MPLS, fornece uma infraestrutura de fácil implementação e extremamente flexível, permitindo disponibilizar serviço *metro ethernet* em grande escala. Como ilustra a Figura 3.15, os *routers* PE estendem o domínio *ethernet* entre o "CE-1.1" e "CE-2.1", se as redes forem iguais. Se as redes forem diferentes, é necessário utilizar *routers*, "CE-1.2" e "CE-2.2".

Só nas VPN-L2 é que os circuitos são identificados com um número, e o porto do *router* PE não tem endereço IP, pois é da camada 2. O tráfego do cliente é comutado com base no endereço MAC existente nos pacotes *ethernet*, e o VPLS pode transportar pacotes IPv4 e IPv6. Mas existe uma desvantagem: a tabela ARP de cada comutador de todos os *routers* associados à VPLS cresce exponencialmente, e num domínio LAN há muitos *broadcast*. Um *host* ao se ligar, procura a sua *gateway*, logo procura o seu endereço MAC por *broadcast* na LAN. Há também o perigo de vir a ocorrer problemas com os *loops*.

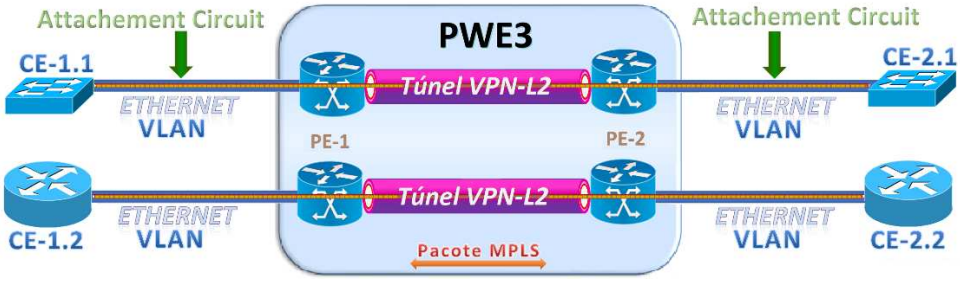

Figura 3.15 – Criação de dois serviços de domínio *ethernet* extendidos para dois clientes diferentes.

Instância de comutaçao virtual

O serviço de rede local privada (*virtual private LAN service,* VPLS) permite troca de tráfego *ethernet* entre vários sites servido por um *backbone* MPLS. Para os dispositivos CPE, o *backbone* MPLS não existe, o que existe é uma extensão do domínio de *broadcast* dessa ligação lógica. Para se poder configurar uma VPLS é necessário primeiro criar uma instância de comutação virtual (*virtual forwarding instance*, VFI), também designado *virtual switch instance* (VSI), em cada *router* PE associado ao serviço. O VFI é um agente que interage com o plano de controlo, semelhante ao VRF, mas para uma VPN da camada 2 (VPLS). Na camada 2 é possível agrupar várias VLAN numa única instância, o que permite simular uma rede local utilizando um *backbone* MPLS. A instância VFI contém os endereços (IPLB) dos outros *routers* PE *peer* que pertencem ao domínio de comutação *(bridge domain)* e o tipo de mecanismo de sinalização. O conjunto das instâncias VFI formado pela interconexão dos circuitos virtuais é chamado de instância VPLS, permitindo, assim, a existência de um domínio de comutação (camada 2) numa rede comutada por pacotes (camada 3). Os *routers* PE associados a uma instância VPLS usam a instância VFI para utilizar a malha completa de um circuito virtual emulado (*label switched path*, LSP) com todos os outros *routers* PE. A instância VPLS recebe um ID de VPN exclusivo dentro do *backbone [3.11-4]*.

O VFI é componente da VPLS configurado no *router* PE e está associado aos portos virado para o *router* CE, e não ao *router ID* (IPLB), conforme ilustrado a amarelo na Figura 3.16. Todos os *routers* CE, que dispõe de serviços associados à VPLS-1, trocam tráfegos *ethernet* entre si. O *router* PE utilizado no encaminhamento é indiferente, pois a decisão de encaminhamento é ao nível do MPLS. Assim é possível criar-se uma *interface* virtual de uma VLAN com endereço IP. É como se o *backbone* MPLS fosse um “super” comutador. Esta *interface* virtual permite que o tráfego da VLAN seja comutado por IP.

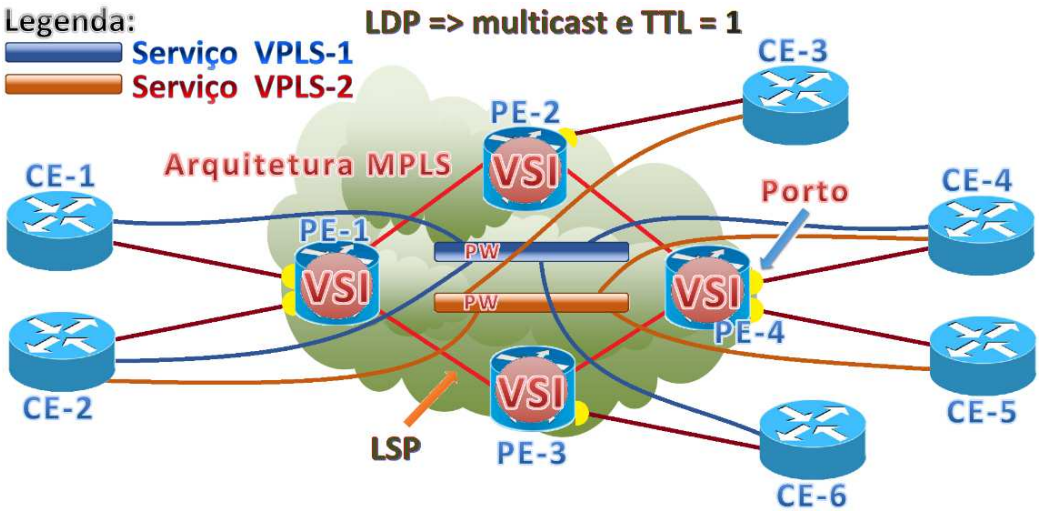

Figura 3.16 – Várias redes privadas virtuais *ethernet* num domínio MPLS (VPN-L2).

Rede privada na camada 3

Na arquitetura IP tradicional, os pacotes podem ser encaminhados num túnel, recorrendo ao encaminhamento IP e, assim, permitir que locais remotos usem as mesmas gamas de endereços IP (privados) nas interligações. No MPLS, é possível criar VPN de camada 3 (VPN-L3) ao se adicionar mais um rótulo contextual (além do rótulo de comutação). São constituídas por grupos de *routers*, instalados em diferentes pontos geográficos do mesmo cliente e que compartilham informações de encaminhamento comum, para permitir encaminhar o seu tráfego IP. Para não aumentar enormemente a tabela de encaminhamento (global), essa tabela foi segmentada em sub-tabelas de encaminhamento atribuídas a cada VPN-L3 *[3.11-5]*.

Mecanismo *virtual routing and forwarding*

O mecanismo *virtual routing and forwarding* (VRF), também designado por "VPN *routing and forwarding"* permite que várias tabelas de encaminhamento coexistam no mesmo *router* ao mesmo tempo. O mecanismo VRF interage com o plano de dados, e fornece um encaminhamento independente entre as diferentes VPN existentes no mesmo *router* físico. Assim, como as instâncias de roteamento são independentes, os endereços IP iguais ou sobrepostos podem ser usados sem conflitos entre si. Isto implica a compreensão dos atributos da comunidade estendida BGP: *route distinguisher* (RD) e *route target* (RT). O encaminhamento é realizado na VPN-L3 utilizando apenas a tabela RIB virtualizada associados ao VRF do PE, que, em cada *router* PE *peer*, foram anunciados os seus prefixos de rede pelo MP-BGP. Entre cada *router* PE, as tabelas RIB globais são diferentes, mas as tabelas RIB virtualizadas de cada VRF podem ou não ser iguais em todas os *routers* PE onde a mesma VPN-L3 esteja configurada. Após a criação e configuração da VPN-L3, esta passa a ser uma extensão da rede do cliente. Os prefixos de rede que constam da tabela RIB do VRF podem ser compartilhadas entre os vários VRF existentes nos *routers* PE onde a VPN-L3 está configurada. Os *routers* P existentes no domínio MPLS não conhecem nada sobre os VRF e não precisam.

A utilização do mecanismo VRF permite o encaminhamento de IP privados numa rede pública ao recorrer a uma tabela RIB virtualizada. Ou seja, é uma forma de atribuir a cada subescritor um

equipamento (*router* virtual), que por sua vez dispõe de uma própria tabela RIB (mas virtual). Este mecanismo substitui a necessidade dos operadores utilizarem o *network address translation* (NAT) e os *access control list* (ACL) quando os IP de destino são iguais e de clientes diferentes. Somente os portos associados a um determinado VRF podem trocar pacotes IP entre si.

- Instância *VRF lite*

A diferença entre um VRF e uma instância *VRF lite* reside na plataforma em que é utilizado. A instância *VRF lite* é uma versão mais básica do VRF, tendo por base o mesmo conceito, é utilizado nos *routers* convencionais (CE), e não utiliza os atributos RD e RT. Cada *router* CE instalado nas extremidades precisam de serem configurados com uma instância *VRF lite*. Para usar a versão *VRF lite*, não é necessário como pré-requisito a existência do *backbone* MPLS.

Nos comutadores, as VLAN teriam pouca utilidade se não existisse o conceito de tronco (*trunk*). Da mesma forma, nos *routers* convencionais (CE), a instância *VRF lite* não teria utilidade se não existisse a possibilidade de se poder utilizar vários *VRF lite* num único *router* (convencional). Assim, a instância *VRF lite* é utilizado num ambiente LAN onde é necessária a separação entre redes no mesmo dispositivo. Esta possibilidade permite que todas as instâncias *VRF lite* possam trocar os seus pacotes utilizando o mesmo porto *trunk* do *router* físico.

As principais vantagens na utilização das VPN-L3, comparando com o VPN-L2, prendem-se com uma reduzida dimensão da tabela ARP, pois esta fica com menos endereços MAC e não há problemas com os *loops*. A Figura 3.17 ilustra três portos físicos ligados ao *router* "CE-1" a trocarem pacotes IP com os três portos de *routers* CE diferentes. Na troca de tráfego dos diversos serviços segmentados entre o *router* "CE-1" e o *router* "PE-1" é utilizado o mesmo AC. Apesar da instância *VRF lite* não reconhecer o MPLS, mas sim a arquitetura IP, todos os tráfegos dos diferentes serviços existentes no *router* "CE-1" são segmentados e mapeados para o respetivos VRF *lite*. O tráfego, segmentado, é trocado entre o VRF *lite* e o VRF existente no PE *ingress* ("PE-1") associado ao respetivo serviço VPN-L3. No domínio MPLS, são utilizados diferentes VRF, um por cada serviço, no transporte do tráfego entre os diferentes *routers* que participam no transporte. Esta solução permite que o tráfego se mantenha segmentado no domínio MPLS. Por questões de segurança, no encaminhamento de pacotes IP entre o VRF *lite* e o VRF a que está associado no PE *ingress*, é configurado um *default gateway*. Ou seja, esta solução faz com que o CE não conheça os prefixos de rede que o VRF conhece, no entanto, o VRF deve de conhecer os prefixos de rede existentes no VRF *lite*.

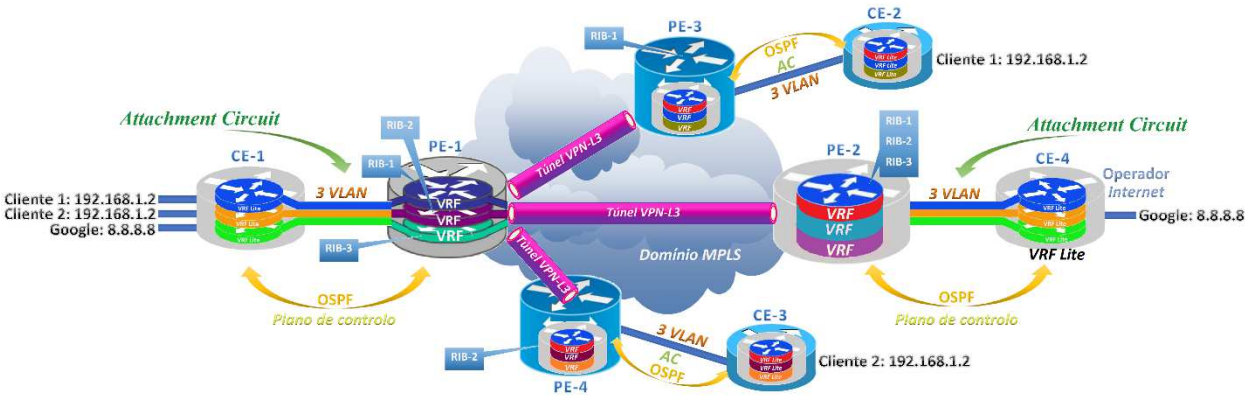

Figura 3.17 – Rede privada virtual IP num domínio MPLS.

A troca de prefixos de rede VPN-IPv4, entre os diferentes VRF, é realizada no plano de controlo com a utilização do protocolo MP-BGP. A configuração (construção) do serviço VPN-L3 utiliza, nas suas extremidades associadas, os IPLB (*router ID*) dos *routers* PE *ingress* e *egress*. A Figura 3.17 ilustra uma situação em que existem, no *router* "CE-1", dois serviços a solicitar troca de pacote IP com IP de destino igual e no MPLS consegue identificar os respetivos *routers* CE, pois o tráfego está separado pelo seus respetivos VRF. Na Figura 3.17 tal não está representado, mas o "Cliente 2" também pode alcançar qualquer um dos outros *routers* PE ("PE-2" e "PE-3"), bastando associar os IPLB do novo PE *peer* à VPN-L3. Apesar do identificador VRF ter apenas um significado local, é prática comum utilizar o mesmo identificador para o serviço VPN-L3 a que está associado, pois o identificador VPN-L3 (RD) tem que ser único no domínio MPLS.

A Figura 3.18 ilustra uma topologia de malha completa no domínio MPLS e as ligações (*attachement circuit*) entre o mesmo *routers* PE e vários *routers* CE. Um *router* PE pode, efetivamente, encaminhar diversos tráfegos, de diversos serviços diferentes, recebidos em cada um dos seus portos e associar-los às respetivas VPN. É assim possível encaminhar dados de diferentes clientes recorrendo a múltiplas redes virtuais e, utilizando múltiplas instâncias VRF configurados nos *routers* PE e definir os caminhos que os diferentes pacotes devem de seguir.

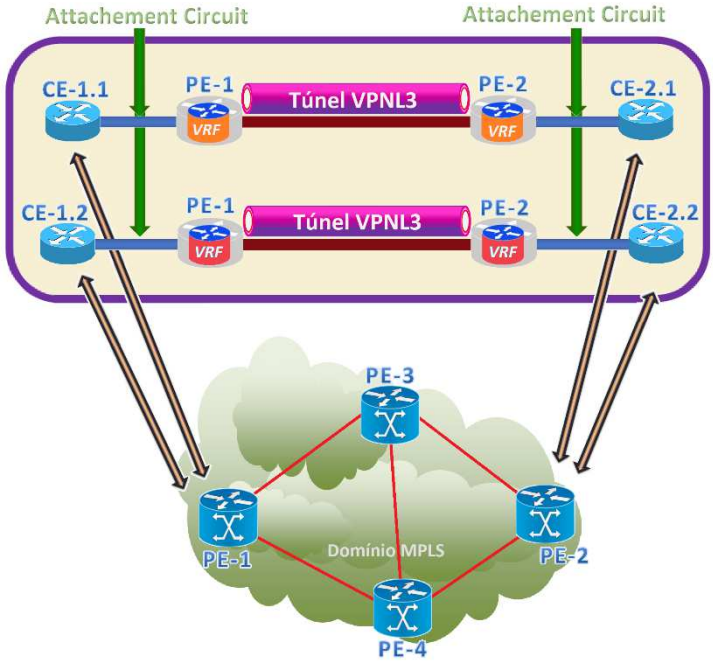

Figura 3.18 – VPN sobre um domínio MPLS.

- Extensão do multiprotocolo *border gateway protocol*

O protocolo de encaminhamento BGP versão 4 (BGP-4) é mais complexo que o OSPF ou IS-IS, mas garante a eficiência da *internet*, pois é orientado à segurança. É um protocolo de encaminhamento do tipo *link path* e é executado pelos *routers* de borda (*border gateway*) dos sistemas autónomos (*autonomous system*, AS). Designa-se "sistema autónomos" ao grupo de *routers* com a mesma política de encaminhamento, o mesmo protocolo de encaminhamento, e é gerida pela mesma entidade. O protocolo BGP é melhor para gerir caminhos redundantes, sendo estável, pois estabelece sessões TCP com o *router* PE vizinho, e estando a sessão ativa, o

router PE vizinho é sempre opção. O protocolo de encaminhamento OSPF utiliza o UDP para enviar pacotes dos objetos descritores (*link-state advertisement*, LSA), e é "sem coneção", ou seja, não sabe se o *router* vizinho recebe os pacotes de objetos descritores. Um cuidado que é necessário considerar é que o BGP, por padrão, não usa autenticação para as sessões estabelecidas, sendo recomendável configurar a utilização da autenticação no estabelecimento das sessões.

O *multi-protocol extensions for border gateway protocol* (MP-BGP) é uma extensão do protocolo BGP-4 e é utilizado exclusivamente no anuncio de prefixos de rede do tipo VPN-IPv4 entre os VRF associados à mesma VPN-L3. O prefixo de rede VPN-IPv4 advém da conversão do endereço IPv4, ao se acrescentar um atributo *route distinguisher* que identifica a que VPN-L3 pertence. Transporta pacotes de objetos descritores, que contém informação dos prefixos de rede, e não os dados úteis dos clientes. O MP-BGP adota uma terminologia semelhante ao protocolo de encaminhamento BGP tradicional no que se refere à vizinhança *(peering)*: *(i)* MP-iBGP, utilizado nos *routers* PE *peers* do mesmo sistema autónomo; e *(ii)* MP-eBGP, utilizado nos *routers* PE vizinhos *(peer)* entre *routers* localizados em 2 sistemas autónomos diferentes, designados por *border gateway*.

A utilização do protocolo de encaminhamento BGP obriga a uma rede com uma topologia de malha completa que interligue todos os *routers* que recorrem a esse protocolo de encaminhamento. Pois, o BGP necessita de estabelecer sessões TCP com todos os *routers* que fazem parte da sua tabela de encaminhamento. Na impossibilidade física de realizar essa topologia, é utilizado um *route reflector* que simula essa topologia. Assim, em vez de todos os *routers* comunicarem entre si, um *router* é eleito como "*master*", que neste caso é o *route reflector*, e recebe todos os pacotes de objetos descritores dos *routers* com quem estabelece sessões TCP, numa topologia *hub and spoke*. Esses pacotes, de objetos descritores, são processados pelo *route reflector* e enviados individualmente para cada um dos *routers* que participam na rede de topologia de malha completa. Com este método, as VPN ficam fáceis de configurar, pois só é necessário considerar as suas duas extremidades e, de uma forma automática, o MPLS encarrega se de transportar os pacotes MPLS.

- Atributo *route distinguisher*

O atributo *route distinguisher* (RD) é utilizado para tornar um endereço IPv4 único nas diferentes VPN-L3 existentes num *router* PE. Basicamente, o RD é um identificador, com significado local, codificado em 8 octetos (64 bits) e está associado a cada prefixo de rede IP tradicional (que utiliza 4 octetos) existente num determinado VRF. É um prefixo de rede anunciado no plano de controlo, via sessões TCP, e permite distinguir os caminhos de diferentes serviços, com o mesmo IP de destino. O atributo *route distinguisher* garante a singularidade dos caminhos VPN-IPv4 trocados entre *routers* PE, mas não define como os prefixos de rede devem ser inseridos nos VRF dos *routers* PE. A singularidade da VPN é a sua unicidade, ou seja, pode-se ter redes iguais de diferentes clientes no mesmo *router* físico, uma vez que existe segregação de tráfego entre clientes *[3.11-6]*.

A Figura 3.19 ilustra uma implementação de uma VPN-L3 multiponto entre os 4 *routers* PE, em que o mecanismo VRF é o mesmo, sendo que a distinção do atributo *route distinguisher* é realizada pelo próprio IPLB de cada *router* PE.

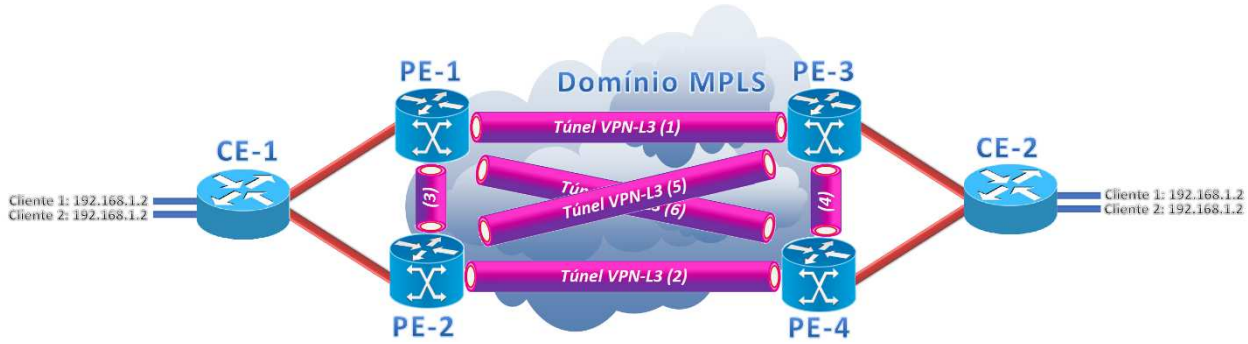

Figura 3.19 – Utilização do atributo *route distinguisher* para balancear carga.

É possível balancear tráfego, e ao mesmo tempo definir qual o tráfego que se pretende balancear. Pois o *router* "CE-1" ao enviar o tráfego para os *routers* "PE-1" e "PE-2", estes configuram o tráfego recorrendo à construção do atributo *route distinguisher* que utiliza o seu próprio IPLB. A outra componente do atributo *route distinguisher* é o mecanismo VRF, e que pode ser o mesmo, o que permite que o tráfego chegue separado e balanceado aos *routers PE peer* "PE-3" e "PE-4", o que facilita a gestão da rede. Ou seja, para balancear o tráfego é necessário existirem *route distinguisher* diferentes para o mesmo tráfego (prefixo de rede).

A Figura 3.20 ilustra dois caminhos destinados à rede 192.168.3.0. Considerando os pacotes IP a chegarem ao *router* "PE-3", se não existir nenhuma informação adicional no cabeçalho do pacote VPN-IPv4, o *router* "PE-3" não sabe para qual dos *routers* CE ("CE-2" ou "CE-3") deve enviar os dados, logo não há possibilidade de sucesso na entrega. Para superar este problema de endereçamento, no domínio MPLS, foi implementada a solução de se adicionar uma identificação a cada VPN-L3. Assim, as VPN-L3 estão conectadas aos VRF existentes nos *routers* PE.

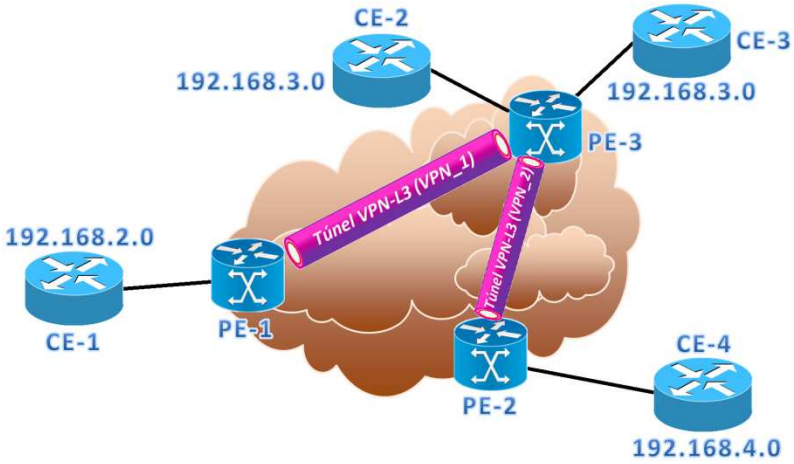

Figura 3.20 – Endereçamento de IP em vários VPN-L3.

Cada serviço VPN-L3 tem um VRF conectado a cada *router* PE *peer*, com encaminhamento que utiliza a técnica de comutação por rótulos entre *routers* PE, e o tráfego é transparente para os *routers* P do *backbone* MPLS. Ou seja, as entradas das tabelas de encaminhamento são

propagadas para todos os *routers* PE *peers* da mesma VPN, mas nunca para os P, pois estes apenas necessitam dos *label switched path* (LSP) para comutar o tráfego. A implementação da VPN-L3 possibilita uma manutenção fácil e uma elevada escalabilidade. Todos os VRF conectados à VPN-L3 tem as suas próprias tabelas de encaminhamento, e o encaminhamento de pacotes IP é realizado exclusivamente na sua VPN-L3, com base no endereço IP. A identificação da VPN-L3 transportada pelo protocolo de encaminhamento BGP é designada de *route distinguisher* (RD). A identificação consiste em adicionar mais um rótulo aos pacotes MPLS. Portanto, os pacotes MPLS passam a dispor de dois rótulos empilhados para comutação.

- Atributo *route target*

Enquanto que o atributo *route distinguisher* é utilizado para manter a exclusividade entre prefixos de rede idênticos nos diferentes VRF, o atributo *route target* permite ao administrador da rede ter controlo no anuncio dos prefixos de rede (VPN-IPv4) na VPN. Esse anúncio e as respetivas atualizações por parte do mecanismo VRF é realizado pelo o mecanismo *route target* de importação e exportação (RTi e RTe). Ou seja, é assim possível implementar um filtro de prefixos de rede que devem constar nas tabelas RIB associadas a cada VRF de cada *router* PE *peers*. Os prefixos de rede VPN-IPv4 (12 octetos) são construídos localmente pelos *routers* PE, conforme ilustrado na Figura 3.21, e são sempre anunciados recorrendo a pacotes de objetos descritores, transportados pelo protocolo MP-BGP. É o plano de controlo que gera esses pacotes que permitem a atualização das tabelas RIB dos VRF associados a mesma VPN-L3.

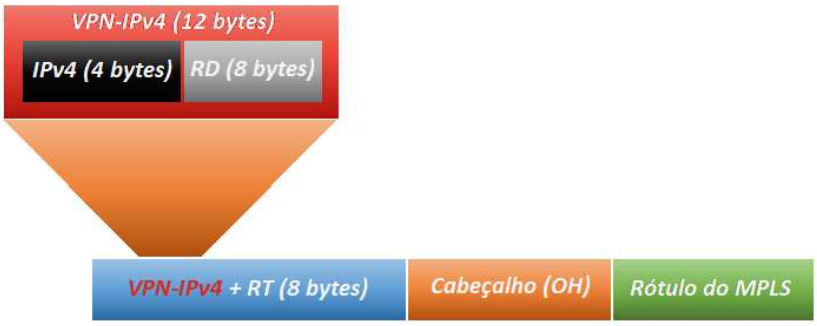

Figura 3.21 – Mensagem do plano de controlo para atualizações das tabelas RIB dos mecanismos VRF.

No plano de dados, é necessário adicionar um rótulo que identifique a VRF, além do rótulo de comutação no domínio MPLS, conforme o formato da Figura 3.22.

Figura 3.22 – Formato do rótulo do pacote transmitido numa VPN-L3 no domínio MPLS.

Conforme ilustrado na Figura 3.23, cada serviço mencionado na Tabela 3.1 que acede ao *router* "PE-1", vindo do "CE-1", tem o seu próprio VRF.

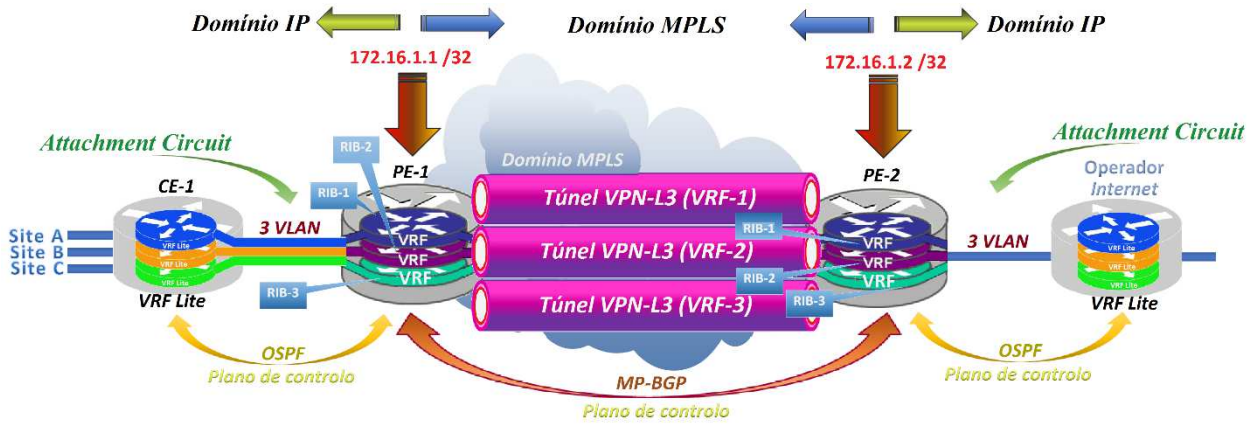

Figura 3.23 – Vários mecanismos VRF diferentes associam-se aos seus respetivos VRF no *router* PE *peer*.

Para ser mais fácil, em caso de avaria, utiliza-se uma metodologia para definir a numeração do atributo *route distinguisher*: "*ASN: nn*" ou "*IP-Address: nn*", em que o "*nn*" é o identificador local RD, e é independente do *router* físico PE. Também não é obrigatório que este identificador seja igual na outra extremidade do túnel. Utiliza-se o número do sistema autónomo para definir o "*ASN*" ou o IPLB do *router* PE para definir o "*IP-Address*". Assim, cria-se um RD por cada VRF criado num *router* PE, e utiliza-se a mesma identificação no outro RD do *router PE peer* (ou nos outros, se for multiponto).

Tendo como exemplo o *site* "A" da Tabela 3.1, o RD é definido pela junção de duas variáveis: *(i)* IPLB do *router* PE; e *(ii)* o número do serviço associado (VRF). Este prefixo de rede VPN-IPv4 será anunciado com o RTe 63456:10, e só o VRF do *router* PE *peer* que tiver na sua configuração o RTi 63456:12 é que pode atualizar a sua tabela RIB. Neste exemplo, o RTe 63456:10 só dispõe de um prefixo de rede VPN-IPv4, mas pode anunciar mais se estes existirem na tabela RIB do VRF. Ou seja, apesar do MP-BGP transportar todos os prefixos de rede existentes no VRF para os VRF do *router* PE *peer* associados a mesma VPN-L3, só depois de validados com o RT *import* é que os prefixos de rede são atualizados as suas tabelas RIB. A tabela RIB do "VRF-11", do *site* "B", será atualizada com os prefixos de rede VPN-IPv4 dos sites "A" e "C". Na construção do identificador RD é utilizado o VRF, pois permite balancear tráfego.

Note-se que no *site* "A" o recetor só atualiza se o campo "RTi" tiver "63456:12", e ao anunciar a sua tabela coloca no campo "RTi" com "63456:10".

Routers	RD (IPLB:VRF)	RT Export	RT Import
Site A	10.130.254.1 : 10	63456 : 10	63456 : 12
Site B	10.130.254.2 : 11	63456 : 11	63456 : 10
Site C	10.130.254.3 : 10	63456 : 10	63456 : 12

Tabela 3.1 – Exemplo 1 de atribuição de RD, RTe e RTi (domínio : serviço).

Tendo como exemplo o *site* "D" da Tabela 3.2, a tabela RIB do "VRF-10" será atualizada com todos os prefixos de rede VPN-IPv4 existentes nos VRF dos sites "A", "B" e "C" (da Tabela 3.1), pois os RTi configurados no *router* correspondem ao RTe desses sites.

É assim possível coexistirem diferentes (instâncias de) *routers* virtuais num único *router* físico, permitindo maximizar os recursos do hardware existente, por partilha e servindo vários clientes (VPN).

Routers	RD (IPLB:VRF)	RT Export	RT Import
Site D	10.130.254.4 : 10	63456 : 10	63456 : 11
		63456 : 12	63456 : 10

Tabela 3.2 – Exemplo 2 de atribuição de RD, RTe e RTi (domínio : serviço).

A Figura 3.24 ilustra 4 clientes a comunicar no mesmo domínio MPLS. A gama de endereço IP utilizado pelo "Cliente-1" pode ser igual ao do "Cliente-2", sendo apenas necessário diferenciar os respetivos encaminhamentos. Para garantir a segmentação dos dados entre clientes diferentes que utilizem o mesmo *router* PE, é necessário utilizar o atributo *route distinguisher*. O pacote é assim convertido de pacote IP para pacote VPN-IPv4. Além disso, os endereços IPv4 voltam a ser utilizados fora do domínio MPLS. Os *routers* PE atualizam os prefixos de rede VPN-IPv4 no VRF mediante o valor do atributo *route targets import* (RTi).

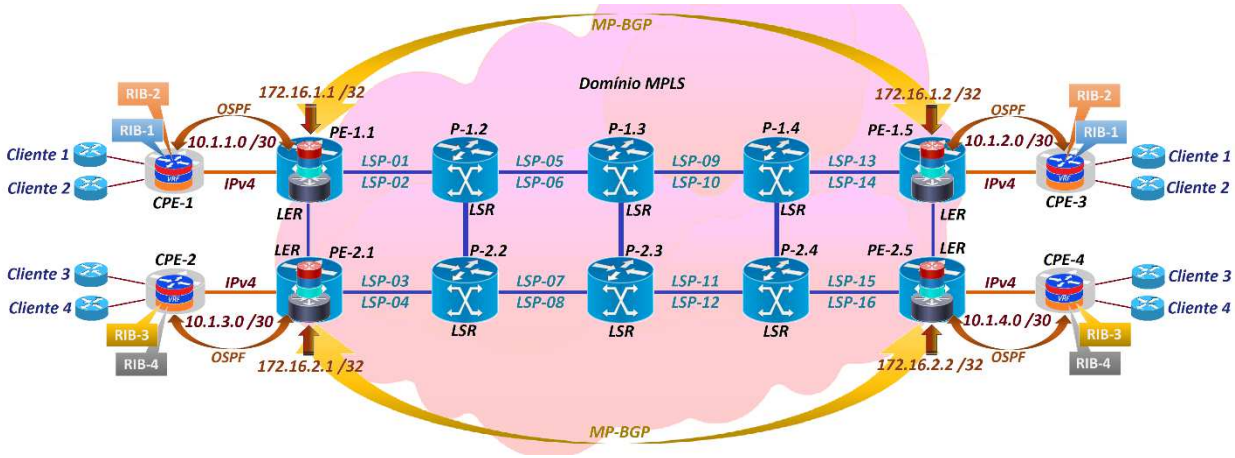

Figura 3.24 – Várias redes privadas virtuais IP num domínio MPLS (VPN-L3).

3.12 Qualidade de serviço

A qualidade do serviço (*quality of service*, QoS) é definida como a medida do desempenho de um sistema de transmissão que reflete a qualidade da transmissão e a disponibilidade do serviço. A introdução de mecanismos de QoS surge como uma medida de gestão dos recursos de transmissão existentes nos sistemas de comunicação, na tentativa de o sistema dar a resposta mais adequada a cada tipo de tráfego. O tráfego é classificado para poder ser diferenciado dos outros tráfegos que acedam ao dispositivo. São atribuídas políticas de QoS aos diferentes tráfegos, por exemplo, pela definição de limites mínimos e máximos do débito de transmissão, e

de prioridades relativas ou absolutas com base na largura de banda disponível. A atribuição de políticas de QoS pode ser feita por classe ou agregado de tráfego, fluxo ou até mesmo por ligação individual. A execução de ações de condicionamento do tráfego, de acordo com a sua classificação, é dividida em ações de "policiamento" e de "modelação". Estas ações podem consistir, por exemplo, na eliminação seletiva ou arbitrária de pacotes no porto de entrada, no encaminhamento direto para o porto de saída ou na colocação dos pacotes em filas de prioridades, tal como na limitação do débito máximo de um dado tráfego. O escalonamento estipula a ordem e o ritmo com que os pacotes de dados são transmitidos pelo sistema, por forma a permitir cumprir com os parâmetros definidos nas políticas de QoS. A gestão de QoS é um dos principais benefícios que as empresas de telecomunicações procuram para implementar soluções de transporte de voz e vídeo.

Na arquitetura IP, é utilizado a *class of service* (CoS), que atua unicamente no segmento de rede (VLAN), para se ter algo parecido com a qualidade de serviço. O QoS, que atua no traçado completo, reserva percentagens (%) de largura de tráfego para diferentes tipos de serviços, não permitindo assim que o tráfego mais importante anule o tráfego menos importante. Apenas usa pesos para os diferenciar. Se o porto estrangular, os pacotes são descartados. Quanto maior a QoS maior será a confiabilidade no prestador de serviço. O QoS é um elemento crítico numa rede de provedor de serviço e é uma definição abstrata como sendo um método para permitir diferenciar tráfego.

O QoS caracteriza-se pela sua capacidade de fornecer um meio de comunicação que diferencia os diferentes fluxos que utilizem a rede. Para garantir um elevado nível de exigência na capacidade da rede em fornecer um serviço de ponto a ponto com um determinado tráfego (níveis de serviço), o mecanismo QoS prioriza o tráfego. Esta priorização visa assegurar uma transmissão de dados de modo mais eficiente, conseguida pela reserva de recursos para os serviços e sem interrupções. A disponibilidade de rede adequada é um pré-requisito para uma implementação do mecanismo QoS bem-sucedida, e os principais critérios avaliados são: *(i)* confiabilidade (perda de pacotes); *(ii)* atraso na entrega de pacotes (latência); *(iii)* atrasos ondulatórios (*jitter*); *(iv)* entrega de pacotes desordenada; e *(v)* largura de banda (*throughput*). Entende-se por perda de pacotes uma medida comparativa entre o número de pacotes recebidos e o número total de pacotes que foram transmitidos. O atraso na entrega do pacote considera o tempo necessário para que estes alcancem o seu destino. O *jitter* mede a diferença entre os diversos atrasos provocados até chegarem ao seu destino. Por exemplo, se um pacote necessitar de 50 milissegundos (ms) para percorrer o traçado, e um outro pacote necessitar de 60 milissegundos, então a variação de atraso seria calculada como 10 milissegundos. O *throughput* é a capacidade de processamento e não a largura de banda (ritmo efetivo) das *interfaces* físicas (camada 1) ou do processamento, conforme o contexto. O *throughput* considera o processamento dos pacotes da camada 2 e 3, e dos serviços ativos associados, como o IPSec e outros níveis de segurança. A troca de tráfego entre a camada 2 e 3 ocorre ao nível do processamento.

3.13 Elevada resiliência

Para ajudar a evitar a interrupção devido a operações de manutenção na rede (como atualizações do sistema operativo), ou em caso de falha de um nó, além da implementação de uma topologia redundante, foram acrescentados mecanismos que permitem garantir elevada disponibilidade

(*high availability*). A Cisco desenvolveu diversos mecanismos, dos quais se destacam: *(i) nonstop forwarding* (NSF), também designado por *graceful restart* (GR); *(ii) stateful switchover* (SSO); *(iii) non stop routing* (NSR); *(iv) fast rerouter*; *(v) link aggregation group* (LAG).

Caminho alternativo

Em caso de alteração de topologia da rede devido a falha no caminho primário (e protegido), o requisito fundamental do caminho alternativo é o de fornecer uma solução à falha. Essa solução deve estar livre de *loops* e impedir que os *routers* adjacentes iniciem o algoritmo de re-convergência, pois não devem de serem avisados da ocorrência da falha. Assim que o algoritmo do protocolo de encaminhamento OSPF encontra uma solução para a falha, a ligação de proteção volta a ficar em modo repouso.

Microloop avoidance local

Os protocolos de encaminhamento do estado da ligação (*link-state*) convergem para um estado sem *loops* dentro de um período de tempo finito após uma alteração de topologia da rede. Durante esse período de convergência podem ser enviados pacotes IP num hiato de tempo muito reduzido devido a uma diferença de convergência entre os nós de rede afetados. Ou seja, há um período de tempo, muito reduzido, em que são enviados pacotes IP, pois o *router* ainda não considerou a falha. Também pode ocorrer a formação de um *microloop* durante o período de tempo em que a rede ainda não tenha convergido após uma alteração de topologia, que é causada pela inconsistencia da tabela *forwarding information base* (FIB). Ou seja, durante a atualização da tabela RIB, a nova informação ainda não passou para a tabela LIB, podendo resultar numa perda de tráfego. Mas se a duração do *microloop* for muito reduzida, os pacotes IP poderão eventualmente ser encaminhados até ao seu destino. Os *microloops* formados entre um dispositivo com falha e seus vizinhos são chamados de *microloops* locais, ao passo que os *microloops* que são formados entre dispositivos que são de saltos múltiplos são chamados *microloops* remotos *[3.13-1]*.

Considerando o *router* “A” na topologia ilustrada pela Figura 3.25, e supondo que cada ligação na topologia tem a mesma métrica, o caminho mais curto do *router* “A” para o prefixo ***Pfx_1*** consiste em utilizar a ligação “AC”.

Se a ligação “AC” falhar, e durante o processo de convergência, se o *router* “A” reencaminhar para o *router* “B” o tráfego destinado a ***Pfx_1***, o *router* “B” reencaminhará de volta ao *router* “A” o mesmo tráfego. E assim gera retorno de tráfego em ciclo (*loop*). O *microloop* ocorre no instante em o pacote vai de “A” para “C”, e durante o estabelecimento da ligação entre o ponto “A” e “B”, o pacote volta a ser reenviado de “C” para “A”. E os números de saltos são contabilizados pelo campo “*Time to Live*” (TTL) existente no cabeçalho do pacote IP.

O mecanismo *IP FRR* fornece convergência rápida durante os eventos de falha de ligação (*link-down*), encaminhando o tráfego para um caminho alternativo pré-calculado até que o mecanismo de convergência calcule um caminho melhor. Como o tráfego é encaminhado para o caminho pós-convergência, podem ocorrer *microloops*, se o nó convergir antes dos seus vizinhos.

Pode ser utilizado um recurso local para evitar o *microloop* habilitando o "*microloop avoidance*" para prefixos protegidos por *loop-free alternate* (LFA) ou LFA remoto. A prevenção *microloop avoidance* local suporta os seguintes gatilhos: *(i)* evento “*down”* na *interface*; *(ii)* evento “*down”*

da adjacência devido à sessão de deteção de encaminhamento bidirecional (BFD); *(iii)* evento "*downside*" adjacente devido ao tempo de espera do vizinho ter expirado.

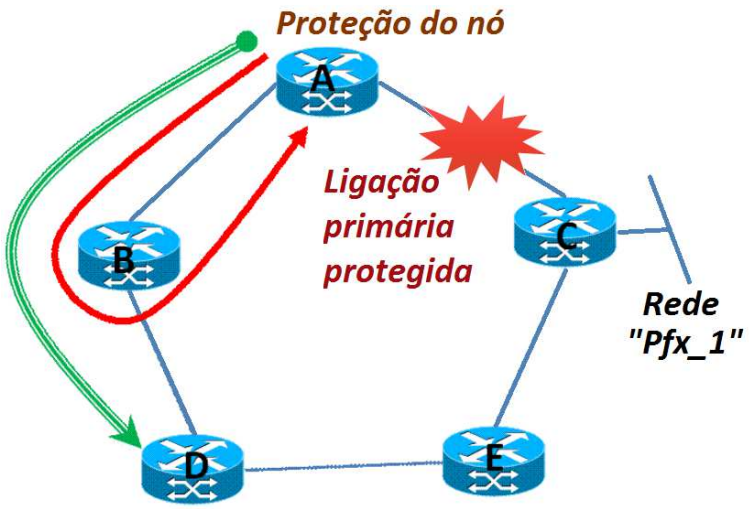

Figura 3.25 – *Loop-free alternate* numa topologia de anel.

