UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

TUTORIAL DE TRATAMENTO DE FALHAS DE REDES DE TRANSMISSÃO EM REDES DE TELECOMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2014

JEAN MARCELL FERREIRA
CARLOS EDUARDO CONRADO RAMOS
CHARLES RENAN DA COSTA

TUTORIAL DE TRATAMENTO DE FALHAS RELACIONADAS A REDES DE TRANSMISSÃO EM REDES DE TELECOMUNICAÇÕES

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica – DAELN – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Ubiradir Mendes Pinto.

CURITIBA
2014

JEAN MARCELL FERREIRA
CARLOS EDUARDO CONRADO RAMOS
CHARLES RENAN DA COSTA

Tutorial de Tratamento de Falhas Relacionadas a Redes de Transmissão em Redes de Telecomunicações

Este trabalho de conclusão de curso foi apresentado no dia 16 de Outubro de 2013, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____

Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____

Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____

Prof. Dr. Kleber Kendy Horikawa Nabas

_____

Prof. Ubiradir Mendes Pinto
Orientador

_____

Prof. M.Sc. Alexandre Jorge Miziara

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

AGRADECIMENTOS

Agradecemos a Deus pela dádiva mais preciosa, a Vida, aos nossos Pais, Irmãos e familiares que nos mostraram o caminho e nos ensinaram a percorrê-lo. Às nossas esposas pela paciência, pelo carinho e apoio, aos amigos que partilharam dos mesmos esforços e a todos os Professores do curso Sistemas de Telecomunicações, especialmente nosso professor orientador Ubiradir, por compartilhar os seus conhecimentos e nos acompanharam nessa jornada.

RESUMO

FERREIRA, Jean M.; RAMOS, Carlos E. C.; COSTA, Charles R. da. **Tutorial de Tratamento de Falhas Relacionadas a Redes de Transmissão em Redes de Telecomunicações**. 2013. 259f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná - UTFPR. Curitiba, 2014.

Este trabalho tem por objetivo a produção de um documento em forma de tutorial visando minimizar as dificuldades enfrentadas por novos colaboradores. Demonstra as principais causas de falhas em redes de transmissão e suas respectivas formas de correção. De forma sintetizada apresenta a estrutura e o funcionamento operacional de uma empresa de telecomunicações, as principais teorias sobre redes de telecomunicações e as tecnologias utilizadas do ponto de vista de transmissão, apresenta também alguns dos equipamentos mais utilizados e topologias de rede de forma genérica.

Palavras Chave: Falha. Rede. Transmissão. Tutorial.

ABSTRACT

FERREIRA, Jean M.; RAMOS, Carlos E. C.; COSTA, Charles R. da. **Tutorial Treatment Failures Related to Transmission Networks in Telecommunication Networks**. 2013. 259f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná - UTFPR. Curitiba, 2014.

This work has as objective the production of a document as a tutorial with intention reduces the difficulty confronted by new collaborator demonstrating the main causes of failures in transmission networks and their respective forms of correction. The synthesized form presents the structure and operation of a telecommunications company, the main theories on telecommunications networks and the technologies used from the viewpoint of transmission, also presents some of the most used equipment and network topologies generic form.

Key Words: Failures. Networks. Transmission. Tutorial.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ANSI	*American National Standards Institute*
ATM	*Asynchronous Transfer Mode*
BRAS	*Broadband Remote Access Server*
CGR	Centro de Gerência de Rede
CoS	*Class of Service*
CWDM	*Coarse Wavelength Division Multiplexing*
DGO	Distribuidor Interno Ótico
DHCP	*Dynamic Host Configuration Protocol*
DID	Distribuidor Intermediário Digital
DIO	Distribuidor Interno Ótico
DSLAM	*Digital Subscriber Line Access Multiplexer*
DTMF	*Dual Tone Multi-Frequency*
DVB-ASI	*Digital Video Broadcast-Asynchronous Serial Interface*
DWDM	*Dense Wavelength Division Multiplexing*
EAPS	*Ethernet Automatic Protection Switching*
ESCON	*Enterprise Connection Systems*
FC	*Fiber Connector*
FICON	*Fibre Connetion*
GFP	*Generic Framing Procedure*
GPON	*Gigabit Passive Optical Network*
HSRP	*Hot Standby Router Protocol*
IETF	*Internet Engineer Task Force*
IMA	*Inverse Multiplexing for ATM*
ISDN	*Integrated Services Digital Network*
IS-IS	*Intermediate System-to-Intermediate System*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
LAN	*Local Area Network*
LCAS	*Link Capacity Adjustment Scheme*
MAC	*Media Access Network*
MAN	*Metropolitan Area Network*
MGCP	*Media Gateway Control Protocol*
MOT	*MPLS over Transport Port*
MPLS	*Multiprotocol Label Switching*
MSPP	*Multi-Service Provisioning Platform*
MSTP	*Multiple Spanning Tree Protocol*
NGN	*Next Generation Networks*
NNI	*Network Network Interface*
NOC	*Network Operation Center*
ODU	*Optical channel Data Unit*
OSI	*Open System Interconnection*
OSPF	*Open Shorted Path First*
OTN	*Optical Transport Network*
PABX	*Private Automatic Branch Exchange*
PAM	*Pulse Amplitude Modulation*

PCM	*Pulse Code Modulation*
PDH	*Plesyochronous Digital Hierarchy*
POTS	*Plain Old Telephone Service*
PSTN	*Public Switched Telephone Network*
PVC	*Permanent Virtual Circuit*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial In User Service*
RDSI	Rede Digital de Serviços Integrado
RIP	*Routing Information Protocol*
RPR	*Router Processor Redundancy*
RSTP	*Rapid Spanning Tree Protocol*
SDH	*Synchronous Digital Hierarchy*
SFP	*Small Form-factor Pluggable*
SIP	*Session Initiation Protocol*
SNMP	Simple Network Management Protocol
SONET	*Synchronous Optical Network*
STM	*Synchronous Transfer Module*
STP	*Spanning Tree Protocol*
TCP/IP	*Transmission Control Protocol/ Internet Protocol*
TDM	*Time Division Multiplexer*
UNI	*User Network Interface*
VLAN	*Virtual Local Area Network*
VOIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
xDSL	*Digital Subscriber Line*

SUMÁRIO

1 INTRODUÇÃO

O CGR (Centro de Gerência de Rede) ou mais conhecido como NOC (centro de operação de rede - *Network Operation Center,* em inglês), é o coração de toda empresa de telecomunicações, nele são concentrados todos os sistemas de gerência com objetivo de monitorar todas as plataformas de tecnologia.