Mecanismo *fast rerouter*

O mecanismo *fast reroute* fornece redundância para um caminho *label switched path* (LSP). Quando se habilita o *fast reroute*, as alternativas são pré-calculados e pré-estabelecidos ao longo do LSP. No caso de uma falha de rede no caminho atual do LSP, o tráfego é reencaminhado rapidamente para uma das alternativas.

Mecanismo de reencaminhamento rápido alternativo e livre de *loop*

Quando uma ligação falha, e utilizando o IGP, o *router* deve sinalizar o evento aos seus vizinhos, para que estes possam recalcular um novo próximo salto para todos os prefixos afetados. O IGP não suporta dois caminhos para o mesmo prefixo (em simultâneo, na tabela de encaminhamento). A Cisco desenvolveu um mecanismo, que designou de mecanismo de reencaminhamento rápido alternativo e livre *loops (loop-free alternate fast reroute*, LFA FRR), que permite uma solução funcional. Este mecanismo só existe no MPLS e dá ao *router* autonomia para resolver sozinho as falhas de ligação, mediante parâmetros pré-configurados. É possível definir se *(i)* um determinado tráfego pode ou não ter redundância; *(ii)* só deve ter um caminho possível, ou vários caminhos pré configurados com os critérios de escolha definidos. O tempo que demora esse recálculo faz com que o tráfego associado aos prefixos afetado pela falha seja descartado. Esse processo pode levar centenas de milissegundos. O mecanismo LFA *fast reroute* permite que o circuito virtual ("túnel" de comunicação) permaneça ativo mesmo quando o *router* intermediário cair após ocorrer uma falha, pois existe um caminho alternativo disponível. Todo o tráfego chega ao seu destino recorrendo a um caminho alternativo, mas só se o caminho primário estiver protegido *[3.13-2]*.

Uma rede com este recurso permite reduzir as perdas de pacotes e tem menos *microloops* do que uma rede sem o mecanismo IP FRR. Há casos em que ainda ocorrem perda de pacotes, uma

vez que a eficiência do IP FRR não é uniforme, além disso, na pior situação possível, a convergência da rede com IP FRR é sempre melhor que uma rede sem *fast reroute*.

A Figura 3.26 ilustra como um *router* com o mecanismo LFA *fast reroute* ativado reage a uma falha de ligação. Um *router*, com caminhos primários protegidos, calcula os caminhos alternativo dos prefixos associados a esses caminhos primários protegidos e memoriza-os na sua tabela de encaminhamento. Assim, na presença de uma falha do caminho primário protegido, o *router* reencaminhará imediatamente todo o tráfego do caminho primário para o caminho alternativo, já pré-calculado e memorizado, sem que outros *routers* tenham que iniciar imediatamente o processo de convergência ou mesmo estarem ciente de que a topologia da rede mudou.

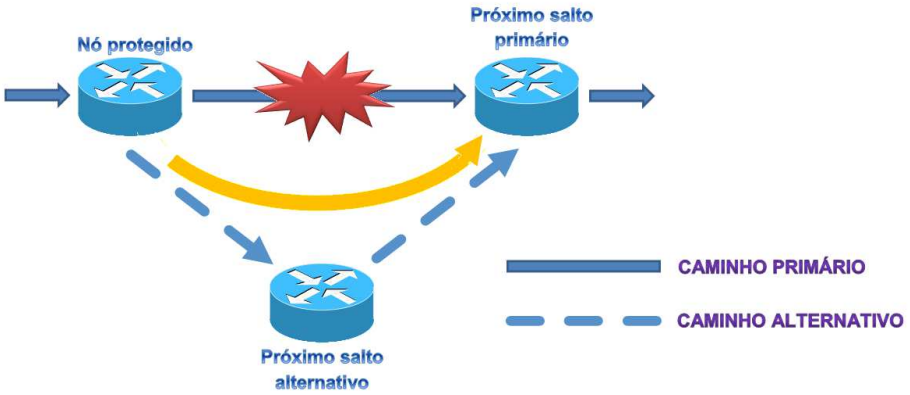

Figura 3.26 – Mecanismo *fast reroute*.

A base do bom desempenho do *fast reroute* é a existência de caminhos alternativos já pré-calculados pelos *routers* mais próximos do ponto de falha (serão os primeiros a saber da falha) que podem ser utilizados para reencaminhamento dos pacotes IP sem *loops*, nem necessidade de esperar pelo resultado da convergência devido à adaptação a nova topologia da rede.

Nota-se que não se deve confundir o mecanismo LFA *fast reroute* com o mecanismo BFD, que ajuda a detetar mais depressa a falha da ligação, mas não a resolve, e os mecanismos NSF e NSR.

Mecanismo *nonstop forwarding* e *stateful switchover*

O mecanismo *nonstop forwarding* (NSF) é utilizado quando a falha ocorre no processador do *router* e permite reduzir o tempo de reação à falha para valores inferiores a 50 milissegundos utilizando um caminho alternativo pré-calculado, no caso de a ligação primária falhar, de modo a que o caminho alternativo possa ser rapidamente utilizado quando é detetada a falha. O mecanismo *stateful switchover* (SSO) permite que o processador que está em standby mantenha sessões TCP com os *routers* vizinhos, para numa situação de alterar o seu modo de funcionamento (standby para ativo) não haja necessidade de iniciar o processo de estabelecer sessões TCP. O mecanismo NSF, associado ao *stateful switchover* (SSO), permite que numa situação em que um processador falhe, o encaminhamento dos pacotes continue a ser suportado pelo outro. Não confundir o mecanismo NSF com o NSR, pois apesar de terem por missão impedir a re-convergência da rede durante uma transição/flutuação, são diferentes. O perigo de se perderem pacotes só existe caso haja mesmo uma alteração à topologia da rede, daí que, para minimizar este perigo, se utilize o NSF com o mecanismo SSO e dois processadores. Os processadores têm funções diferentes, pois um desempenha a função de primário (ativo) e outro

de secundário (*standby*). O que a Cisco designa de *stateful switchover* (SSO) a Juniper designa de *graceful routing engine switchover* (GRES). Consegue-se assim maior disponibilidade e proteção contra o tempo de inatividade não planeado devido a problemas de *hardware* ou *software*. A implementação dos mecanismos NSF/SSO em locais críticos melhora a disponibilidade do sistema mesmo quando se está a atualizar o software (*in service software upgrade*, ISSU). O mecanismo Cisco NSF/SSO resulta de melhorias progressivas para reduzir o impacto de interrupções realizadas ao mecanismo conhecido como redirecionar o processamento do encaminhamento (*route processor redundancy*, RPR). Através do uso de *hardware* redundante no mesmo dispositivo e a separação do plano de controle do plano de dados, permite o encaminhamento contínuo sem perda de pacotes, mesmo que ocorram falhas no processador. Além disso, é considerado como sendo boa pratica realizar a atualização do sistema operativo nos dispositivos no laboratório, pois minimiza os riscos, apesar de poder ser realizado com os equipamentos em produção. Depois de realizar a atualização, deve-se verificar se os serviços ficaram afetados. Em caso de avaria de um processador, a sua troca tem que considerar que o novo equipamento deve ser igual ao anterior *[3.13-3]*.

Mecanismo *non stop routing*

O problema com as trocas do plano de controle é que as adjacências ao protocolo de encaminhamento são interrompidas. Quando um plano de controle primário fica inoperacional, qualquer *router* vizinho que tenha uma sessão de *peering* (vizinhança), deteta a falha na sessão de vizinhança (falha na ligação física). O *router* X, ao ativar o plano de controle secundário, reestabelece a adjacência, mas nesse hiato de tempo, o *router peering* (*router* Y) anuncia aos seus outros vizinhos que o *router* X não é mais "um próximo salto válido", e os outros *routers* vizinhos iniciam o processo de re-convergência da rede. Quando o plano de controle secundário fica operacional e restabelece adjacências, o seu *router* Y anuncia que o *router* X está novamente disponível como "um próximo salto válido" e todos os *routers* reiniciam o cálculo para descobrir a nova topologia da rede. Tudo isso pode ser altamente prejudicial para a rede. O objetivo do NSR é prevenir, ou pelo menos minimizar, o efeito de sessões de vizinhança interrompidas. Uma primeira tentativa de controlar adjacências interrompidas durante as trocas do plano de controle (primário para secundário) é a extensão do mecanismo *nonstop forwarding* (NSF). Quando o plano de controlo de um *router* X deixa de responder aos seus *routers* vizinhos *(peering)*, em vez de reportar imediatamente a seus *routers* vizinhos que o *router* X ficou indisponível, aguarda um determinado período de tempo (o período de tolerância). Se o plano de controle do *router* voltar à normalidade e restabelecer as sessões de vizinhança antes que o período de tolerância expire, não chega a haver perturbação na rede. Existem, além disso, alguns problemas com mecanismo NSF: *(i)* os *routers* vizinhos são obrigados a suportar as extensões do mecanismo NSF; *(ii)* as comutações do plano de controle são mais prejudiciais nos *routers* PE.

Mecanismo *link aggregation group*

O mecanismo *link aggregation group* (LAG) é designado por *portchanne*l e *etherchannel* pela Cisco. As duas designações apenas distinguem o sistema operativo do fabricante Cisco. O mecanismo LAG consiste em agregar vários portos físicos num único porto lógico para permitir redundância e o aumento da largura de banda. Este mecanismo permite o balanceamento da carga (por VLAN e não por pacotes individuais), permitindo assim resolver falhas que possam ocorrer numa das suas ligações, contribuindo assim para a sua resiliência. O IGP encaminha os pacotes para a porto lógico e o mecanismo LAG escolhe o porto físico. Pode ser configurado nos

seguintes modos: *(i) port aggregation protocol* (PAgP), proprietário do fabricante Cisco; *(ii) link aggregation control protocol* (LACP); e *(iii)* Modo ligado. Nos modos PAgP ou LACP, para determinar quais os portos que devem de estar ativos, o sistema negoceia com a outra extremidade da ligação. O *switch* força todos os portos compatíveis a se tornarem portos LAG ativos. Outra extremidade da ligação, o porto deve ser também configurado no modo "ligado", caso contrário, pode ocorrer perda de pacotes. Portos incompatíveis são suspensos.

A redundância com *multi-chassis link aggregation group* (MC-LAG, IEEE 802.1aq - *shortest path bridging*) é um tipo de grupo de agregação de ligações (*link aggregation group*, LAG) com os portos envolvidos que terminam em chassis separados, com o objetivo principal de fornecer redundância em caso de falha de um dos chassis. Também é designado por *stack* e nem todos os equipamentos suportam esta tecnologia. A *firewall Adaptive Security Appliance* (ASA), do fabricante Cisco, não suporta o *portchannel [3.13-4].*

3.14 Conclusão

Uma característica da tecnologia baseada em hierarquia digital plesiócrona (PDH) é o estabelecimento de ligações ponto-a-ponto, e utilizar a multiplexagem dos dados para colocá-los nas unidades elementares *time slot*. As *time slots* são depois mapeadas em trama de transmissão designadas por E1. Os níveis superiores da hierarquia são obtidos pela junção de 4 níveis inferiores, e está normalizada até os 140 Mbps. Não possibilita redundância, nem disponibilizou capacidade para a motorização e opera ao nível da camada 1 do modelo OSI. A tecnologia baseada em SDH segue a mesma metodologia, mas permite ritmos de transmissão mais elevados, monitorização e redundância. Uma atualização do SDH, designada por NG SDH, veio permitir uma melhor eficiência no transporte do tráfego *ethernet*.

Numa arquitetura IP, o encaminhamento de pacotes IP está dependente da análise individual do cabeçalho, associado ao pacote de dados, análise essa que é realizada em todos os *routers* em que o pacote IP é encaminhado. E este encaminhamento não atende ao estado de carga de cada troço da rede, o que, por vezes, leva a que sejam escolhidos caminhos congestionados em detrimento de caminhos com mais saltos, mas nos quais existem os recursos que satisfaçam o encaminhamento.

O MPLS, arquitetura baseada na comutação de pacotes, vem colmatar as deficiências associadas as tecnologias anteriores e maximiza as suas vantagens. Permite encontrar os melhores caminhos e que tenham efetivamente recursos suficientes para suportar as capacidades necessárias para o transporte do tráfego. A análise para a atribuição de uma determinada classificação para encaminhamento por classes equivalentes, do fluxo de dados, é realizada apenas uma vez e é à entrada da rede. Tal permite que, nos *routers* subsequentes, o cabeçalho do pacote IP não necessite de ser novamente processado, bastando analisar o rótulo adicionado ao pacote no encaminhamento.

O MPLS suporta grande largura de banda, que pode crescer exponencialmente, tem baixa latência. As suas principais vantagens são a possibilidade de redundância, melhores níveis de segurança, um custo por *bit* muito inferior ao oferecido pela tecnologia de comutação por circuito. Apesar de não estabelecer uma ligação ponto-a-ponto, permite implementar um acordo de nível de serviço com elevados parâmetros e qualidade de serviço equivalente ao existente com a utilização do SDH. O MPLS assenta num sistema de telecomunicações com conetividade

multiponto e considera as seguintes características essenciais: *(i)* escalabilidade; *(ii)* fiabilidade; *(iii)* robustez; *(iv)* eficiência; *(v)* flexibilidade; e *(vi)* confiabilidade.

A grande escalabilidade é conseguida com a implementação de uma rede hierárquica. Este conceito, de organização por níveis de hierarquias, permite distribuir os elementos de rede considerando as funções que estes desempenham na rede de forma ideal. Assim, os elementos de rede dentro do mesmo nível hierárquico têm propriedades semelhantes e comportam-se de igual modo.

A robustez é conseguida com a elevada resiliência da rede conseguida com *(i) nonstop forwarding* (NSF), também designado por *graceful restart* (GR); *(ii) stateful switchover* (SSO); *(iii) nonstop routing* (NSR); *(iv) fast rerouter*; *(v) link aggregation group* (LAG). O mecanismo *carrier-delay timer*, no protocolo *open shortest path first* (OSPF), permite a re-convergência da rede e evita que este se faça caso não haja necessidade. Este mecanismo reduz o tempo de indefinição por forma a contribuir para uma melhor fiabilidade, logo menor descarte de pacotes.

A tendência emergente às comunicações nas subestações modernas passa por uma aposta numa infraestrutura de comunicação baseada em *ethernet*/IP. É cada vez mais comum encontrar um ambiente *ethernet* nas subestações, pois a construção de redes *ethernet* são cada vez menos dispendiosas e lida com a transferência de dados de forma mais eficiente do que as redes tradicionais de comutação de circuitos.

A sua flexibilidade permite integrar serviços *legacy* (tradicionais) com facilidade, suportando uma estrutura unificada e convergente. Permite uma gestão centralizada a partir de uma única plataforma de gestão. É confiável porque isola tráfego com facilidade e garante serviços aos serviços críticos. O mecanismo MPLS-TE permite providenciar rotas que suportem requisitos específicos das aplicações ou serviços sujeitos as exigentes restrições de qualidade de serviço. No estabelecimento de um caminho explícito, não é dada a possibilidade ao protocolo IGP escolher o melhor caminho, mas sim ser o administrador de rede que o define.

O mecanismo *bidirectional forwarding detection* permite detetar falhas, atuando com gatilho ao mecanismo LFA *fast reroute*. A confiabilidade é garantida com o mecanismo LFA *fast reroute*, que fornece uma convergência rápida da rede na presença de uma falha na ligação.

O protocolo de encaminhamento BGP é melhor para gerir caminhos alternativos e é estável, pois estabelece sessões TCP com o *router* PE vizinho, e estando ativa, o *router* PE vizinho é opção. Devido à complexidade de se construir uma rede de topologia de malha completa, é considerado boa prática instalar na rede de telecomunicações dispositivos designados por *route reflector*. O *route reflector* simula que o desenho da rede é malha completa e utiliza o protocolo MP-BGP, e com a topologia em estrela, distribui os prefixos VPNv4.

O princípio de funcionamento do serviço rede privada virtual (*virtual private network*, VPN), é fornecer uma infraestrutura partilhada, com os mesmos benefícios que uma infraestrutura privada. As VPN MPLS simplificam muito a implementação do serviço em comparação com VPN IP tradicional. Quando o número de rotas e clientes aumentam, as VPN MPLS podem suportar facilmente a carga, proporcionando ao mesmo tempo um bom nível de confidencialidade. Eles também podem transportar os endereços IP não-exclusivos. Ou seja, pode-se utilizar qualquer IP privado de um cliente, e o prestador de serviço nem sequer precisa de saber qual é, pois não precisa de saber o IP para realizar o encaminhamento. As VPN MPLS são mais fáceis de gerir e expandir do que as VPN convencionais. Quando um novo *site* é adicionado a uma VPN MPLS, apenas é necessário configurar o *router* PE que fornece serviços ao site. O atributo *route*

distinguisher é utilizado para tornar o endereço IPv4 único nas diferentes VPN. O atributo *route target* permite anunciar os prefixos de rede com regras

O MPLS utiliza toda a infraestrutura física de transporte existente, em fibra ótica, mitigando assim os custos de implementação associados a adoção de novas tecnologias.

4. Metodologia

A necessidade de migração teve por objetivo renovar a rede de telecomunicações da EEM. Esta migração permite substituir a tecnologia de transmissão baseada na comutação de circuitos, por uma baseada em comutação de pacotes. A comutação de circuitos recorre ao método de transmissão TDM para agregar diferentes fontes de informação, utilizando uma infraestrutura baseada na arquitetura hierarquia digital plesiócrona/síncrona (SDH/PDH), que necessita de estabelecer uma ligação virtual entre os intervenientes para garantir a entrega da informação. Este assunto é abordado com mais detalhes nos *"Apêndice 2 – Arquitetura Hierarquia Digital Plesiócrona* " e *"Apêndice 3 – Arquitetura Hierarquia Digital Síncrona*".

A rede baseada no MPLS da EEM veio substituir a rede SDH e passou a designar-se por "WAN SCADA". A "WAN SCADA" transporta todo o tráfego de todos os diferentes serviços, de qualquer instalação para os dois *datacenters* principais e um outro alternativo aos dois existentes na EEM. Um dos *datacenters* fica no centro de controlo do despacho, sendo que o seu *datacenter* alternativo fica nas Virtudes. O segundo *datacenter* é para os serviços administrativos e fica na sede da EEM, sendo que o seu *datacenter* alternativo oas dois principais ficam nas Virtudes. Cada *datacenter* tem as suas politicas de segurança e privacidade definidas por serviço.

A EEM, na sua opção de construir a sua rede, descartou a solução *dual core* por ser demasiado cara, optando pela solução ilustrada pela Figura 4.1. Cada *router* PE está ligado a pelo menos dois outros *routers* PE.

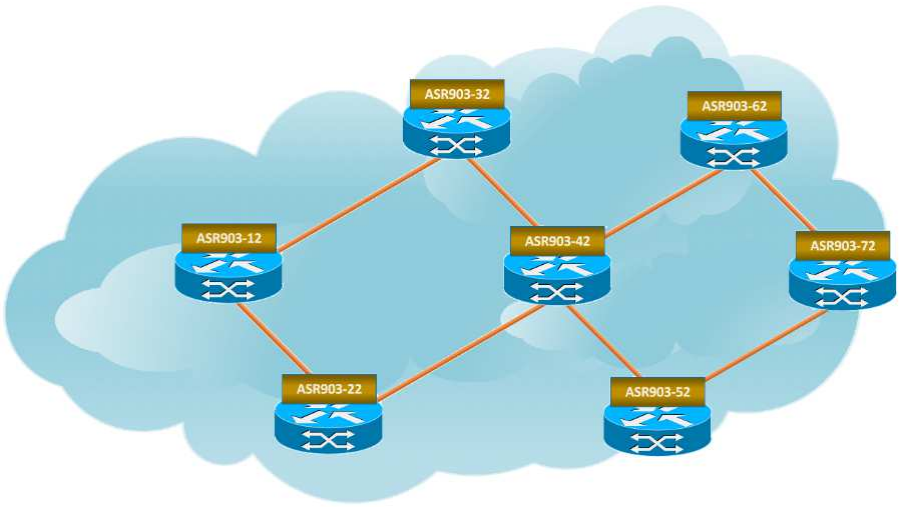

Figura 4.1 – Arquitetura implementação do *backbone* da EEM.

Outra estratégia que a EEM definiu foi implementar uma hierarquia colapsada, em que todos os níveis permitem acesso à rede. Foi instalado o mesmo tipo de equipamento nos diferentes níveis hierárquicos apenas com processadores diferentes. Assim, a eficiência do *core* sofre uma pequena redução na sua eficiência devido à dupla função (comutar por rótulo e adicionar rótulos). O ideal seria o *core* ser dedicado apenas para a troca de rótulos.

Na implementação da rede "WAN SCADA" foram utilizados *routers provider edge* (PE) e *customer provider edge* (CPE). Este foram instalados nas 36 instalações do SEPM (subestações, postos de seccionamento/corte, centrais hidroelétricas e Centro de Despacho).

4.1 A necessidade de migrar para a rede MPLS

As primeiras versões das aplicações SCADA necessitavam de modelos de comunicação centralizados, que estabelecia ligações ponto-a-ponto com as subestações, recorrendo a tecnologia *plesiochronous/sinchronous digital hierarchy* (PDH/SDH), baseada no método de multiplexagem por divisão temporal. Refira-se que durante um período de 12 anos, a tecnologia PDH/SDH satisfez as necessidades de transporte de telecomunicações da EEM. Mas, com a demanda atual, passou a haver dificuldades de mapeamento de tráfego devido ao facto de a largura de banda estar no seu limite. O mapeamento é abordado no ponto "*Princípio da multiplexagem na tecnologia SDH*" do "*Apêndice 3 – Arquitetura Hierarquia Digital Síncrona*". A rede PDH/SDH provou, ao longo de vários anos, que era, e ainda é, fiável, confiável e segura. Mas não é nem robusta, nem eficiente, nem flexível.

Antes da migração, a rede PDH/SDH suportava os serviços de telecomando, teleproteção das linhas de alta e média tensão (AT/MT), monitorização da qualidade da onda, telecontagem das subestações, e disponibilizava a rede corporativa. As "linhas AT/MT" são designações utilizadas para distinguir as diferentes redes de energia conforme a potência elétrica que transportam. A substituição da tecnologia PDH/SDH tinha que garantir à EEM que satisfazia os seguintes requisitos: *(i)* garantia uma elevada resiliência da rede; *(ii)* facilidade de migração no suporte aos serviços *legacy* (tradicionais); *(iii)* isolamento de tráfego; *(iv)* ser suportada por uma estrutura unificada e convergente; *(v)* permitir serviços críticos; *(vi)* ser barata; e *(vii)* permitir uma gestão centralizada.

Para satisfazer estes requisitos, o MPLS dispõe de algumas características, destacando-se a elevada disponibilidade (*high availability*, HA) e elevada resiliência da rede, por utilizar estes diferentes mecanismos: *(i) nonstop forwarding* (NSF); *(ii) stateful switchover* (SSO); *(iii) nonstop routing* (NSR); *(iv) fast rerouter*; *(v) link aggregation group* (LAG). Note-se que o NSF, também designado por *graceful restart* (GR).

Por forma a garantir níveis de confiança elevados junto dos seus consumidores, a EEM preparou a sua nova rede de telecomunicações para suportar tráfego gerado pelos seguintes desenvolvimentos tecnológicos: *(i)* SCADA EMS/(A)DMS; *(ii)* AMI*;* e *(iii)* novos dispositivos IED. Estas diferentes tecnologias necessitam de uma rede de telecomunicações multisserviços que suporte uma grande largura de banda, as comunicações devem ser bidirecionais, com baixa latência, e baseadas em dois pilares fundamentais: segurança e redundância. A segurança da rede no mundo de hoje, apesar de importante, não tem definições, principalmente quando se trata de segurança empresarial, pois não se sabe de quem se pretende proteger. Mas, na EEM, e devido a essência da sua atividade, esta é uma questão central e que não é descurada. Apesar de ser um assunto de extrema importância, mas por fugir ao âmbito deste trabalho, não será desenvolvido.

Devido aos valores de investimento envolvidos no processo de migração, a solução foi implementada faseadamente. Assim, a implementação começou com um projeto piloto, permitindo a coexistência das duas tecnologias por forma a que não ocorresse um grande impacto nos serviços em funcionamento. A solução adotada foi do MPLS que permite acompanhar a demanda por largura de banda, oferece um custo por *bit* muito inferior ao oferecido pela tecnologia de comutação por circuito e com a mesma qualidade de serviço *(quality of service, QoS)*. A QoS mede o conjunto de informações que definem o desempenho da rede, utilizando seis métricas essenciais: *(i)* largura de banda; *(ii)* perdas de informação; *(iii)* atrasos na propagação; *(iv)* atrasos ondulatórios (*jitter)*; *(v)* erros; e *(vi)* disponibilidade da rede. O *jitter* é a

variação no tempo atrasado e na sequência com que os pacotes são entregues, provocada pelos nós da rede.

Uma das características do método de transmissão TDM é que a informação da rede elétrica está centralizada num único Centro de Despacho, podendo, numa situação crítica, o SEPM ficar sem controlo. Nota-se que se entende como uma possível situação critica a destruição das instalações. Essa nova arquitetura, associada à utilização de mais do que um *datacenter*, permite que o Centro de Despacho possa ser implementado em qualquer lugar e muito rapidamente.

A eficácia do MPLS assenta num sistema de telecomunicações com conetividade multiponto e considera as seguintes características essenciais: *(i)* escalabilidade; *(ii)* fiabilidade; *(iii)* robustez; *(iv)* eficiência; *(v)* flexibilidade; e *(vi)* confiabilidade. É extraordinariamente escalável, sendo fácil garantir o crescimento exponencial do sistema. A fiabilidade garante um serviço estável (contínuo). A robustez diz respeito a margens de segurança, com soluções redundantes. A robustez garante operacionalidade da rede em condições adversas como: *(a)* carga elevada ou mesmo congestionamento; *(b)* interrupções (temporárias ou persistentes); e *(c)* avarias de equipamentos, implementações deficientes ou incorretas. A eficiente visa obter taxas de erros quase nulas. A flexibilidade permite segmentar a rede, com base em critérios lógicos e não físicos. O ser muito flexível, permite combinar diferentes métodos de transmissão (*legacy* e IP), ao mesmo tempo que permite a implementação das novas aplicações. A confiabilidade relaciona a alta disponibilidade da rede na entrega dos pacotes.

O MPLS fornece recursos inigualáveis à otimização da rede de telecomunicações da EEM, pois possibilita a gestão a partir de uma única plataforma. Permite maximizar a rentabilidade, tanto no aspeto económico, como no técnico, das infraestruturas com um aumento exponencial no seu desempenho e ser extraordinariamente escalável. Esta nova tecnologia utiliza toda a infraestrutura física de transporte existente, em fibra ótica, mitigando assim os custos de implementação associados à adoção de novas tecnologias.

4.2 Implementação da rede hierárquica

A implementação da rede hierárquica baseou-se em três níveis fundamentais, diferenciados pela necessidade de largura de banda e capacidade de processamento. Da mesma forma, a topologia da rede e o dimensionamento dos elementos de rede implementados na rede “WAN SCADA” refletem esta hierarquia dos fluxos de tráfegos.

A escolha que definiu o posicionamento na rede para a instalação do *core* foi a localização dos três *datacenters* (dois principais e um alternativo aos dois principais). Os dispositivos de *core* comunicam entre si, inicialmente, a 10 Gbps, podendo, além disso, expandir em múltiplos de 10 Gbps e de forma redundante. A camada de agregação agrupa o tráfego dos diferentes anéis da camada de acesso (instalações adjacentes). A camada de agregação liga-se ao *core* com ligações de 10 Gbps e de forma redundante. A camada de acesso é composta pelas restantes instalações ligadas em anel, ou linear, à camada de agregação. Na camada de acesso a largura de banda é de 1 Gbps.

A implementação do *core* na rede “WAN SCADA” considera as necessidades de transporte de todo o tráfego, para permitir: *(i)* aquisição de dados e controlo para o, e do, SCADA; *(ii)* implementar esquemas de proteção de integridade do sistema; *(iii)* serviço “teleproteção”; *(iv)*

segurança física às instalações (controle de acesso e câmaras de videovigilância); *(v)* acesso remoto para o trabalhador (comunicações de voz, sistemas de mapeamento de informações geográficas, localização remota, gestão dos recursos humanos em campo); *(vi)* aquisição de informação ambiental das subestações (temperatura, estado da bateria, velocidade do vento, etc.); *(vii)* disponibilizar serviços a infraestruturas de medição avançada; *(viii)* tráfego empresarial (dados corporativos, correio eletrónico, ferramentas de colaboração, operações comerciais).

A rede "WAN SCADA" suporta os antigos serviços operacionais, também designados por serviços *legacy* (tradicionais), tais como as redes de comunicação para: *(i)* o telecomando; *(ii)* as teleproteções das linhas de AT/MT; e *(iii)* o comando e controlo dos parques eólicos. A Figura 4.2 ilustra a arquitetura de referência utilizada pela EEM na implementação da rede hierárquica:

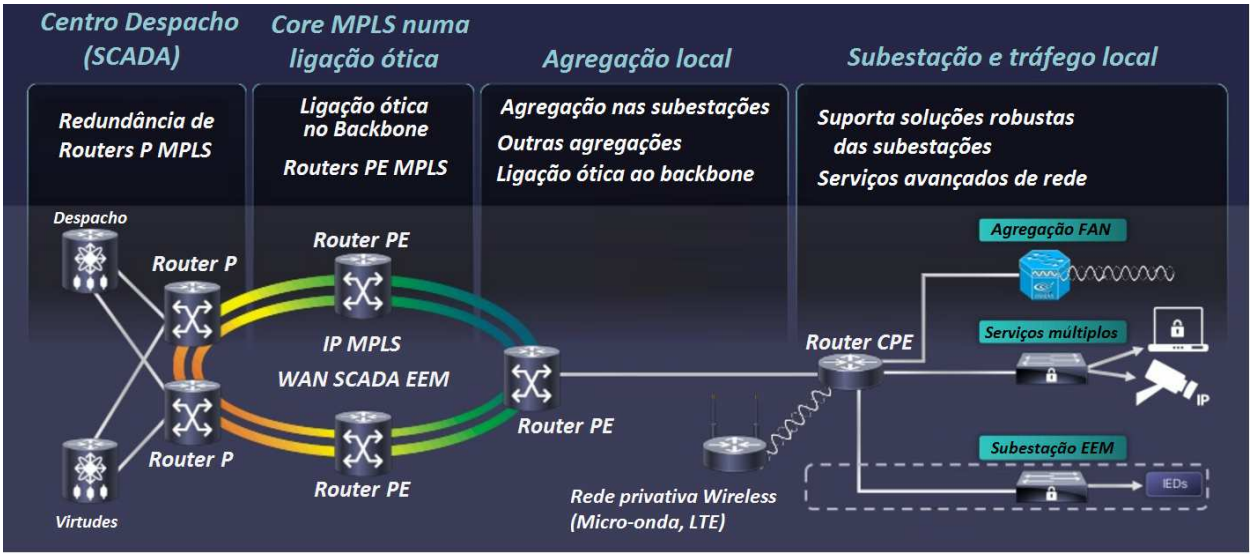

Figura 4.2 – Arquitetura de referência para a rede "WAN SCADA" *[4.2-1]*.

A arquitetura do transporte do tráfego baseia-se em três níveis fundamentais: *(i)* tráfego entregue aos diversos *datacenters* da EEM; *(ii)* tráfego que circula no *backbone*; e *(iii)* tráfego de acesso (*on-net substation e field area network*). O CPE instalado nas infraestruturas permite o acesso à rede "WAN SCADA" da EEM aos diversos serviços existentes nas subestações e postos de secionamento, como os serviços da agregação *field area network* (FAN), serviços múltiplos e subestações. A FAN, é a designação dada à rede de acesso por Wifi e *endpoints* existentes numa infraestrutura, garante a integridade da rede, fornecendo assim um acesso seguro e privacidade dos dados. Os *endpoint* podem ser: *(a)* terminais VoIP; (*b)* os dispositivos que monitorizam os transformadores; *(c)* dispositivos que comunicam com os carregadores dos carros elétricos; ou *(d)* sistemas que controlam a iluminação pública. A rede Wifi permite a introdução da mobilidade do funcionário EEM.

Nível de core

Para o transporte de todo o tráfego da rede "WAN SCADA", proveniente das subestações, foram utilizados equipamentos de elevada capacidade de processamento. O tráfego gerado pelas subestações é entregue a dois *datacenters* (primários): *(i)* o *datacenter* operacional, onde estão

alojados os servidores relativos aos serviços operacionais, servidores do serviço “SCADA”, servidores de telemetria, servidores de medida de qualidade de onda; e *(ii)* o *datacenter* corporativo, onde estão alojados os servidores relativos aos serviços corporativos da EEM, *webmail*, e *proxy-server* para acesso à *internet*.

A Figura 4.3 ilustra a solução implementada da rede “WAN SCADA”, onde é possível distinguir os principais elementos de rede.

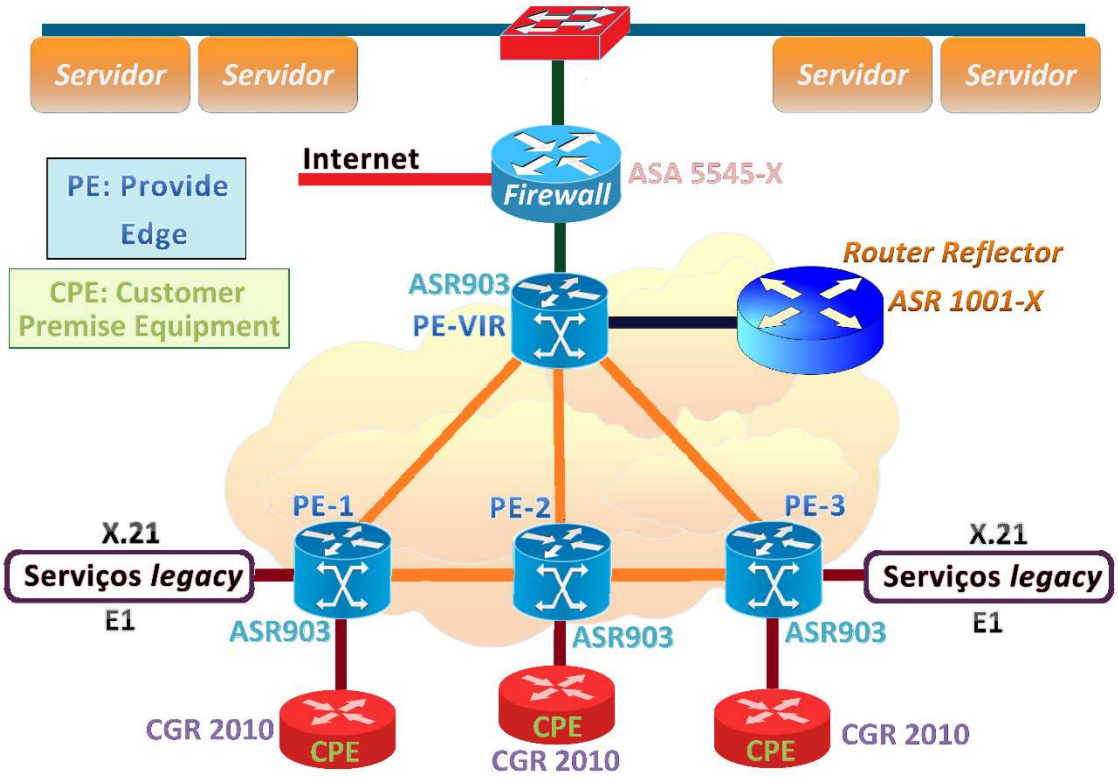

Figura 4.3 – Arquitetura hierárquica implementada na rede “WAN SCADA”.

O *router* “P-1” representa o *backbone* da rede “WAN SCADA”. Os *routers* “PE-1”, “PE-2” e “PE-3” são o que garantem aos *routers* CPE (Cisco CGR 2010) o acesso ao *backbone* MPLS. O *router* CGR 2010 é abordado no na seção "*12.3 - Dispositivo Cisco Connected Grid Router (CGR 2010)*" do apêndice 7. Note-se que na rede “WAN SCADA”, e por questões meramente económicas, a EEM optou por implementar uma hierarquia colapsada, daí os *routers* P e PE também serem utilizados para fornecer o acesso ao *backbone* MPLS. Todos os *routers* P e PE garantem serviços *legacy*. O *route reflector* permite realizar sessões com todos os *routers* existentes no *backbone* MPLS, para construir a malha completa virtual. Todo o tráfego é canalizado para a *firewall*, que faz fronteira com os servidores e o serviço internet, para ser inspecionado *[4.2-2]*.

Nível de agregação

A nível de agregação foram utilizados equipamentos de menor capacidade de processamento do que os utilizados no nível de *core*. Este nível de agregação é responsável pela agregação do

tráfego proveniente das subestações em locais específicos da rede, que é depois entrega ao nível de *core*.

Nível de acesso

O terceiro nível é o de acesso local, com equipamentos de baixa capacidade de processamento, e recebe todo o tráfego (LAN) da subestação (*on-net substation e field area network*). Este nível permite a ligação direta aos equipamentos das subestações, nomeadamente aos concentradores de dados local *(remote terminal unit*, RTU), *intelligent electronic device* (IED), equipamentos de telecontagem, IP CCTV, etc. Será também responsável por assegurar os mecanismos de segurança ao nível da subestação.

Na subestação, a rede LAN é constituída pelo barramento de serviços operacionais e barramento de serviços múltiplos. O barramento de serviços operacionais é um dispositivo que possibilita a comunicação entre os diversos elementos operacionais instalados nas subestações. O barramento de serviços múltiplos é um dispositivo que possibilita o serviço *ethernet* nas subestações.

4.3 Topologia da rede

A topologia da rede "WAN SCADA" é constituída por vários anéis que interligam os dispositivos das subestações, terminando, sempre que possível, em dois dispositivos de agregação diferentes, para garantir a redundância de ligação física. Na rede "WAN SCADA" não foi utilizado o conceito de "área", conforme ilustrado na Figura 4.4, mas sim o conceito de sistema autónomo (*autonomous system*, AS).

Áreas OSPF

A Figura 4.4 ilustra o conceito de "áreas" OSPF permite mais eficiência no encaminhamento ao protocolo *open shortest path first* (OSPF), pois permite a sumarização dos prefixos de rede. Esse conceito permite reduzir a dimensão das tabelas de encaminhamento, pois com apenas um registo (índice de consulta na tabela RIB) é possível encaminhar vários prefixos de rede, caracterizados por serem sequenciais (agrupadas).

No entanto, no MPLS, a sumarização dos prefixos de rede gera um problema no plano de controlo (do MPLS), pois gera problemas com a distribuição de rótulos. Como no MPLS há um rótulo RD por cada prefixo de rede VPN-IPv4, ao se optar pela sumarização das várias rotas, só um VRF é que irá receber. Daí, na construção da rede "WAN SCADA", a EEM optou por não utilizar o conceito de áreas.

Assim, e considerando a Figura 4.4, para encaminhar pacotes para a rede 10.1.2.24 (associada ao *router* D) basta encaminhar para os prefixos de rede 10.1.2.0 /24. Qualquer *host* de outras áreas, consegue enviar os seus pacotes ao *router* D, utilizando o *router* de fronteira (*area border router*, ABR) que interliga a área 0, obrigatória, e a área 2. O mesmo acontece com os prefixos de rede 10.1.3.0 /24, em que os pacotes chegam ao *router* de fronteira ABR que interliga a área 0 e a área 3. Este raciocínio aplica-se às outras áreas, sempre considerando prefixos de rede sequências na mesma área.

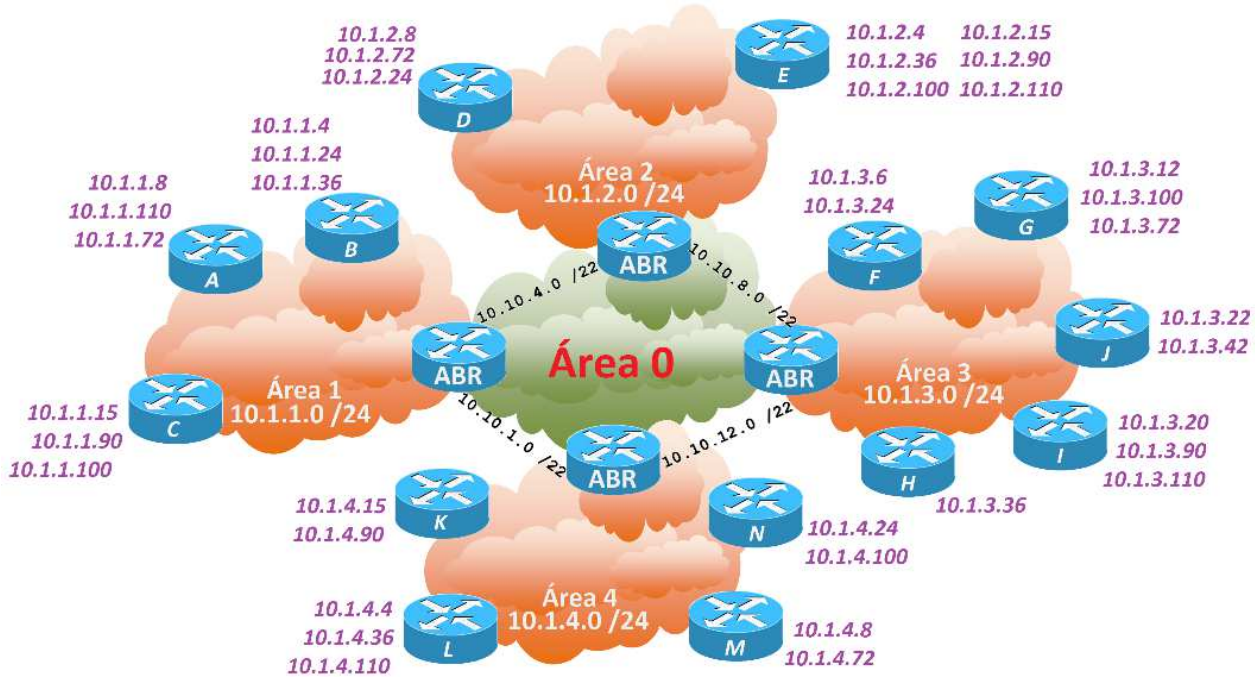

Figura 4.4 – Conceito de "área" no IGP *Link State*.

Sistema autónomo

Designa-se "sistema autónomo" ao grupo de *routers* com a mesma política de encaminhamento, que utiliza o mesmo protocolo de encaminhamento (IGP) e é gerida pela mesma entidade. A Figura 4.5 ilustra a topologia da rede "WAN SCADA" da EEM que está implementada, onde é possível distinguir os diferentes elementos de rede essenciais e os sistemas autónomos a que estão associados.

Foram seguidas diversas regras de construção de rede, de que se destacam as seguintes: *(i)* um servidor/*datacenter* nunca liga a um agregador. É sempre a um *router* CPE, porque a troca de tráfego entre um servidor e um dispositivo de rede é realizado ao nível da camada 2 do modelo OSI; *(ii)* o *Identity Services Engine* (ISE), por ser uma aplicação instalada num servidor (UCS 220 3515), não pode ser ligado ao *router* ASR903; *(iii)* aos *routers* "ASR903-VIR" / "ASR903-FUN" / "ASR903-DES" chegam tráfegos transportados pelas diferentes VPN-IPv4 e estes são entregues às *firewalls* (Cisco ASA 5545-X) em diferentes VLAN. A *firewall* não reconhece a instância VRF *lite*, daí a necessidade de enviar o tráfego numa VLAN para se ter o tráfego segmentado. Depois a *firewall* reenvia esse tráfego inspecionado para o *router* PE da rede "WAN SCADA" (pode ser o mesmo ou não) mas noutra VLAN. O tráfego de cada VPN é mapeado (associado) à sua própria VLAN; *(iv)* tanto o porto do ASR903 que envia o tráfego para a *firewall*, como o porto da *firewall* que o recebe devem de ter IP estático. O IP estático permite encaminhar o tráfego para o porto correto. A *firewall* protege as subestações e não o *datacenter*, pois o *datacenter* tem o seu próprio mecanismo de defesa.