A partir de programas de gerência específicos de cada equipamento (normalmente cada fabricante tem seu próprio programa para gerência de seu equipamento), ou programas desenvolvidos para determinada tecnologia tem-se visibilidade de toda a rede em tempo real.

Os elementos da rede (NEs – *Network Elements*, em inglês) podem ser computadores, roteadores, switchs, gateways, SDHs, centrais telefônicas, DSLAMs, entre outros.

O operador do NOC esta responsável pelo monitoramento da rede, quando detectado um eventual problema ou falha deve ser capaz de localizar a origem do defeito e corrigir o mais rápido possível. Por isso deve conhecer os equipamentos e as tecnologias pela qual esta responsável.

São muitas as tecnologias dentro de uma rede tais como: SDH, xWDM, ATM, IP, xDSL, V5.2, Voip entre outras. Desta forma as tecnologias são divididas conforme sua aplicação: Rede de Acesso, Rede de Comutação, Rede de Transmissão, Rede de Dados e Infraestrutura.

São de responsabilidade do NOC a administração, o controle, o monitoramento e operação diária de todas as infraestruturas físicas e lógicas da rede. O trabalho do NOC deve garantir altos níveis de disponibilidade, rendimento e operação da rede 24 horas por dia, 7 dias por semana , 365 dias por ano.

1.1 PROBLEMA

Como o fluxo de trabalho no setor é muito alto para a quantidade de funcionários, não é sempre que o novo funcionário consegue acompanhar as tratativas junto aos mais antigos.

Há poucos documentos e procedimentos escritos e os que existem estão espalhadas e desatualizados, a dificuldade de encontrar informações precisas prejudica o tempo de tratamento das falhas e o aprendizado dos novos colaboradores é comprometido.

Muitas das informações são descritas pelos próprios funcionários em documentos particulares, portanto há a necessidade de reunir todas as informações e disponibiliza-las em um único documento em local acessível a todos.

1.2 JUSTIFICATIVA

A proposta de criação de um tutorial que irá reunir todas as informações necessárias para o tratamento de falhas relacionadas à rede de transmissão em um único documento em local acessível a todos os funcionários do setor. Desta forma deverá facilitar o entendimento e aprendizado sobre o funcionamento e funcionalidades da rede, funcionamento do setor e tecnologias utilizadas.

Irá facilitar o acesso a informações objetivas e seguras tanto para os funcionários mais antigos que desejam tirar alguma dúvida ou revisar algum procedimento, quanto para os novos funcionários que estão aprendendo sobre a função.

O documento será desenvolvido para a rede de transmissão de uma operadora de telecomunicações genérica atuante no mercado brasileiro.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Desenvolver um tutorial para tratamento de falhas relacionadas à rede de transmissão de uma operadora de telecomunicações.

1.3.2 Objetivos Específicos

- Estudar as teorias sobre as tecnologias envolvidas em redes de telecomunicações.
- Conhecer o NOC, e a forma como são divididas as tecnologias conforme sua aplicação.
- Conhecer os equipamentos utilizados.
- Levantar e conhecer a topologia da rede.
- Desenvolver o tutorial para tratamento de falhas relacionadas à rede de transmissão.

1.4 METODOLOGIA

Para o desenvolvimento deste trabalho será realizado um levantamento bibliográfico para fundamentação teórica e conhecimento das tecnologias abordadas, onde serão estudados os princípios de redes de telecomunicações.

Para o tutorial serão reunidas as informações necessárias com base em documentos já existentes e nas experiências adquiridas e vivenciadas dentro do NOC em situações cotidianas e, portanto comprovadamente eficazes.

No tutorial constarão os principais problemas e falhas que ocorrem nas redes de transmissão, e o *troubleshooting* realizado, que é a forma como os problemas foram resolvidos, buscando sempre localizar a raiz do problema e corrigi-lo.

Durante todas as etapas de produção do tutorial o mesmo será testado e revisado pela equipe responsável pelo monitoramento da rede de transmissão do NOC para garantir que esteja dentro das necessidades do setor.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 REDES DE TELECOMUNICAÇÕES

É o conjunto de todas as estruturas físicas e lógicas interconectadas com objetivo de realizar a comunicação de qualquer tipo de informações de um lugar para outro.

Uma das formas mais comuns de exemplificar uma rede é a do sistema telefônico, que permite a comunicação entre dois assinantes, nela temos a conexão elétrica do telefone até a central telefônica que estabelece a conexão entre os dois assinantes. “A ligação física dos telefones até as centrais de comutação é realizada através da rede de acesso e a interligação entre os equipamentos de comutação é realizada pelos sistemas de transmissão” (WIKIPÉDIA, 2012).

São muitas as tecnologias dentro de uma rede de telecomunicações, desta forma a rede é dividida conforme sua aplicação: Rede de Acesso, Rede de Comutação, Rede de Transmissão, Rede de Dados e Infraestrutura.

Rede de Acesso - Faz a interligação entre os clientes e a central de comutação e ou Servidores de Dados (BRAS). É a parte da rede onde se concentra o maior número de conexões da rede, ela se estende desde a casa do cliente até as operadoras de telecomunicações. Utiliza uma grande variedade de tecnologias e protocolos de comunicação que dependem dos serviços proporcionados ao cliente (NASCIMENTO; TAVARES, 2002).