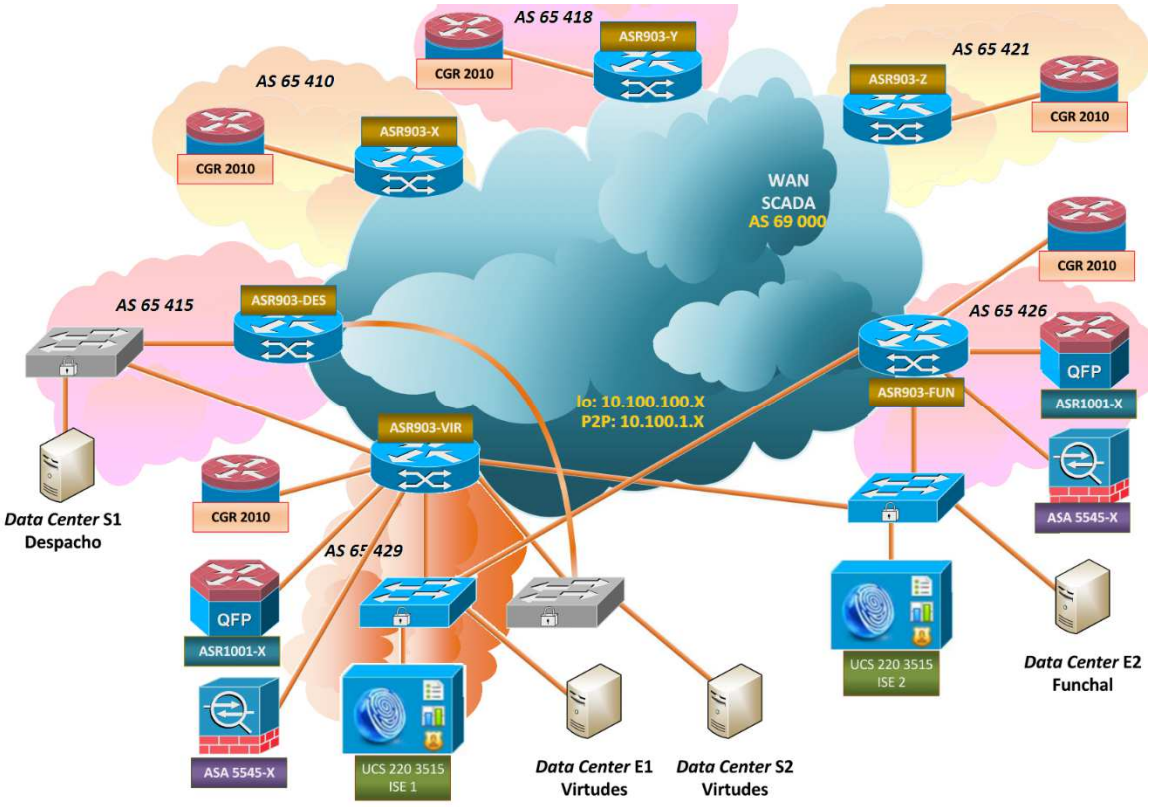

Figura 4.5 – Distribuição dos elementos de rede implementada na EEM.

4.4 Convenção para nomear as instalações

É reconhecido nos *guide line* do fabricante como boa prática utilizar uma convenção para normalizar a atribuição de uma referência aos elementos de rede. A Tabela 4.1 apresenta alguns nomes das instalações e as respetivas abreviaturas (acrónimo) que ajudaram a construir uma referência a atribuir aos elementos de rede instalados.

Nome da instalação	Acron	Nome da instalação	Acron	Nome da instalação	Acron
Central Hidrica Ribeira Janela	RDJ	SE Calheta 30	CTS	SE Ponte Vermelha	PVM
Central Hidrica Serra Água	SDA	SE Calheta 60	CTA	SE Prazeres	PRZ
Central Hidrica Socorridos	SCR	SE Caniçal	CNL	SE Santa Quitéria	SQT
SE Aeroporto	AEP	SE Meia Serra	MSR	SE Vitória 60	V60
SE Alegria	ALE	SE Palheiro Ferreiro	PFE	SE Viveiros	VIV

Tabela 4.1 – Acrónimos do nome de algumas instalações.

E respeitando a regra de atribuição de referências aos elementos de rede, foi construída a Tabela 4.2, onde é apresentada parte dos nomes dos dispositivos presentes na rede “WAN SCADA”.

Nome da instalação	Função	I	Nome	Função	I	Nome	Função	I	Nome
Central Hidrica Ribeira Janela	PE	1	RDJ-PE-01	CE	1	RDJ-CE-01	CE Switch	1	RDJ-SW-01
Central Hidrica Serra Água	PE	1	SDA-PE-01	CE	1	SDA-CE-01	CE Switch	1	SDA-SW-01
Despacho	CORE	1	DES-CORE-01						
Emacom FX	CORE	1	FCH-CORE-01	CE	1	FCH-CE-01	CE Switch	1	FCH-SW-01
SE Amparo	PE	1	AMP-PE-01	CE	1	AMP-CE-01	CE Switch	1	AMP-SW-01
SE Virtudes	CORE	1	VIR-CORE-01	CE	1	VIR-CE-01	CE Switch	1	VIR-SW-01

Tabela 4.2 – Lista de alguns nomes atribuídos aos dispositivos existentes na rede "WAN SCADA".

4.5 Configurações gerais dos portos

Sem as configurações gerais dos portos não é possível ocorrer a troca de pacotes entre dispositivos ligados fisicamente entre si. Para garantir a conetividade no *backbone* foram implementados dois tipos de *interfaces* SFP: *(i)* 10 Gbps, no estabelecimento da ligação entre os *routers* P com os *routers* PE (P-PE) e configuradas com L3/MPLS; e *(ii)* 1 Gbps, no estabelecimento da ligação entre os *routers* PE (PE-PE), *router* PE com os *routers* CE (PE-CE), e configuradas com L3/MPLS. A designação "L3/MPLS" deve-se ao fato de não se poder ter VPLS (L2). A *interface* de ligação, tem que reconhecer o protocolo OSPF e o MPLS. Note-se que os portos FE dos elementos de rede são todos "*aware*", ou seja, não são transparentes. Ser "*aware*" obriga a que os portos FE verifiquem sempre o rótulo dos pacotes *ethernet* que chegam ao porto de acesso.

MTU no *core* e no *edge*

É obrigatório configurar a dimensão da MTU nos portos num valor máximo exequível. Foram analisados os portos de 1 e de 10 *gigabit ethernet* da série ASR900, dos CGR 2010. Estes equipamentos são abordados na seção "*12.1 – Dispositivo Cisco Aggregation Services Router 903*" e "*12.3 - Dispositivo Cisco Connected Grid Routers*" do apêndice 7. A capacidade da MTU da série ASR900 é de 9216 octetos, mas no módulo de *ethernet* dos CGR 2010 é de 9000. Dado o elevado número de tipos de encapsulamento que podem ser utilizados, é difícil prever com exatidão a dimensão da MTU. Além disso, como os futuros serviços podem exigir uma dimensão mais elevada que a atual, a EEM optou por configurar, em todos os portos dos dispositivos, uma dimensão fixa que é suportada em todos os elementos de rede: 9000 octetos.

4.6 IP estáticos

A rede "WAN SCADA" necessita de IP estáticos, para gerir os elementos de rede e os serviços, e o espaço de endereçamento disponível para a nova rede EEM é baseado no intervalo de endereços RFC1918. O documento RFC1918 normaliza como os endereços privados podem ser atribuídos. A EEM definiu duas redes de classe B e por motivos de segurança por este documento ser público, essas referências foram omitidas neste documento e foram substituídas pelas redes: 13.68.0.0 /16 e 13.68.1.0 /16.

A EEM utilizou três *subinterface* atribuídas ao IPLB: *(i)* 0 (zero); *(ii)* 10; e *(iii)* 100. O IPLB zero é utilizado pelo IGP na construção da tabela de estado de ligação (*link-state database*, LSDB). Os IPLB 10 e IPLB100 servem para segmentar os tráfegos da sincronização (*precision time protocol*, PTP) e da gestão. O Exemplo de código 2 é reconhecido nos *guide line* do fabricante como boa prática para atribuir um identificador ao *router*, em que é atribuído ao identificador "*router ID"* o IPLB 13.68.1.03 /32, no processo (*process id*) 100 da área 0.

```
interface Loopback0
 ip address 13.68.1.08 255.255.255.255
 ip ospf 100 area 0
```

Exemplo de código 2 – Atribuição de um identificador ao *router* (IPLB0).

O *Precision Time Protocol*, PTP, é utilizado como relógio de elevada precisão, sendo por isso necessário que esse tráfego tenha o seu próprio VRF (PTP). Para o *Syslog* essa informação não exige esse elevado valor de precisão, e é por isso utilizado o relógio NTP, com a informação transportada pelo VRF de gestão dos elementos de rede (VRF "IB_MGMT").

A Figura 4.6 ilustra as diversas *subinterfaces* IPLB atribuídos à alguns elementos de rede de que é constituída a rede "WAN SCADA". O endereço IP, com máscara /30, também é utilizado para definir a sub-rede que permite o transporte de tráfego entre dois *routers* vizinhos. Neste exemplo, a zona assinalada pelo ponto 1 define a rede que interliga ao *router* PE "ASR903-SE" e o *router* CPE CGR 2010, designado por *attachment circuit*. A zona assinalada pelo ponto 2 define as 2 redes *(inside* e *outside*) que interligam o *router* PE "ASR903-VIT" e a *firewall* da Vitória. A zona assinalada pelo ponto 3 define as duas redes *(inside* e *outside*) que interligam o *router* "ASR903-VIR" (PE) e a *firewall* das Virtudes. A zona assinalada pelo ponto 4 define as quatro redes que interligam os *routers* PE "ASR903-VIT" e "ASR903-VIR" e os dois *routers* CPE ISR 4431, um instalado na Vitória (Centro de Despacho) e outro nas Virtudes. A zona assinalada pelo ponto 5 define *backbone* "WAN SCADA". Os pontos 7 a 13 identificam os IPLB configurados nos diversos elementos de rede. Os elementos de rede ASR 1001-X e o datacenter do Funchal não estão representados. Todos os elementos de rede de cada *datacenter* estão inseridos no seu sistema autónomo.

A Tabela 4.3 ilustra parte dos IPLB0 atribuídos para a gestão dos elementos das redes. O IPLB10 permite ao *router* trocar tráfego de sincronismo, utilizando o VRF "PTP", pois é o seu IP de destino. Este assunto é abordado na seção "*4.10 – Sincronização da rede*". Ao identificador "*router ID"* também é atribuído o IPLB100 para que o administrador da rede possa alcançar o *router*, via SSH e utilizando o VRF "IB_MGMT". O VRF "IB_MGMT" permite segmentar o tráfego e o IPLB100 permite sessões rápidas. As outras VRF conhecidas no domínio "WAN SCADA" não precisam do IPLB, pois o tráfego é trocado para "fora" dos dispositivos.

A Tabela 4.4 ilustra parte dos IPLB10 (PTP) atribuídos aos *routers* PE para a sincronização. Esta sincronização com elevada precisão, PTP, é utilizada para fornecer o sincronismo ao protocolo X.21, associado ao serviço "teleproteção", que é uma sinalização crítica para o bom funcionamento do SEPM. Para o *Syslog*, é utilizado o relógio NTP, informação transportada pelo VRF "IB_MGMT".

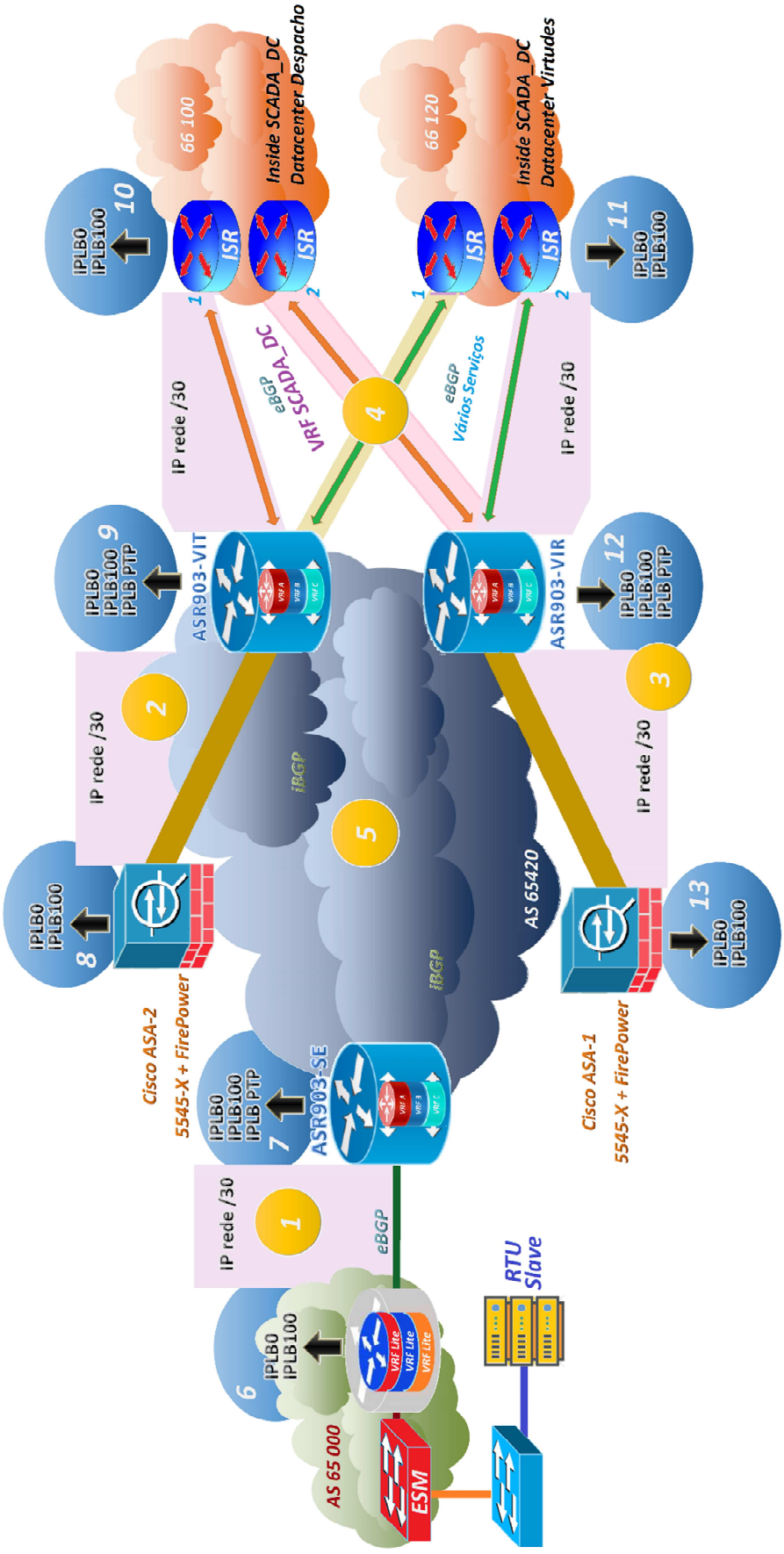

Figura 4.6 – Distribuição da *subinterface* IP *loopback* e de sub-redes.

Tipo	Sub-Tipo	Nº Site	Nome	Hostname	Descrição	IP	Mask	Rede
Loopback 0						13.68.0.0	/32	10.28.0.0
Loopback 0	CORE	1	Edificio 1	ED1-CORE-01	*** Loopback 0 ***	13.68.0.1	/32	13.68.0.1
Loopback 0	CORE	2	Edificio 2	ED2-CORE-01	*** Loopback 0 ***	13.68.0.2	/32	13.68.0.2
Loopback 0	CORE	10	Edificio 3	ED3-CORE-01	*** Loopback 0 ***	13.68.0.3	/32	13.68.0.3
Loopback 0	RR	1	Edificio 1	ED1-RR-01	*** Loopback 0 ***	13.68.0.4	/32	13.68.0.4
Loopback 0	RR	2	Edificio 2	ED2-RR-01	*** Loopback 0 ***	13.68.0.5	/32	13.68.0.5
Loopback 0	AGGREGATOR	6	Subestação 1	SE1-AGG-01	*** Loopback 0 ***	13.68.0.20	/32	13.68.0.20
Loopback 0	AGGREGATOR	3	Subestação 2	SE2-AGG-01	*** Loopback 0 ***	13.68.0.21	/32	13.68.0.21
Loopback 0	AGGREGATOR	7	Subestação 3	SE3-AGG-01	*** Loopback 0 ***	13.68.0.22	/32	13.68.0.22
Loopback 0	PE	24	Subestação 4	SE4-PE-01	*** Loopback 0 ***	13.68.0.40	/32	13.68.0.40
Loopback 0	PE	37	Subestação 5	SE5-PE-01	*** Loopback 0 ***	13.68.0.41	/32	13.68.0.41
Loopback 0	PE	38	Subestação 6	SE6-PE-01	*** Loopback 0 ***	13.68.0.42	/32	13.68.0.42
Loopback 0	CE	2	Edificio 2	ED2-CE-01	*** Loopback 0 ***	13.68.0.100	/32	13.68.0.100
Loopback 0	CE	24	Subestação 4	SE4-CE-01	*** Loopback 0 ***	13.68.0.101	/32	13.68.0.101
Loopback 0	CE	37	Subestação 5	SE5-CE-01	*** Loopback 0 ***	13.68.0.102	/32	13.68.0.102
Loopback 0	CE Switch	2	Edificio 2	ED2-SW-01	*** Loopback 0 ***	13.68.0.178	/32	13.68.0.178
Loopback 0	CE Switch	24	Subestação 4	SE4-SW-01	*** Loopback 0 ***	13.68.0.179	/32	13.68.0.179
Loopback 0	CE Switch	37	Subestação 5	SE5-SW-01	*** Loopback 0 ***	13.68.0.180	/32	13.68.0.180

Tabela 4.3 – Lista dos identificadores IPLB0 utilizados na rede "WAN SCADA".

Tipo	Sub-Tipo	Nº Site	Nome	Hostname	Descrição	IP	Mask	Rede
Loopback PTP						13.68.1.0	/32	10.28.1.0
Loopback PTP	CORE	1	Edificio 1	ED1-CORE-01	*** Loopback PTP ***	13.68.1.1	/32	13.68.1.1
Loopback PTP	CORE	2	Edificio 2	ED2-CORE-01	*** Loopback PTP ***	13.68.1.2	/32	13.68.1.2
Loopback PTP	CORE	10	Edificio 3	ED3-CORE-01	*** Loopback PTP ***	13.68.1.3	/32	13.68.1.3
Loopback PTP	AGGREGATOR	6	Subestação 1	SE1-AGG-01	*** Loopback PTP ***	13.68.1.20	/32	13.68.1.20
Loopback PTP	AGGREGATOR	3	Subestação 2	SE2-AGG-01	*** Loopback PTP ***	13.68.1.21	/32	13.68.1.21
Loopback PTP	AGGREGATOR	7	Subestação 3	SE3-AGG-01	*** Loopback PTP ***	13.68.1.22	/32	13.68.1.22
Loopback PTP	PE	24	Subestação 4	SE4-PE-01	*** Loopback PTP ***	13.68.1.40	/32	13.68.1.40
Loopback PTP	PE	37	Subestação 5	SE5-PE-01	*** Loopback PTP ***	13.68.1.41	/32	13.68.1.41
Loopback PTP	PE	38	Subestação 6	SE6-PE-01	*** Loopback PTP ***	13.68.1.42	/32	13.68.1.42
Loopback PTP	CE	2	Edificio 2	ED2-CE-01	*** Loopback PTP ***	13.68.1.100	/32	13.68.1.100
Loopback PTP	CE	24	Subestação 4	SE4-CE-01	*** Loopback PTP ***	13.68.1.101	/32	13.68.1.101
Loopback PTP	CE	37	Subestação 5	SE5-CE-01	*** Loopback PTP ***	13.68.1.102	/32	13.68.1.102
Loopback PTP	CE Switch	2	Edificio 2	ED2-SW-01	*** Loopback PTP ***	13.68.1.178	/32	13.68.1.178
Loopback PTP	CE Switch	24	Subestação 4	SE4-SW-01	*** Loopback PTP ***	13.68.1.179	/32	13.68.1.179
Loopback PTP	CE Switch	37	Subestação 5	SE5-SW-01	*** Loopback PTP ***	13.68.1.180	/32	13.68.1.180

Tabela 4.4 – Lista dos identificadores IPLB10 (PTP) utilizados na rede "WAN SCADA".

A Tabela 4.5 ilustra parte desses IP atribuídos aos serviços. São os IP que permitem entregar os diferentes tráfegos nas diferentes subestações e *datacenters*, onde também existem diferentes serviços. A sub-rede /29 é utilizada para endereçamento dos serviços que utilizam a rede "WAN SCADA".

Tipo	Sub-Tipo	Nº Site	Nome	Hostname	Descrição	IP	Mask	Rede
Datacenters	Serviço 1					13.68.2.0	/29	13.28.2.0
Datacenters	Serviço 1		ED2-FW-01	ED2-FW-01		13.68.2.1	/29	13.68.2.1
Datacenters	Serviço 1		ED2-CORE-01	ED2-CORE-01		13.68.2.2	/29	13.68.2.2
Datacenters	Serviço 1		ED1-CORE-01	ED1-CORE-01		13.68.2.3	/29	13.68.2.3
Datacenters	Serviço 1		ED3-CORE-01	ED3-CORE-01		13.68.2.4	/29	13.68.2.4
Datacenters	Serviço 2		ED2-FW-01	ED2-FW-01		13.68.2.9	/29	13.68.2.9
Datacenters	Serviço 2		ED2-CORE-01	ED2-CORE-01		13.68.2.10	/29	13.68.2.10
Datacenters	Serviço 2		ED1-CORE-01	ED1-CORE-01		13.68.2.11	/29	13.68.2.11
Datacenters	Serviço 2		ED3-CORE-01	ED3-CORE-01		13.68.2.12	/29	13.68.2.12
Datacenters	Serviço 3		ED2-FW-01	ED2-FW-01		13.68.2.17	/29	13.68.2.17
Datacenters	Serviço 3		ED2-CORE-01	ED2-CORE-01		13.68.2.18	/29	13.68.2.18
Datacenters	Serviço 3		ED1-CORE-01	ED1-CORE-01		13.68.2.19	/29	13.68.2.19
Datacenters	Serviço 3		ED3-CORE-01	ED3-CORE-01		13.68.2.20	/29	13.68.2.20
Datacenters	Serviço 4		ED2-FW-01	ED2-FW-01		13.68.2.25	/29	13.68.2.25
Datacenters	Serviço 4		ED2-CORE-01	ED2-CORE-01		13.68.2.26	/29	13.68.2.26
Datacenters	Serviço 4		ED1-CORE-01	ED1-CORE-01		13.68.2.27	/29	13.68.2.27
Datacenters	Serviço 4		ED3-CORE-01	ED3-CORE-01		13.68.2.28	/29	13.68.2.28
Datacenters	Serviço 5		ED2-FW-01	ED2-FW-01		13.68.2.33	/29	13.68.2.33
Datacenters	Serviço 5		ED2-CORE-01	ED2-CORE-01		13.68.2.34	/29	13.68.2.34

Tabela 4.5 – Lista de IP Serviços (VRF) utilizados na rede "WAN SCADA".

O Exemplo de código 3 é reconhecido como boa prática para a definição do identificador IPLB para identificar o tráfego de gestão e monitorização num *router*, encaminhando o tráfego num VRF.

```
interface Loopback100
 ip address 13.68.1.03 255.255.255.255
 ip ospf 100 area 0
```

Exemplo de código 3 – Atribuição de um IPLB para a gestão e monitorização do *router*.

O "*Loopback100"* também é utilizado para estabelecer uma sessão entre o administrador da rede e o elemento de rede, de modo a permitir que haja transferências de arquivos com o *router*. O Exemplo de código 4 ilustra uma linha de código necessária para se disponibilizar esta opção.

```
ip tftp source-interface Loopback100
```

Exemplo de código 4 – Configuração do TFTP.

A Figura 4.7 ilustra alguns dos diversos IP estáticos, com máscara de rede /30, que permitem o encaminhamento. A máscara /30 permite quatro IP de rede, pois são necessários três IP estáticos, dois para os portos físicos e um terceiro que identifica a rede a que pertence esses dois portos físicos.

O tráfego do serviço "SCADA" é encaminhado pelo CPE para o PE de acesso à "WAN SCADA" pelo attachment circuit, e cada serviço tem a sua rede de encaminhamento. O PE de acesso encaminha o tráfego até ao PE *peer* (PE das Virtudes) utilizando uma VPN-L3. O PE peer (PE da Virtudes) retira o rótulo MPLS ao pacote e encaminha o tráfego para a *firewall*, no domínio de uma arquitetura IP, para que o tráfego possa ser inspecionado. Após essa inspeção, a *firewall* encaminha o tráfego de novo para o PE das Virtudes, que adiciona um novo rótulo MPLS e encaminha o tráfego inspecionado para o PE *peer* (PE do Despacho) para se poder entregar o tráfego ao CPE do Centro de Despacho, numa outra VPN-L3. O tráfego chegando ao PE do Despacho, o rótulo é retirado e entregue ao ISR existente no Centro de Despacho.

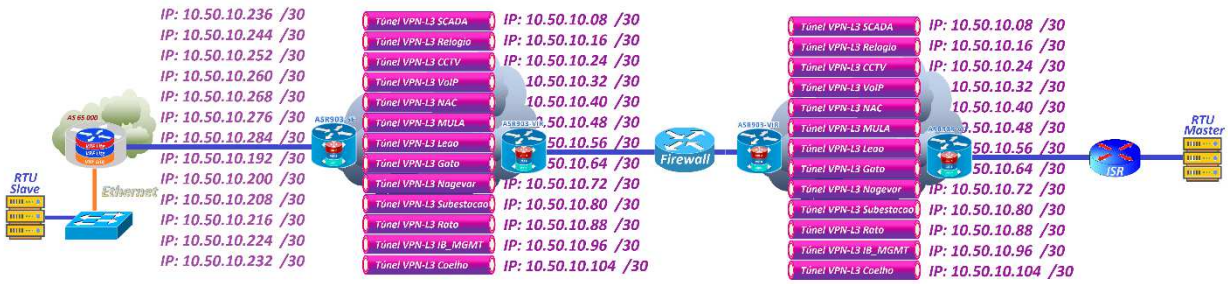

Figura 4.7 – Etapas no transporte do tráfego do serviço "SCADA" gerado pela subestação.

Neste projeto foram configurados 1448 VPN-L3 e foram reservados IP para 130 mil IP (estáticos), distribuídos por necessidades de serviços.

A Figura 4.8 ilustra três serviços, segmentados e configurados no *router* CPE "CGR 2010" em três VRF *lite*, e um deles é o serviço que transporta o tráfego entre a *RTU master* e a *RTU slave*. Na subestação, cada serviço que entra no *router* CPE "CGR 2010" tem a sua *default gateway* para o *router* PE "ASR903-X", para evitar que o *router* CPE "CGR 2010" conheça as redes que o *router* PE "ASR903-X" conhece. O dispositivo *gateway* é um intermediário entre o utilizador e a rede, e permite ligar redes diferentes (com domínios de colisão/ambiente diferentes). O dispositivo *router, firewall, proxy* e *network address translation* (NAT) são famílias de *gateways*. O *router* PE "ASR903-X" da subestação conhece todas as redes dos *datacenters*, e essa informação não interessa ao *router* CPE "CGR 2010". No *datacenter* do Despacho já não é assim, o *router* CPE "ISR 4331" informa o *datacenter* todas as redes que conhece.

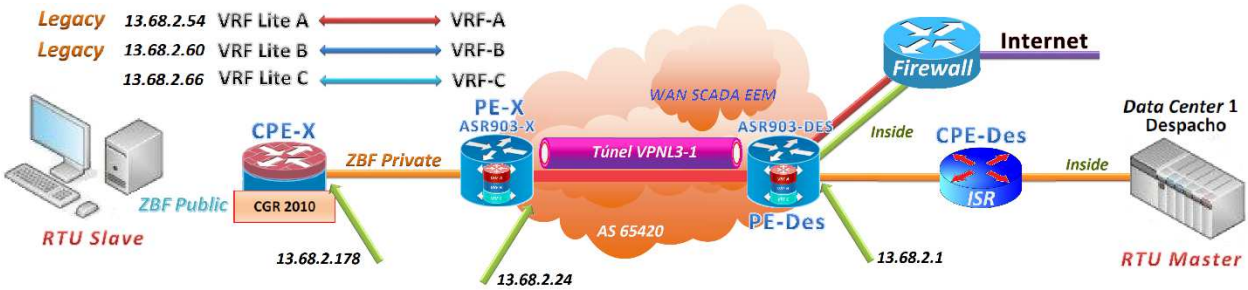

Figura 4.8 – Percurso do serviço SCADA (VRF-A).

A Figura 4.9 ilustra o mesmo serviço, mas o percurso do tráfego com origem no Centro de Despacho até à subestação "X". A *RTU master*, existente no Centro de Despacho (*Datacenter 1*), ao enviar um comando, gera tráfego que é associado à VRF-A (serviço "SCADA"). Essa instrução alcança o *router* CPE "CGR 2010" instalado na subestação "X", porque no cabeçalho do pacote está indicado que o IP de destino é "13.68.2.54". Mas, primeiro, antes de entrar na rede "WAN SCADA", o tráfego é inspecionado pela *firewall*, percurso assinalado pelo ponto "1". O ponto "2" assinala o percurso do tráfego desde que sai da *firewall* até alcançar o *router* "PE-X" existente na subestação "X", percorrendo assim a rede "WAN SCADA". Tal só é possível porque existe uma lista de acesso, no *router* PE "ASR903-VIR" das Virtudes, que valida que o tráfego pertencente a uma gama de IP de destino possa ser aceite pelo seu porto de acesso, encaminhando o tráfego que chega na "VPNL3-11" na respetiva "VPNL3-01". O ponto "3" identifica o *router* PE "ASR903-X" onde termina a "VPNL3-01". O ponto "4" identifica a instância VRF *lite* "A" que reconhece o IP de origem do pacote (RTU *master*). O ponto "5" representa o concentrador de dados local (RTU *slave*), dispositivo de destino do tráfego. O conceito *subinterface* não existe na série ASR900, do fabricante Cisco, mas sim o *bridge domain interface* (BDI). O BDI só é utilizado na comutação para o lado do *router* CPE, e nunca no domínio MPLS.

Na maioria dos *routers* PE, da rede "WAN SCADA", só existem dois prefixos de rede nas suas tabelas de encaminhamento dos VRF configurados, que permitem garantir o caminho primário e o alternativo, assim como o balanceamento de carga. Além disso, os *routers* de *core* (das Virtudes, Funchal e Despacho) e a *firewall*, conhecem a totalidade dos prefixos de rede existentes

na rede “WAN SCADA”. Este fato deve-se ao modelo de topologia *hub and spoke* utilizado e ilustrado na Figura 4.9, em que, neste exemplo, o *router* PE “ASR903-VIR” representa o *hub*.

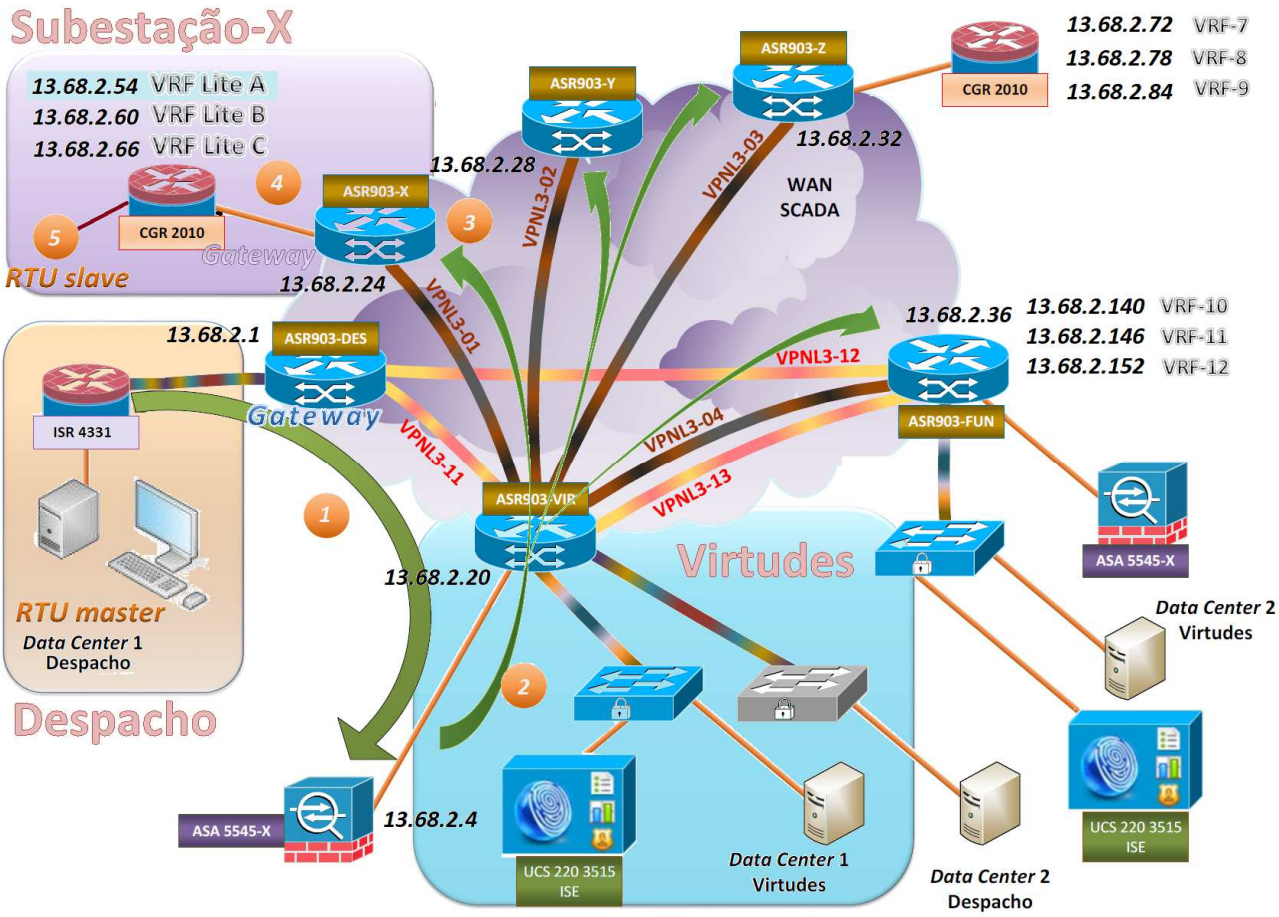

Figura 4.9 – Distribuição de IP por serviços em cada *router* CPE para a troca de tráfego.

Note se que só a firewall tem a capacidade de realizar o leaking (re-encaminhamento de pacotes IP entre VRF diferentes), pois no mesmo PE é impossível. A firewall utiliza o comando “route map” para anunciar os prefixos de rede entre a “WAN SCADA” e os *datacenters*.

O Exemplo de código 5 é reconhecido como boa prática para distinguir os prefixos de rede de outros serviço. Recorrendo à Tabela 4.7, da página 74, o serviço “MULA” tem a identificação RD “10”. O objetivo é distinguir os prefixos de rede de serviço para serviço, pois para além do serviço “MULA” dispor da rede 10.50.10.08, podem existir a mesma rede nos outros serviços que acedem ao *router* CPE.

```
ip vrf MULA
 rd 10.50.10.08:10
```

Exemplo de código 5 – Associação de um rótulo ao prefixo de rede.

O Exemplo de código 6 é reconhecido como boa prática para associar uma *interface* VLAN à instância VRF *lite* num *router* CPE. O IP 10.50.66.113 identifica o VRF associado ao serviço "MULA" no *router* PE da subestação.

```
interface VLAN 10
 description *** Serviços SUB PST – MULA  To PST077-CE-01 ***
 ip vrf forwarding MULA
 ip address 10.50.66.113 255.255.255.248
 no shutdown
```

Exemplo de código 6 – Associação da *interface* VLAN 10 à instância VRF *lite* "MULA".

O Exemplo de código 7 é reconhecido como boa prática para associar o *bridge domain interface* (BDI) ao VRF num *router* PE. O IP 10.50.10.08 identifica a instância VRF *lite* associado ao serviço "MULA" definido no *router* CPE da subestação.

```
interface BDI150
 description *** Serviços SUB PST – MULA  To PST077-CE-01 ***
 ip vrf forwarding MULA
 ip address 10.50.10.08 255.255.255.252
 ip mtu 9000
 cdp enable
  no shutdown
```

Exemplo de código 7 – Associação de uma *interface* BD ao VRF "MULA".

4.7 Auto negociação

A negociação do porto *gigabit ethernet* é ativada por padrão, não existindo a opção de o desativar. Os portos não ficam ativos se as informações trocadas, acerca dos parâmetros dos portos envolvidos, forem diferentes. O Exemplo de código 8 é reconhecido nos *guide line* do fabricante como boa prática para habilitar o mecanismo de auto-negociação nos portos dos dispositivos.

```
interface GigabitEthernet <x/x/x>
 negotiation auto
```

Exemplo de código 8 – Modelo de configuração para habilitar a auto-negociação dos portos.

4.8 Protocolo de encaminhamento

Para anunciar os prefixos de rede IPv4, para a construção da topologia do *backbone* MPLS, a EEM optou pelo protocolo de *gateway* interior (IGP) *open shortest path first* (OSPF) por ser confiável e escalável. O protocolo OSPF é confiável num contexto em que haja muitos nós de *core* implementados numa única área OSPF e é escalável pois permite futuras ampliações da rede sem preocupações em redesenhar a rede. Este protocolo dinâmico é rápido na convergência em caso de falha de nós, ou ligação, e permite reencaminhar por outro traçado dentro do *backbone*.

O protocolo OSPF constrói uma tabela de estado de ligação (*link-state database*, LSDB), que utiliza o "*Loopback0"* para garantir a conetividade aos dispositivos de rede. E, a partir desta tabela LSDB, o OSPF constrói a sua própria tabela de encaminhamento, considerando apenas o melhor caminho possível para alcançar os elementos de rede associados ao sistema autónomo.

O protocolo OSPF permite dividir uma rede completa em áreas, mas esta funcionalidade não foi utilizada. No entanto, é obrigatório definir-se a área 0. Assim, todos os *routers* da rede "WAN SCADA" fazem parte da mesma área de *backbone* do OSPF (área 0). Os testes do fabricante Cisco sugerem que não é sensato ter mais do que 300 *routers* na mesma área pois afeta a eficiência.

Na conetividade entre o *router* CPE e o *router* PE, na ligação designada por *attachment circuits* (AC), é utilizado o protocolo eBGP. Além disso, os *routers* PE não anunciam os seus prefixos de rede aos *routers* CPE (a jusante) de qualquer serviço. Os prefixos existentes no dispositivo *router* CPE são conhecidos pelo *router* PE, mas, e por motivos de segurança, o *router* CPE não conhece os prefixos de rede que o *router* PE conhece. No *router* CPE é configurado a *default gateway* como sendo o *router* PE a que está associado. Assim, o *router* CPE reencaminha todo o tráfego com um prefixo de rede não conhecido. Os prefixos existentes no *router* CPE são anunciados pelo *router* PE aos *route reflectors*. O *router* PE identifica o VRF pelo prefixo dos pacotes que chegam. Só depois deste passo é que pode haver tráfego de dados úteis na rede MPLS.

A Figura 4.10 ilustra estes dois protocolos de encaminhamento utilizados no projeto. A tabela de encaminhamento do *router* CPE fica reduzida a dois índices por serviço, que é basicamente um *gateway* padrão no sentido do PE e outro associado ao *host*. Em direção aos *route reflectors*, os *routers* PE anunciam todos os serviços (prefixos de redes) existentes nos *routers* CPE, para garantir a conetividade MPLS, tanto para o caminho principal como para o alternativo. Tem que existir um rótulo para que o pacote circule pela rede MPLS. O *router* PE sabe o prefixo de rede através da informação do *route reflector*, e o *router* LSR fica a saber o rótulo. O MPLS necessita por isso que ocorra troca de informação entre o *route reflector* e o *router* PE para assim poder criar os rótulos. Um *router* CGR é um *integrated services router* (ISR), logo existem mais funções no *router* para além do encaminhamento, e uma dessas funções é segurança.

Os *routers* de *core* e os *datacenters* terão encaminhamento estático para garantir a conetividade entre dispositivos. Ter um encaminhamento estático significa que não pode ser o OSPF a definir a rota. Assim, as rotas necessárias de cada *datacenters* são alcançadas através de encaminhamento estático, com ligações redundantes de cada *datacenter* para garantir a resiliência.

Para anunciar os prefixos de redes dos serviços (VPN-L3) a EEM optou pelo protocolo de encaminhamento BGP pelos seguintes motivos: *(i)* o BGP escala melhor, pois suporta tabelas tabela de encaminhamento de grandes dimensões, comparando com as tabelas RIB criadas pelo OSPF; *(ii)* a convergência do OSPF só é tão rápida como a do BGP se a sua tabela RIB for de pequena dimensão; e *(iii)* apesar do BGP ser mais complicado de configurar que o OSPF, pois

emprega vários atributos na determinação do melhor caminho para um datagrama, oferece mais flexibilidade e controlo nas políticas de anunciar prefixos de rotas.

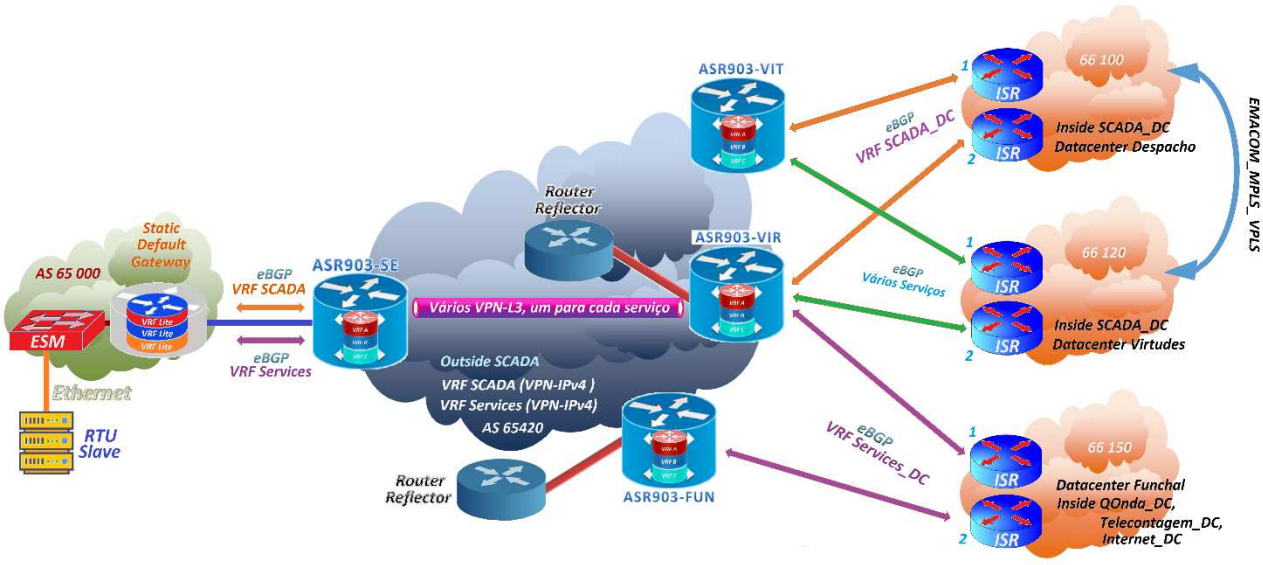

Figura 4.10 – Aspeto geral da escolha do protocolo de alto nível na rede.

O OSPF é caracterizado como um protocolo que avalia o estado da ligação e mantém atualizadas as suas tabelas de estados de ligações (*link-state database*, LSDB), e há problemas na redistribuição entre tabelas RIB diferentes.

A cada serviço existente nas diversas infraestruturas da EEM é-lhe atribuído um VRF com significado local. Cada serviço que acede à rede "WAN SCADA" necessita de ficar mapeado (associado) a um VRF.

Criação e inundação de pacotes *link-state advertisement*

Sempre que existir alteração da topologia da rede, por cada novo prefixo de rede, resulta na geração e redistribuição de pacotes LSA. Assim que o OSPF gere um novo pacote LSA este é imediatamente enviado para os *routers* vizinhos. A resposta é controlada por um temporizador para definir uma reação rápida a eventos isolados ou atrasar a reação em caso de gatilhos muito frequentes. O Exemplo de código 9 é reconhecido nos *guide line* do fabricante como boa prática para a habilitar os tempos para produzir e enviar os pacotes LSA *[4.8-1]*.

```
router ospf [process ID]
timers throttle lsa all 0 150 5000
timers lsa arrival 100
timers pacing flood 15
```

Exemplo de código 9 – Modelo de configuração tipo para habilitar o *LSA*.

O comando "*timers throttle lsa all*" controla o envio dos pacotes LSA. O primeiro pacote LSA é sempre enviado imediatamente após uma alteração de topologia OSPF, e o próximo pacote LSA

gerado é controlado pelo intervalo inicial mínimo. Os pacotes LSA subsequentes enviados para o mesmo pacote LSA são limitados por taxa até que o intervalo máximo seja atingido. O "mesmo pacote LSA" é definido como uma instância LSA que contém o mesmo número de ID LSA, tipo LSA e "*router ID*" de anúncio.

O comando "*timers lsa arrival*" controla o intervalo mínimo para aceitar o mesmo pacote LSA. Se uma instância do mesmo pacote LSA chegar antes do intervalo definido, o pacote LSA será descartado. Recomenda-se que o intervalo de chegada seja menor ou igual aoque o intervalo de tempo de espera dos temporizadores.

O comando "*timers pacing flood*" configura um atraso no temporizador para o envio de pacote de inundação (em milissegundos).

Métricas LSA durante o *Boot Up*

Por padrão, quando um *router* é ligado, conforme ilustrado na Figura 4.11, inicia o *power on self test* (POST) que é executado à partir de um código armazenado na memória ROM (memória somente de leitura).

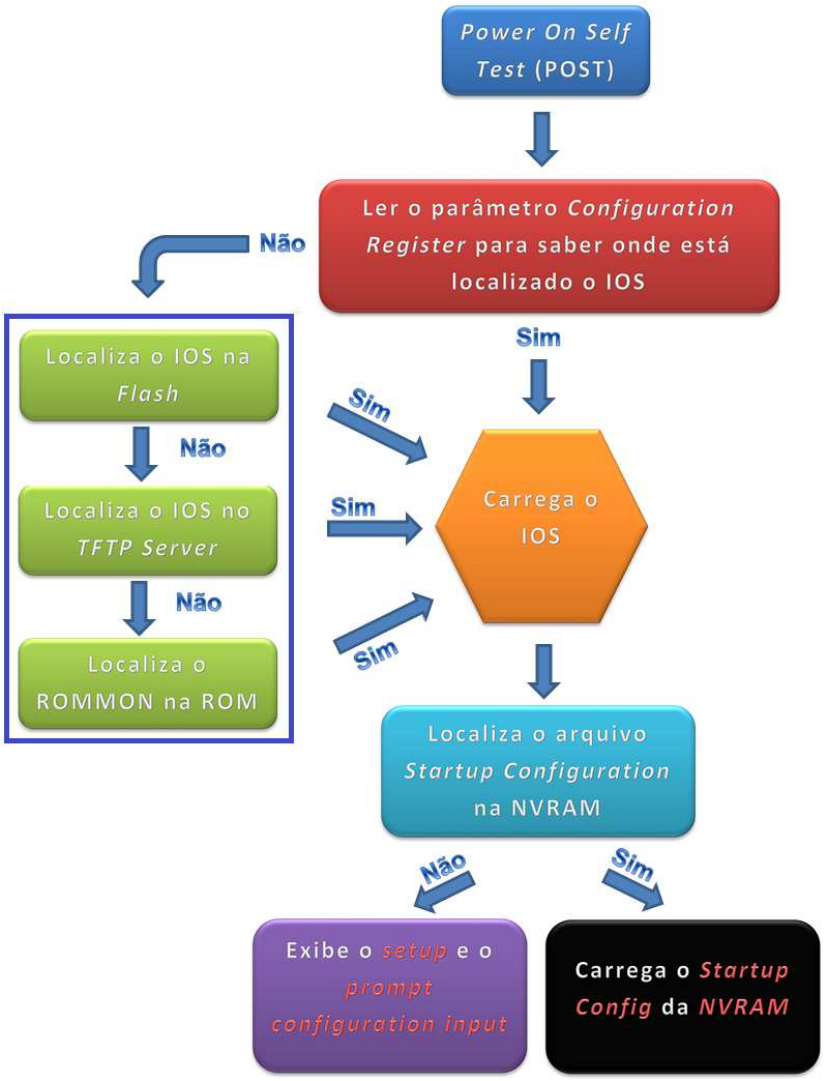

Figura 4.11 – Fluxograma de arranque de um *router*.

O POST testa o *hardware* (incluindo as *interfaces*) para verificar se todos os componentes do dispositivo estão operacionais e presentes. Se estiver tudo operacional, executa o programa de *bootstrap*.

O programa *bootstrap* é um programa armazenado na ROM, sendo responsável pelo inicializar o *hardware* e, se verificar o valor do *configuration register* com um valor padrão 0x2102 (valor hexadecimal), fica a saber da localização do IOS. O valor do *configuration register* 0x2102 permite que o *router*, utilizando o *bootstrap*, carregue a imagem do *software* do sistema operacional Cisco IOS da memória *flash* e a configuração de inicialização. Outra possível localização da imagem do IOS é um servidor *trivial file transfer protocol* (TFTP), configurada num computador. Se o programa *bootstrap* não conseguir encontrar uma imagem válida do IOS, ele atuará como *ROM monitor*. O *ROM monitor* é capaz de fornecer um ambiente de linha de comando que pode ser usado para executar certas tarefas de configuração, como baixar uma imagem do IOS usando TFTP, recuperar uma senha perdida, alterar o valor do registro de configuração, etc.

Depois do IOS estar em execução, é iniciado o processo de encontrar o arquivo de configuração válido armazenado na NVRAM. Este arquivo é chamado de *startup-config*. Se o arquivo de configuração de inicialização (*startup-config*) estiver presente na NVRAM, o *router* carregará e aplicará os comandos de configuração de início. Se não existir um arquivo válido de configuração de inicialização na NVRAM, o IOS exibirá a configuração do *system configuration*. Após carregamento do arquivo de configuração *startup-config*, o IOS apresentará a *interface* CLI no modo "*User*" (utilizador).

Concluídos estes passos, inicia-se a convergência recorrendo ao OSPF e todos pacotes de objetos descritores (*link-state advertisement*, LSA) do *router* são anunciados com métricas de ligações normais. Durante esse período, outros protocolos (como BGP, LDP, etc.) podem não ter tido tempo para convergir e, consequentemente, o tráfego pode ser descartado por um curto período de tempo. O comando "*max-metric router-lsa on-startup* <***value***>" pode ser utilizado para que um *router*, ao inicializar (*Boot up*), envie um pacote LSA com uma métrica OSPF elevada por forma a que os *routers* vizinhos não o considerem ainda na rede.

O Exemplo de código 10 é é reconhecido nos *guide line* do fabricante como boa prática para a definição da métrica no arranque.

```
router ospf [process ID or name]
 max-metric router-lsa on-startup 120
```

Exemplo de código 10 – Configuração para definir uma métrica OSPF no seu arranque.

Mecanismo *bidirectional forwarding detection*

A EEM não utilizou a deteção de falhas baseada em mensagens "*hello*", optando pelo mecanismo *bidirectional forwarding detection* (BFD), pois possibilita melhor um tempo de resposta ao mecanismo IP FRR na deteção de falhas. Para habilitar o mecanismo de deteção de falhas BFD é necessário haver comunicação *full duplex* nos portos elétricos. O Exemplo de código 11 é reconhecido nos *guide line* do fabricante como boa prática para habilitar o mecanismo BFD no OSPF. Note-se que é necessário indicar a que processo (*process ID*) OSPF pertencem estes comandos. O *Cisco IOS* suporta a configuração de múltiplos processos OSPF. Devido a isso, cada

processo OSPF habilitado no *router* requer uma identificação alfanumérica (ID). Este ID tem um significado local, logo não está incluído em nenhum anúncio (pacotes *link-state advertisement*, LSA). Além disso, é recomendável ter o mesmo ID de processo para todos os *routers* no mesmo domínio OSPF. Isso melhora a consistência da configuração e facilita as tarefas de configuração automática.

```
router ospf [process ID]
bfd all-interfaces
! On all interfaces with OSPF adjacencies must be configured for 50 milliseconds
! interval and an interval multiplier of 3
!
bfd-template single-hop <bfd template name>
interval microseconds min-tx 3300 min-rx 3300 multiplier 3
!
! Configura intervalos dos tempos, em milissegundos, para a transmissão e a
! recepção entre pacotes BFD e especifica o número de pacotes de controlo BFD
! consecutivos (3) que devem ser perdidos antes que o BFD declare que um ponto
! não está disponível
!
interface <x/y/z>
 bfd template <bfd template name>
```

Exemplo de código 11 – Modelo de configuração para habilitar o BFD no OSPF.

Mecanismo *loop-free alternate fast reroute*

[4.8-2] O mecanismo *loop-free alternate fast reroute* (LFA FRR), implementado no protocolo OSPF, utiliza um próximo salto alternativo pré-calculado para reduzir o tempo de reação à falha quando ocorrer uma falha no caminho primário protegido. Este mecanismo proporciona que seja possível configurar um caminho alternativo sem perdas de pacotes de prefixos de ligações protegidas, ao reencaminhar esse tráfego para um caminho alternativo. Assim, é possível o restabelecimento do serviço que entrou em falha sem que os outros *routers* adjacentes reajam à falha. O Exemplo de código 12 é reconhecido nos *guide line* do fabricante como boa prática para habilitar o LFA *fast reroute* no OSPF com o sistema operativo Cisco IOS XE.

```
router ospf [process ID]
! create a list of paths considered for LFA fast rerouter:
 fast-reroute per-prefix enable area <area> prefix-priority high
fast-reroute keep-all-paths
```

Exemplo de código 12 – Modelo de configuração para habilitar o LFA *fast rerouter* no OSPF.

- *Mecanismo LFA fast rerouter remoto*

A utilização do mecanismo LFA fornece uma boa opção para garantir um caminho alternativo sem *loops*. Além disso, algumas topologias, nomeadamente as topologias baseadas em anéis, não ficam tão bem protegidas usando apenas os LFA. O mecanismo *LFA fast reroute* remoto foi configurado nos *routers* P e PE. O Exemplo de código 13 é reconhecido nos *guide line* do fabricante como boa prática para a implementação deste mecanismo.

```
! Remote LFA fast rerouter requirement:
mpls ldp discovery targeted-hello accept
 router ospf [process ID]
 fast-reroute per-prefix enable area <area> prefix-priority high
 fast-reroute per-prefix remote-lfa area <area> tunnel mpls-ldp
 fast-reroute keep-all-paths
```

Exemplo de código 13 – Modelo de configuração para habilitar LFA *fast rerouter* remoto no OSPF.

Microloop avoidance local

O Exemplo de código 14 é reconhecido nos *guide line* do fabricante como boa prática para habilitar o *microloop avoidance* do mecanismo LFA *fast reroute*, recurso do sistema operativo Cisco IOS XE.

```
router ospf [process ID]
 microloop avoidance protected
 microloop avoidance rib-update-delay 2000
```

Exemplo de código 14 – Modelo de configuração para habilitar o LFA FRR *microloop avoidance*.

Multi-protocolo BGP

Na rede VPN MPLS da EEM, todos os *routers* PE executarão o MP-BGP. O ASR 903 impõe limites máximos de BGP vizinhos e de número máximo de prefixos que podem ser configurados. Esta limitação protege o *router* do esgotamento de recursos por má configuração, localmente ou no vizinho remoto. Os seguintes limites aplicam-se às configurações BGP: *(i)* um máximo de 400 BGP *peers* (vizinhos); *(ii)* para evitar que um *router* BGP *peer* inunde a rede com anúncios de prefixos, foi estabelecido um limite máximo para o anúncio de 12000 VPN-IPv4. A EEM necessitou de um máximo 40 pares BGP e 20 VPN-IPv4.

Dispositivo *route reflector*

Na rede "WAN SCADA" foram instalados dois *route reflectors* para distribuirem os prefixos VPN-IPv4, utilizando o protocolo MP-BGP e com a topologia do tipo estrela (*hub nd spokes*). Assim, os elementos de rede têm apenas sessões com o *route reflector* para distribuirem as informações relativas aos prefixos de rede. A Figura 4.12 ilustra as sessões virtuais dos ASR903 com os *route reflectors* ("ASR 1001-X").

Os *route reflectors* são *routers* PE pertencem à rede "WAN SCADA", no entanto, não encaminham os dados úteis. Os *route reflectors* utilizam o OSPF para conhecer a topologia física da rede a que pertence, só assim é que pode haver troca de pacotes LDP. O MP-BGP apenar é utilizado para anunciar os prefixos de rede VPNv4, por isso, o RR deve ser vizinho de um *router* ASR903 (PE).

Por conseguinte, devem ser configurados da mesma forma que qualquer outro *router* com OSPF. Por outro lado, não há necessidade de executar o protocolo de distribuição de rótulos (*label distribution protocol*, LDP) em direção aos *route refletors*. O grupo de pares configurado deve incluir todos os endereços de IPLB dos *routers* PE remotos. Não se devem configurar os *route refletors* com VRF pois eles não são o ponto final de qualquer VPN. Os dispositivos ASR 1001-X existentes na rede "WAN SCADA" tem a função de *route reflector*. Cada "ASR 1001-X" possui uma *interface gigabit ethernet* diretamente ligada ao *router aggregation* (*router* PE).

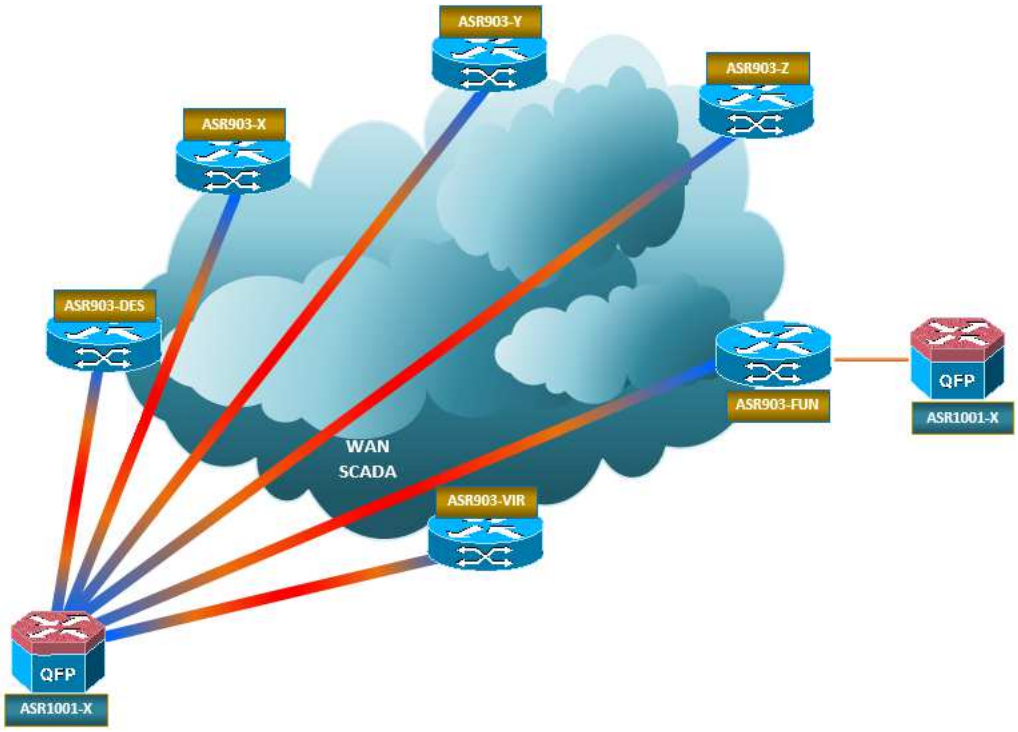

Figura 4.12 – Localização do *route reflector* na "WAN SCADA" da EEM.

Atribuição de nomes às VRF

Os VRF têm uma identificação que é depois utilizada na configuração do *router*. Na escolha para definir a melhor identificação a atribuir ao VRF utiliza-se a identificação do serviço ou cliente. A convenção de nomenclatura VRF deve ser simples o suficiente para permitir que alguém identifique exclusivamente o serviço ou cliente e, potencialmente, o local (*site*) dentro do nome da VRF *[4.8-3]*. As identificações utilizados na EEM para os VRF não serão mostrados por uma questão de segurança, mas seguem o exemplo da Tabela 4.6:

Note-se que o serviço PTP_1588 permite o sincronismo exigido pelas tramas E1 e X21.

Nome VRF	*Nome do serviço*
MULA	*SCADA*
RELOGIO	*PTP 1588 Telecom Profile*
LEÃO	Teleproteção
GATO	*Video vigilância*
RATO	*Telefonia VoIP*
COELHO	*Network Access Control*
NAVEGAR	*Dados internet*

Tabela 4.6 – *VRF* do *backbone* "EEM WAN".

Route distinguisher

Os prefixos de rede só são anunciados nos *spokes* ASR903 de cada subestação. Os *hubs* são os dois *routers* ASR903 das Virtudes e Despacho. As redes conhecidas pelos *routers* CPE (CGR 2010) também são conhecidos no *router* PE (ASR903) a que estão associadas.

A convenção atual para alocação RD é a seguinte: <***Ip loopback***>:<***number***>. A Tabela 4.7 lista os números de serviço atribuído à cada VRF existente nas subestações.

Nome VRF	*Nº do serviço*	*Nome do serviço*
MULA	10	SCADA
RELOGIO	20	PTP 1588 Telecom Profile
LEÃO	30	Teleproteção
GATO	40	Video vigilância
RATO	50	Telefonia VoIP
COELHO	60	Network Access Control
NAVEGAR	70	Dados *internet*

Tabela 4.7 – Atribuição de identificação RD para os VRF das subestações da EEM.

A Tabela 4.8 lista os números de serviço atribuídos a cada VRF associada ao *site* "Funchal DC".

Nome VRF	*Nº do serviço*	*Nome do serviço*
MULA	1010	SCADA
RELOGIO	1020	PTP 1588 Telecom Profile
LEÃO	1030	Teleproteção
GATO	1040	Video vigilância
RATO	1050	Telefonia VoIP
COELHO	1060	Network Access Control
NAVEGAR	1070	Dados *internet*

Tabela 4.8 – Atribuição de identificação RD para o VRF do Funchal.

A Tabela 4.9 lista os números de serviço atribuídos a cada VRF associada ao *site* "Virtudes DC".

Nome VRF	*Nº do serviço*	*Nome do serviço*
MULA	2010	SCADA
RELOGIO	2020	PTP 1588 Telecom Profile
LEÃO	2030	Teleproteção
GATO	2040	Video vigilância
RATO	2050	Telefonia VoIP
COELHO	2060	Network Access Control
NAVEGAR	2070	Dados *internet*

Tabela 4.9 – Atribuição de identificação RD para os VRF das Virtudes.

Atributo route target

As subestações têm o mesmo *route target* de exportação e o *datacenter* tem um *route target* de exportação diferente e único para cada subestação. Em todas as subestações, o *router* apenas importa os prefixos de rede do *datacenter* e, no *datacenter*, o *router* importa os prefixos das subestações e do outro *datacenter* (alternativo).

Utilizar os mesmos valores de atributo de *route target* (RT) e do *route distinguisher* (RD) simplifica a sua configuração e gestão. A convenção atual para alocação RT é a seguinte: < ***EEM AS*** >:< ***RD_number*** >. A Tabela 4.10 lista os números RT atribuídos a cada subestação.

Nome VRF	*Nº do serviço*	*Nome do serviço*
MULA	64512:10	SCADA
RELOGIO	64512:20	PTP 1588 Telecom Profile
LEÃO	64512:30	Teleproteção
GATO	64512:40	Video vigilância
RATO	64512:50	Telefonia VoIP
COELHO	64512:60	Network Access Control
NAVEGAR	64512:70	Dados *internet*

Tabela 4.10 – Atribuição de identificação RT para os VRF das subestações da EEM.

A Tabela 4.11 lista os números RT atribuídos ao *site* "Funchal DC".

Nome VRF	Nº do serviço	Nome do serviço
MULA	64512:1010	SCADA
RELOGIO	64512:1020	PTP 1588 Telecom Profile
LEÃO	64512:1030	Teleproteção
GATO	64512:1040	Video vigilância
RATO	64512:1050	Telefonia VoIP
COELHO	64512:1060	Network Access Control
NAVEGAR	64512:1070	Dados *internet*

Tabela 4.11 – Atribuição de identificação RT para os VRF do Funchal.

A Tabela 4.12 lista os números RT atribuídos ao *site* "Virtudes DC".

Nome VRF	Nº do serviço	Nome do serviço
MULA	64512:2010	SCADA
RELOGIO	64512:2020	PTP 1588 Telecom Profile
LEÃO	64512:2030	Teleproteção
GATO	64512:2040	Video vigilância
RATO	64512:2050	Telefonia VoIP
COELHO	64512:2060	Network Access Control
NAVEGAR	64512:2070	Dados *internet*

Tabela 4.12 – Atribuição de identificação RT para os VRF das Virtudes.

A Figura 4.13 explica como são distribuídos os prefixos de rede do serviço 65000.

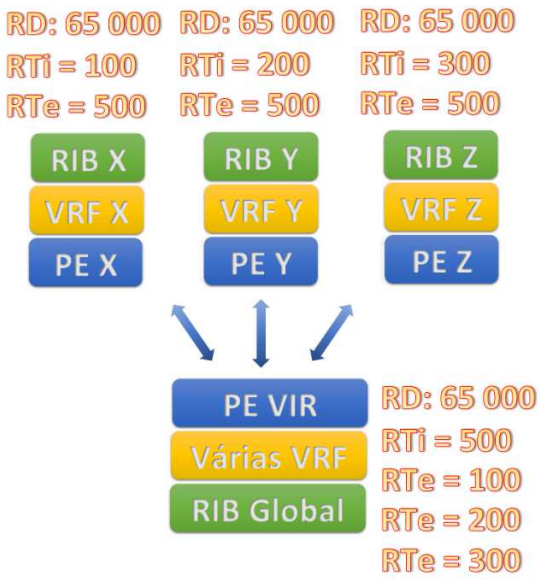

Figura 4.13 – Distribuição dos prefixos de rede.

Esta configuração salvaguarda que as outras subestações não saibam os prefixos de rede umas das outras. Só o "*hub*" (*router* "ASR903-VIR") é que sabe de todas, apesar do serviço ser comum a todos os *routers* ASR903, é salvaguardado que não troquem todos informações entre si.

MPLS *traffic engineering*

No estabelecimento de um caminho explícito, o administrador consegue maximizar a eficiência da rede. Todos os *routers* que participam nos dois caminhos (primário e alternativo) devem ficar definidos por configuração manual. Conforme ilustrado na Figura 4.14, cada circuito criado necessita de dois IP de destino: "*Loopback0"* , que identifica o *router* PE, e o da *interface* A que estabelece a ligação ao *router* PE.

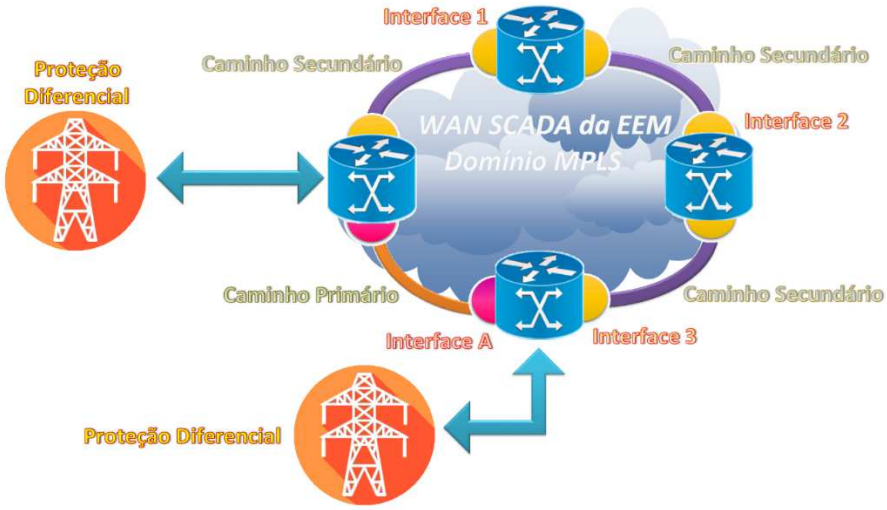

Figura 4.14 – Dois caminhos explícitos definidos pelo administrador de rede.

O segundo caminho (alternativo) só difere do IP da *interface* (do 1 ao 3), pois o "*Loopback0"* é o mesmo. No segundo caminho, devem ser indicados todos os "*Loopback0"* de cada *router* e o respetivo *interface* de chegada. Assim, os "*Loopback0"* definem as extremidades do circuito e os IP das *interfaces* indicam como chegam ao "*Loopback0"*. O circuito (caminho) é unidirecional, sendo por isso necessário configurar dois circuitos para cada caminho. Este mecanismo é essencial para o funcionamento do serviço "teleproteção". Conseguem-se tempos de comutação de caminho inferiores a 50 milissegundos, valor característico do SDH. Na realidade, na generalidade dos casos, consegue-se tempos inferiores a 10 milissegundos.

4.9 Sincronização da rede

Ao contrário dos serviços *legacy*, o serviço *ethernet* não possui informações de sincronização de relógio. Para se obter sincronismo existem 3 tipos de relógios: *(i)* o NTP; *(ii)* o PTP; e *(iii)* o SyncE.

O relógio *network time protocol* (NTPv4 IEEE 1588), ou o *simple network time protocol*, funciona na camada 2 e na camada 3, utilizando pacotes UDP no envio das suas mensagens.

Os relógios *precision time protocol* (PTP, IEEE 1588-2008 v2) e *synchronous ethernet* (SyncE, ITU-T G8262) são soluções para a distribuição de sincronização em redes de pacotes baseadas em IP, como redes *ethernet* IP, MPLS, xPON e xDSL, para os serviços *Legacy*. O *Sync-E* funciona na camada física e é independente do congestionamento ou da carga da rede (funciona como se não existisse tráfego na rede), e não sobrecarrega a rede ao fornecer a sincronização.

Tanto o relógio NTP como o relógio PTP utilizam o serviço de transmissão de tempo fornecido pelo GPS. Os sinais de GPS estão sempre disponíveis, em qualquer lugar, desde que exista uma linha de vista desobstruída para os satélites de GPS.

Existem quatro níveis de hierarquias de precisão (níveis *stratum*). *Stratum* 1 define um grau de precisão de $1\ x10^{-5}$ ppm). O relógio *Stratum* 1 é também designado por relógio Atómico (césio ou rubídio) e é o nível de precisão mais elevado. São também conhecidos por PRC. O sinal não será regenerado, pois é necessária uma licença. O sinal de relógio que realize mais do que 8 salto necessita de regeneração.

A sincronização de rede na EEM é obtida utilizando um par redundante (um primário e um alternativo) de relógios *Stratum* 1 ligadas aos Centros de Controlo do Funchal e do Despacho (Vitória). Ambos os relógios (tráfego *ethernet*) são transportados utilizando o *SyncE*. É reconhecido nos *guide line* do fabricante como boa prática configurar o fuso horário apropriado em todos os dispositivos. Sem uma configuração apropriada de fuso horário, o *router* ou o comutador padrão utiliza o Horário Universal.

Os *routers* ASR903 de *core* obtêm o seu tempo NTP, permitindo-os atuar como mestres NTP (*Stratum* 1) em relação aos outros ASR903, e cada PE, instalado nas subestações, pode ser usado como mestre (*Stratum* 2) para os equipamentos que agrega. A Figura 4.15 ilustra as entradas físicas externas (10 MHz, BITS, SyncE, TDM, 1PPS, TOD) para fornecer o relógio ao sistema ou usar as funções PTP 1588v2 (*slave, BC*) para a frequência e a fase. Para o *Syslog* e o serviço "teleproteção", a EEM utiliza o PTP 1588v2, pois os outros relógios não oferecem uma precisão tão elevada devido a esta característica da fase. A EEM implementou um VRF ("20") para o transporte do tráfego do sinal de relógio.

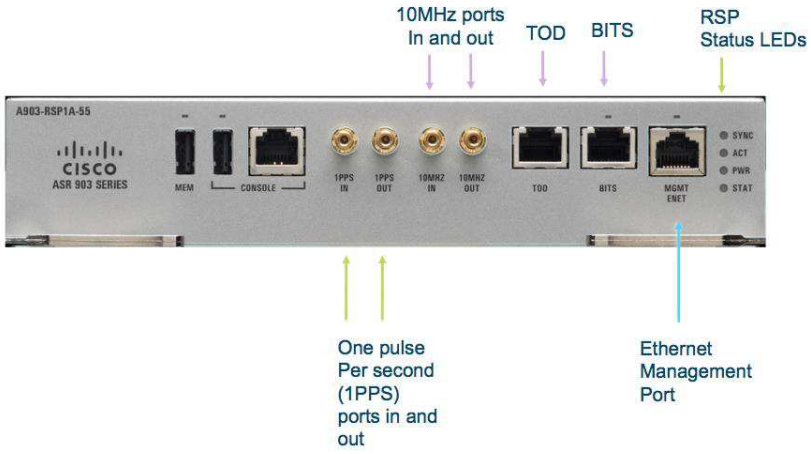

Figura 4.15 – *Sincronização da rede com o ASR 903 RSP*.

Note-se que a configuração do IPLB 1588 (IPLB PTP) dedicado nos *routers* ASR903 é obrigatória para usar corretamente o relógio PTP. Se for o IPLB do "*router ID*", pode perturbar a sincronização uma vez que o identificador IPLB do "*router ID*" é utilizado para várias coisas. O número IPLB pode variar entre 0 e 65535. Esta *interface* só pode ser utilizada para relógio PTP e não responderá ao comando *pings*.

4.10 Serviço "teleproteção"

O serviço "teleproteção" permite a troca de tráfego entre duas proteções diferenciais, instaladas em subestações diferentes, e que utiliza o protocolo X21. Tem que existir uma proteção diferencial associada a cada terno de alta tensão. Designa-se "terno" o conjunto das três fases constituintes de uma linha de alta tensão. Entende-se por uma linha de alta tensão o segmento, limitado por duas subestações, normalmente num traçado construído em anel. Estas duas proteções diferenciais, que medem as caraterísticas físicas do cabo, trocam entre si informações críticas no tempo. Este tempo condiciona a escolha dos *routers*.

Protocolo CESoPSN e SAToP

Foi utilizado o SAToP para transportar os pacotes E1 (de forma transparente), e o CESoPSN para transportar os pacotes X21. É transparente, pois a trama E1 é processado como se fosse PCM32, ou seja, não precisa das sinalizações utilizadas nos canais elementares básicos TS15 e TS31. A Tabela 4.13 lista algumas das instalações onde é necessário considerar o serviço "teleproteção" e tipo de tecnologia correspondente.

ID	Origem	Destino	Type
1	SE Machico [MCH]	SE Palheiro Ferreiro [PFE]	E1
2	SE São João [SJO]	SE Viveiros [VIV]	X21
3	SE Ponte Vermelha [PVM]	SE Pedra Mole [PMO]	E1

Tabela 4.13 – Algumas instalações com serviço "teleproteção".

O módulo *IM derive Sync Serial port* (IMASER14A/S) instalado nos *routers* da série Cisco ASR900, suporta tipos de *pseudowire* que utilizam o *circuit emulation service over packet-switched network* (CESoPSN), no modo E1, para transportar o tráfego X21 de sincronização. O módulo suporta velocidades de dados N x 64kbps (N varia de 1 a 32). A Figura 4.16 ilustra a ligação entre a proteção diferencial e o módulo IMASER14A/S. O módulo CESoPSN difere do SAToP devido à velocidade, porque o X21 necessita do sincronismo e o SAToP não.

Para a linha *serial* Nx64 kbps, o número de intervalos de tempo numa determinada moldura TDM é definido com base na velocidade da linha X21. O CESoP requer o módulo IMASER14A/S de 14 portas, e destas, apenas os portos 8 ao 13 podem ser utilizadas para X21. O IMASER14A/S transmite o relógio via *backplane*. Devem de ser utilizados cabos *Smart serial* na ligação física entre o módulo IMASER14A/S e a *interface* das proteções diferenciais. O conetor DCE deve ser

ligado ao *router* ASR e o DTE ao dispositivo de teleproteção. A configuração de uma *pseudowire* entre o *router* PE local e o dispositivo remoto não é suportada se forem utilizadas velocidades diferentes nos portos de sincronização. Ou seja, não se pode utilizar a velocidade de um E1 num acesso, e na sua entrega o X21 (TS).

O teste é realizado de duas formas: *(i)* virtualmente em que se desliga a *interface* e regista-se o tempo que demora a ativar o caminho alternativo; e *(ii)* instala-se o conjunto das proteções diferenciais e regista-se esse mesmo tempo. Os tempos aceites são inferiores a 10 milissegundos.

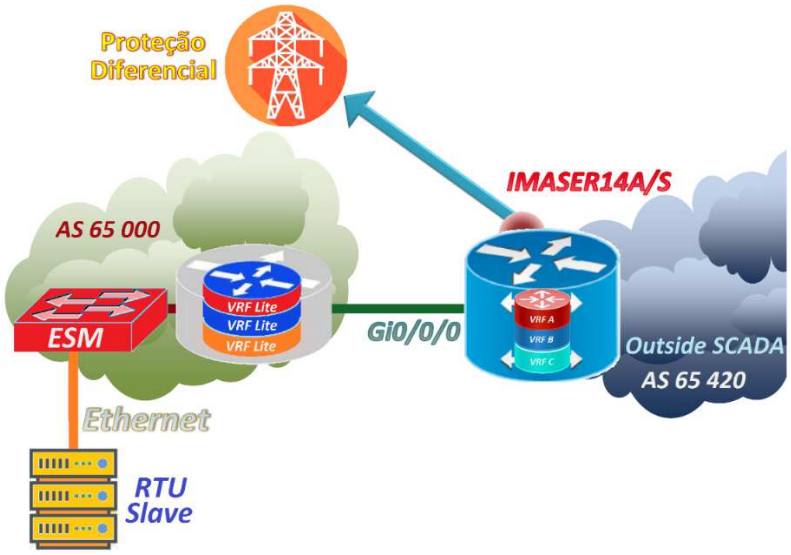

Figura 4.16 – O módulo IMASER14A/S permite integrar método de transmissão TDM no MPLS.

4.11 Serviço SCADA

O tráfego VPN-L3 do serviço "SCADA" tem um *site* primário (Despacho) e um alternativo (Virtudes). Por motivos de segurança, todo o tráfego nos sentido Despacho → Subestações e Subestações → Despacho é inspecionado por uma das duas *firewall*s associadas à rede "WAN SCADA". Foi necessário criarem-se duas VPN distintas, designadas por Despacho (Ssubestações → *firewall*) e "SCADA" (despacho → *firewall*), para que os tráfegos dos diferentes serviços fossem diferenciados. Cada serviço, e em cada sentido, foram mapeados em VLAN. O reencaminhamento entre diferentes VPN-L3 (*leaking*), também referido na literatura por "vazamento", é realizado pela *firewall*. Os VRF não fazem *leaking* entre si, pois foi configurado pelo administrador de rede que os VRF não anunciam os seus prefixos de redes entre si existentes no mesmo *router*. É considerado um nível de segurança, para além da segmentação do tráfego por serviços, esse tráfego não é encaminhado entre VRF de subestações sem serem inspecionado pela *firewall.*

O serviço "SCADA" permite a troca de tráfego entre a subestação e o *datacenter* do Centro de Despacho. O concentrador de dados local (RTU *slave*) da subestação liga-se ao *switch* do CGR2010 utiliza a VLAN "SCADA". O módulo de comutação de *ethernet* (*ethernet switch module*, ESM) permuta os pacotes com o "módulo" *router* CGR 2010 utilizando o *backplane*. No *router*

está configurado um VRF *lite*, designado por "SCADA", para permitir associar o tráfego da VLAN "SCADA" à camada 3, ilustrado na Figura 4.17.

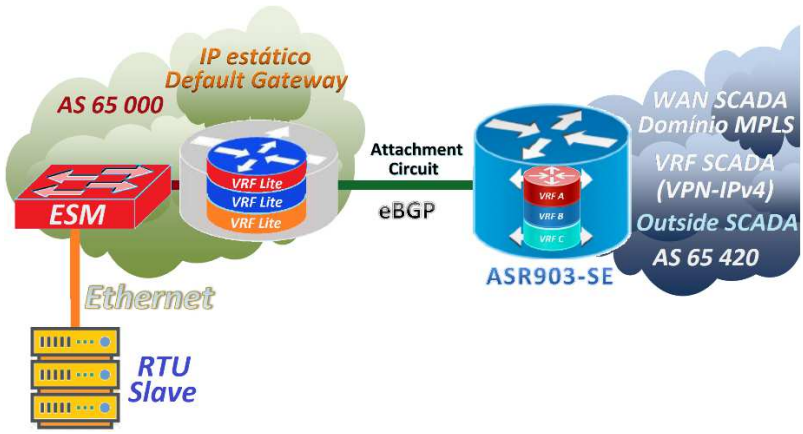

Figura 4.17 – Ligação lógica da VLAN "SCADA" da subestação dos Prazeres ao VRF "SCADA".

Na subestação, no anúncio dos prefixos de rede entre o *router* CPE e o *router* PE é utilizado o protocolo de encaminhamento eBGP. No *router* CPE é configurada que o seu *default gateway* é o *router* PE a que está associado. A Figura 4.18 ilustra a troca de tráfego do VRF "SCADA" entre os *routers* CE e o PE.

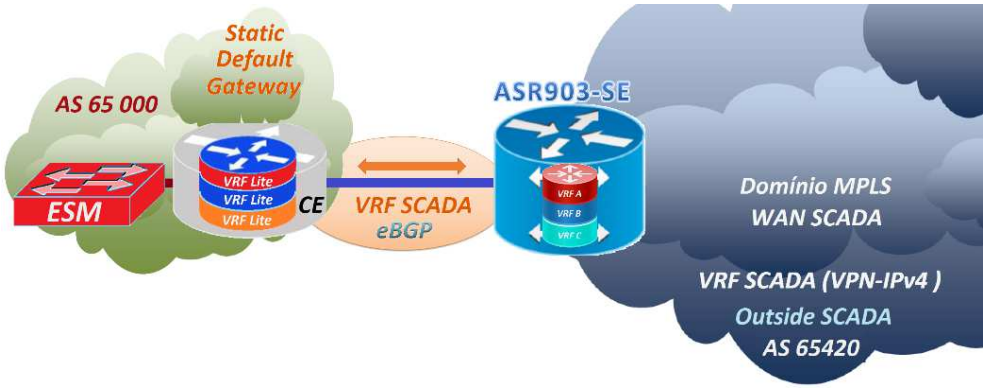

Figura 4.18 – Tráfego SCADA trocado entre os *routers* CE e PE.

A Figura 4.19 ilustra o próximo passo, em que o *backbone* MPLS recorre a topologia de malha completa para fazer com o tráfego alcance o *router* PE ASR 903 das Virtudes ("ASR903-VIR").

A Figura 4.20 ilustra o o *router* "ASR903-VIR"que envia o tráfego recebido da RTU *slave*, que chegou numa VPN-L3 associado ao VRF "SCADA", para a *firewall*. A *firewall*, após inspecionar o tráfego gerado pela subestação, coloca esse tráfego inspecionado noutra VPN-L3 (VRF "SCADA_DC"), e reenvia-o para o *router* "ASR903-VIR", para que o tráfego possa chegar ao *datacenter* do serviço "SCADA" utilizando o *backbone* MPLS.

A *firewall* recebe o tráfego numa ligação e reenvia esse mesmo tráfego, inspecionado, de novo para o *router* "ASR903-VIR", mas mapeado numa outra VPN-L3. Na realidade, a arquitetura

considerada nos *guide line* do fabricante como boa prática sugere que se utilize um *Switch Cluster* entre o *router* PE e a *firewall*. O *Switch Cluster* permite garantir redundância no acesso à *firewall* e faz uso da *bridge domain interface* (BDI). Uma BDI é uma sub-*interface*, que é utilizada pelos ISR/CGR do fabricante Cisco, mas é um mecanismo desenvolvido para os agregadores PE do fabricante Cisco.

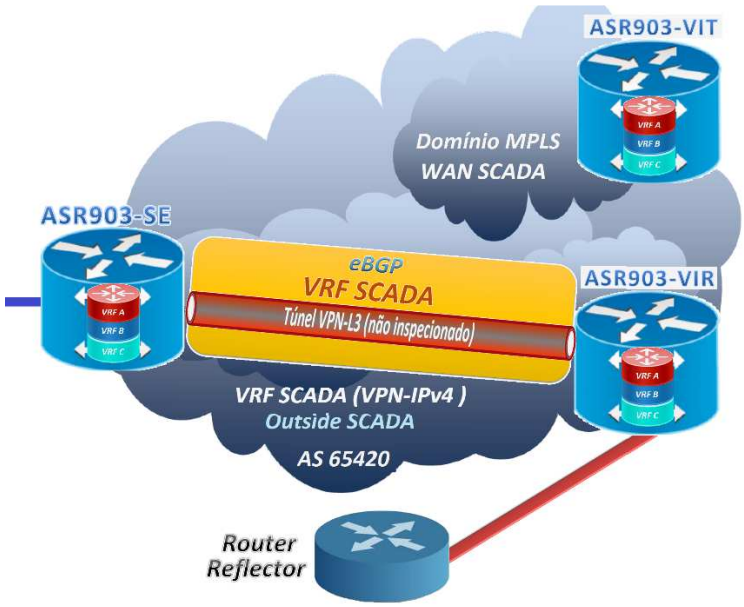

Figura 4.19 – Tráfego do serviço "SCADA" trocado entre os *routers* PE.

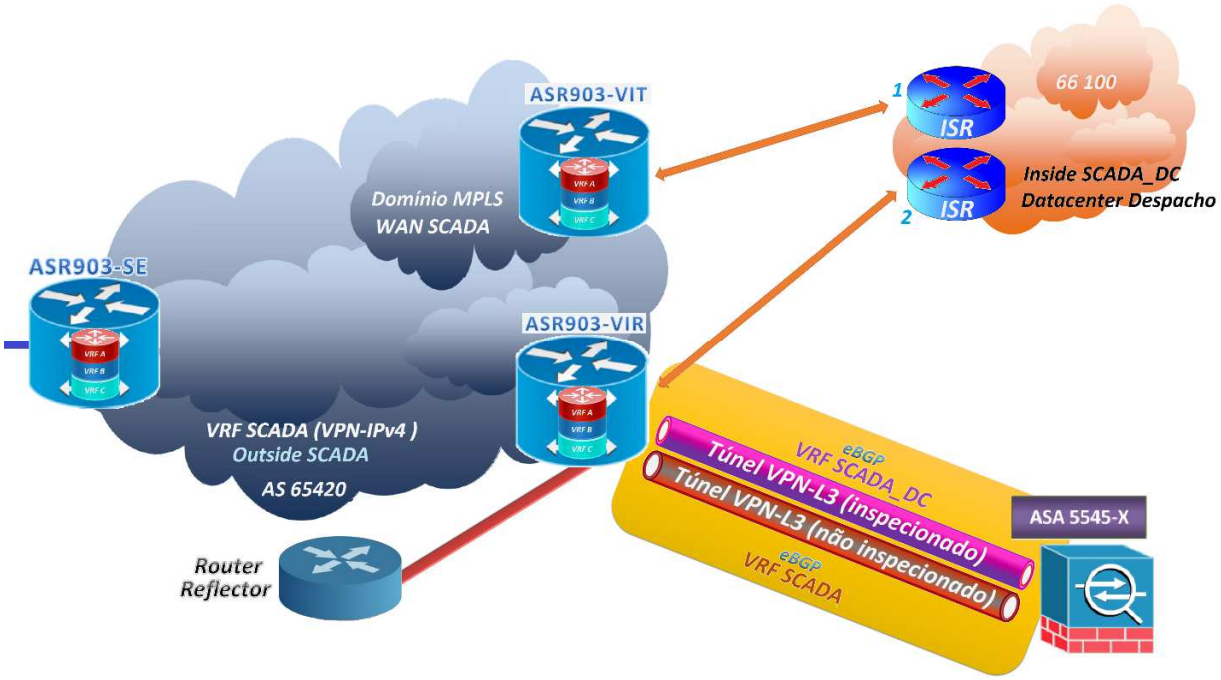

Figura 4.20 – Tráfego do VRF "SCADA" para ser inspecionado e encaminhado para o VRF "SCADA_DC".