Rede de Comutação - Basicamente é composta por centrais telefônicas que são responsáveis pelo encaminhamento de chamadas telefônicas, realiza a conexão entre os assinantes reservando o circuito (caminho físico) apenas para esta utilização, desocupando novamente após o termino da chamada.

Rede de Dados ou Rede IP – O funcionamento lógico das redes de dados segue o modelo TCP/IP, por este motivo também é chamada de rede IP. É composta por elementos de rede como switches e routers que realizam a comutação e roteamento de informações, ou seja, é responsável pelo controle e direcionamento dos dados da rede, outro elemento de rede importante é o BRAS (Servidor de Acesso Remoto de Banda Larga, do inglês *Broadband Remote Access Server*) ele realiza autenticação

de clientes, concentra o tráfego de assinantes de banda larga e posteriormente transfere para a Internet (TITTEL, 2003).

Rede de Transmissão – Também chamada de Rede de Transporte, realiza a interconexão entre os elementos da rede, transporta as informações entre a Rede de Acesso, a Rede de Dados e a Rede de Comutação. Possui equipamentos de alta capacidade de tráfego de dados e em sua grande maioria são transmitidos por fibra ótica utilizando tecnologias como o ATM, SDH, DWDM, entre outras (SOARES NETO, 2000).

Infraestrutura – É o conjunto de todo o sistema responsável pelo suporte aos equipamentos, assegurando o pleno funcionamento e integridade física das redes citadas acima. É composto por sistema de eletricidade, aterramento, sistema de refrigeração, sistema de incêndio, sistema de segurança e do próprio local de instalação do equipamento.

2.2 TOPOLOGIAS DE REDE

Os equipamentos da rede podem ser interligados de diferentes formas, o modo como à informação será distribuída na rede é que define qual topologia será a mais adequada. Há dois tipos de topologias, a física e a lógica. A topologia física é a forma como a estrutura é organizada, como os elementos de rede são interligados. A topologia lógica é caminho que é percorrido pelos dados na rede.

Ponto-a-Ponto: É a forma mais simples de topologia em que dois elementos de rede são conectados entre eles. Normalmente é utilizada para conectar dispositivos.

Linha: Os elementos de rede são conectados como na topologia ponto-a-ponto de forma que um elemento se conecte no máximo a dois elementos. É muito utilizada em Backbones que cobrem grandes distâncias, com isso há a necessidade de equipamentos regeneradores ao longo do caminho.

Barramento: Todos os elementos de rede são conectados por um único cabo, desta forma toda a informação contida neste cabo chega a todos os elementos de rede, sendo assim necessário o endereçamento da informação para que seja lida somente pelo destinatário. É muito usada nas redes Ethernet.

Anel: É interligado como na topologia em linha, porém o primeiro elemento se conecta ao ultimo fechando um anel. Quando um elemento quer se comunicar com outro que não seja seu vizinho a informação é transmitida pelos elementos até chegar ao seu destino. A comunicação na topologia em anel pode ser unidirecional ou bidirecional. Na unidirecional as informações são transmitidas em apenas um sentido do anel, já na bidirecional as informações são transmitidas pelos dois lados. É muito utilizada em redes SDH, pois caso haja falha de comunicação em um dos lados ainda há o outro para comunicação.

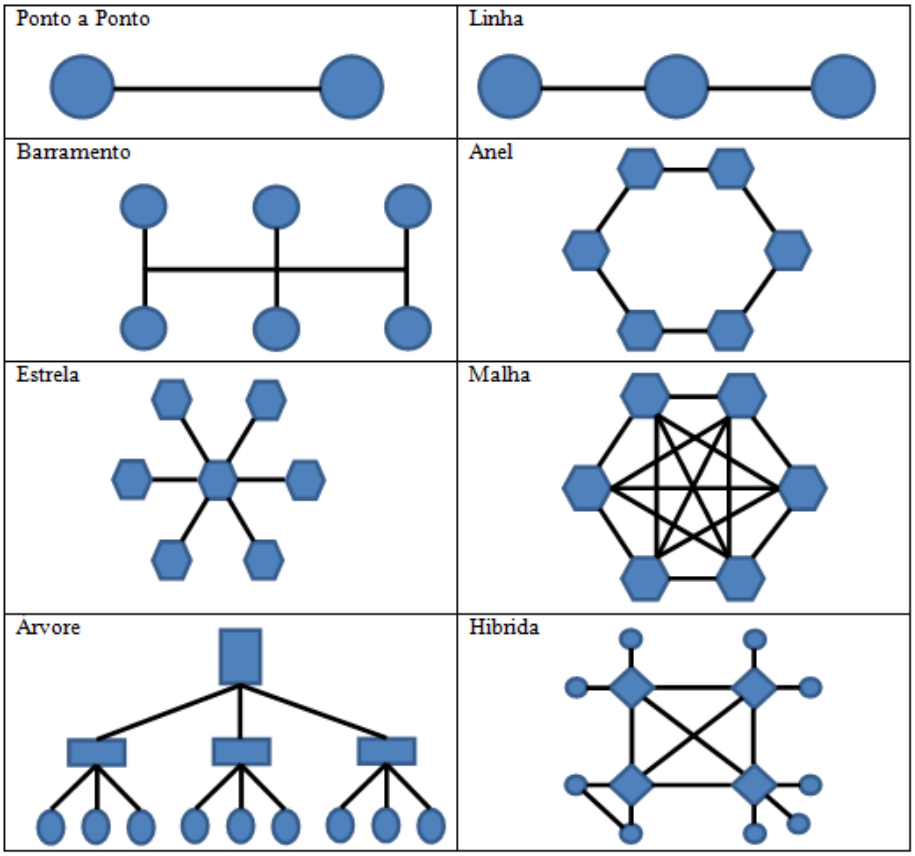
Estrela: Todos os elementos se conectam a um elemento central como, por exemplo, em uma rede de computadores, todos os elementos são conectados por um switch.