Não é possível implementar a instância VRF *lite* na *firewall* (*router* Cisco ASA 5545-X), daí a necessidade de se encapsular o tráfego de cada VRF numa VLAN, e cabe ao BDI realizar essa comutação. Ou seja, o *router* PE recebe o tráfego do *backbone* e utiliza o BDI para retirar esse tráfego da VRF e encaminha-o para o porto que interliga com o porto da *firewall*. Quando recebe o tráfego inspecionado, o BDI recebe-o e comuta-o para o respetivo VRF. O pacote está sempre salvaguardado pelo IP de destino indicado no cabeçalho do pacote para chegar ao seu destino.

A Figura 4.21 ilustra a próxima etapa, em que o *router* "ASR903-VIR" envia o tráfego do VRF "SCADA_DC" para o "ISR-2", existente no *datacenter* do Despacho, utilizando o protocolo de encaminhamento eBGP. Está representado o caminho primário e secundário.

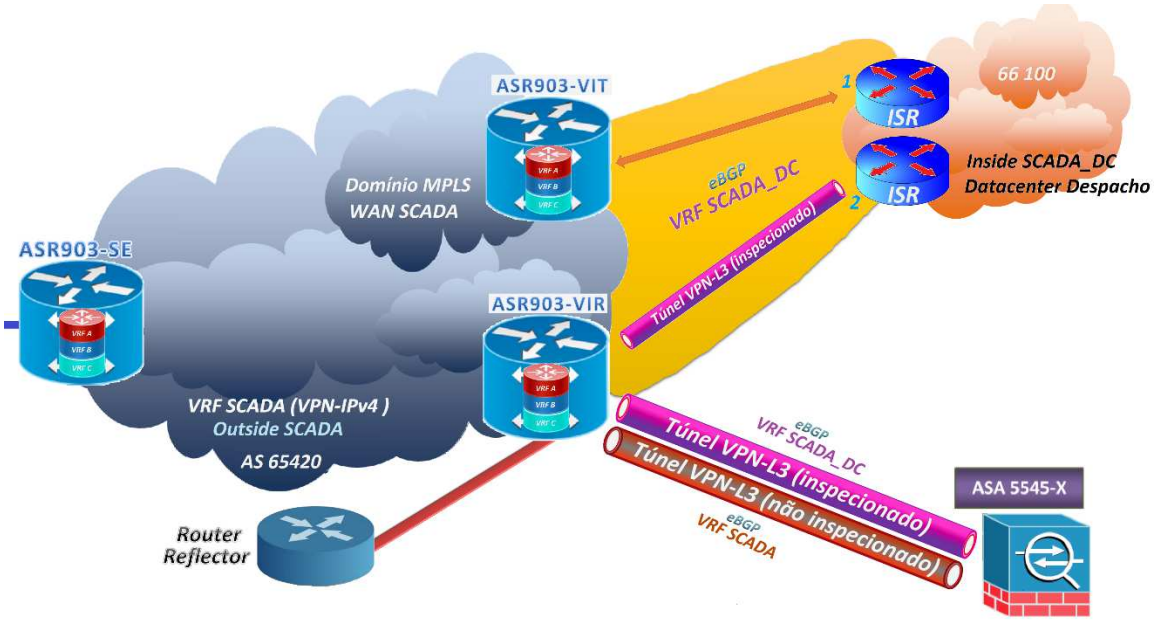

Figura 4.21 – O tráfego inspecionado é encaminhado pelo *router* PE das Virtudes para o *router* ISR.

A Figura 4.22 ilustra o encaminhamento do tráfego do *datacenter* para a subestação, em que a abordagem é a mesma mas com o fluxo em sentido oposto. O ponto "1" é utilizado o eBGP para encaminhar o tráfego para o *router* "ASR903-VIR". O ponto "2" o eBGP é utilizado para encaminhar o tráfego não inspecionado até à *firewall* para ser inspecionado. O protocolo de encaminhamento é o eBGP. O ponto "3" o eBGP é utilizado para encaminhar o tráfego inspecionado até ao *router* "ASR903-VIR", que garante o acesso à rede "WAN SCADA". O protocolo de encaminhamento é o eBGP. O ponto "4" representa o caminho que o tráfego inspecionado percorre para chegar ao ASR 903 da subestação. O protocolo de encaminhamento é o iBGP. O ponto "5" representa o caminho que o tráfego inspecionado percorre para chegar ao CGR 2010 existente na subestação. O protocolo de encaminhamento é o eBGP. O ponto "6" representa o caminho que o tráfego inspecionado percorre para chegar ao ESM que está associado ao CGR 2010. O protocolo de encaminhamento é o OSPF.

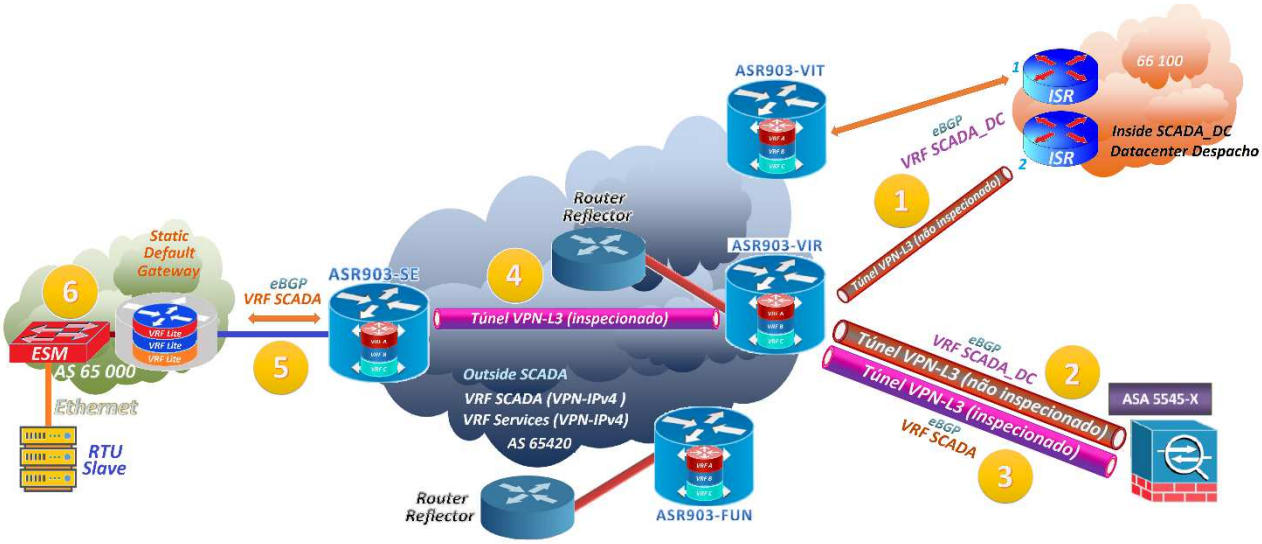

Figura 4.22 – Envio de tráfego gerado no *datacenter* do Despacho para a subestação.

Esta solução é também utilizada pela EEM por forma a permitir exercer o mesmo tipo de supervisão e controlo aos postos de transformação (PT). A Figura 4.23 ilustra o *front end* apresentado aos operadores do Centro do Despacho, com características do PT do "Campo de Cima I" (Porto Santo).

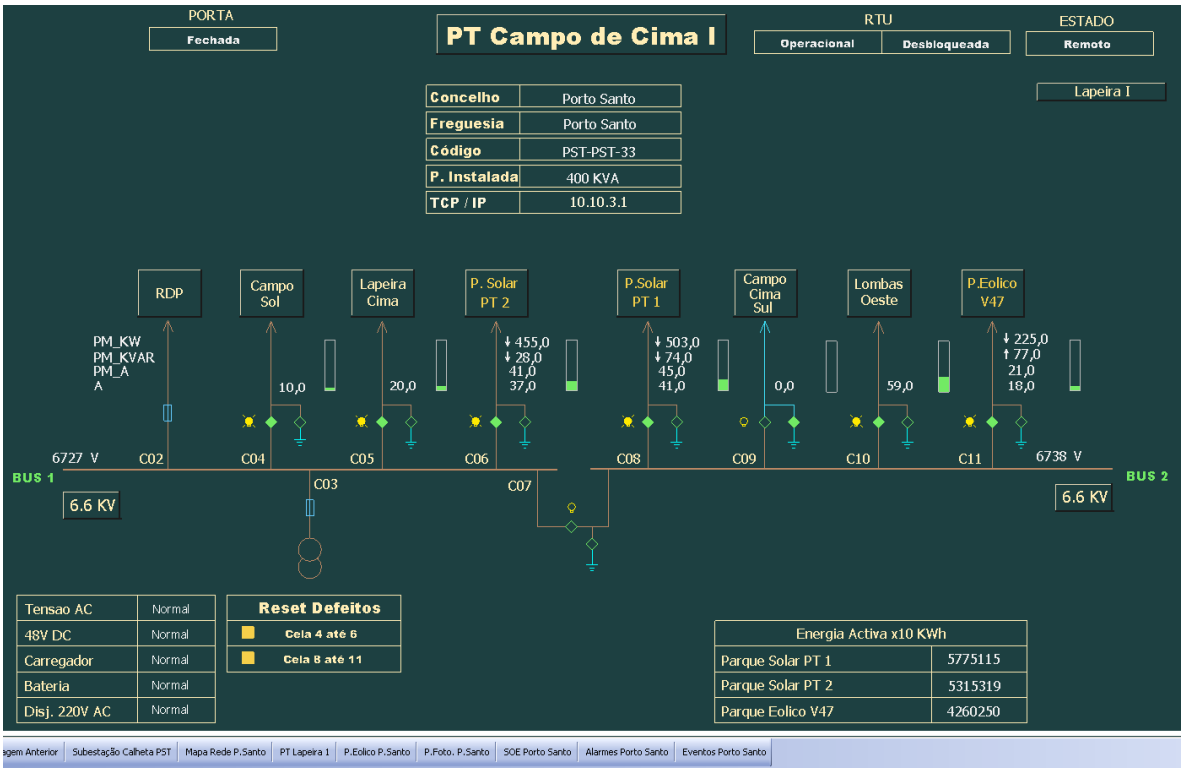

Figura 4.23 – Exemplo de algumas características elétricas do PT do Campo de Cima I.

Os dois transformadores estão ligados à rede SEPM, recebendo assim carga a fornecer aos seus respetivos barramentos do secundário. Como se pode observar, este PT dispõe de redundância através de 5 ligações, e recebe carga por dois parques de painéis fotovoltaicos e um eólico. A ligação ao PT "Campo de Cima Sul" está desativada.

4.12 Arquitetura de segurança

A solução de segurança consiste em duas plataformas diferentes: *(i)* Cisco *Identity Services Engine* (ISE); e *(ii)* duas *firewalls* (Cisco ASA 5545-X). As duas soluções dispõem de redundância.

A plataforma contextual ISE permite a gestão de pontos de extremidade (*endpoints*) e força qualquer um a se autenticar. A autenticação tanto pode ser a nível de utilizador, como de dispositivo com endereço MAC. A solicitação de autenticação é conseguida pelo protocolo 802.1x, se for utilizador humano, ou MAB se for máquina. A comunicação é realizada utilizando um "túnel" VPN para impossibilitar que o *endpoints* não autenticado possa aceder aos recursos da rede. Após validação pelo ISE, e utilizando o agente *Network Access Control* (NAC), é fornecido autorização ao porto do comutador, com as configurações dos níveis de acesso definidas pelo administrador de rede. O ISE também possibilita a configuração de perfis. A plataforma está instalada em duas máquinas virtuais. Foram implementadas as seguintes funcionalidades: *(i)* forçar a autenticação do utilizador antes de qualquer acesso à rede*; (ii)* gestão dos pontos de extremidade (*endpoints*) que podem aceder à rede; *(iii)* controlo do acesso VPN; *(iv)* assegurar a autenticação de *endpoints* sem capacidades 802.1x.

As *firewalls* estão colocadas no *datacenter* das Virtudes. Este modelo não dispõe de portos óticos, nem tolera outro dispositivo na ligação entre eles. Tem como objetivo garantir a disponibilidade dos serviços de segurança e uma interligação segura entre os dois *datacenters*. Os *Adaptives Security Appliances* (ASA) também são responsáveis pelo controlo do fluxo de tráfego, incluindo o tráfego das subestações. Têm a capacidade de analisar padrões e detetar anomalias.

O sistema de prevenção de intrusão (*intrusion prevention system*, IPS) inspeciona o tráfego que flui através de uma rede e é capaz de bloquear ou corrigir fluxos que determina que são maliciosos. Usualmente utiliza-se uma combinação de assinaturas de tráfego e arquivos, e análise heurística de fluxos. Estes fluxos são processos cognitivos empregados em decisões não racionais, sendo definidas como estratégias que ignoram parte da informação com o objetivo de tornar a escolha mais fácil e rápida. O IPS pode impedir que um determinado tráfego atinja os diferentes destinos na rede. Possibilita ver todo o tráfego durante um período de tempo definido pelo utilizador onde o IPS irá construir uma base de dados sobre o que é conhecido como sendo tráfego e quando o tráfego pode estar fora de ordem.

O sistema de deteção de intrusão (*intrusion detection system*, IDS) é uma *security network appliance* e é semelhante ao IPS, mas não afeta os fluxos (apenas regista ou cria alertas sobre o tráfego malicioso). Assim, o IDS está encarregado de monitorizar a rede e determinar se um ataque está ou não em curso, mas não impede que o ataque atinja os diferentes recursos. Não recebe o tráfego real do cliente que vai para o servidor ou do servidor para o cliente, ele basicamente recebe uma cópia do dispositivo de rede anexado.

A *firewall* é um aplicativo de segurança da rede por excelência. Permite ou bloqueia o tráfego entre *interfaces* com base em regras configuradas. Muitas vezes tem uma função de tradução de endereço de rede (NAT) para isolar endereços de rede privados (RFC 1918) do público. Pode inspecionar o tráfego por conformidade com o comportamento correto do protocolo e descartar o tráfego não conforme. As *firewalls* geralmente possuem como opcional um componente IDS / IPS para ver todo o tráfego que deve ser sujeito a inspeção e análise adicionais, como é feito pelo IDS / IPS. As *firewalls* conhecidas pela designação de próxima geração, vão da camada 2 a 7. A inspeção do tráfego é balanceada por serviços, apesar de uma das ligações ser a alternativa da outra. Apesar de ser um assunto de extrema importância, mas por fugir ao âmbito deste trabalho, não será desenvolvido.

4.13 Conclusão

A rede MPLS está sobre uma rede IP e utiliza o protocolo *open shortest path first* (OSPF), o tráfego de pacotes IP dos clientes está sobre a rede MPLS e utiliza o protocolo de encaminhamento BGP. Para anunciar os prefixos de rede IPv4, para a construção da topologia do *backbone* MPLS, a EEM optou pelo OSPF por ser confiável e escalável. O protocolo OSPF permite dividir uma rede completa em áreas, mas esta funcionalidade não foi utilizada. A EEM optou por vários sistemas autónomos e constituída por vários anéis para garantir a redundância de ligação física.

A opção por uma hierarquia colapsada permite que os equipamentos de *core* recebam serviços sem prejudicar muito a eficiência dos mesmos. Os processadores foram escolhidos mediante a necessidade de tráfego. A implementação da rede hierárquica baseou-se em três níveis fundamentais: *core*, agregação e acesso, e em que se diferenciam pela necessidade de largura de banda e capacidade de processamento.

Foram implementados dois tipos de *interfaces* na conetividade entre os elementos de rede do *backbone*. A capacidade de largura de banda no estabelecimento da ligação entre os *routers* P e PE é de 10 Gbps e na ligação entre os *routers* PE e PE é de 1 Gbps. Em todos os portos *(interfaces)* foram configuradas para reconhecer o protocolo OSPF e o MPLS, em modo de auto-negociação e a MTU com a mesma capacidade.

A EEM utilizou três *subinterface* para identificador os IP *loopback* IPv4 /32 (IPLB): 0 (zero), 10 e 100. O IPLB0 é utilizado pelo IGP na construção da tabela de estado de ligação (*link-state database*, LSDB). Os IPLB10 e IPLB100 servem para segmentar os tráfegos da sincronização e monitorização.

Foram seguidas diversas regras de construção da rede, destacando-se as seguintes: *(i)* um servidor/*datacenter* nunca liga diretamente a um agregador, mas sim a um *router* CPE, porque a troca de tráfego entre um servidor e um elemento de rede é realizado ao nível da camada 2 do modelo OSI; *(ii)* o servidor da aplicação *Identity Services Engine* (ISE), também não pode ser ligado diretamente a um agregador; *(iii)* o tráfego transportado pelas diferentes VPN-IPv4 é entregue às *firewalls*. A *firewall* protege as subestações e não o *datacenter*, pois o *datacenter* tem o seu próprio mecanismo de defesa.

Na conetividade entre o *router* CPE e o *router* PE, ligação designada por *attachment circuits* (AC), é utilizado o protocolo de encaminhamento BGP. Além disso, os *routers* PE não anunciam os seus prefixos de rede aos *routers* CPE (a jusante) de qualquer serviço. Não há vantagens em que o

router CPE saiba as redes conhecidas pelo *router* PE, logo o anúncio de prefixos de rede só se realiza pelo *router* CPE. Assim, a tabela de encaminhamento do *router* CPE fica reduzida a um índice por serviço, que é basicamente um *gateway* padrão por serviço. Em direção aos *route reflectors*, os *routers* PE anunciam todos os serviços (prefixos de redes) existentes nos *routers* CPE.

Um dos principais motivos para a escolha do protocolo de encaminhamento BGP para anunciar os prefixos de redes dos serviços é que escala melhor, pois suporta tabelas de encaminhamento de grandes dimensões.

Os *routers* de *core* e os *datacenters* terão encaminhamento estático para garantir a conetividade entre os elementos de rede. O ter um encaminhamento estático significa que não pode ser o DHCP a atribuir os IP aos portos.

No estabelecimento de um caminho explícito, o administrador de rede consegue maximizar a eficiência da rede. No caminho explícito, todos os *routers* que participam nos dois caminhos (primário e alternativo) ficam definidos por configuração manual. Este mecanismo é essencial para o funcionamento do serviço "teleproteção". Consegue-se tempos de comutação de caminho inferior aos 50 milissegundos, valor característico do SDH.

Uma das vantagens do MPLS é a possibilidade de se ter *datacenters*, e Centro de Despachos, em vários lugares.

A solução de segurança consistiu na implementação do *Triple A*, gerido pela plataforma contextual Cisco *Identity Services Engine* (ISE), e duas *firewalls*. As duas soluções dispõem de redundância.

A plataforma contextual ISE permite a gestão de pontos de extremidade (*endpoints*) e força qualquer um a autenticar-se. A autenticação tanto pode ser a nível de utilizador, como de dispositivo com endereço MAC. A solicitação de autenticação é conseguida pelo protocolo 802.1x, se for utilizador humano, ou MAB se for máquina. A comunicação é realizada utilizando um "túnel" VPN para impossibilitar que o *endpoints* não autenticado possa aceder aos recursos da rede. Após validação pelo ISE, e utilizando o agente *Network Access Control* (NAC), é fornecido autorização ao porto do comutador, com as configurações dos níveis de acesso definidas pelo administrador de rede. O ISE também possibilita a configuração de perfis.

A *firewall* é um aplicativo de segurança de rede por excelência. Permite ou bloqueia o tráfego entre *interfaces* com base em regras configuradas. Todo o tráfego gerado numa subestação é inspecionado, ao nível da camada 3, pelo mecanismo *zone-based firewall* (ZBF), permitindo passar apenas as redes autorizadas. A firewall, associada ao aplicativo *FirePower* inspecionam o tráfego até à camada da aplicação. No sentido inverso, o procedimento repete-se. Para aumentar a segurança, os *routers* CPE existentes nas subestações não conhecem os prefixos de rede da rede "WAN SCADA". Qualquer serviço que acede ao *router* CPE chega ao *router* PE recorrendo a um *gateway* padrão por serviço, e todo o tráfego é encaminhados para a *firewall*. As *firewalls* estão colocadas no *datacenter* das Virtudes. Este modelo não dispõe de portos óticos, nem toleram outro os elementos de rede na ligação entre eles. Tem como objetivo garantir a disponibilidade dos serviços de segurança e uma interligação segura entre os dois *datacenters*. Os *Adaptives Security Appliances* (ASA) também são responsáveis pelo controlo do fluxo de tráfego, incluindo o tráfego das subestações. Tem a capacidade de analisar padrões e detetar anomalias. O Sistema de Prevenção de Intrusão inspeciona o tráfego que flui através de uma rede e é capaz de bloquear ou corrigir fluxos que ele determina que são maliciosos. Pode impedir que um determinado tráfego atinja os diferentes destinos na rede. O Sistema de Deteção de Intrusão

é semelhante ao IPS, mas não afeta os fluxos (apenas regista ou cria alertas sobre o tráfego malicioso). Assim, o IDS está encarregado de monitorizar a rede e determinar se um ataque está ou não em curso. Não impede que o ataque atinja os diferentes recursos. Não recebe o tráfego real do cliente que vai para o servidor ou do servidor para o cliente, ele basicamente recebe uma cópia do os elementos de rede anexado.

5. Conclusão

A EEM tem a responsabilidade de produzir, transportar, distribuir e comercializa a energia elétrica consumida na RAM, serviço público prestado sobre o Sistema Elétrico de Serviço Público da Madeira (SEPM). Para assegurar o cumprimento deste serviço, a EEM criou o serviço de telecomunicações para transportar toda a informação relacionada com os parâmetros que caracterizam cada nó da rede até para o Centro de Despacho. Os parâmetros são essencialmente os valores de tensão, corrente, fator de potência e estado dos elementos mecânicos, recolhidos nas subestações e direcionados para o Centro de Despacho. A missão do Centro de Despacho é otimizar a gestão, em tempo real, oferecendo ganhos de eficiência no transporte da energia e disponibilidade de serviço. Mediante a análise dos parâmetros, o Centro de Despacho pode enviar, se for necessário, comandos remotos, de abertura ou fecho de dispositivos (disjuntores, seccionadores), de subida ou descida das tomadas dos transformadores. Além disso, os relés de proteção dispõem de capacidade de processamento da informação lida pelos sensores que lhe estão acoplados e de interagir com os disjuntores de corte. Essas informações são também enviadas ao Centro de Despacho.

Um sistema de telecomunicações moderno associado a um sistema elétrico deve responder aos desafios exigidos pelas constantes evoluções de um sistema elétrico, como ser simples de operar, com baixos custos de manutenção, oferecer fiabilidade, eficiência, flexibilidade, confiabilidade, robustez e segurança.

A tecnologia PDH opera ao nível da camada 1 do modelo OSI e permite o princípio da transparência, ou seja, não impõe restrições ao tipo de tráfego. Além disso, as tramas são construídas por multiplexagem assíncrona. A multiplexagem também é utilizada para associar múltiplos de 4 níveis de elementos agregados. As principais desvantagens associadas à tecnologia PDH são o não permitir redundância e a gestão dos canais elementares ser complexa. Essa gestão obriga a constantes desmultiplexagens e multiplexagens, e essa complexidade aumenta à medida que a largura de banda aumenta. Não oferece eficiência, nem flexibilidade, e sempre que se pretende inserir ou extrair um tributário, é necessário multiplexar e desmultiplexar a trama, bit a bit, para os vários níveis da hierarquia até chegar ao TS pretendido. Outras desvantagens são a existência de três normas distintas e não foi projetado para permitir monitorização.

A tecnologia SDH resolveu alguns problemas associados ao PDH, tais com: *(i)* permite a interligação com dispositivos de outros fabricantes, uma vez que a carta de linha (ótica) está normalizada; *(ii)* oferece proteção automática na ligação (redundância) de rota em caso de falha da ligação, em menos de 50 milissegundos; *(iii)* menor complexidade, em que a gestão do canais elementares é mais eficiente, e custos que a tecnologia PDH; *(iv)* elevado débito, normalizados, que possibilita reservar amplos recursos para a monitorização do desempenho do sistema; e *(v)* permite a monitorização dos seus elementos de rede. As tramas são construídas por multiplexagem síncrona para obter uma estrutura de base padrão (STM), que inclui toda a informação necessária para a gestão da trama.

Com a tecnologia SDH/PDH, a ligação deve ficar estabelecida enquanto durar a troca de dados. A criação de circuitos é complexa, pois é necessário analisar se é E1, *ethernet*, ou ambos, e se o tráfego *ethernet* é transparente. Para agravar esta complexidade há que considerar que qualquer alteração de circuitos obriga a desligar todos os serviços associados. Foram desenvolvidos

mecanismos que garantem melhores resultados no desempenho da utilização da largura de banda com integração de serviços *Ethernet* nos circuitos SDH, designada por *next generation* SDH (NG SDH).

A tecnologia NG SDH permite estender as VLAN a diferentes instalações, mas pode inadvertidamente provocar *loops* ao se configurar um circuito primário e um circuito alternativo, ou pretender balancear a carga (por VLAN) numa malha completa. Nas cartas *ethernet* associadas ao SDH não se utiliza o STP porque a sua implementação é extremamente complexa. Esta extensão das VLAN cria tabelas ARP de grandes dimensões nos comutadores e a quantidade de tráfego de *broadcast* ocupam muita largura de banda.

Outras desvantagens residem *(i)* na matriz de conetorização, que impede uma gestão eficiente da largura de banda, e na gestão das WAN (VLAN); *(ii)* na capacidade de gestão de quantidades de WAN varia de modelo para modelo, tal como a possibilidade de atribuir um segundo rótulo ao tráfego; *(iii)* não dispõe de mecanismos que evitem que pessoas mal-intencionadas (*hacker*), ao utilizar um qualquer PC existente na rede, possa entrar na rede de gestão dos elementos de rede, via TNMS, ou possa provocar uma negação de serviço (*deny of service*, DoS) ao comutador L3.

Também a solução IP associada à solução NG SDH ficou obsoleta devido ao encaminhamento (convencional) ser muito limitado, pois este apenas pode ser realizado pelo traçado mais curto, o que não permite otimizar a utilização dos recursos. Por vezes o caminho mais curto fica sobrecarregado, havendo outros possíveis traçados com disponibilidade para transportar o tráfego. Outra desvantagem é o facto do encaminhamento somente ocorrer com base no seu destino, não permitindo o encaminhamento por classes equivalentes. Um fluxo de informação é uma sequência de pacotes relacionados e que recebem idêntico tratamento em cada nó até chegar ao seu destino final. A arquitetura IP oferece eficiência e robustez, mas consome muito dos recursos de processamento. Outra desvantagem desta arquitetura reside na ordem de chegada dos pacotes, que podem seguir por rotas diferentes, o que obriga o recetor a reordenar os pacotes. Esta reordenação consome tempo e provoca mais latência ao sistema e que, em determinados serviços, pode ser considerado um problema.

São estas desvantagens que estiveram na origem do desenvolvimento do MPLS. O MPLS é baseado no encapsulamento de diferentes protocolos das camadas 2 e 3 do modelo OSI, numa única arquitetura. É um protocolo que permite executar tanto a comutação como o encaminhamento, daí a afirmação de que é uma arquitetura associada à camada 2 e meio, pois não está vinculado a nenhuma camada específica. Disponibiliza vários serviços: *(i)* de qualidade diferenciada, recorrendo ao modelo de serviço diferencial (*DiffServ*); *(ii)* serviços que permitam garantir um nível de serviço contratado (*service-level agreement*, SLA); *(iii)* tráfego de engenharia; *(iv)* serviços de rede privada virtual (VPN); *(v)* serviços de voz sobre IP (VoIP)*;* e *(vi)* transporte qualquer protocolo sobre MPLS.

O MPLS divide-se em três planos lógicos, e o plano de controlo baseia-se na informação recolhida pelo protocolo IGP, daí a designação IP MPLS. Comparando com a arquitetura IP, que se baseia no encaminhamento pelo processo do "próximo salto" até chegar ao seu destino, o MPLS permite melhor, em muito, eficiência no encaminhamento dos pacotes IP. Consiste na utilização do mecanismo de comutação aproveitando o encaminhamento por IP, o que proporciona o melhor dos dois mundos: a flexibilidade e robustez da arquitetura IP e qualidade de serviço do SDH. Esta arquitetura associada aos mecanismos adicionais (extensões), como a engenharia de tráfego, permite garantir a qualidade de serviço e a segurança dos serviços. A engenharia de tráfego oferece métodos e mecanismos de controlo de encaminhamento que permitem otimizar

o uso dos recursos, assegurando a qualidade de serviço nos critérios mais importantes como o da largura de banda, e nos tempos de atraso. Permite também direcionar o tráfego através de uma rota específica, o que não é feito necessariamente pelo menor custo (no sentido lato). Os administradores de rede podem implementar políticas para garantir uma ótima distribuição de tráfego e melhorar a utilização global da rede.

Uma das vantagens do MPLS, ao ser comparada com a comunicação baseada no método de transmissão TDM, é a sua flexibilidade proporcionada pela gestão dinâmica da sua largura de banda. Em contraste com uma largura de banda fixa por canal oferecida pelo método TDM, no MPLS a largura de banda disponível pode ser distribuída entre os diversos serviços existentes. Otimiza fluxos de múltiplas aplicações sem reduzir o desempenho da rede. É muito flexível, pois permite combinar diferentes aplicações *legacy* e IP. Ou seja, possibilita que as duas tecnologias estejam em uso ao mesmo tempo. Oferece suporte as *interfaces* tradicionais *(legacy)*, o que permitiu uma fácil migração de toda a rede existente e disponibiliza várias opções de sincronização. Esta arquitetura dispõe de mecanismos de recuperação rápida em caso de falhas na rede, como o *loop-free alternative fast rerouter*. Garante diversos encaminhamentos assim como o balanceamento da carga.

Uma rede elétrica é considerada como sendo uma infraestrutura crítica, e por isso, o seu serviço de telecomunicações tem que dispor de um elevado desempenho e confiabilidade. Com milhares de dispositivos inteligentes distribuídos nas suas infraestruturas, esta arquitetura oferece os melhores tempos de resposta ao problema, menor número de interrupções, e por isso, reduz os custos de inoperância e aumenta exponencialmente a eficiência.

A migração da tecnologia deveu-se ao novo posicionamento da EEM face ao paradigma "*smart grid*", em que a tendência emergente para as comunicações nas subestações modernas passa por uma aposta numa infraestrutura de comunicação baseada na comunicação de pacotes. As necessidades atuais para um sistema de comunicação da subestação moderna estão vocacionadas, e otimizadas, para redes que utiliza a comutação baseada em pacotes por forma a possibilitar suportar os modernos *intelligent electronic device* (IED) multifuncionais. É cada vez mais comum encontrar um ambiente *ethernet* nas subestações, pois a construção de redes *ethernet* é cada vez menos dispendiosa e permitem lidar com a transferência de dados de forma mais eficiente do que as redes tradicionais de comutação de circuitos.

O MPLS permite uma extraordinária escalabilidade que advém da utilização do conceito VRF, pois não cria limitações na utilização de redes iguais para serviços diferentes. É assim possível criar-se mais serviços, adicionar mais elementos de rede, sem riscos de provocar sobrecarga da rede de telecomunicações.

Apesar da convergência ser rápida, menos de 50 milissegundos, utilizando o mecanismo *loop-free alternative fast rerouter*, há serviços que exigem melhores tempos de reposição de serviço, como é caso da teleproteção. E esta arquitetura disponibiliza um mecanismo, designado engenharia de tráfego, que permite estipular uma rota alternativa explicita, não sendo por isso necessário recálculo. Os tempos de reposição são inferiores a 10 milissegundos. Para receber este tráfego tradicional (X21) o fabricante Cisco disponibiliza módulo que emulam de circuito sobre a rede com comutação de pacotes CESoPSN e SAToP.

O MPLS permite implementar VPN, tanto da camada 2 como 3, muito mais facilmente e sem constrangimentos. Ou seja, o encaminhamento na VPN é controlado utilizando comunidades de destino de rota VPN, o que permite encaminhar pacote com o mesmo IP de destino de cliente diferentes, utilizando o atributo *route distinguisher*. Este mecanismo também permite isolar o

tráfego do mesmo cliente, recorrendo ao atributo *route target*. O atributo *route target* é utilizado para criar a topologia em estrela.

A segurança da rede no mundo de hoje, apesar de importante, não tem definições, principalmente quando se trata de segurança empresarial, pois não se sabe de quem se pretende proteger. O MPLS permite integrar na rede um conjunto de controlos associados à cibersegurança, entre os quais uma camada de *firewall* de perímetro, acesso remoto via *VPN IPSec* e controlo de acesso à rede.

A opção de subdividir o sistema autónomo em áreas foi descartada por não haver necessidade, e por esta solução implicar um planeamento diferente na atribuição de IP. É necessário ponderar a sumarização, pois é a base de funcionamento das áreas. A EEM optou por subdividir o seu sistema autónomo em outros sistemas autónomos. Assim, a rede de transporte pertence a um único sistema autónomo e as diversas instalações do SEPM são diferentes sistemas autónomos. Daí a necessidade de escolher o protocolo de encaminhamento dos pacotes IP ser o OSPF e os prefixos de rede VPN-IPv4 serem anunciados pelo protocolo de encaminhamento BGP. Como o protocolo exige *router* de fronteira, foram definidos os *routers* PE. E como o protocolo de encaminhamento BGP obriga a sessões com todos os *routers* de fronteira, foi instalado um *route refletor* que permite simular uma rede com topologia de malha completa. Esta opção permite redundância e reduzir o tráfego de sessão.

O projeto implementado na EEM responde aos requisitos conhecidos à data da sua implementação, mas poderá vir a responder a futuros serviços que venham a ser necessários implementar sem exigir melhorias no projeto. Esta nova arquitetura, também garante flexibilidade necessária aos futuros serviços que venham a ser implementados, reduzindo assim os riscos de inoperância. Os futuros serviços podem exigir ligações adicionais, o que pode implicar alterações das condições existentes, mas em que será possível uma convergência rápida da rede, por forma a garantir a sua eficiência.

Os equipamentos do fabricante Cisco, por forma a garantir uma elevada resiliência, dispõem de mecanismos que permitem evitar interrupções no encaminhamento de pacotes em caso de falha de um processador (mecanismo NSF) ou ligação ótica (mecanismo NSR). A falha da ligação ótica pode ser melhorada com o mecanismo LAG, que permite agregar dois portos óticos numa única ligação virtual. Esta tecnologia evolui para o *multi-chassis link aggregation group* (MC-LAG), que consiste em que os portos óticos da mesma ligação virtual podem divergir para dispositivos diferentes, salvaguardando assim uma eventual falha de um dispositivo.

Possibilidade de gestão da rede de telecomunicações a partir de uma única plataforma. Essa possibilidade implica um planeamento de IP estáticos, para atribuir aos dispositivos de rede.

Possibilidade de alargar a outros serviços, como facilidade em implementar soluções de cibersegurança e segurança física das instalações (camaras, pontos de acessos).

Prespectivas de trabalhos futuros

Como parte da implementação da solução *smart grid*, a EEM projeta o seu futuro com base em aplicações de rede inteligentes, que exigem sistemas avançados de comunicação multiponto. É necessário garantir uma elevada resiliência e segurança ao sistema de telecomunicações, que deve ser capaz de agregar e transportar todos os serviços ao mesmo tempo que disponibiliza serviços empresariais. Isso é possível graças à implementação de uma tecnologia baseada na troca de rótulos e num ambiente *multi-protocolo*, em que, numa única infraestrutura comum, é possível transportar um grande número de serviços, fornecendo ao mesmo tempo um elevado nível de segurança. Devido à variedade de assuntos, este trabalho não abordou todos estes temas, tais como: *(i)* a implementação de unidades de medição de fase (*phasor measurement units*, PMU) e sistemas *wide area monitoring systems* (WAMS), que oferecem oportunidades para melhorar as proteções convencionais de integridade de um sistema elétrico. Essas melhorias podem aumentar a conscientização dos sistemas de proteção do estado do sistema, proporcionando robustez para distúrbios imprevistos e segurança operacional aprimorada para eventos extraordinários; *(ii)* ao contrário dos sistemas de proteção convencionais aplicados para proteger um elemento específico do sistema de energia, os SIPS são instalados para proteger a integridade do sistema de energia ou partes estratégicas do sistema. Os SIPS abrangem os esquemas de proteção wspecial (*special protection schemes*, SPS), *remedial action schemes* (RAS) e variedades de outras redes de segurança.

Hoje em dia, e devido a evolução, as infraestruturas de energia são controladas por sistemas computadorizados interligados através de uma rede de telecomunicações. Existe uma dependência cruzada, em que a energia depende das telecomunicações e as telecomunicações dependem da energia. Devido a essa combinação muito sensível e fulcral, as empresas do sector ficam sujeitas a ataques informáticos e sequestro de informações. Também deve ser ponderada colocar a informação em sites onde a segurança não é garantida. As empresas devem de fazer auditorias de segurança que permitem determinar os seus riscos. Depois dessas análises de riscos promovendo a sua cibersegurança, por forma a poder se tomar medidas para que esse risco seja mitigado. Este trabalho não aprofundou este tema tão importante, cibersegurança. É possível implementar segurança na rede, no acesso aos dados e quem os pode aceder, utilizando ferramentas como o Identity Services Engine, *firewall*, *FirePower*, sistema de prevenção e de deteção de intrusão.

6. Apêndice 1 – Sistema ótico

Hoje em dia, os sistemas de telecomunicações assentam em duas tecnologias distintas: *(i)* rádio, que garante serviços com recurso à propagação pelo espaço livre; *(ii)* ou numa ligação física por guia de onda eletromagnética. Uma onda eletromagnética é constituída por um campo elétrico e outro magnético, que oscilam à mesma frequência. Os dois campos, perpendiculares entre si, propagam se no meio numa direção ortogonal ao plano em que os campos oscilam. O guia de onda tanto podem ser fios metálicos como fibra ótica *[6]*.

6.1 Fibras óticas

No contexto do desenvolvimento excecional ocorrido nas telecomunicações, a fibra ótica tem demonstrado, integrada em sistemas de transporte de telecomunicações de grandes capacidades, ser uma excelente solução técnica para a transmissão. É uma tecnologia que permite o transporte de dados a alta velocidade, com baixas perdas, sendo hoje em dia a tecnologia dominante nos *backbones*. Já está a ser implementada nas redes de acesso, substituindo assim paulatinamente os fios metálicos por forma a satisfazer a demanda, cada vez maior, dos subscritores.

A fibra é constituída por um meio dielétrico, de secção circular, provido de caraterísticas físicas que possibilitam a propagação. Um material (constituinte de um meio) dielétrico é um material em que não existem cargas elétricas livres. É de baixo custo de produção, uma vez que a matéria-prima utilizada no seu fabrico, areia, existe em abundância. Pode ser instalada em qualquer ambiente industrial, ou até explosivo, pois não existe a possibilidade de iniciar combustão, ou em infraestruturas onde existem grandes potências elétricas. A tecnologia, por ser insensível a perturbações provocadas pelas interferências eletromagnéticas (IEM), possibilita agrupar milhares de fibras no mesmo cabo. O cabo de fibras (agrupadas) é muito mais leve que um cabo de fios metálicos com a mesma quantidade física de guias de onda metálicos e, como tem um diâmetro menor, o seu manuseamento é mais fácil. As fibras óticas podem ser utilizadas nas infraestruturas de passagem de cabos de cobre existentes, permitindo assim baixos custos na sua disseminação. A disponibilidade de serviço não é afetada no caso do cabo, ou da caixa de junta de cabos, ficar submersa devido às inundações das instalações, graças à estanquicidade dos materiais utilizados. Um cabo de fibra tem uma vida útil superior a 25 anos e suporta temperaturas de operação que variam entre -60 a +85 ˚C, sendo que a degradação ocorre mais ao nível do revestimento do cabo do que da fibra, pois esta resiste mais à corrosão. Como a fibra não conduz eletricidade, não existe a possibilidade de provocar um curto-circuito numa operação de correção ou manutenção, e não são possíveis derivações indetetáveis. As técnicas utilizadas no processamento do sinal, modulação e desmodulação do sinal, podem ser as mesmas que eram utilizadas na tecnologia de fio de cobre, mas ao possibilitar portadoras da ordem dos 100 000 GHz, disponibiliza uma enorme largura de banda.

As desvantagens na utilização da fibra são a sua pouca resistência aos esforços mecânicos. São também necessários dispositivos específicos, e mais caros do que os utilizados numa infraestrutura de cabo de cobre, na implementação de uma instalação nova, ou na correção, e para os respetivos ensaios. Além disso, em caso de falha de energia nos dispositivos de acesso, ou mesmo remotos, não é possível alimentá-los usando a fibra, sendo necessário prever infraestruturas de alimentação independentes.

Tipos de fibras

Um modo guiado define a propagação da radiação eletromagnética ao longo da fibra. Nos sistemas de telecomunicações consideram-se geralmente dois tipos de fibra: multimodo e monomodo. A distinção baseia-se na forma como a luz se propaga pela fibra e está intimamente relacionada com o diâmetro do núcleo.

As fibras multimodo são caracterizadas por proporcionarem a propagação de vários modos do mesmo sinal no núcleo. Estas fibras óticas permitem uma maior facilidade no acoplamento da luz ao núcleo e um baixo custo da fonte de luz. Além disso, a fibra multimodo é bastante sensível à dispersão modal, o que reduz o comprimento do traçado.

A fibra monomodo padrão tornou-se a escolha incontornável nos sistemas de telecomunicações, pois oferece um bom desempenho num sistema de transmissão ótico, apesar de ter um diâmetro de núcleo pequeno. Ao ter um diâmetro pequeno, cria condições para que só exista um único modo de propagação, contribuindo assim para a eliminação da dispersão modal. Além disso, cria dificuldades no acoplamento eficiente do feixe, obrigando a que a fonte ótica tenha que ser um *díodo laser*. A atenuação característica das fibras monomodo é mais baixa do que a um multimodo, possibilitando assim o aumento do comprimento do traçado, sem ser necessário regenerar o sinal.

6.2 Fenómenos que afetam o desempenho das transmissões

O bom desempenho de um sistema de telecomunicações é caracterizado pelo facto do recetor receber uma potência suficiente que lhe permite distinguir o sinal (útil) do ruído detetado. Num ambiente de propagação ótico este desempenho está dependente de fenómenos lineares e não-lineares, afetando tanto a sua qualidade como limitando o aumento da capacidade de transmissão. Para melhorar o desempenho e a qualidade do sistema, é necessário reduzir os fenómenos de atenuação e de espalhamento, que nunca serão nulos.

Fenómenos de atenuação

Para resolver o problema causado pela atenuação, a solução não passa por intensificar o nível de potência de emissão para atender aos requisitos de sensibilidade do recetor pois *(i)* tal também pode agravar, de forma exponencial, os efeitos não lineares na fibra; *(ii)* ou provocar o aumento das reflexões, gerando instabilidade na cavidade do díodo laser. As reflexões são devidas ao efeito de *Fresnel*, e podem representar até 4%, ou mais devido a sujidades nas faces expostas da fibra, quando se ligam os cordões (*patch-cord)*. Essa sujidade também pode ser queimada devido à potência, deixando partículas opacas. Essa instabilidade provocada pelas reflexões traduz-se em fenómenos não lineares na cavidade do díodo laser e pode, no limite, danificar o próprio díodo laser.

Nota-se que o efeito de *Fresnel* está relacionado com o fenómeno de reflexão-refração de ondas eletromagnéticas na transição entre dois meios cujo índice de refração é diferente. O efeito de *Fresnel* descreve a relação entre as potências da onda incidente e das ondas refletida e transmitida.

Fenómenos de dispersão

A dispersão corresponde ao alargamento dos impulsos de luz durante a sua propagação ao longo de uma fibra. Ao provocar o alargamento do impulso, este afeta negativamente a capacidade de transporte de informação, pois potência o surgimento de interferência inter-simbólica. Devem-se considerar três formas de dispersão: modal (exclusivo no multimodo), cromática, e do modo de polarização. A Figura 6.1 ilustra os vários fenómenos de dispersão.