Malha: Nesta topologia todos os elementos de rede se conectam a todos, ou seja, existe uma conexão física entre todos os elementos. É muito utilizada em redes de dados com roteadores e switchs quando é necessária alta disponibilidade dos elementos e baixa tolerância a falhas.

Árvore: É a interligação entre vários elementos já conectados em estrela, semelhantes a uma árvore onde todas as ramificações estão convergindo para uma raiz.

Híbrida: Consiste na combinação de duas ou mais topologias de forma que as redes possam expandir e integrar-se em outras redes, um exemplo disso é a rede de telecomunicações.

O Quadro 1 apresenta os tipos de redes citados.



Quadro 1 - Exemplos de topologias
Fonte: Autoria própria.

2.3 PSTN (PUBLIC SWITCHED TELEPHONE NETWORK)

A Rede Pública de Telefonia Comutada (RPTC) é uma rede comutada por circuitos, utilizada para comunicações de voz em tempo real.

Durante uma chamada telefônica é realiza a conexão entre os assinantes reservando o circuito (caminho físico) apenas para esta utilização, desocupando novamente após o termino da chamada. Todo o trabalho de criação de um caminho provisório é realizado pelas centrais de comutação e o caminho que foi estabelecido é chamado de circuito virtual.

Feito a conexão não ocorrerá indisponibilidade durante a chamada, pois somente os assinantes estarão utilizando esta linha, desta forma a comutação por circuito apresenta alto nível de confiabilidade (TITTEL, 2003).

Como a quantidade de chamadas simultâneas utilizando a rede telefônica é muito grande, geralmente é empregada a multiplexação, o método mais comum é a Multiplexação por Divisão de Tempo (TDM), abordaremos este assunto posteriormente.

Segundo Pinheiro (2005) as redes telefônicas são classificadas conforme sua hierarquia e são divididas em redes locais e redes interurbanas. Na rede local temos ainda a rede de assinantes que é a interligação entre o assinante e a central telefônica, e a rede de entroncamentos que interliga as centrais locais. As centrais telefônicas são a inteligência da rede, elas realizam a concentração, distribuição, interligação e tarifação das chamadas produzidas pelos assinantes.

As centrais telefônicas são classificadas como públicas ou privadas. Centrais privadas são normalmente utilizadas em empresas que necessitem de grandes quantidades de linhas telefônicas, como exemplo pode citar o PABX (*Private Automatic Branch Exchange*) onde cada telefone a ele conectado é chamado de ramal. As centrais públicas são classificadas conforme a sua aplicação e posição na rede e são divididas em centrais locais, tandem e transito. A central local é onde é realizada a comutação local, pois é conectada a linha do assinante. A central tandem interliga as centrais locais e interurbanas, não possui terminais de assinantes. A central de transito interliga “sistemas” locais, interurbanos e internacionais (ALENCAR, 1998).

O número de telefone de cada assinante funciona como um endereço, em um número de telefone padrão como 51 41 3123 4567, o 51 é o código do país, o 41 é o código de área, os dígitos 3123 identificam o comutador local dentro da companhia telefônica, estes dígitos são chamados de comutação (Exchange), os últimos quatro dígitos 4567 identificam uma linha telefônica individual (TITTEL, 2003).

2.4 NGN (NEXT GENERATION NETWORKS)

As redes de nova geração são baseadas na convergência de todos os tipos de informação (sendo voz, dados e vídeo) na mesma infraestrutura da rede.

Segundo Tronco (2011), o foco das NGN é separar o *hardware* do *software* dos equipamentos de telecomunicações, através de interfaces padronizadas.

Neste tipo de arquitetura os elementos de rede são divididos em quatro camadas funcionais:

Camada de Acesso – também chamada de *Edge Layer* é a camada mais próxima do usuário, pois são os dispositivos que são instalados na residencial ou empresa do cliente, esses dispositivos podem ser telefones fixos e celulares, PABX, computadores, modems, roteadores.

Camada de Núcleo – também é conhecida como *Core Layer*, é a camada responsável pelo encaminhamento e transporte das informações desde o usuário até o seu destino. Os equipamentos desta camada de rede são comutadores e agregadores de transporte, eles possuem alto tráfego e processamento de informações.

Camada de controle da rede – do inglês, *Network Control Layer*, esta camada é responsável pelo estabelecimento das rotas de sinalização de chamada entres as camadas de Acesso e Núcleo.

Camada de serviços e aplicações – nesta camada é realizado o gerenciamento dos serviços fornecidos, nela é realizada a autenticação e tarifação dos usuários.

Como forma de padronização os elementos das redes NGN são divididos conforme a sua aplicação, são eles:

***Media Gateways* (GW)** – São utilizados na camada de acesso, são divididos em *Media Gateway* de Acesso que conecta os equipamentos dos usuários a rede NGN e *Media Gateway* de Tronco que conecta a rede NGN a PSTN. Os GWs convertem as informações dos usuários (voz, dados e vídeos) em Protocolo Internet (IP).

Media Gateways Controller (MGC) – Mais conhecido como *Softswitch* ou Servidor de Chamadas (SC), realiza o encaminhamento das chamadas telefônicas utilizando rotas sobre a rede IP.

Controlador de Rotas (CR) – Realizada o cálculo das rotas para encaminhamento das chamadas na rede IP.

***Gateway* de Sinalização (SGW)** – converte a sinalização telefônica convencional (SS#7) em sinalização de chamada na rede IP.

Rede de Pacotes (Núcleo) – Composta pelos equipamentos da camada de Núcleo (TRONCO, 2011).

A Figura 1 representa o modelo da NGN dividido por camadas.

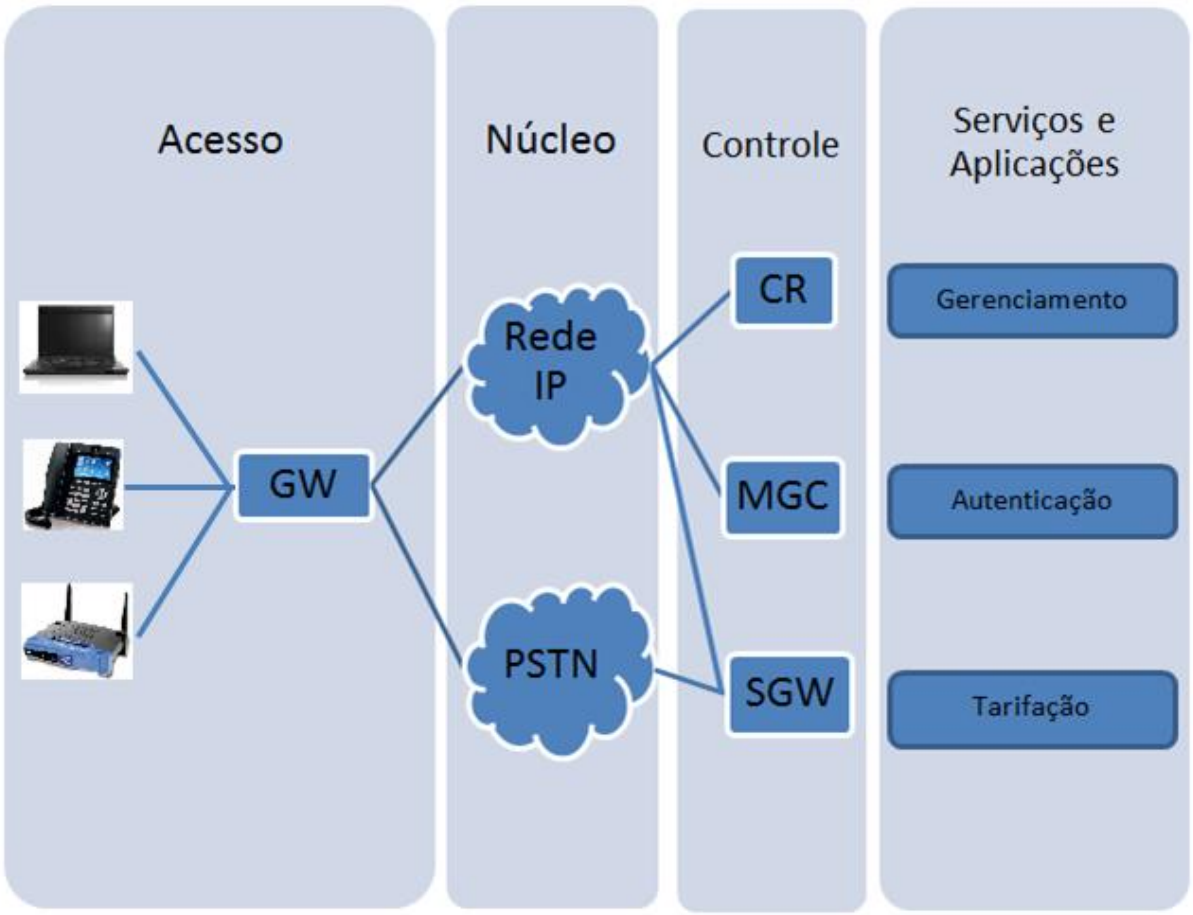


Figura 1 - Modelo da NGN dividida por Camadas
Fonte: Autoria Própria.

2.5 TECNOLOGIAS

2.5.1 TDM

A Multiplexação por Divisão do Tempo ou TDM (*Time Division Multiplexer)* surgiu no inicio de 1970 e é muito utilizado em telecomunicações, por exemplo, para transmissão de voz. O sinal passa pela técnica PCM (*Pulse Code Modulation*). Nesta técnica como a voz é analógica, a mesma deve ser convertida para um formato digital de forma que em seguida possa ser multiplexada. Para isso primeiramente o

sinal é amostrado em intervalos de tempo regulares, neste caso a 8000 Hz que é o dobro da frequência máxima a ser amostrada, processo explicado pelo estudo de Nyquist. Após ocorre a quantificação, ou seja, as amostras são convertidas em um código binário de 8 bits. Logo temos para um canal de voz um sinal codificado de 64 Kbits, que é justamente 8000 amostragens X 8 bits. Após este processo as amostras em formato binário são transmitidas agrupadas no meio de transmissão por meio de um multiplexador, e quando chegam ao seu destino são recuperadas por um demultiplexador (SOARES NETO, 2000).

A Figura 2 representa a multiplexação TDM:

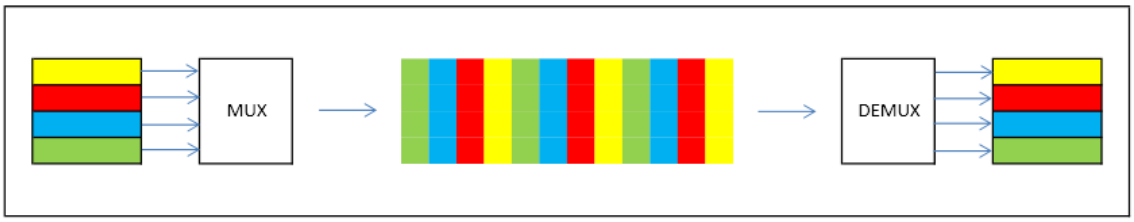


Figura 2 – Multiplexação TDM
Fonte: Autoria Própria.