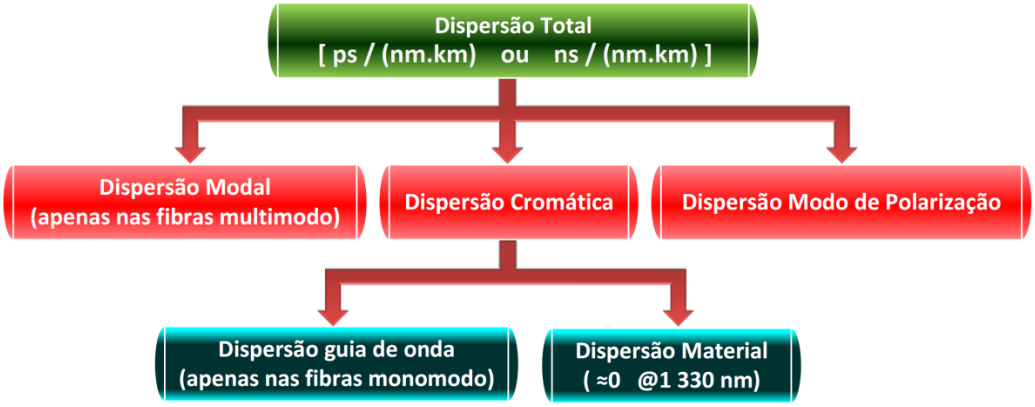

Figura 6.1 – Fenómenos de dispersão nas transmissões.

- *Dispersão cromática*

Nos *backbones* o conhecimento e controle do mecanismo de dispersão cromática (ou intermodal) é decisivo na obtenção de um bom desempenho na propagação de impulsos curtos e para baixar os custos de operação. Os impulsos curtos estão associados a ritmos de transmissão elevados. Os efeitos dispersivos podem obrigar a regenerar o sinal antes da atenuação degradar o sinal.

- *Dispersão do modo de polarização*

Uma fibra monomodo é uma fibra que só permite o modo fundamental, que na realidade corresponde a dois modos ortogonais, independentes entre si e idênticos, mas com planos de polarizações ortogonais. O fato de o núcleo sofrer de assimetria geométrica, por exemplo provocada por uma forma elíptica, ou por existirem imperfeições na estrutura do vidro, ou por suportar tensões residuais externas, faz com que o núcleo sofra de birrefringência. Esta variação devido à birrefringência (fraca) cria condições para que os modos tenham velocidades de grupo diferentes e ocorra uma rotação aleatória do eixo de propagação ao longo da fibra, provocando o desfasamento entre esses dois modos, ilustrado na Figura 6.2. É este desfasamento que caracteriza o fenómeno não linear de dispersão de modo de polarização (*polarization division multiplexing*, PMD).

Utilizando 1550 nm como portadora, a PMD característica é de 0,2 ps, mas devem ser consultadas as características de transmissão no catálogo no fabricante. O problema relacionado com a dispersão do modo de polarização surge nas taxas de transmissão a partir dos 10 Gbps, e os problemas agravam-se quando se estão a utilizar taxas de transmissão superiores a 40 Gbps.

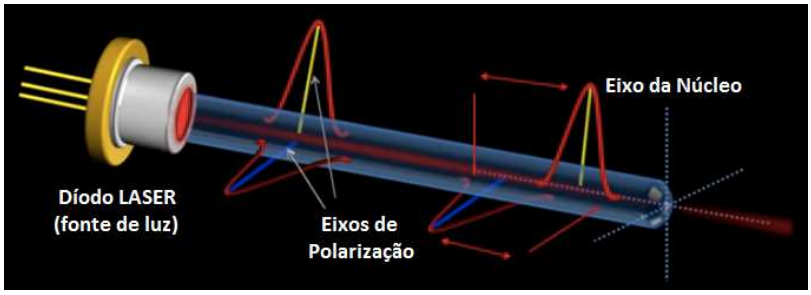

Figura 6.2 – Dispersão do modo de polarização *[6.1-1]*.

Diâmetro modal do modo fundamental

Um outro parâmetro que influencia o desempenho de um sistema ótico é o diâmetro modal do modo fundamental (*mode field diameter,* MFD). Um determinado nível de potência, aplicado a uma pequena área efetiva, proporciona uma elevada densidade de potência, o que potência os fenómenos não lineares. A Figura 6.3 ilustra o facto da potência do campo elétrico se distribuir num diâmetro superior ao diâmetro do núcleo, tendo a forma aproximada de uma gaussiana. Assim se explica que as curvaturas mais acentuadas na fibra causem mais atenuação, pois parte da energia propaga-se na bainha e é desperdiçada.

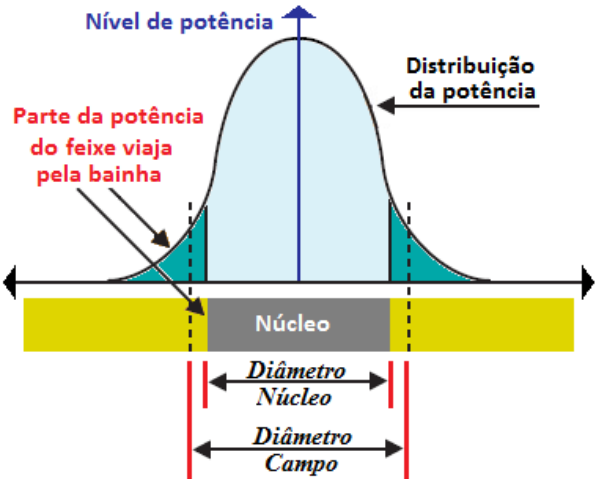

Figura 6.3 – Diâmetro efetivo do núcleo (MFD) numa fibra monomodo.

Utilizando 1550 nm como portadora o MFD característico é de 9,8 ±0,5 nm (a variação depende da fibra), mas devem-se consultar as características de transmissão no catálogo do fabricante.

Janelas de transmissão

A Figura 6.4 ilustra as contribuições individuais dos fenómenos mais significativos (ignorando os fenómenos não lineares) que degradam o sinal ótico numa fibra monomodo, e o seu somatório (representado pela linha amarelo escuro), numa fibra.

É também possível identificar as três janelas de transmissão: *(i)* a primeira janela é utilizada com fibras multimodo, em sistemas de baixo débito, com uma largura de banda de 100 nm, e situa-se nos comprimentos de onda que se situam entre os 800 e os 900 nm com uma atenuação

característica de 3 dB/km; *(ii)* a segunda janela, com uma largura de banda de 100 nm, situa-se nos comprimentos de onda que se situam entre os 1260 e os 1360 nm com uma atenuação característica de 0,4 dB/km, e ainda é utilizada nas fibras monomodo; *(iii)* a 3ª janela, tem uma largura de 200 nm, e situa-se nos comprimentos de onda que se situam entre os 1460 e os 1675 nm. Qualquer comprimento de onda inferior a 800 nm não é utilizado nos sistemas de telecomunicações óticas, porque a atenuação, devido ao espalhamento de *Rayleigh* é demasiado elevada. Outro fenómeno que contribui para as perdas na fibra a partir dos 1550 nm, é a absorção de material no IV (que aumenta muito rapidamente com o aumento do comprimento de onda de interesse).

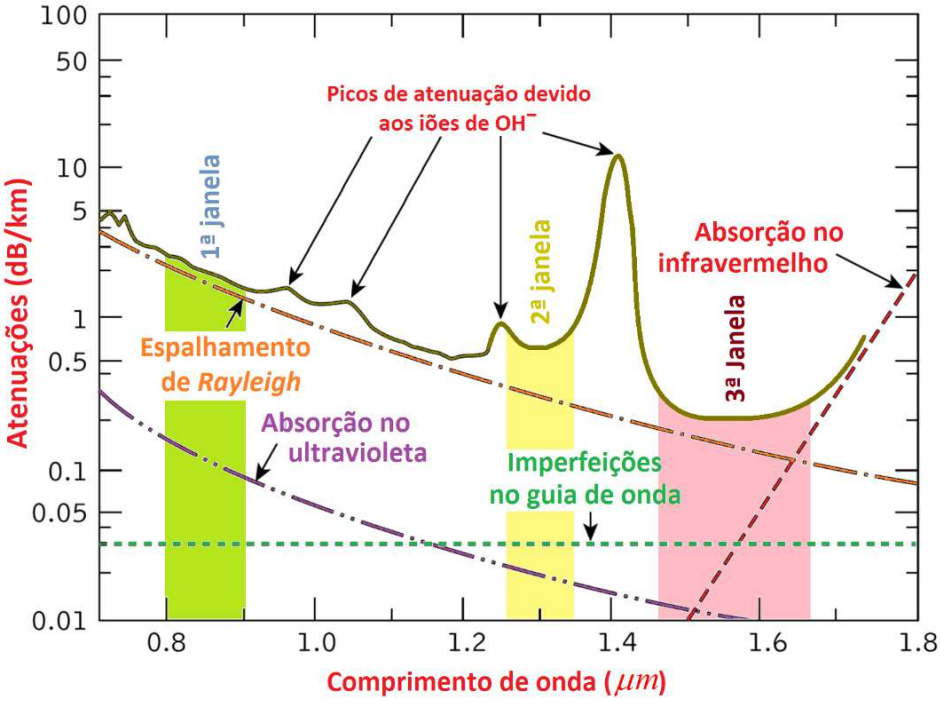

Figura 6.4 – Os vários fenómenos geradores de atenuação *[6.1-2]*.

Os comprimentos de onda com utilização comercial nas telecomunicações são também divididos em 6 bandas: *(i)* banda O, banda original, que se situa entre os 1260 e os 1360 nm; *(ii)* banda E, banda estendida, que se situa entre os 1360 e os 1460 nm; *(iii)* banda S, banda de comprimentos de ondas curtos, que se situa entre os 1460 e os 1530 nm; *(iv)* banda C, banda convencional ("*erbium window*"), que se situa entre os 1530 e os 1565 nm; *(v)* banda L, banda de comprimentos de ondas longos, que se situa entre os 1565 e os 1625 nm; *(vi)* banda U, banda de comprimentos de ondas ultralongos que se situa entre os 1625 e os 1675 nm. As mais usadas comercialmente são as "O" (1310) e "C" (1550).

6.3 Técnica de multiplexagem WDM

Embora os sistemas de comunicação utilizem geralmente o método de transmissão TDM num único comprimento de onda, na procura de uma melhor eficiência dos recursos instalados, uma nova tecnologia surgiu no início dos anos 90: a técnica da multiplexagem por divisão de comprimento de onda *(wavelength division multiplexing,* WDM). A ideia é "injetar" vários

comprimentos de onda simultaneamente numa única fibra, conforme ilustrado na Figura 6.5. A fibra ótica é adequada para este tipo de utilização, porque tem uma largura de banda, extremamente elevada (dezenas de Tbps). Tem por isso um potencial da multiplexagem de muitos canais, e para longas distâncias.

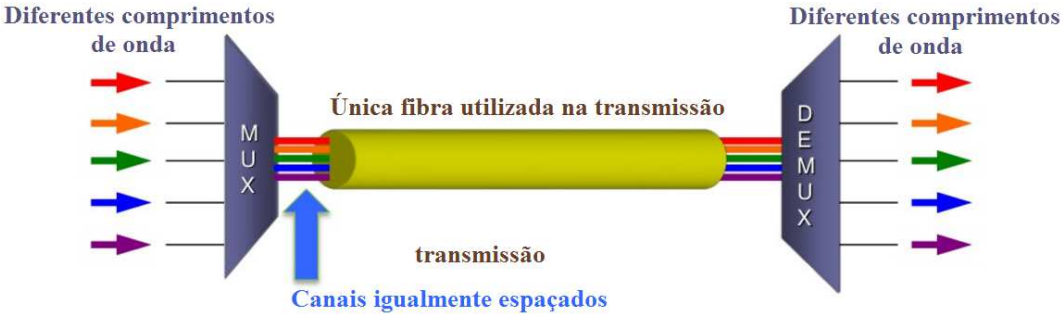

Figura 6.5 – Técnica WDM.

A WDM permite melhorar a utilização da largura de banda, desenvolvida especificamente para ser utilizada com fibras óticas do tipo monomodo, permitindo aos operadores de telecomunicações obter muita mais largura de banda sem terem que investir nas suas infraestruturas de fibra ótica. O WDM tem um fator limitativo na utilização de amplificadores óticos EDFA, pois estão limitados a um valor típico de 5 THz, e entre cada canal deve existir uma largura de banda de guarda de 50 Gbps (ITU-T G.692). Os sistemas WDM multiplexam até 400 comprimentos de ondas, com uma capacidade individual de 10 Gbps, a distâncias que podem chegar aos 120 km sem necessitarem de serem regenerados.

O padrão internacional utilizado é o ITU-T G.692 (*interfaces* óticas para sistemas multicanais com amplificadores óticos) que define a gama de comprimentos de onda da janela de transmissão, que se situa entre os 1530 e os 1565 nm, que é onde ocorre o menor valor de atenuação.

Comercialmente existem várias designações, mas o princípio é o mesmo: *(i)* designa-se *Coarse* WDM a técnica que consiste em injetar entre 8 e 16 comprimentos de onda; *(ii)* por *dense wavelength-division multiplexing* (DWDM) a técnica que consiste em injetar entre 16 e 160 canais; *(iii)* por *ultra* WDM que consiste em injetar entre 160 e 400 comprimentos de onda.

7. Apêndice 2 – Arquitetura Hierarquica Digital Plesiócrona

A tecnologia baseada em PDH estabelece ligações ponto-a-ponto e têm uma característica que a diferencia da tecnologia síncrona: não necessita de estar sincronizada com o relógio da rede, realizando o controlo localmente. Esta tecnologia assenta na utilização de uma técnica baseada na multiplexagem dos dados para canais elementares (básicos), com uma capacidade de 64 kbps. Na tecnologia PDH, o *time slot (TS)*, ou tributário E0, é o primeiro nível da hierarquia desta tecnologia que contém a informação, e é mapeada numa trama E1 (norma europeia, e que foi a utilizada neste documento) sem ter em conta a sua ordem de chegada. Refira-se que "tributário" surge na literatura técnica como uma abreviatura para designar "trama de tributário", que é a informação presente no canal de comunicação ou o débito binário no acesso ao canal. O mapeamento consiste em mapear os tributários nos TS da trama E1. Uma trama E1 é constituída por 32 TS, com um débito binário total de transmissão de 2 048 kbps, de duração fixa de 125 µs, conforme ilustrado na Figura 7.1, sendo por isso necessários 3,90625 µs para transmitir cada TS.

Esta tecnologia permite que se tenha uma taxa de transmissão mais elevada, agrupando dados de baixo débito. Por não ser síncrono, o procedimento necessário para encontrar (identificar na trama E1) um determinado sinal de baixo débito, obriga a uma constante utilização do multiplexador e desmultiplexador (processo realizado bit a bit) para realizar tarefas básicas, como a de extrair/inserir (*Drop/Insert*) dados de um tributário. Este ciclo repetitivo torna o processo lento e complexo, elevando o custo da operação de transmissão, sendo propício à geração de erros e atrasos.

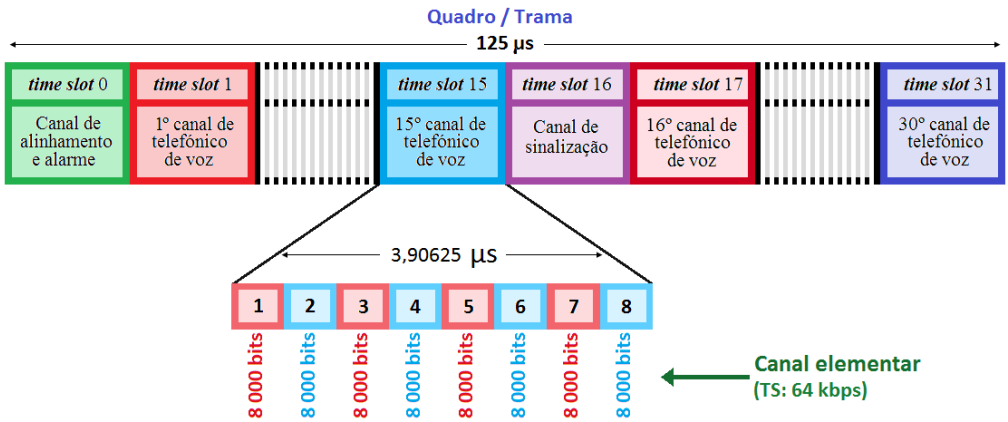

Figura 7.1 – Constituição de uma trama E1.

Esta tecnologia de multiplexagem não possibilita redundância, e opera ao nível da camada 1 do modelo OSI. Além disso não foi projetada para permitir uma monitorização e gestão centralizada, pois não disponibiliza os bits necessários a essa monitorização. Outro constrangimento reside no facto de não existir uma, mas sim três normas distintas: a europeia; a americana; e a japonesa, conforme a Figura 7.2, não proporcionando uma livre escolha entre os diversos fabricantes. Para realizar as interligações são necessários equipamentos adicionais, de adaptação aos diferentes débitos. A recomendação ITU-T G.702, *digital hierarchy bit rates*, define os ritmos de transmissão da hierarquia de transmissão PDH. Os níveis superiores da hierarquia, na norma europeia, são

obtidos pela junção de 4 níveis inferiores. Assim, o E2 é o resultado da junção de 4 E1, o E3 é o resultado da junção de 4 E2, e o E4 é o resultado da junção de 4 E3. Mas não se obtém um E4 com a junção de 64 E1. É preciso passar pelos passos intermédios. Refira-se que esta tecnologia (na norma europeia) está normalizada até os 140 Mbps.

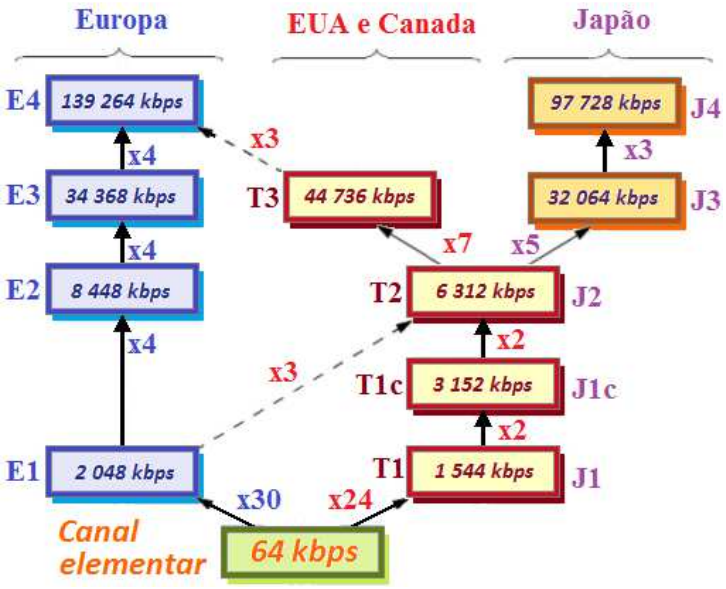

Figura 7.2 – Hierarquias normalizadas das diferentes normas PDH.

A recomendação ITU-T G.703 descreve o padrão do encapsulamento da trama E1, definindo *(i)* as características físicas e elétricas das *interfaces* digitais hierárquicas para a transmissão de voz, ou dados, através de ligações digitais para os operadores, como o E1, ou T1 na versão americana, com taxas de transmissão de 1 544 kbps; *(ii)* fornece as especificações da modulação por código de pulso (PCM).

8. Apêndice 3 – Arquitetura Hierarquica Digital Síncrona

Devido às limitações da tecnologia baseada em PDH na adaptação aos novos desafios requeridos pelo mercado das telecomunicações, em 1988, resultante de uma série de recomendações da ITU, os operadores de telecomunicações passaram a dispor da tecnologia SDH. Esta é uma tecnologia vocacionada para o transporte de informação em redes que percorrem longas distâncias, alavancadas pela utilização da fibra ótica. Comparando com a tecnologia baseada no PDH, esta representa um salto tecnológico e surgiu já normalizada, permitindo atender às necessidades dos operadores *[8]*.

Na arquitetura TCP/IP, a tecnologia SDH situa-se na camada 1 do modelo OSI, e oferece soluções totalmente controladas, fiáveis, taxas elevadas de transmissão, proteção automática na ligação, e permite a interconexão com equipamentos de outros fabricantes.

Quando surgiu a tecnologia SDH, esta respondia a vários objetivos: flexibilidade, facilidade de exploração, e escalabilidade para altos débitos binários. A normalização da tecnologia ocorre ao nível da carta de linha ótica (*optical line card*, OLC), pois é o que permite a interconexão entre diferentes sistemas. Entende-se por "carta", uma carta eletrónica que se instala num dispositivo e que realiza uma determinada tarefa. A entidade básica desta tecnologia é a *Synchronous Transfer Mode* (STM), obtida pela agregação de vários tributários, recorrendo à multiplexagem, no domínio dos tempos. Cada trama é composta por duas zonas distintas: uma de dados úteis (*payload*) e uma de dados de serviço (cabeçalho e ponteiro). O cabeçalho e o ponteiro, que são bits suplementares, destinam-se à monitorização e gestão da trama. A trama STM é estruturada em octetos, e o sinal útil é colocado num invólucro adaptado a cada tributário, chamado de recipiente, ou contentor (*container, C*). O contentor é uma entidade na forma de bloco de octetos cuja capacidade está dimensionada para assegurar o transporte de um dos diferentes débitos de acesso (tributários) definidos pela ITU-T para a norma SDH. Um tributário chega com uma determinada taxa de débito, é alojado no respetivo contentor e, se necessário, são-lhe adicionados octetos de enchimento. Os octetos de enchimento têm o papel de adaptar a taxa de débito (capacidade variável) ao contentor (capacidade fixa).

Um contentor virtual (*virtual container*, VC) é uma estrutura de informação constituída por um contentor e um cabeçalho de caminho (*path over head*, POH), e são classificados em ordem inferior (*low order*, LO) e ordem superior (*high order*, HO). O POH é criado no momento em que o tributário entra na rede SDH e é extraído à saída. É utilizado para caracterizar o serviço dado ao sinal transportado, sendo constituído por um conjunto de bits que possibilita a gestão do tráfego. A caracterização assenta na avaliação do estado do encaminhamento, da estrutura útil de carga transportada, da origem e do destino do tributário. O *virtual container low order* (VC LO) tem uma capacidade inferior a 45 Mbps, permitindo assim suportar diferentes tipos de sinais tais como: PDH; *asynchronous transfer mode* (ATM); *fiber distributed data interface* (FDDI), alojados nos VC-11, VC-12, VC-2 e VC-3, e têm um período de 500 µs. Os VC-11, VC-12, VC-2 e VC-3 são subgrupos do VC LO. Cabe à função de multiplexagem a adaptação do contentor LO ao HO (de período de 125 µs). O alinhamento consiste em adicionar um ponteiro ao VC LO, pois o VC LO não tem uma posição fixa no dados úteis da trama STM-N, mas o ponteiro tem.

A flexibilidade de um sistema de multiplexagem síncrono advém da facilidade em reorganizar a trama, uma vez que possibilita um acesso direto a um determinado tributário transportado na trama STM-N. Esta capacidade funcional de reorganizar a trama STM-N, que consiste em

adicionar e/ou extrair tributários até à granularidade de um VC-11/12, é designada por "*add/drop multiplexer*" (ADM), e funciona sem ser necessário multiplexar (montar) e desmultiplexar (desmontar) toda a trama. A informação necessária para a realização da função ADM está contida no POH. O VC-11 é utilizado para mapear os tributários PDH da norma americana (T1), e o VC-12 é para os tributários da norma europeia (E1).

Multiplexagem na tecnologia SDH

A multiplexagem, neste contexto, é uma técnica utilizada para associar vários tributários num outro tributário de maior capacidade, garantindo ao mesmo tempo que não haja interferência entre eles. A Figura 8.1 ilustra os diversos passos necessários à construção de uma trama STM-1. A trama E1, tributário de menor capacidade neste contexto (SDH), é primeiro alojada num contentor C12, mas sem qualquer informação adicional, apesar da estrutura de trama ser de maior capacidade. Essa capacidade extra permite adaptar pequenas variações de velocidade dos débitos binários da fonte e é preenchida com octetos de justificação fixa (*stuffing*). O octeto de justificação fixa não é informação útil, apenas serve para adaptar a capacidade do contentor. Mas, como o contentor necessita de informação adicional para entrar na rede SDH, é-lhe adicionado um cabeçalho de caminho (POH), transformando-o assim num VC-12.

A unidade tributária (*tributary unit*, TU) é um VC LO e existem 4 variantes: TU2; TU3; TU11; TU12. É adicionado um ponteiro ao TU que permite assim localizá-lo devido à flutuação a que fica sujeito em relação a estrutura do VC HO *[8-1]* em que está alojado. O primeiro bit do VC LO dentro do VC HO é referênciado por um ponteiro da unidade tributária. Assim, ao se adicionar um ponteiro ao VC-12 obtém-se o TU-12.

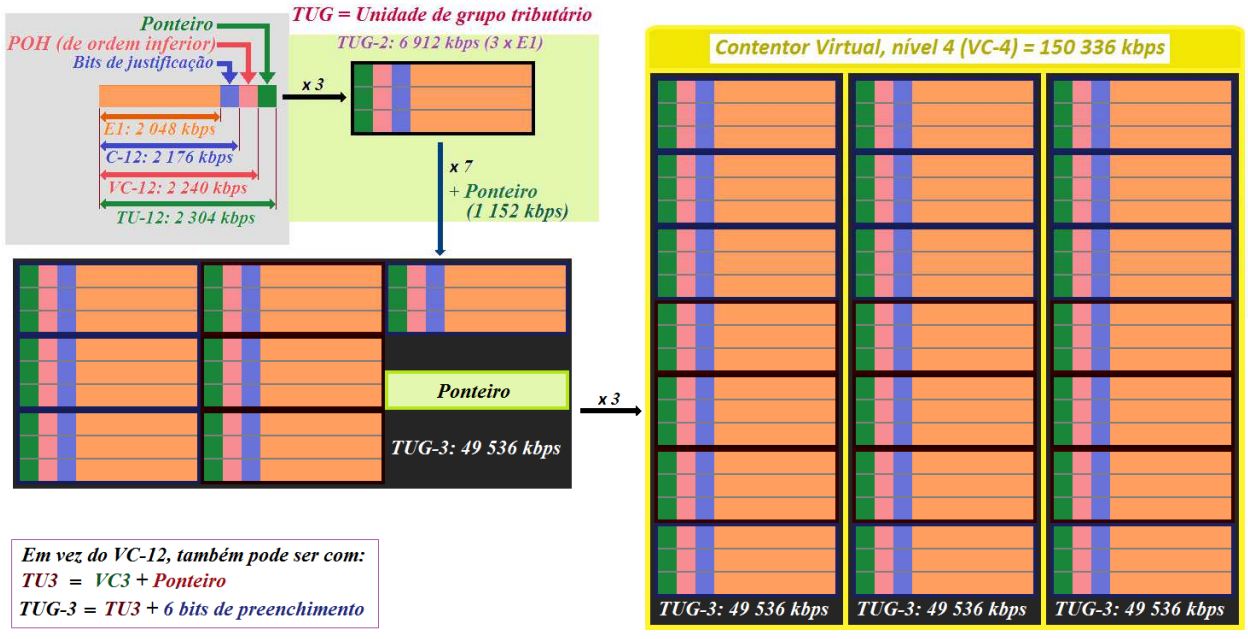

Figura 8.1 – Construção de uma estrutura VC-4.

A partir da combinação de várias TU resulta o designado grupo de unidade tributária (*Tributary Unit Group*, TUG), que é um VC HO e disponibilizado em duas variantes: TUG2 ou TUG3. Uma TUG2 pode ser construída por conjuntos de 4 TU-11, ou 3 TU-12 (conforme exemplo utilizado na

Figura 8.1), ou ainda por um TU-2. Todos eles têm capacidades diferentes, mas a capacidade do TUG2 é fixa, pelo que é preciso preencher os espaços em branco, quando existam, com *stuffing*, para adaptar os débitos binários *[8-2]*. Com 7 TUG-2 e um ponteiro de localização, obtém-se um TUG-3.

Agregando 3 TUG-3 resulta num VC-4 (VC OH), de capacidade 150 336 kbps, que somado com a capacidade de 5 184 kbps do *section overhead* (SOH), resulta na capacidade da trama STM-1 (155, 52 Mbps). O SOH para além de ter as mesmas funções que o POH, também permite o alinhamento da trama e a comutação automática da proteção, permitindo assim qualidade de serviço e grandes aumentos de disponibilidade. O SOH divide-se em três partes: *(i)* regenerador da secção do cabeçalho (*regenerator section overhead*, RSOH)*; (ii)* multiplexador da secção do cabeçalho (*multiplex section overhead*, MSOH)*; (iii)* e ponteiro da unidade administrativa, como ilustrado na Figura 8.2. O RSOH contém informações que indicam aos elementos de rede (NE) da rede SDH como devem proceder para realizarem a regeneração da trama STM-N. O MSHO contém informação que indica aos elementos de rede como proceder para extrair tributários da trama e como proceder em caso de falha de ligação física.

Os níveis seguintes de hierarquia, STM-N, obtêm-se através da junção, por multiplexagem de 4 níveis anteriores. A tecnologia SDH está normalizada até 40 Gbps, mas só é possível obter-se essa capacidade através da utilização de VC HO (VC-4).

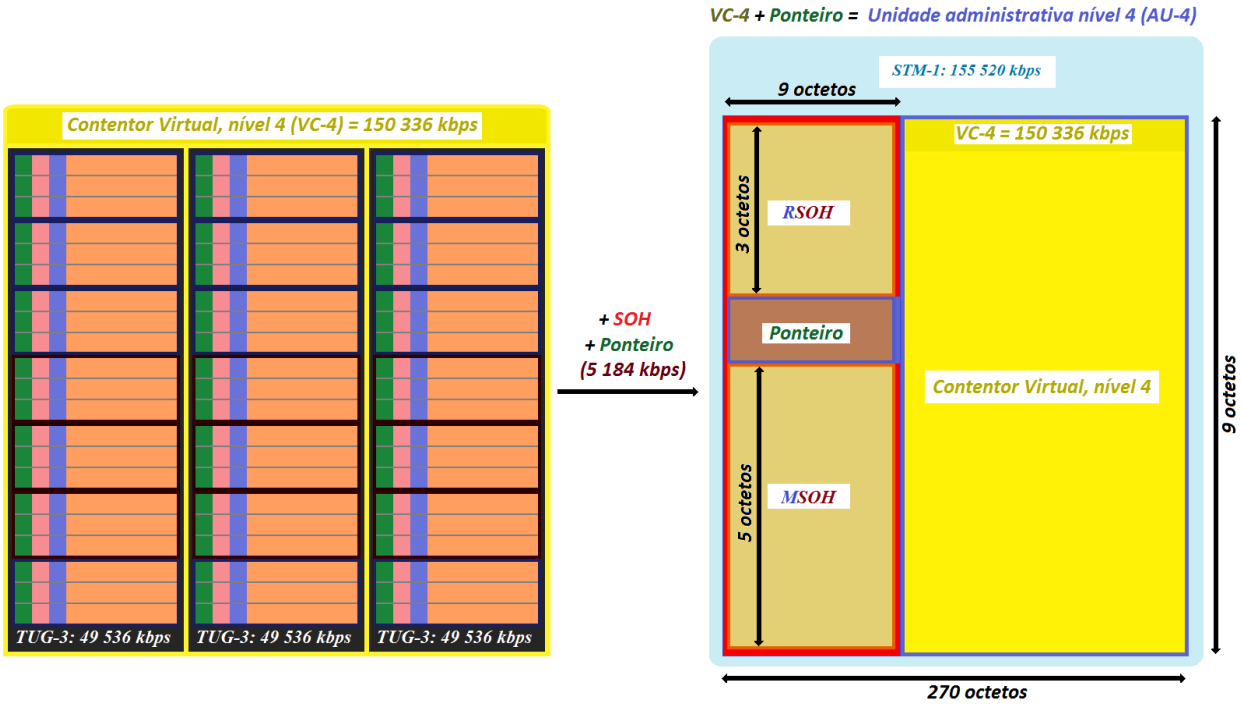

Figura 8.2 – Construção de uma estrutura STM-1.

Na tecnologia SDH o mapeamento consiste em associar os diferentes contentores virtuais na trama STM-N. Na tecnologia PDH, o TS tem uma posição predeterminado na trama E1, acontecendo o mesmo com os diferentes tributários no mapeamento para a STM-N. Para o mapeamento da trama E1 utiliza-se numeração sequencial, salvaguardando as posições reservadas, TS0 e TS16. Na trama STM-N utilizam-se coordenadas “k, l e m” para mapear o

tráfego e assim permitir a sua localização. Assim, a função ADM utiliza essas coordenadas armazenadas nos ponteiros para localizar o tributário pretendido.

Proteção da ligação

A tecnologia SDH possibilita a construção de uma rede com proteção da ligação ótica, recorrendo a duas ligações físicas distintas. Para distinguir os dois circuitos, estas têm designações diferentes. O circuito com o tráfego permanente é designado por circuito "*Working*", e o circuito de proteção (securizado) é designado por "*Protection*". Assim, em caso de anomalia no traçado "*Working*", o sistema comuta automaticamente para a ligação "*Protection*". Essa capacidade de comutação automática é designada por *automatic protection switching* (APS) e atua em menos de 50 milissegundos na pior das situações (recomendação ITU-T G.841). Na realidade é geralmente muito menos que os 50 milissegundos, uma vez que a norma considera que esse é o valor máximo numa ligação de 22 500 km, e não existem traçados com esse comprimento. Existem 3 configurações possíveis para realizar esta proteção: *subnetwork connection protection* (SNCP), *multiplex section protection* (MSP), *multiplex section shared protection rings* (MS-SPRings).

Hierarquia Digital Síncrona de próxima geração

A tecnologia baseada na SDH foi originalmente desenvolvida para o tráfego de voz. Mas com a demanda cada vez maior de tráfego *ethernet* (serviço integrado), foi desenvolvida a tecnologia *next generation* SDH (NG SDH). Esta tecnologia é o resultado da convergência de duas tecnologias distintas: SDH (nativa) e *ethernet*. As modificações introduzidas na tecnologia SDH vieram permitir que a nova tecnologia seja muito mais eficiente.

Na arquitetura TCP/IP, a tecnologia NG SDH situa-se na camada 2 do modelo OSI, e a utilização do serviço *ethernet* veio oferecer simplicidade, flexibilidade, eficiência no tráfego de dados, e qualidade de serviço. O tráfego *ethernet* apresenta mais flexibilidade, permitindo dimensões variáveis nas tramas, até um máximo 9 000 octetos *(jumbo frames)*. A eficiência nos débitos de transmissão deve-se à introdução de novas funções de concatenação, associadas a esta evolução tecnológica, oferecendo escalabilidade. As novas funções são esquemas de concatenação que permitem flexibilizar os débitos do tráfego *ethernet* de forma dinâmica.

A função *generic framing procedure* (GFP, recomendação ITU-T G.7041) é uma de três novas funções introduzidas. Ao tráfego *ethernet* está associada a transmissão de tramas em rajada (*burst*), o que o torna incompatível com o tráfego TDM, uma vez que este dispõe de débito fixo. A função GFP possibilita um mapeamento eficiente do tráfego *ethernet* pois socorre-se de um *buffer* elástico.

A função *virtual concatenation* (VCAT, recomendação ITU-T G.707) é outra função que possibilita ganhos de eficiência, pois acomoda o tráfego de forma mais flexível, devido ao seu passo mínimo de incremento (granularidade): VC-12. Possibilita assim o ajustamento à capacidade da ligação (largura de banda). Ou seja, se já se dispõe de uma configuração para uma ligação com um tráfego de 20 Mbps, e se pretende aumentar para 22, basta associar mais um VC-12. Mas quando se pretende uma largura de banda de 21 Mbps, não é possível devido à granularidade ser de 2 Mbps (VC-12).

A função LCAS (recomendação ITU-T G.7042), é a última função introduzida e é uma extensão melhorada do VCAT, pois disponibiliza uma gestão dinâmica da largura de banda do grupo

concatenado *(payload)* distribuindo-o por VC de outras tramas STM-N. Ou seja, se o cliente já estiver com alguma largura de banda, e se pretender aumentar essa largura, é possível sem ser necessário refazer todo o circuito *[8-3]*. Também permite que o tráfego seja encaminhado por outras tramas STM-N e traçados físicos diferentes.

9. Apêndice 4 – Arquitetura NG SDH

Por simplificação, os dispositivos SURPASS hiT7020, hiT7050 e hiT7060, do fabricante Siemens serão designados por 7020, 7050, 7060, e 70xx quando as características foram iguais para estes três modelos.

Matriz de conectorização cruzada

A função de conectorização cruzada (*digital cross-connect*, DXC), nos dispositivos SDH, recorre a uma matriz de comutação (*switch matrix*). Esta matriz é na realidade uma EPROM onde consta as linhas de código com instruções para realizarem a conectorização cruzada.

O modelo 7020 é um *customer premises equipment* (CPE) e a capacidade máxima da matriz de comutação para contentores virtuais de baixa ordem (*low order virtual containder switch matrix, LO VC SM*) é de 252 *cross connect*. Essa capacidade máxima da matriz de comutação reduz-se para 16 *cross connect* se forem utilizados contentores virtuais de alta ordem (*high order virtual containder switch matrix, HO VC SM*).

No modelo 7050, a capacidade máxima da *LO VC SM* é de 2016 *cross connects* e de 32 *cross connects* se forem utilizados *HO VC*. No 7060 a capacidade máxima da *LO VC SM* é de 2016 *cross connects* e de 448 *cross connects* se forem utilizados *HO VC*.

A utilização do modelo 7060 obriga a um planeamento rigoroso, pois a utilização de LO VC leva a um esgotamento rápido da matriz de comutação, limitando a capacidade de transmissão à um máximo de 5 Gbps, e 40 Gbps se forem utilizado HO VC. Utilizando tráfego do acesso local, nem sempre é possível utilizar HO VC.

A Figura 9.1 ilustra como se mapeia um VC-12 entre duas tramas STM-1, e em que a matriz de comutação necessita de realizar 63 conectorizações.

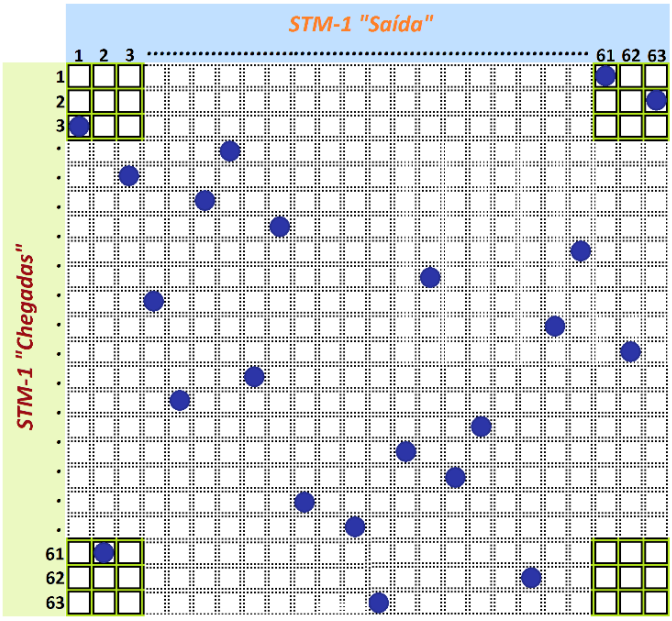

Figura 9.1 – LO VC SM para mapear o tráfego entre duas tramas STM-1.

A conectorização cruzada consiste em retirar o tráfego de um VC-12, alojado na posição “k, l e m” de uma STM-1 e colocá-lo num outro VC-12, com uma determinada coordenada (pode ser a mesma), de outra trama STM-1. Por exemplo, o VC-12 da STM-1 “Saída”, da posição 1 é mapeada para a posição 3 da STM-1 “Chegada”, consumindo uma conectorização cruzada.

Um *LO VC SM* para administrar 8 tramas STM-1, ou 2 STM-4, necessita de 1008 conectorizações cruzadas. Se o administrador de rede utilizar HO VC, VC-4, só necessita de utilizar 16 *cross connect* para encaminhar a mesma capacidade de tráfego. Ao se mapear tráfego local para uma trama STM-N também consome *cross connects*, e a quantidade necessária depende sempre da quantidade de contentores virtuais.

9.1 SURPASS hiT 70xx

A série 70xx é uma plataforma de múltiplos serviços (*multi-service provisioning platform*, MSPP), pois disponibiliza vários tipos de tributários, tais como E1 (PDH), STM e *ethernet*. Tem a capacidade de *(i)* multiplexar o sinal (*terminal multiplexer*, TMX) gerando tramas STM-N; *(ii)* inserir e adicionar até à granularidade VC-12 sem ser necessário desmultiplexar (desmontar) toda a trama; *(iii)* e realizar conectorização cruzada. A capacidade de processamento pode chegar aos 40 Gbps, dependendo do modelo instalado e se forem usados VC HO. O fabricante disponibiliza diversos tipos de cartas de tributários: 2M, 34/45M, 155M, STM-1/4/16, FE, GbE. Este equipamento disponibiliza várias soluções de anéis de securização para o tráfego TDM: SNCP, MSP, MS-SPRing.

Em 2006, e numa primeira fase (de três), a EEM começou por instalar o modelo 7050, criando uma rede em anel semelhante à representada na Figura 9.2. É semelhante pois na figura só estão representados 4 dispositivos, quando na realidade eram 9. O 7050 suporta cartas de linha ótica (*optical line card,* OLC) STM-1 e STM-4, mas a EEM só adquiriu OLC STM-1. Fisicamente, o 7050 tem uma largura de 19” (482,6 mm) e uma altura de 6U (132 mm), e dispõe de 4 *slots* para receber as cartas funcionais, representadas pelos blocos a azul na Figura 9.2, e dispõe de alimentação securizada de 48 VDC. Na EEM, as cartas funcionais instaladas na *shelf* foram: *(i)* E1 (PDH *Card*) e conectada a um painel frontal com 21 portos elétricas de E1 (P21), utilizando na sua cablagem cabo coaxial (com uma impedância característica de 75 Ω); *(ii)* duas OLC STM-1 com dois portos óticos (O155-2) ou com quatro portos óticos (O155-4). A instalação de duas *optical line cards* permite construir um circuito em anel que garante a proteção e ainda oferece acessos óticos; *(iii)* e de *ethernet* (E100-8), com 8 portos *fast ethernet* (FE).

A segunda fase de alargamento da tecnologia NG SDH, em 2007, veio disponibilizar tráfego *ethernet* às diversas delegações espalhadas pela ilha, reduzindo custos associados ao aluguer de circuitos. Para o efeito foram adquiridos dispositivos mais compactos: os equipamentos 7020.

Fisicamente, o 7020 tem uma largura de 19” (482,6 mm) e 1U (44 mm) de altura. Dispõe de 8 portos E1, 4 de FE e uma *optical line card* com dois portos óticos. Todos estes portos são integrados ao chassi e disponibiliza duas formas de alimentação securizada: 48 VDC ou 220 VAC. Esta alimentação, por estar também ela integrada ao chassi, é necessário no ato da encomenda já estar definida. O 7020 tem uma capacidade máxima de transmissão de 2x600 Mbps, se forem usados contentores virtuais de alta ordem. A utilização do 7020 implica a aceitação de três desvantagens: *(i)* só possui uma *optical line card* com dois portos óticos. Esta limitação não permite oferecer um acesso ótico ao tráfego local. No caso de se utilizar num acesso ótico, perde-se a possibilidade de se ter o circuito protegido (securizado).

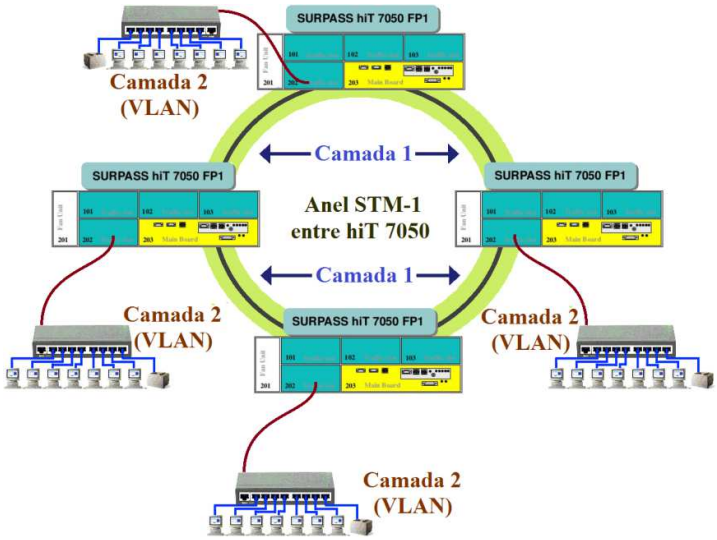

Figura 9.2 – Anel utilizando tecnologia SDH e dispositivos SURPASS hiT 7050.

A Figura 9.3 ilustra o circuito de proteção que recorre a um lacete, também designado por anel, ótico; *(ii)* esta carta ótica está integrada no chassi. Um lacete pode começar num porto e termina num outro, do mesmo dispositivo, ou iniciar num dispositivo e terminar num outro, o objetivo é disponibilizar algum nível de garantia de ligação em caso de anomalias no sistema. As cartas funcionais integradas no dispositivo, tal como a fonte de alimentação, forçam a substituição do dispositivo em caso de avaria de uma delas. Torna-se por isso obrigatório possuir uma cópia da configuração de cada elemento de rede num dispositivo de armazenamento; *(iii)* a configuração desses dois portos óticos tem que ser igual (STM-1 ou STM-4). Pelo facto de não existir a possibilidade de configurar uma largura de banda diferente para cada porto ótico, pode dificultar a criação de lacetes com elemento de rede de modelos diferentes. A título de exemplo, se numa das extremidades do lacete estiver ligado um porto ótico STM-4, já não é possível integrar um 7050 no lacete. Na construção do lacete, o procedimento correto é ligar uma das extremidades numa *optical line card* e a outra extremidade noutra *optical line card*. Assim em caso de avaria de uma das *optical line card*, o tráfego não é interrompido.

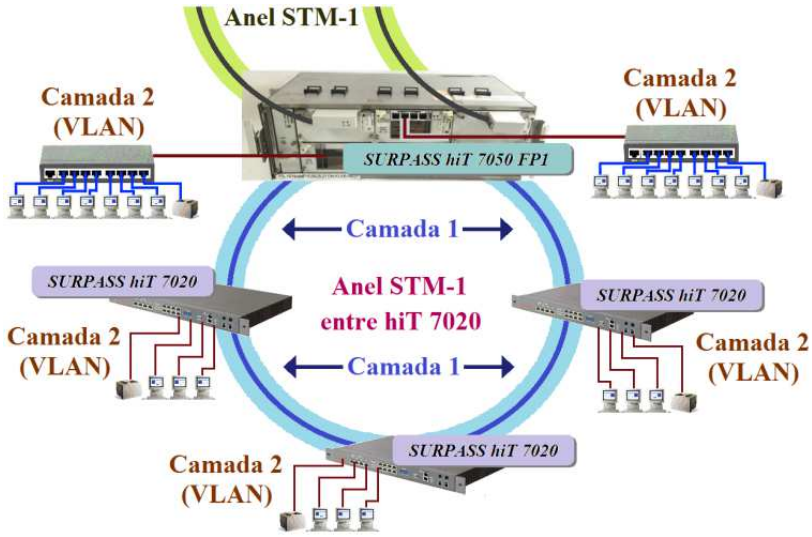

Figura 9.3 – Anel utilizando tecnologia SDH e dispositivos 7020 agregados ao 7050.

A terceira fase do alargamento da tecnologia NG SDH, veio permitir disponibilizar tráfego *ethernet* a clientes externos à EEM, permitindo receitas extras que ajudam a custear o serviço de telecomunicações. Na escolha dos elementos de rede do *core*, a EEM optou pelo 7060.

O 7060 tem mais capacidade de processamento que o 7020, podendo chegar aos 40 Gbps, se forem utilizados VC HO. É mais flexível no tipo de serviço que oferece, pois disponibiliza 8 posições (*slots*) para cartas de diferentes tipos de tributários (TC) e mais oito posições para cartas de linha (LC). A EEM adquiriu apenas uma única carta tributária E1, designada por TC P21, igual ao painel frontal de E1 do 7050, com a diferença que a cablagem utilizada é UTP, com uma impedância característica de 120 Ω. No 7060, cada *optical line card* (OLC) instalada tem uma capacidade de *throughput* de até STM-16 (2,5 Gbps). As OLC STM-16 só têm um porto ótico e as OLC STM-4, tal como as STM-1, têm 4 portos óticos *[9.1-1]*.

Integração do FMX na rede SDH (hiT 7050)

A Figura 9.4 ilustra como passou a ser construída a rede PDH integrada na rede SDH. Todos os FMX instalados nas mesmas subestações onde existe o 7050, interromperam o ramal e passaram a entregar os E1 no painel frontal P21, de 21 portos elétricos E1.

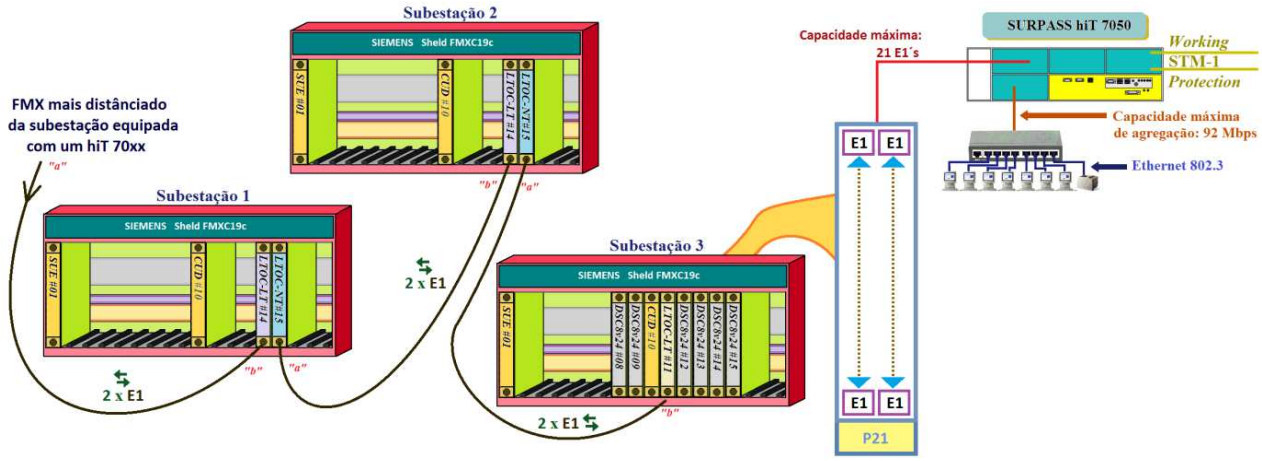

Figura 9.4 – Oferta de serviços PDH e tráfego *ethernet* sobre SDH (EoS).

Foi assim possível integrar a rede PDH, mantendo todos os serviços a funcionar, conforme está ilustrado na Figura 9.5. A linha a tracejado representa a ligação lógica. Nesta integração, destacam-se 6 grandes vantagens: *(i)* a utilização de todos os elementos de rede da rede PDH; *(ii)* a rede PDH com possibilidade de crescer sem que isso afete a arquitetura da rede SDH; *(ii)* utilização de 4 apenas fibras óticas no Centro de Despacho, em vez das 17 que existiam; *(iv)* ter traçados mais curtos, sem necessidade de se regenerar o sinal; *(v)* ligação protegida (securizada); *(vi)* e disponibilização de tráfego *ethernet*.

A Figura 9.5 ilustra a rede PDH lógica da EEM, resultando em ramais de FMX mais reduzidos. Os FMX-2 pertencem aos SNUS. O SNUS do Funchal recebe o tráfego do Porto Santo, via linha alugada ao operador "OPER_1", e das SE dos Viveiros, Virtudes, Alegria e Central Hídrica da Calheta de Inverno. O SNUS do Centro de Despacho (Vitória) recebe o tráfego das outras subestações.

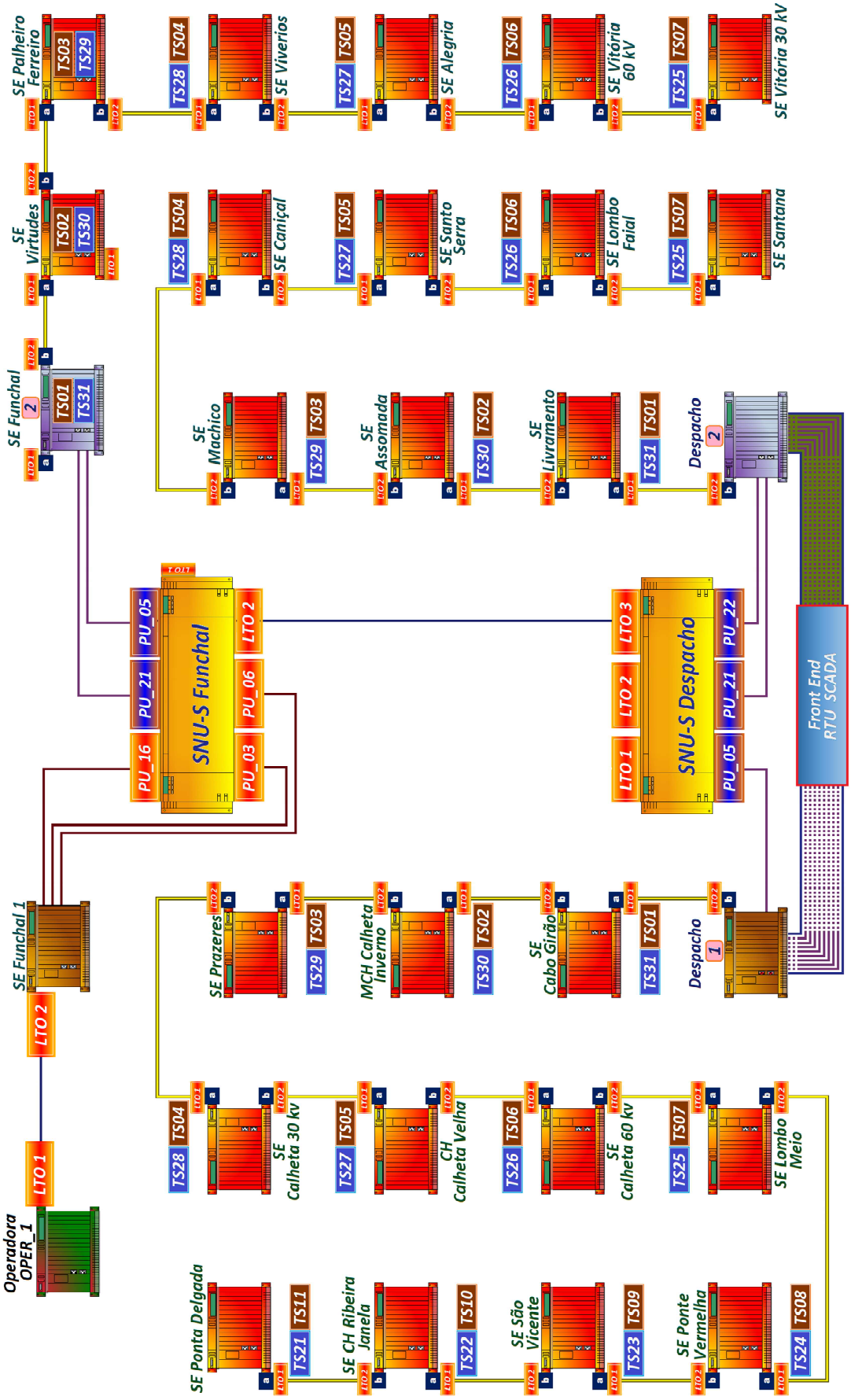

Figura 9.5 – Rede lógica de acesso PDH.

9.2 Tráfego *ethernet*

As cartas *ethernet* da série 70xx distinguem-se em dois aspetos muito importantes: *(i)* o tráfego é transparente no 7050 e não o são nos 7020 e 7060; e *(ii)* na capacidade de processamento de *throughput*, que no caso do 7020 e 7050 está limitado ao dispositivo (sendo esse limite de 92 Mbps, apesar dos portos serem FE) e no 7060 esse limite está associado a 31 WAN das 32 possíveis. Na tecnologia SDH do fabricante Siemens, a terminologia para a "VLAN" é "WAN".

Tráfego *ethernet* nativo

Como se pode verificar pela Figura 9.6, o tráfego *ethernet* de cada porto é associado ao seu grupo, configurado pelo administrador da rede. Como já foi abordado na seção "*Hierarquia Digital Síncrona de próxima geração*" do "Apêndice 4 – *Hierarquia Digital Síncrona*", a função GFP acomoda o tráfego *ethernet* nos VC-12, consumindo um *cross connect* por cada 2 Mbps. Só depois é que são mapeados na trama STM-1, recorrendo à função de conectorização cruzada e utilizando as coordenadas "k, l, e m", o que permite o encapsulamento do tráfego *ethernet* na trama STM-1.

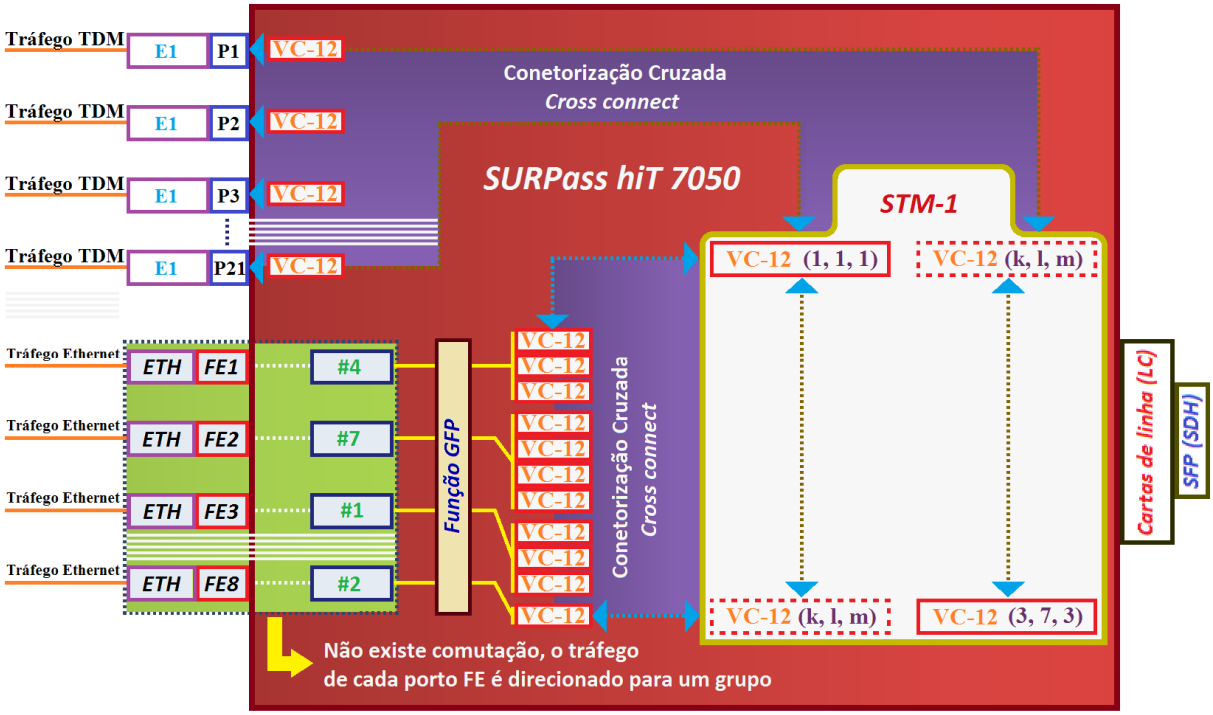

Figura 9.6 – Mapeamento do tráfego *ethernet* num dispositivo SURPASS hiT 7050.

Para haver gestão da VLAN é necessário instalar um comutador, e o porto agregador (*trunk*) do comutador deve ser ligado a um dos portos FE do 7050, conforme o traço de cor castanho da Figura 9.2. Além disso, nada impede que o tráfego *ethernet* nativo possa ser mapeado para uma trama STM-1. Mas se o tráfego transportado for *ethernet* nativo, no ponto de entrega, a operadora não saberá distinguir a que cliente pertence o tráfego.

Cada carta *ethernet* (e não o porto) consegue acomodar no máximo 46 VC-12, processando assim um máximo de 92 Mbps (VC-12-46v), apesar dos portos serem FE (100 Mbps).

O 7020, ao contrário do 7050, permite a comutação do tráfego *ethernet*, pois os portos FE têm a capacidade de lerem o campo "*Ethertype*". Se o código do *ethertype* não for 0x8100 (*dot1q*), o porto FE adiciona o rótulo *dot1q* à trama, procedimento idêntico ao porto de acesso de um comutador convencional. Se o *ethertype* for *dot1q*, então o porto verifica se o rótulo é igual ao configurado, caso contrário a trama é descartada. Se o *ethertype* for *doubleTAG* a trama também é descartada.

Tráfego *ethernet dot1q*

No contexto SDH, o *Port VLAN ID* (PVID) é uma numeração (rótulo) que se atribuir ao tráfego *ethernet* ao aceder ao porto FE, sendo necessário que o administrador de rede configure o porto com esse PVID. Apesar do 7020 permitir distinguir os rótulos que acedam aos portos FE, existe um problema de base: a carta *ethernet* só reconhece blocos de 512 rótulos e com numeração seguida. Ou seja, os 4 096 rótulos possíveis estão divididas em 8 blocos, conforme ilustrado na Figura 9.7. Se o sistema já estiver a utilizar um dos 8 blocos para a numeração do tráfego, e um determinado serviço solicitar ao administrador da rede uma numeração que não pertença a esse mesmo bloco, não é possível satisfazer o pedido, a não ser que o porto fique transparente.

Figura 9.7 – Blocos de VLAN permitidos no SURPASS hiT 7020.

No 7020 o tráfego *ethernet* ao aceder pelo porto FE é comutado para uma WAN, recorrendo à função de comutação, conforme ilustrado na Figura 9.8.

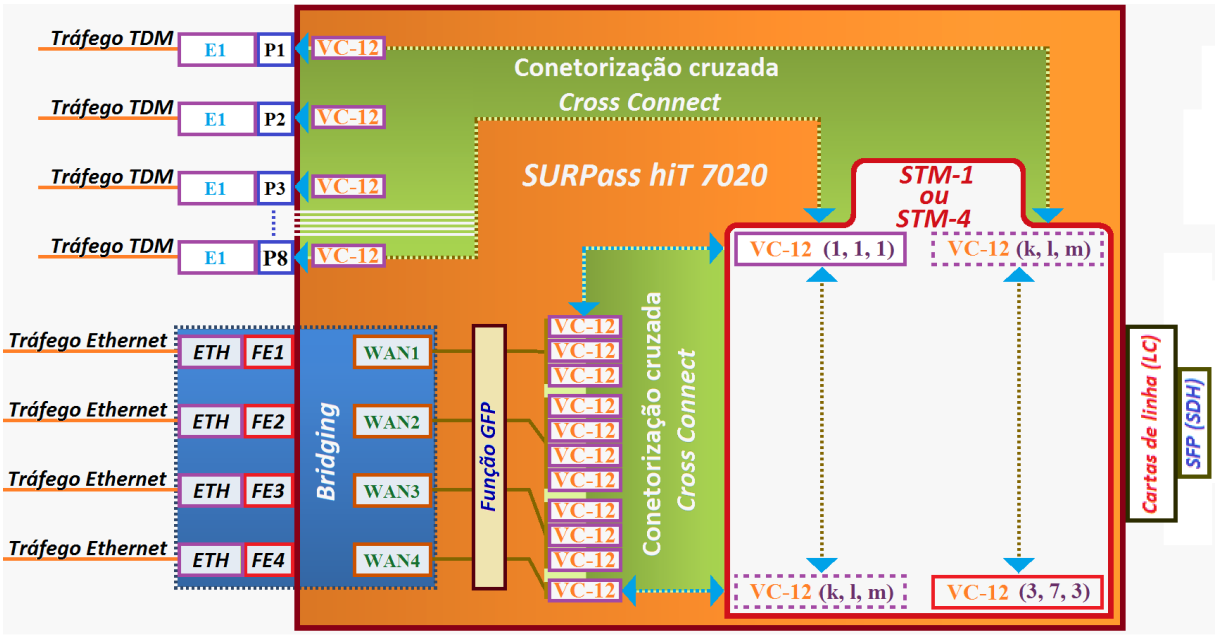

Figura 9.8 – Mapeamento do tráfego num dispositivo SURPASS hiT 7020.

Neste contexto SDH, a designação “WAN” tem um significado diferente da rede de computadores existente numa grande área geográfica. É um porto de rede local (LAN), lógico (domínio de *broadcast*), mais conhecido por VLAN numa rede com elementos de rede do fabricante Cisco, e respeita o protocolo *dot1q*. As WAN são rótulos de significado local, que o administrador de rede atribuiu por configuração, uma determinada largura de banda. O modelo 7020 possibilita gerir (comutar) o tráfego entre os 4 portos FE e 4 WAN diferentes. A capacidade de gestão possibilita, se assim entender o administrador da rede, que o tráfego que acede pelos 4 portos FE possa ser todo ele associado a uma única WAN. Ou seja, ao tráfego que chega aos portos FE1, FE3 e FE4 pode ser atribuído ao rótulo “WAN2”, e o tráfego FE2 pode pertencer a uma outra WAN (“WAN1”, “WAN2” ou “WAN4”).

A função GFP aloja (adapta) o tráfego *ethernet*, associado às WAN, ao VC-12, utilizando múltiplos de VC-12 (2 Mbps) em função da capacidade definida pela WAN. É possível visualizar, na Figura 9.8, que o tráfego da: *(i) “*WAN1” tem uma largura de banda de 6 Mbps, pois está agrupado a 3 VC-12; *(ii)* “WAN2” tem uma largura de banda de 8 Mbps; *(iii)* “WAN3” de 6 Mbps; e *(iv) “*WAN4” de 2 Mbps. Estas WAN ocupam 19 VC-12 dos 63 possíveis na trama STM-1.

Como já foi abordado na seção "*Hierarquia Digital Síncrona de próxima geração*" do “Apêndice 4 – *Hierarquia Digital Síncrona*”, a função LCAS dá a possibilidade ao administrador da rede de poder alterar dinamicamente essa mesma largura de banda, e o tráfego pode ser mapeado sem ser sequencialmente agrupado, dando assim liberdade e flexibilidade ao administrador da rede.

Tráfego *ethernet QinQ*

O 7060 disponibiliza dois tipos diferentes de cartas para o tráfego *ethernet*. Um tipo de carta reconhece o protocolo IEEE 802.1Q, tal como o 7020 e tem mais uma outra carta com opção para tráfego IEEE 802.1ad (*QinQ*). No exemplo da Figura 9.9, o tráfego *ethernet* que chegam na trama STM-1 pelo porto ótico “LC 2.1” e são retirados dos VC-12 (que estavam alojados na trama STM-1, em coordenadas fixas) pela função GFP e são atribuídos às respetivas WAN da carta *ethernet* “LC6”.

A função *bridge* comuta os diversos tráfegos associados às diversas WAN para os portos FE ou para as WAN da carta *ethernet “*LC7”. Cada carta *ethernet* disponibiliza oito portos FE e dois portos GE.

A carta de *ethernet QinQ* do 7060 é a única que consegue modificar o campo “*Ethertype”* do cabeçalho. Ou seja, recebe o tráfego *dot1q*, e acrescenta para *QinQ*. Se o tráfego chegar sem qualquer rótulo (nativo) essa carta tem a capacidade de passar logo para *double Tag*. O protocolo *QinQ* não é reconhecido pela tecnologia SDH, apenas pelas cartas que reconhecem o protocolo IEEE 802.1ad (*QinQ*).

As cartas *ethernet* instaladas no 7060 permitem uma numeração para os rótulos (PVID) de 1 a 4096 num único bloco, e oferece um esquema de proteção no acesso múltiplo com deteção de portadora (*carrier sense multiple access*, CSMA) o *rapid spanning tree protocol* (RSTP).

Cada carta *ethernet*, e não o elemento de rede, possibilita gerir 32 WAN, sendo que a “WAN1” é a única que suporta múltiplos VC-4 (150 Mbps), enquanto as outras 31 WAN só aceitam múltiplos de VC-12. Estas 31 WAN estão limitadas individualmente a uma capacidade máxima na agregação de 46 VC-12 (92 Mbps). A “WAN1” pode ser construída usando 6 VC-4 (VC-4-6v), possibilitando uma agregação de 900 Mbps de tráfego útil. Ao se instalar em múltiplas cartas *ethernet* no 7060, conseguem-se ter múltiplos de 32 WAN. Como já foi mencionado, as numerações dos rótulos

atribuídas ao tráfego numa carta *ethernet* não têm que coincidir com as numerações dadas na outra extremidade da ligação ótica. E dentro do mesmo elemento de rede, quando o tráfego é direcionado para outra WAN, é porque existe uma outra carta *ethernet* instalada na mesma *shelf*.

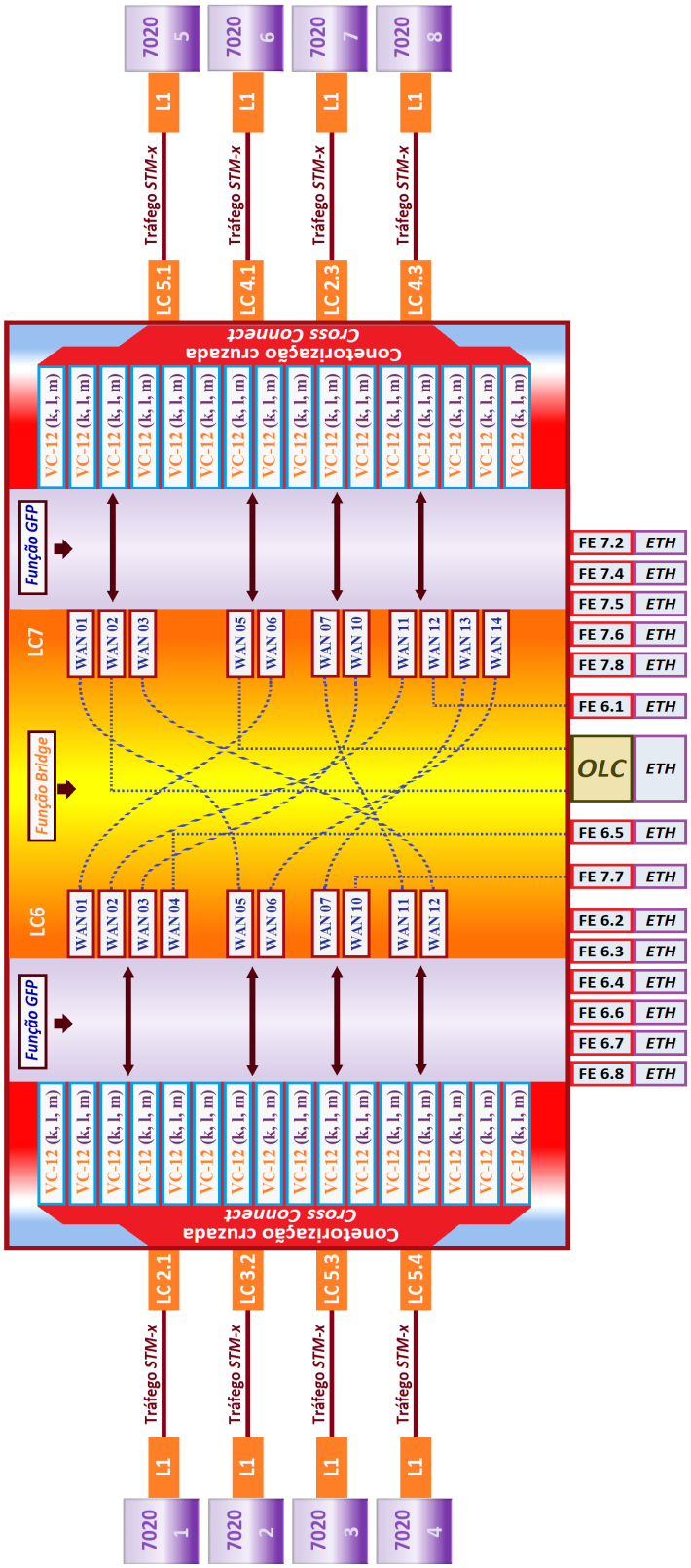

Figura 9.9 – Mapeamento do tráfego num dispositivo SURPASS hiT 7060.

9.3 Rede SDH da EEM

A Figura 9.10 ilustra a rede lógica do tráfego *ethernet* agregado na instalação P1. As áreas #1 e #2 pertencem ao mesmo lacete, mas o tráfego *ethernet* só pode seguir por uma das rotas, caso contrário tem-se um *loop*. Na área #1, na trama STM1 que transita entre o "7020-LM" e o "7060-P1" existem duas WAN em cada dispositivo. As "WAN1" e "WAN3" do "7020-LM" associam-se as WAN "WAN16" e "WAN17" do "7060-P1". Na "WAN3", configurada com 10 Mbps, transita o tráfego sem rótulo da "VLAN127" e na "WAN1", configurada com 4 Mbps, transita o tráfego sem rótulo da "VLAN128". Tal é realizado sem rótulo porque a EEM necessitava de um *router* CPE transparente, e a Siemens disponibiliza esse tipo de dispositivo. O tráfego da "VLAN145", associado a "WAN2" e configurado com 2 Mbps, vai para o "7020-C6", e é desencapsulado da trama STM-1, pois está associado a "WAN4", conforme a Figura 9.8.

Nas áreas #1 e #2 da Figura 9.10, o tráfego que existe entre as ligações "7020-C6"/"7020-C3", "7020-C3"/"7020-CHCI", e "7020-CHCI"/"7020-LV" pertencem as "VLAN128" e "VLAN145". Ou seja, em cada uma destas subestações, estas "VLAN" são "retiradas" da trama STM-1, que circula pelos 7020, e são atualizadas com o tráfego local, e voltam a ser "inseridas", mas na outra trama STM-1 que sai (função ADM). A "WAN3" do "7020-CHCI" agrega as "VLAN144", "VLAN146" e "VLAN147" (tráfego da delegação da Calheta), é mapeada na STM-1 e é associado a "WAN11" (10 Mbps) do "7060-P1". A "WAN2" do "7020-LV" agrega o tráfego das "VLAN67", "VLAN123" e "VLAN127", além das "VLAN128" e "VLAN145". Esta "WAN2" é mapeada na STM-1, e é associado a "WAN22" do "7060-P1". Não existe nenhuma "fronteira" entre a área #1 e #2 da Figura 9.10, pois o tráfego da "WAN3" do "7020-C3" vai para a área #1, e o tráfego que transita pela "WAN1" do "7020-C3" vai para a "WAN2". Essa fronteira serve apenas para ajudar a interpretar o sentido do fluxo do tráfego *ethernet*.

Na área #3 da Figura 9.10 é possível visualizar que todo o tráfego *ethernet* está associado a "WAN4" do "7060-P1", com exceção da "WAN2" do "7020-PSBC", que apenas transita pela rede SDH. Transitar na rede SDH significa utilizar a função *cross connect* nos diversos elementos de rede até entregar o tráfego da "WAN2" ("VLAN141" e "VLAN511") na "WAN3" do "7020-DESP3" (área #5).

Na área #4 da Figura 9.10 o tráfego da "VLAN127", associado a "WAN24" do "7060-P1", transita até a "WAN4" do "7020-RJ1", onde a "VLAN127" é "retirada" da trama STM-1 e é atualizada com dados locais. As VLAN que chegam da área #6 ("VLAN128", "VLAN135" e "VLAN145") são associadas a "WAN2" do "7020-RJ1", onde são atualizadas com informações locais, e voltam a ser associadas, agora a "WAN1", e transmitidas para a "WAN2" do "7020-SV". No "7020-SV", são associadas a "WAN1" as "VLAN67", "VLAN123", "VLAN127", "VLAN128", "VLAN135" e "VLAN145" e são transmitidas para a "WAN3" do "7060-P1".

Na área #7 da Figura 9.10 o "7020-PD" associa a "WAN2" o tráfego das "VLAN128", "VLAN1352 e "VLAN145", que chegam do "7020-PM", e reenvia pela sua "WAN1" este tráfego, após atualização das VLAN com o tráfego local, para a "WAN2" do "7020-RJ1".

Na área #8 da Figura 9.10 é possível ver-se uma solução para o problema do 7020 possuir apenas uma OLC de dois portos óticos, quando nesta instalação era necessário mais um. Como se pretendia tráfego *ethernet*, a solução passou pela instalação de mais um 7020 e utilizaram-se os portos FE no estabelecimento de uma ligação entre eles. O "7020-SA2" recebe o tráfego (ótico) do "7020-SA3", converte o sinal ótico para elétrico e transmite para o porto FE do "7020-SA1".

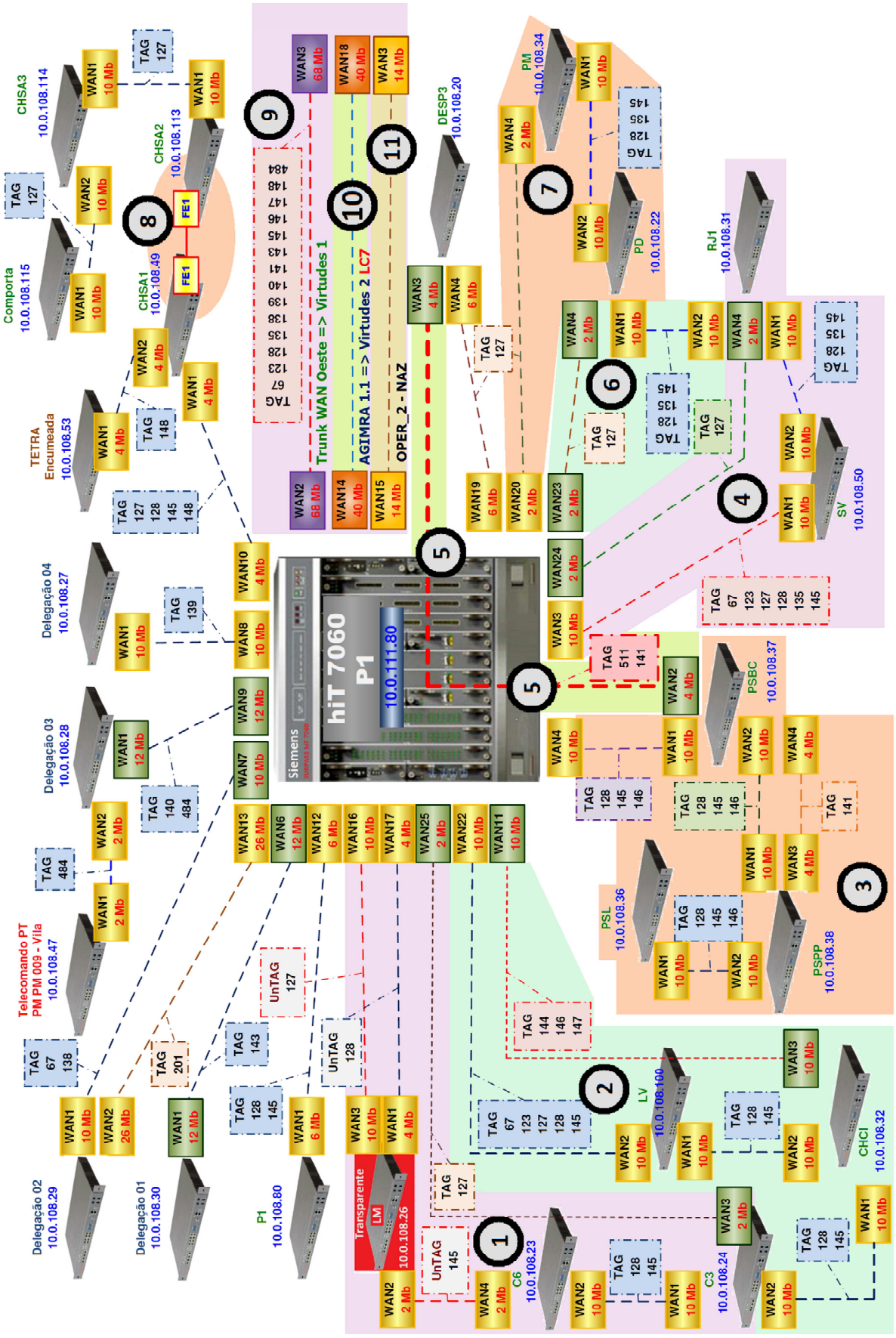

Figura 9.10 – Rede lógica de serviços *Ethernet* da EEM - Zona Oeste.

Na área #9 da Figura 9.10 estão as três WAN do *backhaul*. A “WAN2” do “7060-P1”, de 68 Mbps, está associada a “WAN3” do “7060-V1”. A “WAN14” do “7060-P1”, de 40 Mbps, está associada a “WAN18” da carta “LC7” do “7060-V2” (área #10). A “WAN15” do “7060-P1”, de 14 Mbps, está associada a “WAN3” do “7020-NAZ” (área #11). O tráfego das “WAN14” e “VLAN15” não estão associados a “WAN2” do “7060-P1” porque o tráfego é de clientes, e esta é uma solução para separar tráfego que não pertence à EEM.

10. Apêndice 5 – Implementação da VPN na arquitetura SDH

A EEM dispunha de uma rede baseada na tecnologia SDH, o que lhe permitia garantir serviços de transporte de tráfego *ethernet*, com a topologia ilustrada pela Figura 10.1.

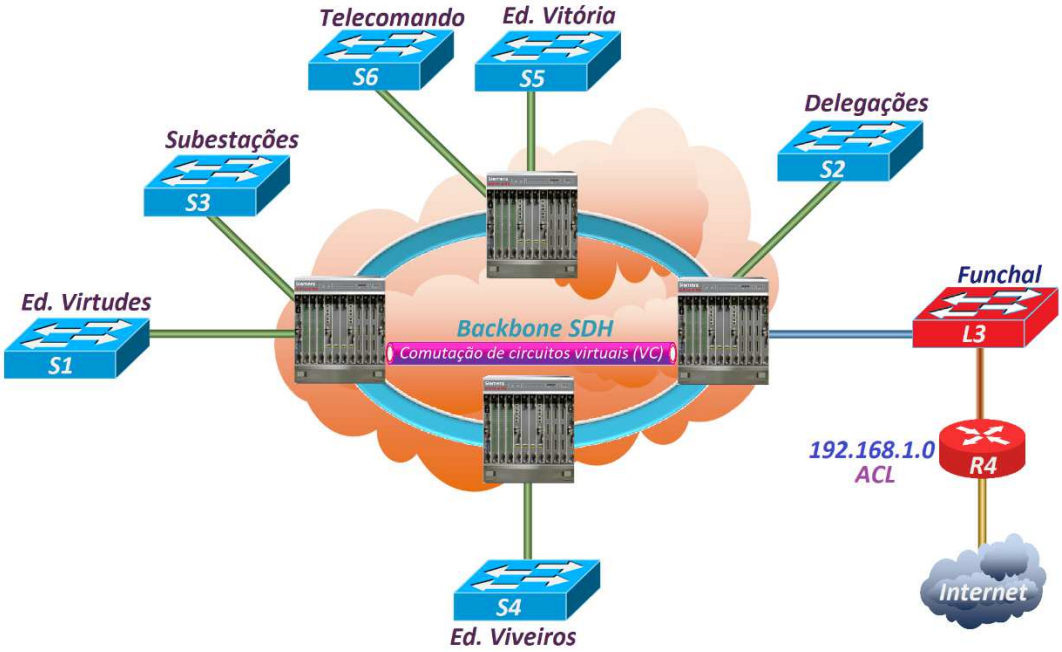

Figura 10.1 – Topologia da rede de transporte *ethernet*, com *backbone* SDH.

O transporte do tráfego *ethernet* era realizado pelo SDH, que estabelecia um circuito dedicado entre cada comutador instalado em vários edificios da EEM e o comutador L3 do Funchal. No acesso ao exterior era sempre utilizado o comutador L3.

A Figura 10.2 representa a rede lógica para o transporte do tráfego *ethernet*. O *backbone* SDH permitia realizar uma extensão às VLAN, em que o comutador do Funchal também executava o encaminhamento. Como os comutadores só comutam tráfego das mesmas redes, cabe ao comutador do Funchal, por dispor de funções L3, encaminhar o tráfego entre outras VLAN. Além disso, existem algumas diferenças entre os dispositivos de rede, apesar de que hoje em dia essa diferença ser cada vez mais esbatida, pois tudo depende do custo de aquisição. Um dispositivo de encaminhamento dispõe de uma tabela de resolução de endereços de IP (ARP) e outra tabela de resolução de endereços MAC, enquanto que um comutador apenas dispõe da tabela de resolução de endereços MAC. Um dispositivo desenhado para exercer a função de encaminhamento, e comparado com um comutador, dispõe de mais RAM, melhor processamento e aceita vários protocolos de encaminhamento em simultâneo. A vantagem de um comutador é o número de portos de que dispõe e o facto de ser mais barato. Além disso, um comutador com capacidade de encaminhamento tem como principal desvantagem a dimensão da tabela MAC, conforme ilustrado na Figura 10.3, agravado pela reduzida capacidade de RAM e de processamento. Conforme se pode observar, todos os endereços MAC conhecidos pelos diversos comutadores, são também conhecidos pelo comutador L3 do Funchal. A procura do endereço MAC correto nas tabelas MAC, armazenadas nas memórias RAM (as mais caras), consome imensos ciclos de processamento. O ambiente de comutador funciona muito à base do

envio de mensagens em modo *broadcast* para todas as máquinas a solicitar respostas. O objetivo é saber a que porto está associado um determinado endereço MAC de destino, produzindo assim, muito tráfego desnecessário.

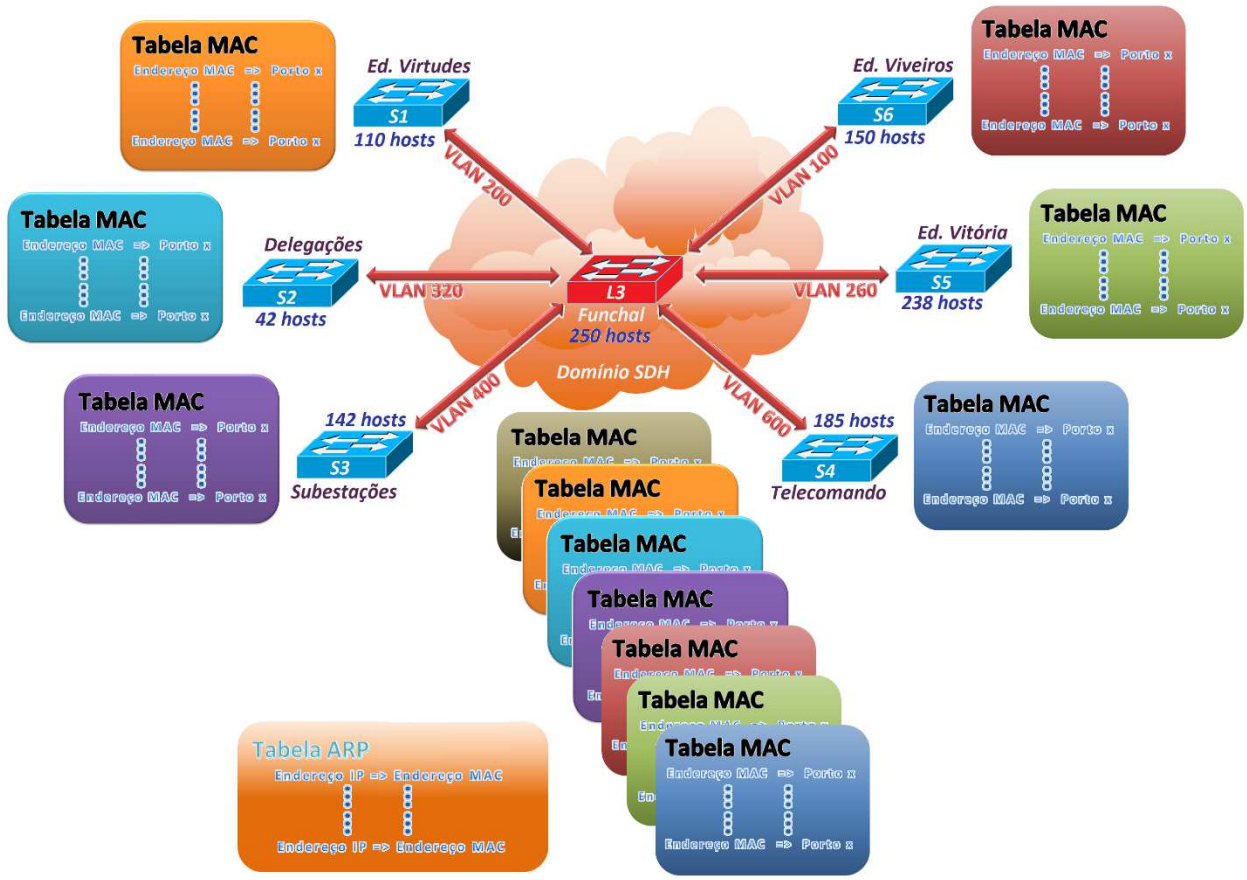

Figura 10.2 – Rede virtual para o transporte de tráfego *ethernet*, utilizando apenas comutadores.