A multiplexação TDM pode ser síncrona (Figura 3) ou assíncrona (Figura 4). No processo síncrono há apenas um sinal de clock tanto para o multiplexador quanto para o demultiplexador, não havendo byte de sincronismo. Neste caso o tempo é dividido em intervalos de tempo de tamanho fixo, chamados frames, e os frames são subdivididos em slots por onde será encaminhada a informação. Mesmo quando os canais não estão sendo utilizados, os mesmo ocupam banda. No caso do processo assíncrono é necessário um cabeçalho que identifique a mensagem que esta sendo transmitida. Neste caso só será transmitida a informação, e os canais não utilizados ficarão livres, não havendo assim o desperdício de capacidade do canal (SOARES NETO, 2000).

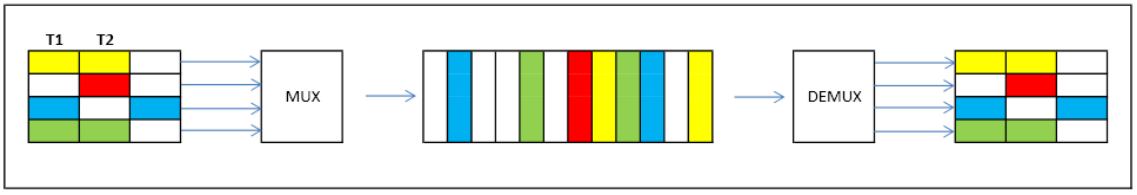


Figura 3 – TDM Síncrono
Fonte: Autoria Própria.

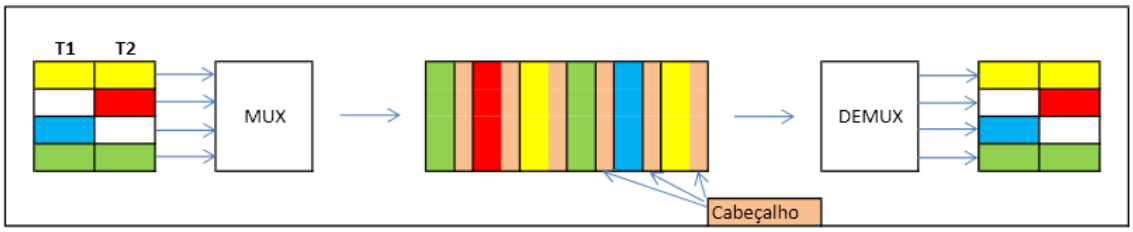


Figura 4 - TDM Assíncrono
Fonte: Autoria Própria.

2.5.2 V5.2

V5 é uma família de protocolos da rede de telefonia definidos pelo ETSI e ITU-T, que permitem a comunicação aberta entre a central telefônica (LE) e o assinante ou sistema de acesso (AN). O AN possui as linhas físicas de assinantes, e por não apresentar característica de comutação deve ser conectado a uma central telefônica pública comutada (LE) responsável também por fornecer diversos serviços exigidos pelo usuário. Possui protocolos baseados em troca de mensagens que são independentes da interface do usuário, e da tecnologia ou arquitetura do AN e do LE (GONZAGA, 2004)

A Interface V5.2 é definida na norma ETS 300 347-1 da ETSI e G.965 da ITU-T. Permite a concentração de 16 sistemas de 2048 kbps (E1's) em uma mesma interface, concentrando vários assinantes em uma mesma portadora, e permite o fornecimento de serviços do tipo PSTN e RDSI-PRI. Pela Interface V5.2 trafegam as informações de voz ou dados (*payload*), sinalização de assinantes, controle de portas, controle da interface, alocação dinâmica de canais de voz/dados, controle dos enlaces, e proteção dos canais de controle.

Engloba as três primeiras camadas do modelo OSI (camada física, enlace de dados e rede).

A camada física utiliza as recomendações do feixe E1. A camada de enlace de dados tem suas funções desempenhadas pelo protocolo LAPV5 e a camada de rede consiste em um grupo de protocolos (sinalização, controle de portas, controle comum, controle BCC, controle de enlaces, controle de proteção) (GONZAGA, 2004).

2.5.3 ATM

Asynchronous Transfer Mode surgiu em 1990 e foi desenvolvido como um protocolo de comunicação de alta velocidade que objetiva integrar funções de LAN's, MAN's e WAN's. Implementa um protocolo ponto-a-ponto, *full-duplex*, orientada a conexão e comutado por pacotes de tamanho fixo que são denominados de célula, dedicando largura de banda para cada estação de rede, e utilizando-se da multiplexação por divisão de tempo assíncrona para o envio de informações, atendendo assim todos os tipos de aplicações de voz, dados e vídeos. Opera sob largura de banda de 25 a 622 Mbps, sendo a de 155 Mbps a mais comumente utilizada. Estas velocidades são possíveis porque o ATM foi desenhado para ser implementado por hardware em vez de software (CEREDA, 1997).

Na Figura 5 está representado o modelo de camadas ATM. A camada física é responsável pelos meios de transmissão da célula ATM e é subdividida em subcamada de meio físico (PM) e subcamada de convergência de transmissão (TC). PM é responsável pela especificação das características físicas e também por sincronizar os bits do quadro de acordo com o relógio de transmissão/recepção. TC é responsável por mapear as células ATM no formato dos quadros da rede de transmissão. A Camada ATM é responsável por um grande número de funções, porém sua função principal é direcionar as informações recebidas a seu destino. A camada de adaptação ao ATM (AAL) é responsável pela adaptação do fluxo de informações das camadas superiores à camada ATM e no sentido contrário, funcionando como uma camada de ligação, suportando múltiplos protocolos. Apresenta duas subcamadas uma de convergência (CS) que determina os serviços e funções necessárias para a conversão entre protocolos ATM e não ATM e também controla as conexões virtuais, e subcamada de segmentação e recomposição (SAR), responsável por fragmentar a informação para ser encapsulada na célula ATM. Este modelo é uma simplificação do modelo representado pelo ITU-T, normalmente utilizado para estudos. O modelo ITU-T é baseado em um modelo tridimensional que conta com camadas de plano de gerência, controle e de usuário e também gerencia de planos e gerência de camadas (CEREDA, 1997).

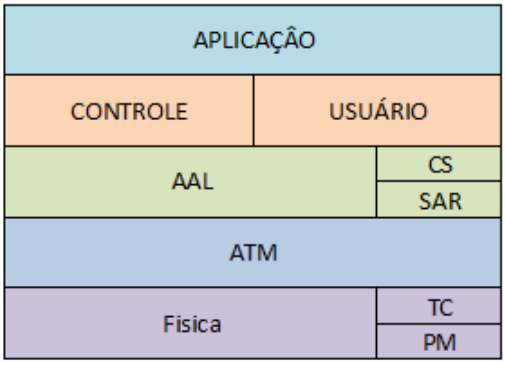


Figura 5 - Modelo de Camadas ATM
Fonte: Adaptado de Cereda (1997, p. 26)

A interligação entre os dispositivos segue dois tipos de interconexão sendo eles a UNI (Interface Usuário-Rede), que é a conexão de entre equipamentos de usuário ou de acesso a equipamentos de rede, e a NNI (Interface Rede-Rede) responsável pela conexão entre equipamentos de rede. Ambas estabelecem regras para viabilizar a interconexão e a interoperação dos sistemas em rede. Os dois formatos possíveis da célula ATM estão representado na figura 6, ambas apresentam o mesmo tamanho, diferenciando-se apenas pelo seu cabeçalho (B. FILHO, 2003).

A Figura 6 apresenta o cabeçalho UNI e NNI:

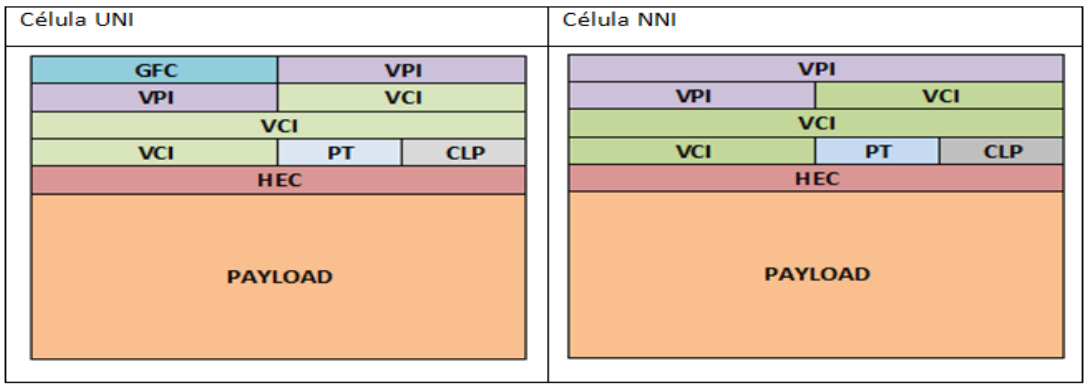


Figura 6 - Formato dos cabeçalhos das células ATM
Fonte: Cereda (1997, p.32)

O cabeçalho é composto por 5 bytes e o *payload* tem o tamanho de 48 bytes. No total a célula tem 53 bytes. VPI (*Virtual Path Identifier*) tem 8 bits em UNI e 12 bits em NNI, e sua função é identificar a conexão, representando a parte mais significativa. O campo VCI (*Virtual Chanel Identifier*) tem 16 bits tanto em UNI quanto em NNI e é a parte menos significativa na identificação da conexão. VCI e VPI são os campos necessários para que os comutadores possam efetuar a comutação das

células. O campo PT (*Payload Type)* identifica o tipo de informação contida na célula. Seu tamanho é de 3 bits. CLP (*Cell Loss Priority*) com um tamanho de 1 bit, indica a prioridade para o descarte de células pelos comutadores. O *Header Error Check* (HEC) composto por 8 bits que permite à camada física a verificação da integridade do cabeçalho, garantindo a correção de simples erros e detecção de múltiplos erros de cabeçalho, auxilia também no delineamento das células. O campo GFC (*Generic Flow Control*) aparece somente no cabeçalho das células UNI. É composto por 4 bits, é utilizado no controle de fluxo, marcar a célula como ociosa, informação de manutenção e operação da camada física(B.FILHO, 2003).

Por ser um protocolo orientado a conexão, é necessário que um circuito virtual seja estabelecido entre os equipamentos envolvidos para permitir que a rede reserve os recursos necessários para a comunicação. Três conceitos (TP, VP e VC) são utilizados para gerar estas conexões. *Transmission Path* (TP) é o caminho de transmissão física entre dois equipamentos de rede, *virtual path* (VP) é o caminho virtual criado entre os equipamentos e agrupa todos os canais virtuais que tem a mesma origem ou destino. *Virtual channel* (VC) é o canal virtual configurado entre os equipamentos em conexão. A partir destes três conceitos definem-se a conexão de canal virtual (VCC), e conexão de caminho virtual (VPC). VCC é uma concatenação de VC's, e é um circuito virtual onde o encaminhamento das células é baseado no valor dos campos VPI e VCI de cada célula. VPC é uma concatenação VP's, e também é um circuito virtual, porém o encaminhamento das células é baseado apenas nos campos VPI de cada célula (CEREDA, 1997).

A tecnologia ATM provê suporte à qualidade de serviço (QoS) habilitando-a atender qualquer tipo de tráfego sobre uma mesma rede. Cada conexão pode ter seus próprios pré-requisitos de QoS. Classes de serviços de acordo com a qualidade esperada, mecanismos de sinalização e controle de trafego e congestionamentos também são regulamentados nesta tecnologia (CEREDA, 1997).