Sempre que um comutador recebe uma trama com um endereço MAC desconhecido, é enviada para todos os portos uma solicitação para que o dispositivo em causa se identifique. Caso não haja uma resposta, é reenviada para todos os portos a mesma solicitação, gerando assim imenso tráfego sem informação útil. E é aqui que podem surgir problemas com *loops* se houver erros de configuração. Após uma resposta positiva a essa solicitação, é registado na tabela de endereço MAC o porto que respondeu.

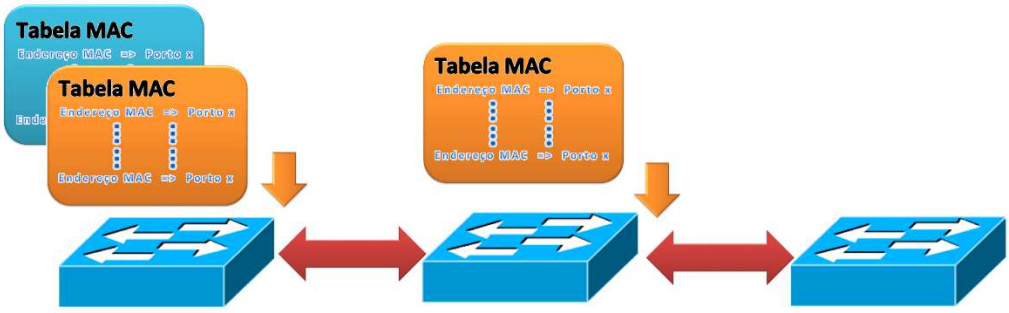

Figura 10.3 – Crescimento acentuado da tabela MAC num comutador.

Ao se configurar um circuito primário e um circuito alternativo, ou ao pretender-se balancear a carga (por VLAN) numa malha completa, há o perigo de se proporcionar a geração de ciclos sem fim (*loops*). A camada 2 não suporta *loops*, sendo por isso necessário implementar um protocolo de resolução de *loops*, como o *spanning tree* (STP). O mecanismo STP seleciona um comutador para ser o r*oot bridge* e utiliza uma mensagem BPDU para detetar a existência de *loops* na malha completa. Os portos do comutador devem de ter a função *portfast* BPDU ativadas.

O *router* só conhece os endereços MAC dos portos vizinhos e tem uma tabela ARP, que é mais reduzida, conforme ilustrado na Figura 10.4 . O *router* também envia mensagens em *broadcast* a solicitar que o *host* de um determinado IP informe o seu endereço MAC.

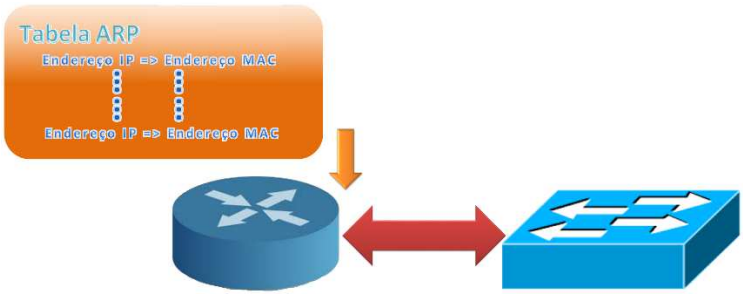

Figura 10.4 – O *router* só conhece o MAC dos portos vizinhos.

Nas cartas *ethernet* associadas ao SDH não se utilizava o STP porque a sua implementação é extremamente complexa. Ou seja, num passado recente, a EEM dispunha de uma rede de transporte que não era segura, pois o perigo de se configurar um serviço poderia criar a possibilidade de surgirem *loop*.

Uma pessoa mal-intencionada, ao utilizar um qualquer PC existente nas instalações da EEM, poderia entrar na rede de gestão dos elementos de rede, via TNMS. Uma vez conseguido esse acesso, a pessoa mal-intencionada poderia provocar uma negação de serviço (*deny of service*, DoS) ao comutador L3 do Funchal, que tinha a função de *core* uma vez que dispunha de algumas funcionalidades de encaminhamento. Assim, ao ser aplicado um DoS ao comutador L3 do Funchal, este ficava inoperacional, prejudicando todo o transporte de tráfego, pois era esse comutador que distribuia o tráfego entre as diversas VLAN existentes na EEM.

A resolução do problema da dimensão da tabela ARP e da ocupação da largura de banda com as mensagens de *broadcast*, passou pela adoção do MPLS. Esta arquitetura também permitiu anular o problema provocado pelos *loops*, aplicar segurança à rede, tal como a implementação da qualidade de serviço ao longo de todo o caminho.

11. Apêndice 6 – Arquitetura *Multi-Protocol Label Switching*

A arquitetura MPLS possibilita o encaminhamento dos pacotes IP com base na comutação por rótulos e surgiu da necessidade de desenvolver uma solução baseada nos aspetos positivos do *overlay* e do IP, atenuando os seus problemas.

A solução *overlay* é uma rede baseada em circuitos virtuais (exemplo: *asynchronous transfer mode*, ATM) sobre uma rede IP. As suas desvantagens são: *(i)* elevados custos, pois é necessário manter as duas redes em paralelo e com equipamentos distintos; *(ii)* pouca estabilidade, principalmente recorrendo ao protocolo do tipo *link state*; e *(iii)* disponibiliza uma menor eficiência de largura de banda, pois o ATM recorre a células muito pequenas (48 octetos de dados).

11.1 Tipos de protocolos

A arquitetura TCP/IP impõe três tipos de protocolos: *(i)* protocolo de comunicação (IP); *(ii)* protocolo de encaminhamento (IGP/EGP); e *(iii)* protocolo de sinalização (TCP, RSVP, LDP, etc.). A Figura 11.1 ilustra esses três tipos de protocolos.

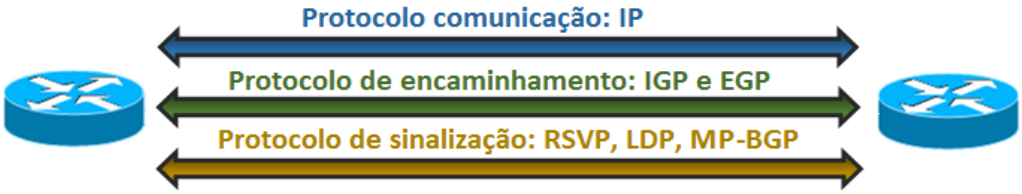

Figura 11.1 – Tipos de protocolos.

Protocolo de comunicação

O protocolo IP é o único protocolo de comunicação e faz parte da camada 3 do modelo OSI. É um dos principais protocolos da *internet*, pois possibilita o transporte de pacotes IP, sem, além disso, garantir a sua entrega. Este procedimento de encaminhar pacotes sem garantias deste chegar ao seu destino é designado por *best effort [11.1-1]*. O termo inglês "*best effort*" é um modelo de serviço utilizado pela arquitetura IP. Consiste num utilizador que envia um fluxo de dados, ao mesmo tempo que a largura de banda é partilhada com todos os fluxos de dados enviados por outros utilizadores, ou seja, estas transmissões são concorrentes entre si. Na realidade, o protocolo IP processa os pacotes IP independentemente uns dos outros e escolhe o melhor encaminhamento ao instante. A tomada de decisão é determinística, individual no encaminhamento dos pacotes e consome recursos (processamento e consequentemente, mais tempo). Uma decisão determinística significa que se trocarmos unicamente o elemento de rede, o cálculo resulta sempre na mesma solução. O protocolo de encaminhamento determina o destinatário da mensagem baseando-se em três campos: *(i)* o campo de endereço IP destino; *(ii)* o campo de máscara de sub-rede; e *(iii)* o campo do *gateway* padrão. O *gateway* padrão *(gateway default)* serve de intermediário entre a rede a que o utilizador pertence (LAN) e a rede

exterior (WAN) que possibilita alcançar o *host* de destino. Ou seja, permite ligar redes diferentes (com domínios de colisão/ambiente diferentes). Gateway descreve uma família de elementos de rede, sendo que *router*, *firewall*, *proxy* e *network address translation* (NAT) são elementos dessa família.

Protocolo de encaminhamento

O protocolo de encaminhamento é um componente fundamental na gestão de redes, pois permite ao *router* ter conhecimento da topologia da rede. O *router*, conhecendo a topologia da rede a que pertence, fica capacitado a, e de forma autónoma, tomar decisões de encaminhamento dos pacotes IP que lhe chegam. O IGP, do tipo *link state*, permite ao *router* criar uma base de dados da topologia da rede (tabela LSDB), que é utilizada para construir a tabela RIB. A tabela RIB é utilizada para reencaminhar todos os pacotes recebidos, permitindo assim ao pacote IP alcançar a sua máquina de destino. Esta solução é mais robusta que uma solução baseada numa ligação ponto a ponto, pois em caso de interrupção da ligação física, o *router* procura outro caminho possível, recalculando um novo caminho alternativo, ao consultar a tabela LSDB. O encaminhamento IP é, portanto, dinamicamente adaptável ao estado da rede e recorre a saltos consecutivos para alcançar o destino do pacote.

Protocolo de sinalização

O protocolo de sinalização, no MPLS, solicita a reserva de recursos e distribui rótulos. Existem dois protocolos de sinalização para solicitar a reserva de recursos aos *routers* que participam na criação do traçado *label switched path* (LSP): *(i) resource reservation protocol* (RSVP); e *(ii)* RSVP *traffic engineering* (RSVP-TE).

Para a distribuição de rótulos, entre *routers*, existem quatro protocolos de sinalização: *(i) label distribution protocol* (LDP); *(ii) tag distribution protocol* (TDP), proprietário do fabricante Cisco; *(iii)* MP-BGP que é utilizados nos circuitos da camada 3; *(iv) constraint-based routed label distributed protocol* (CR-LDP). O TDP e o CR-LDP já não se utilizam.

- Protocolo de reserva de recursos

O protocolo que solicita a reserva de recursos (*resource reservation protocol*, RSVP) aos *routers* que participam no estabelecimento do caminho é um agente que interage com o plano de controlo dos *routers*. A solicitação consiste em providenciar uma ligação virtual, e, numa negociação dinâmica, solicita os recursos necessários, aos *routers*, que permitam satisfazer os critérios de prioridade da qualidade de serviço. A reserva de recursos só ocorre por iniciativa dos recetores, que escolhem o melhor caminho, e reenvia uma outra mensagem tipo (RESV), para confirmar os recursos que ficaram cativos por um curto espaço de tempo. Após confirmação de que há condições, pelo *router* LER_i, é iniciado o envio de todos os pacotes do fluxo pelo mesmo caminho. Quando termina, os recursos são libertados. O RSVP não efetua função de encaminhamento de pacote úteis, pois essa função cabe ao protocolo IGP e não impõe qualquer tipo de política de controlo de admissão, de escalonamento, ou de permissões de carácter administrativo (*policy control*), pois são tarefas do plano de controlo do próprio *router*.

O RSVP permite o encaminhamento convencional, determinado pelo IP de destino do pacote, utilizando a mensagem *label object* (LO). O RSVP-TE é uma extensão para estabelecer um

caminho com critérios, forçando assim um encaminhamento explícito. O protocolo RSVP-TE utiliza a mensagem *explicit routing Object* (ERO).

Protocolo de distribuição de rótulos

O MPLS admite duas formas de propagar as informações que permitem as atualizações das tabelas LFIB: *(i)* estende a funcionalidade dos protocolos já existentes (BGP e OSPF); ou *(ii)* utiliza um novo protocolo dedicado à distribuição de rótulos (*label distribution protocol*, LDP). O LDP é o agente que possibilita a criação do LSP e é o protocolo utilizado para a propagação das tabelas LIB, geradas pelos *routers* vizinhos. É necessário o estabelecimento de sessões TCP entre *routers* vizinhos para garantir a receção das informações baseado em *multicast*, com endereço IP 224.0.0.2 e o campo "*Time to Live*" (TTL) igual a "1".

Protocolo de distribuição de rótulos com engenharia de tráfego

O *label switched path - traffic engineering* (LSP-TE), elemento do mecanismo MPLS-TE, permite o estabelecimento de uma ligação (unidirecional) de forma explícita, independente do protocolo de encaminhamento e cumpre com os critérios de qualidade de serviço *(quality of service, QoS)*. O LSP-TE é utilizado no estabelecimento de uma ligação ponto a ponto, no restabelecimento rápido em caso de perda de ligação (*fast reroute*), e no compartilhamento de carga.

Distribuição de rótulos

O protocolo de sinalização *label distribution protocol* (LDP) é responsável pela distribuição da tabela LIB, aos outros *routers* LSR adjacentes, permitindo, assim, o tráfego nos LSP. O processo do protocolo LDP resume-se a quatro fases, ilustrado na Figura 11.2: *(i)* o *router* MPLS tem a iniciativa de iniciar o processo LDP; *(ii)* envia uma mensagem de descoberta, do tipo "*hello*"; *(iii)* são enviadas mensagens a pedir uma sessão LDP, estabelecendo-a, mantendo-a e de fecho de sessão; e *(iv)* mensagens de advertência.

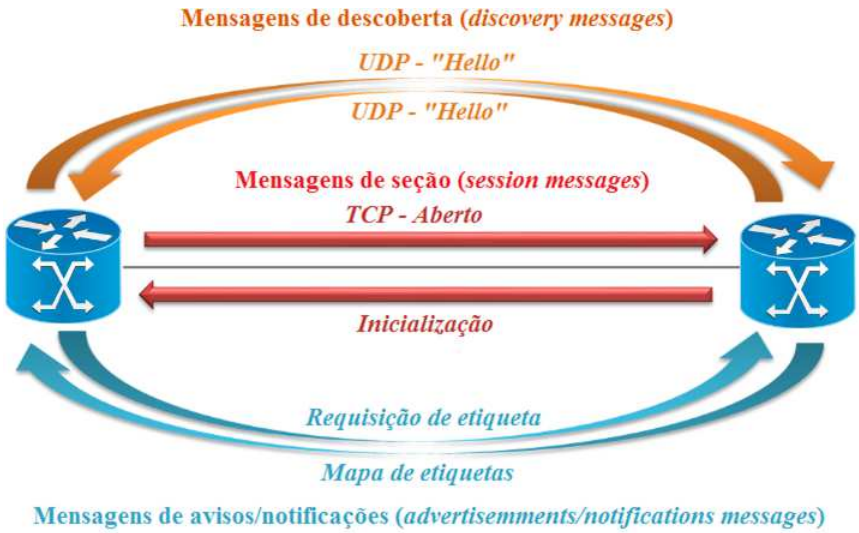

Figura 11.2 – Princípio do funcionamento do LDP.

O processo recorre a uma ligação orientada à conexão (sessão TCP), é bidirecional, o que permite atuar como um mecanismo de transporte de troca de mensagens confiável entre os *routers* MPLS adjacentes. A mensagem do tipo "*hello*" permite anunciar, e/ou manter, os *routers* MPLS adjacentes à sua presença na rede. A mensagens de advertência permite criar, alterar e apagar associações entre o encaminhamento por classes equivalentes e o rótulo, distribuição dinâmica de rótulos que permite a construção, e atualizações da tabela LIB. Esta distribuição dinâmica de rótulos confere autonomia ao *router* para que se possam preencher as tabelas LFIB.

- Método *unsolicited downstream*

Neste método, desde que um *router* LSR associe um rótulo ao encaminhamento por classes equivalentes, informa automaticamente todos os seus vizinhos desta operação. O funcionamento deste método de distribuição de rótulos é ilustrado na Figura 11.3.

Figura 11.3 – Funcionamento do método *unsolicited downstream*.

- Método *downstream on demand*

O funcionamento deste método de distribuição de rótulos é ilustrado na Figura 11.4.

Figura 11.4 – Funcionamento no método *downstream on demand*.

Neste modo, o *router* a montante (*upstream*) pergunta o *router* a jusante (*downstream*) para lhe fornecer o número do rótulo a ser associado a um determinado encaminhamento por classes equivalentes. O *router upstream* envia o tráfego para o *router downstream*, quando passa um pacote que ainda não está associado a uma classe de encaminhamento, o *router upstream* vai exigir a associação de um rótulo para esta classe de encaminhamento ao próximo *router* (do LSR *downstream*). Este método é utilizado pelo protocolo RSVP-TE (é mais confiável que o LDP e é utilizado no contexto MPLS-TE).

11.2 Regras para a atribuição de uma referência ao elemento de rede

Para respeitar a convenção, a atribuição de uma referência aos elementos da rede seguiu as seguintes regras: *(i)* os nomes dos elementos de rede são formados por 3 grupos de caracteres, todos em letras maiúsculas; *(ii)* cada grupo de caracteres é separado pelo caractere hífen "-"; *(iii)* o primeiro grupo de caracteres define o nome do edifício da sua instalação; *(iv)* o segundo grupo de caracteres define a função do elemento de rede; e *(v)* terceiro grupo de caracteres define a instância. A sintaxe para a nomeação do dispositivo é ilustrada pela Figura 11.5.

Figura 11.5 – Convenção seguida para a atribuição de nomes aos dispositivos de rede.

11.3 MTU

No contexto de redes de telecomunicações, "MTU" é o acrónimo para a expressão inglesa *maximum transmission unit*, que em português significa "unidade máxima de transmissão". A MTU refere-se à configuração da dimensão máxima do pacote que pode ser transmitida. O parâmetro MTU está associado a cada *interface* e protocolo.

Conforme ilustrado na Figura 11.6, a *subinterface* para encaminhar a MTU *(i)* herda o MTU da *interface* principal; *(ii)* adicionando 4 octetos para cada *tag* VLAN configurada na *subinterface*. Assim, existem 4 octetos para uma *subinterface dot1q* (IEEE 802.1Q, *custom-TAG*, C-TAG) e 8 octetos para uma *subinterface QinQ* (IEEE 802.ad, *double TAG*, *service VLAN*, *S-VLAN*, *service tag, S-Tag*).

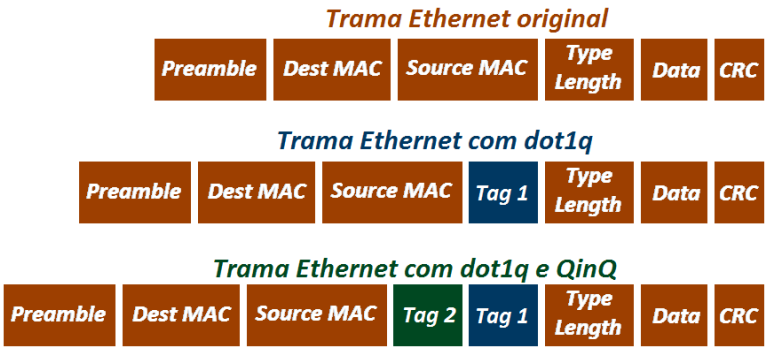

Figura 11.6 – Construções de diferentes do cabeçalho (*overhead*, OH).

O campo "*Preamble*", de 7 octetos, indica que é o início de uma nova trama, e o delimitador de início de trama (*start frame delimiter*, SFD) indica que o início da trama vai começar. O campo "CRC" permite verificar a integridade da trama. O campo "*Type Length*" ou "*Ethertype*", com um comprimento de dois octetos, serve para informar a função *bridge* qual é o protocolo *ethernet*

utilizada na trama: *dot1q* ou *QinQ*. O protocolo *dot1q* consiste em adicionar um rótulo ao tráfego *ethernet,* ou caso tenha o rótulo, verifica-o. O protocolo *QinQ* consiste em adicionar um segundo rótulo ao tráfego *ethernet,* ou no caso de já ter um rótulo, verifica-o. Se o campo "*Type Length*" estiver preenchido com o código "0x8100", o protocolo utilizado é o *dot1q*, se for "0x88a8", "0x9100" ou "0x9200", o protocolo utilizado é o *QinQ*. A utilização do *QinQ* permite um segundo nível de administração para o tráfego *ethernet*. Por regra os responsáveis pelas redes informáticas das empresas acabam por usar a mesma numeração para definir as a rede local (VLAN). Por exemplos, todas as empresas têm VLAN 10, 20, 30, etc. Assim, o operador de telecomunicações, para distinguir as redes locais com a mesma numeração, mas de clientes diferentes, coloca um segundo rótulo. A numeração pode variar entre 1 e 4096 tanto no protocolo *dot1q* como no *QinQ*.

Existem diferentes tipos de encapsulamento que podem ser utilizados para o tráfego do cliente: *(i)* VPN de camada 3, em que são adicionados pelo menos 2 rótulos (8 octetos de *overhead*); *(ii)* MPLS *traffic engineering* e IP *fast rerouter*, em que se adicionam até 2 rótulos (8 octetos de *overhead*); e *(iii) ethernet* sobre MPLS (EoM), em que adiciona até 26 octetos de *overhead.* Este adicional de 26 octetos no *overhead* resulta de serem necessários: *(a)* 6 octetos do endereço MAC de destino pertencente ao quadro *ethernet* original; *(b)* 6 octetos do endereço MAC de origem pertencente à estrutura *ethernet* original; *(c)* 4 octetos de campo "802.1q"; *(d)* 2 octetos tipo/comprimento do campo; *(e)* 4 octetos para a rótulo do encaminhamento *(label switched path,* LSP*)*; *(f)* 4 octetos para o rótulo do circuito virtual.

11.4 *Cisco Discovery Protocol*

O *Cisco Discovery Protocol* (CDP) é um protocolo proprietário da camada 2, com a função essencial de descobrir os dispositivos (*hosts*) que acedem ao comutador, facilitando a compreensão da topologia da rede e da sua arquitetura. Nos *routers* que utilizam o sistema operativo *Cisco IOS*, e por segurança, este protocolo vem por padrão desativado. Os portos que sejam definidos para estarem em utilização, são configurados para que este protocolo ficasse ativado.

É recomendado que o CDP fique também desativado nos portos como a *interface* ligada a provedores de acesso à *internet* pois o CDP envia informações sobre arquitetura ou a plataforma da rede interna da empresa, que podem ser utilizadas por terceiros. Para habilitar o CDP, primeiro é necessário ativar o CDP globalmente no *router* e, depois deve ser ativado nos portos *[11.4-1]*.

12. Apêndice 7 – Equipamentos Ciscos instalados na rede "WAN SCADA"

Este capítulo apresenta a descrição dos equipamentos implementados, dando principal enfâse às características mais relevantes.

A Cisco é um líder mundial no fabrico dessa gama de equipamentos para redes corporativas. Tendo sido um dos fundadores da tecnologia de comutação por rótulos, é bastante coerente que esta empresa ofereça soluções para a criação de *backbones* que utilizam o MPLS. Além disso, existe outros fabricantes de referência mundial como é o caso da *Lucent* e da *Juniper*, duas empresas especializadas em redes, que fizeram uma parceria para desenvolver solução que satisfaçam o mercado das telecomunicações. Também a *Nortel* oferece várias soluções para interconectar redes corporativas que utilizem domínios MPLS.

A escolha do fabricante Cisco por parte da EEM baseou-se em vários critérios: a existência de uma academia que permitiu o surgimento de fóruns que se dedicam ao tema, e por já possuir de uma ferramenta de gestão de redes: *Cisco Prime Infrastructure*. Esta renovada ferramenta foi adquirida num projecto anterior. A *Cisco Prime Infrastructure* permite gerir, a partir de uma única solução integrada, os elementos de rede de uma rede de telecomunicações, e veio substituiu as ferramentas *Cisco Prime LMS 4.2* e *Cisco Prime NCS 1.1*.

12.1 Dispositivo Cisco Aggregation Services *Router* 903

O dispositivo *Aggregation Services Router* 903 (ASR 903) foi implementado no *core* e na agregação da rede "WAN SCADA" *[12.1-1]*. O ASR 903 é uma plataforma compacta, permite redundância, utiliza o sistema operacional *Cisco IOS-XE* e dispõe das seguintes características:

- Uma altura de 3RU e aceita até 6 cartas de linha (*interface*);
- Pode ser instalado em armários com profundidade mínima de 300 mm (tem 235 mm);
- A temperatura de operação pode variar entre -40 e os 65 °C;
- Proporciona redundância de fonte de alimentação, ventilação (lateral) e processador;
- Permite atualizar o sistema operativo com o dispositivo em serviço;
- O *backplane* é de 480 *Gbps*, e cada *slot* suporta até 100 *Gbps*;
- A BIOS do processador e das cartas (*interfaces*) podem ser atualizadas;
- Dispõe de uma capacidade de processamento que pode chegar aos 400 *Gbps*, dependendo do processador escolhido (*route switch processor*, RSP);
- Os portos *ethernet* podem ser de 1 ou 10 *Gbps*;
- Suporta tráfego TDM: 16x T1/E1 e 4x STM1 ou 1x STM4;
- Dispõe de cartas de linha "IM" que suportam tráfego *Serial Sync/Async*: RS232, RS485, RS422, X.21, V.35, EIA-449, EIA-530;
- Respeita as normas IEEE-1613 Classe-2 e IEC 61850-3.

Note-se que a caracterização de "robusta", neste contexto, relaciona-se com o facto do equipamento estar otimizado para ambientes agressivos de alguma industria, tal como a indústria energética. A capacidade de 480 Gbps do *backplane* é a capacidade da matriz de comutação. Se este valor for ultrapassado, ocorre o que se designa por *oversubscribed* (excesso de escrita) e é realizado o descarte *(drop)* aos pacotes. As cartas de linha "IM" possibilita implementar serviços tradicionais. É necessário verificar o *datasheet* do fabricante, pois existem

interfaces que só podem ser instaladas em determinadas posições (*slots*). Os serviços tradicionais necessitam do protocolo de sincronismo PTP 1588v2.

O modelo Cisco ASR 903 é um equipamento concebido para aplicações de agregação de tráfego em ambientes com condições ambientais exigentes, permitindo escalabilidade dos serviços. Possui uma configuração modular, com separação da componente de processamento (*route switch processor*, RSP) e das cartas de linha (IM).

À data da escrita deste documento, a série ASR900 não executa o serviço IPSec nem dispõe de portos PoE.

Na gestão e monitorização deve-se utilizar a aplicação *Cisco Prime* para monitorizar e gerir os elementos de rede. A gestão e monitorização podem ser realizadas recorrendo aos portos locais USB, *serial* e *ethernet.*

Descrição dos módulos das cartas de linha "IM"

A EEM adquiriu vários módulos de cartas de linha que foram instalados nos diversos *slots* dos chassis dos ASR 903 adquiridos.

- O módulo A900-IMA2Z. Este módulo fornece dois portos *ethernet* de 10 *gigabit* com conetividade física, e aceita lasers *ethernet small form-factor pluggable plus* (SFP+) ou *small form-factor pluggable high density* (XFP).

- O módulo A900-IMA8S fornece oito portos *ethernet* de 1 *gigabit* e *fast ethernet* com conetividade física (conector RJ45) e só podem ser instalados nas *slots* 4 e 5. Pode ser selecionada a velocidade de cada porto adaptando-se à necessidade pretendida. Este módulo aceita lasers *small form-factor pluggable* (SFP).

- O módulo A900-IMA8D fornece oito portos E1 (ou T1) aos RSP1 ou RSP2 numa plataforma série Cisco ASR 900. Utiliza conector RJ48/120 Ω.

- O módulo A900-IMASER14A/S fornece 14 portos síncronos ou assíncronos, para facilitar a conetividade com dispositivos que requerem conetividade RS-232. Disponibiliza 6 conectores padrão e 2 conectores de alta densidade (de 68 pinos). Juntamente com o recurso e funcionalidade do *raw socket*, este módulo fornece o transporte de protocolos assíncronos tradicionais baseados em série para as redes IP e MPLS. Os protocolos suportados no módulo são configuráveis por *interface* por *software*, o que permite uma implementação flexível e um uso eficiente do *hardware*. O *raw socket* é o protocolo que permite construir a *frame payload + overhead*. "*Socket"* é o conjunto que define o destino do pacote IP + porto TCP. Assim é possivel ignorar a camada 4, e apenas comunica com a camada 3, como o comando "*ping*". Também é utilizado para a comunicação entre o protocolo RS232, em que é assim adicionado um IP ao *payload* (dados úteis). Encapsula um pacote RS232 (camada 1) num pacote IP.

12.2 Dispositivo Cisco Aggregation Services *Router* 1001-X

O ASR1001-X permite realizar sessões, numa topologia *hub and spoke*, possibilitando desempenhar a função de *route reflector* por forma a garantir a malha completa.

A série *Cisco ASR 1000* suporta o sistema operativo *Cisco IOS-XE* (que é um sistema operacional modular). O processador de serviços embutidos (*embedded services processor*, ESP) utilizado

dispõe de um *throughput* (taxa de transferência) atualizável através de compra da licença. O facto de o sistema operacional ser modular implica que depende de licenças para executar mais funções ou aumentar a sua capacidade de *throughput*. O sistema operativo modular significa que é composta por diversos módulos e funciona em modo agregado.

Os dois *routers* Cisco ASR 1001-X foram implementados na rede "WAN SCADA" da EEM para desempenharem a função de *route reflector*.

12.3 Dispositivo Cisco Connected Grid *Router* (CGR 2010)

O *router Cisco Connected Grid Routers* 2010 (CGR 2010) foram concebidos a partir dos *Integrated Services Router* G2 (ISR G2), mas otimizados para oprearem em ambientes agressivos (*rugged)*.

Um ISR G2 inclui inteligências e ligações para suportar o VoIP e vários outros componentes especializados como a *zone-based policy firewall* (ZBF) e a *prevenção de intrusão* (IPS). A Cisco utilizou esta designação ISR para diferenciar seus produtos de outros fornecedores de *routers* (que agora também incluem muitos desses recursos). Um *router* não ISR apenas encaminha pacotes entre diferentes redes (que é a sua função original). A componente ZBF inspeciona o tráfego e define que tráfego pode entrar e que tráfego pode sair, analisando o IP. Não tem controlo sobre tráfego *Legacy*. A ZBF não suporta muitas linhas de instrução. Também é preciso definir o que é o *inside* e *outside*. A função ZBF permite aliviar a carga no *Adaptive Security Appliance* (ASA), pois já é descartado algum do tráfego não aceite.

As principais características do *router* CGR 2010 são:

- Projetado para ser robusto, não dispõe de ventiladores (o arrefecimento é por convecção), suporta uma elevada variação na gama de temperatura de funcionamento (-40 até +60ºC, e num curto período de tempo, suporta até 85ºC) e sem componentes móveis;
- Segurança integrada para ajudar a cumprir os critérios de proteção de infraestrutura crítica;
- Projetado para dispor de redundância e uma elevada disponibilidade;

O *router* CGR aceita os serviços tradicionais, mas não está certificado como está o *router* ASR903. O *router* CGR não suporta o LAG, ou seja, o *portchannel*. Também seria um erro utilizar o mecanismo *PortChannel* com o CGR pois só dispõe de dois portos óticos.

Os *routers* CGR é um dispositivo para ser instalado numa arquitetura IP, mas utilizam a instância VRF *lite* para trocar tráfego com o *router* PE (ASR903).

Módulo comutador ethernet para o CGR 2010

O diagrama ilustrado na Figura 12.1 ilustra a relação entre o *router* CGR e o módulo de comutação *ethernet* (*ethernet switch module*, ESM) *grid router WAN interface card* (GRWIC).

O módulo ESM expande os recursos do CGR integrando a comutação camada 2 a 3, e foi desenvolvido especificamente para a indústria elétrica. Além disso, os seus recursos podem ser utilizados na indústria de distribuição de água, petróleo e gás. O ESM oferece segurança, confiabilidade e escalabilidade à rede.

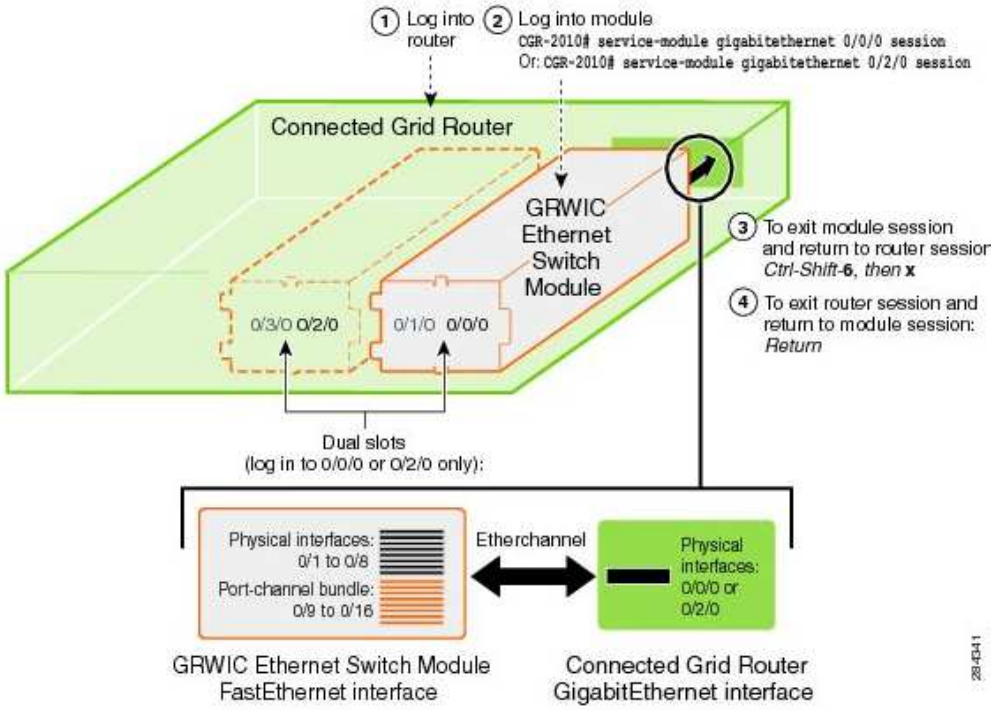

Figura 12.1 – Integração do módulo ESM no Cisco CGR 2010 *[12.3-1]*.

As principais características do Cisco *ethernet switch module* (ESM) são:

- Projetado para ser robusto, não dispõe de ventiladores (arrefecimento por convecção) e está em conformidade com o ambiente de subestação, pois respeita as normas IEC-61850-3 e IEEE 1613 Classe 2;
- Fácil de configurar e de gerir, pois usa uma *interface* gráfica (GUI) do fabricante Cisco, *Configuration Professional*, e as ferramentas de gestão de suporte, incluindo o *CiscoWorks LAN Management Solution* (LMS);
- Alta disponibilidade, comportamento QoS determinista e segurança confiável utilizando o sistema operativo *Cisco IOS*;
- *Modelos Smartport* que implementam configurações de programas (*software*) recomendados para aplicativos de subestações;
- Suporte de *hardware* para IEEE1588v2 (protocolo de sincronismo PTP para os serviços *Legacy*), com um protocolo de temporização de precisão (com precisão ao nível do nanossegundos) para aplicações de temporização precisas;
- Resiliência melhorada do anel com o suporte do *resilient ethernet protocol* (REP) e *flexlink*;
- Suporte *power over ethernet* (PoE)/PoE+ no modelo GRWIC-D-ES-2S-8PC.

O módulo ESM do CGR dispõe de 8 portos, os 4 primeiros são *power over ethernet* (PoE, 802.3af), e a EEM configurou os portos 7 e 8 com o suplicante 802.1X, para que qualquer PC possa aceder a *internet* via VPN. O VoIP deve ser ligado nos portos PoE.

13. Bibliografia

Geral:

Por referência:

[1.2-1] – Automatic meter reading and advanced metering infraestructure, site:

http://home.zcu.cz/~tesarova/IP/Proceedings/Proc_2010/Files/024%20IP2010%20Krutina.pdf, consultado em junho 2017.

[1.2-2] – IEC 61850, site: *https://www.edpdistribuicao.pt/pt/profissionais/projeto-tipoSE_AT_MT/documentacaonormativa/Especificao%20Funcional/EDPDEF-C13-504N.pdf*

Consultado em junho 2017.

[3] – Muitos dos temas abordados neste capítulo tem como referência principal o livro "*Redes MPLS - Fundamentos e Aplicações*", de José Mário Oliveira, Rafael Dueire Lins e Roberto Mendonça, Brasport Livros e Multimédia, 2012 e também o site:

http://slideplayer.com/slide/4900798/, consultado em setembro 2017.

[3.1-1] – Forwarding equivalence classe (FEC), documento "*Os Mecanismos de Qualidade de Serviço em Redes IP",* de Maria Joana Urbano, 2003. Consultado em setembro 2017.

[3.1-2] – Label distribution protocol, site: *http://netzikon.net/rfc/rfc.html*, "*RFC3036 LDP Specification*". Consultado em setembro 2017.

[3.1-3] – Construção de tabelas, site:

https://pg.edu.pl/documents/1112617/28513726/Wyklad%20ASK%20-%20MPLS

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/mpls.pdf

*https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-8/segrt-xe-16-8-book/sr-routing-info-base-support.pdf*Consultado o sítio, em novembro 2017.

Consultado em setembro 2017.

[3.1-4] – Adaptação da figura obtida no site, da atribuição de rótulos e relação entre plano de controlo e dados, site: *https://pt.slideshare.net/LogicalisLatam/diseos-de-red-basados-en-mpls-14206149.* Consultado em setembro 2017.

[3.2-1] – Traffic engineering, site:

https://www.nanog.org/meetings/nanog37/presentations/pete-templin.pdf

Consultado o sítio, em novembro 2017.

[3.4-1] – Pano de controlo, do site:

http://www-igm.univ-mlv.fr/~dr/XPOSE2006/marot/architecture.html

Consultado em novembro 2017.

[3.6-1] - Troca de rótulos, do site:

https://flylib.com/books/en/2.686.1/cell_mode_mpls.html, consultado em outubro 2017.

[3.11-1] – Virtual private wire service, no site:

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-2/lxvpn/configuration/guide/b-l2vpn-cg-asr9000-62x/b-l2vpn-cg-asr9000-62x_chapter_0101.pdf. Consultado em novembro 2017.

[3.11-2] – Structure-agnostic TDM over packet, *site:*

http://www.cisco.com/c/en/us/td/docs/*routers*/asr903/software/guide/chassis/Release3-9-0S/ASR903-Chassis-SW-39/pseudowire.pdf. Consultado em novembro 2017.

[3.11-3] – Virtual private LAN servisse e *virtual forwarding instance*, no site:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/vpls.pdf. Consultado em novembro 2017.

[3.11-4] – Virtual forwarding instance, no site:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-3s/mp-l2-vpns-xe-3s-book/mp-vpls.html. Consultado em novembro 2017.

[3.11-5] – VPN-L3, PDF do fabricante Cisco "*Implementing MPLS Layer 3 VPNs on Cisco IOS XR Software*". Consultado em novembro 2017.

[3.11-6] – Atributo *route distinguisher, d*ocumento do fabricante Cisco: "*Cisco Systems Advanced Services, Telecom Montenegro MPLS/VPN Network (Mipnet), Low Level Design, Version 1.1*". Consultado em novembro 2017.

[3.13-1] – Microloop avoidance local, documento *"Segment Routing Configuration Guide",* site:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16/segrt-xe-16-book/segrt-xe-16-book_chapter_010000.html. Consultado o sítio, em abril 2017.

[3.13-2] – Loop-free alternate fast reroute, no site:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3s/asr903/iri-xe-3s-asr903-book/iri-lfa-frr.pdf

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro-lfa-frr.html. Consultado o sítio, em abril 2017.

[3.13-3] – Mecanismo *nonstop forwarding e stateful switchover,* site:

https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/nsf24s.html

Consultado em n abril 2017.

[3.13-4] – Mecanismo *Link Aggregation Group and Link Aggregation Control Protocol,* site:

https://www.cisco.com/c/en/us/td/docs/switches/metro/me2600x/config/guide/b_ME2600X-scg/b_ME2600X-scg_chapter_0101.pdf

Consultado em abril 2017.

[4.2-1] – Mecanismo IP *fast rerouter*, adaptação da figura obtida no site:

https://pt.slideshare.net/CiscoTurkey/cisco-akll-enerji-smart-energy-cisco-connect-tr-14. Consultado em fevereiro 2018.

[4.2-2] – Boas práticas na implementação de segurança na rede, documento do fabricante Cisco: " *IoT Threat Defense for Manufacturing - SAFE Design Guide - Security Domain: Threat Defense*", atualização em maio de 2018. Consultado em fevereiro 2018.

[4.8-1] – LSA, site: *https://ieoc.com/discussion/29428/ip-fast-reroute-ospf-lfa-with-csr1000v*. Consultado em novembro 2017.

[4.8-2] – Mecanismo IP *loop-free alternate fast rerouter*, site:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro-lfa-frr.html. Consultado em novembro 2017.

Consultado em novembro 2017.

[4.8-3] – Atribuição de identificadores aos VRF, Documento do fabricante Cisco: "*Cisco Systems Advanced Services, Telecom Montenegro MPLS/VPN Network (Mipnet), Low Level Design, Version 1.1*". Consultado em novembro 2017.

[6] – Em vários pontos deste capítulo também se baseou no:

- Nos apontamentos da unidade curricular "Comunicações Óticas", do Prof. Luís A. A. O. Gomes.

- No livro "*Projeto de Sistemas de Comunicações Ópticas*", José Roberto de Almeida Amazonas, 2005.

- No site http://www.ipb.pt/~fmoreira/Ensino/Ondas/Ondas_04_05_cap5.pdf

Consultado em janeiro 2017.

[6.1-1] – Dispersão do modo de polarização, site:

https://wiki.metropolia.fi/display/Physics/(M)+Dispersion+in+Fiber+ Optics

Consultado em agosto 2016.

[6.1-2] – Adaptação da figura obtida do livro "*Optical Fiber Communications - Principles and Practice*", John M. Senior, Pearson Prentice Hall.

[8] – Em vários pontos deste capítulo basearam-se no site:

https://www.slideshare.net/khantloo/pdh-and-sdh1, consultado em janeiro 2017.

[8-1] – Diapositivos do IST "Redes de Telecomunicações", capítulo 4 "Redes de Transporte SDH", Prof João Pires, consultado em janeiro 2017.

[8-2] – Diapositivos do UALG "Redes de Telecomunicações", capítulo "SDH", Prof. Maria do Carmo Medeiros, consultado em janeiro 2017.

[8-3] – Documento "Estudo e análise experimental do mapeamento de tráfego *ethernet* sobre SDH", capítulo IV, de Bruno de Oliveira Monteiro, consultado em março 2017.

[9.1-1] – Documento "*Information SURPASS hiT 7060 3.1 - Technical Manual (A42022-L5969-A 51-1-7618)*".

[11.1-1] – Best effort, site: *https://pt.wikipedia.org/wiki/Best_effort.* Consultado em agosto 2017.

[11.4-1] – *Cisco Discovery Protocol* (CDP), site:

https://pt.wikipedia.org/wiki/Cisco_Discovery_Protocol. Consultado em agosto 2017.

[12.1-1] – O dispositivo *Aggregation Services Router* 903, site:

https://www.cisco.com/c/en/us/products/collateral/*routers*/asr-903-series-aggregation-services-*routers*/datasheet-c78-738339.html

Consultado em dezembro 2017.

[12.3-1] – O dispositivo *Integração do módulo ESM no Cisco CGR 2010,* site:

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/switch_module_swcg/cgr-esm-configuration/access_module.html.

Consultado em dezembro 2017.