2.5.4 PDH e SDH

2.5.4.1 PDH (Hierarquia Digital Plesiócrona)

A Hierarquia Digital Plesiócrona (PDH) surgiu tendo como origem os primeiros métodos de digitalização na transmissão de sinais, com a composição de diversas técnicas, os sistemas de transmissão PDH são oriundos da multiplexação de vários canais PCM30, formando sinais com taxas maiores que 2 Mbps (SOARES NETO, 2000)

Na técnica PCM a informação é transmitida por meio de um código binário, que representa um valor discreto aproximado para cada amostra do sinal que contém a informação. Esta técnica é o agrupamento de técnicas de amostragem de sinal analógico, quantização de amostras, para canais de voz analógicos e codificação para gerar um sinal digital que represente estas amostras quantizadas e logo após ocorre a multiplexação por divisão de tempo (TDM) das amostras do sinal de um canal, ou de suas representações digitais, e assim forma-se a configuração multicanal, composta de 30 destes canais, cada canal com 64kbps, dando origem então ao feixe E1 de 2048kbps.

A partir da montagem do feixe E1, que é o sinal básico do sistema PDH, foram surgindo os demais níveis da hierarquia, sempre padronizados, conforme Tabela 1 a seguir:

Tabela 1- Nível da Hierarquia SDH / PDH

Nível da Hierarquia	Taxa de Bits (Kbps)
E1	2.048
E2	8.448
E3	34.368
E4	139.264

Fonte: Autoria própria

A hierarquia vai aumentando agrupando-se quatro feixes do nível anterior mais os bits de ajuste, sincronismo e canais de controle. O feixe E3 é o mais

comumente utilizado, e permite um tráfego de até 480 canais de voz/dados (SOARES NETO, 2000)

Há hierarquias americana, europeia e japonesa, que em comum apresentam apenas os canais de 64 Kbps. No Brasil, assim como na Europa, padronizou-se que um quadro PCM completo teria 32 intervalos de tempo multiplexados, sendo 30 para transmissão de voz, que são os intervalos de 1 à 15 e 17 à 31, e dois intervalos de tempo especiais, que são o 16, utilizado para transferir dados, pois o equipamento e o próprio sistema de transmissão trabalham com sinalização por canal comum, e o intervalo de tempo 0, que se caracteriza por apresentar alternadamente os sinais de alinhamento de quadro, responsáveis pelo sincronismo do quadro PCM entre o equipamento transmissor e o receptor (TRONCO, 2011).

Quanto ao sincronismo, para os sistemas multiplex digitais de alta ordem é utilizado usualmente o processo de justificação positiva que consiste em se fazer a inserção de informações redundantes em intervalos de tempo reservados para tal, nos quatro sinais tributários de entrada. Para o sistema multiplex de segunda ordem é utilizado um sistema de memória elástica que armazena os sinais de cada tributário de entrada. Ainda temos, quanto à polaridade do sinal binário, a chamada codificação HDB3, que basicamente coloca os valores de bit “1” como um sinal bipolar que se alterna, ou seja, para dois bits “1” seguidos, teríamos um valor positivo e um negativo. Então, quando de uma sequência de zeros um sinal de violação é inserido, que serve para que não ocorra perda de sincronismo.

2.5.4.2 SDH (Hierarquia Digital Síncrona)

A Hierarquia Digital Síncrona (SDH) é um protocolo de comunicação baseado em níveis hierárquicos e projetado para enlace de dados digitais de alta velocidade, tornando a rede mais flexível e econômica. Surgiu da necessidade de se estabelecer um padrão internacional unificado para redes de telecomunicações síncronas, diferentemente do sistema PDH. O conteúdo do sinal transportado pelo sistema é indiferente, podendo ser transmitido voz, dados, entre outros. É capaz de transportar

todos os sinais tributários encontrados nas redes de telecomunicações atuais (SOARES NETO, 2000)

A padronização dos aspectos dos equipamentos SDH fornece a flexibilidade necessária aos operadores de rede para um gerenciamento centralizado e eficiente para o crescimento na largura banda e o provisionamento de novos serviços, e também faz com que os equipamentos oferecidos por diferentes fabricantes possam ser interconectados diretamente. O sistema SDH segue as seguintes normas da ITU-T apresentadas na Tabela 2:

Tabela 2 - Normas da ITU-T

NORMAS	DESCRIÇÃO
G.707	Estrutura de multiplexação, formação do quadro, ponteiros, cabeçalho, etc.
G.783	Tipos de equipamentos SDH e suas estruturas
G.784 G.774 G.773	Gerência de recursos de rede
G.803	Tipos de configurações de rede
G.813	Sincronismo
G841-2	Proteção da rede em anéis
G.957-8	Descrição da camada física

Fonte: ITU-T Recommendation

Módulo de Transporte Síncrono (STM)

O Módulo de Transporte Síncrono (STM) é a estrutura básica de transporte de dados da SDH, constituída de frames no qual os dados são armazenados. O STM-1 é o elemento constitutivo básico e a partir deste, quatro taxas de bit mais altas também são padronizadas: 622,080 Mbps (STM-4), 2.488,320 Mbps (STM-16) e 9.953,280 Mbps (STM-64) e 39.813,120 Mbps (STM-256), estes obtidos através da multiplexação por intercalação de bytes (SOARES NETO, 2000).

Um quadro STM-1 consiste em 2430 bytes arranjados em uma estrutura de 270 colunas por 9 linhas. As primeiras 9 colunas desta estrutura constituem o cabeçalho de seção (SOH) e os ponteiros, enquanto as outras 261 colunas são a Área de Carga Útil (*Payload*). Os bytes são transmitidos de forma serial, linha por linha, da esquerda para a direita e o bit mais significativo de cada byte é transmitido

primeiro. Apresenta taxa de transmissão de 155.520 Mbps e o tempo de duração de cada quadro é de 125µs (TRONCO, 2011).

A Figura 7 representa a estrutura do quadro STM:

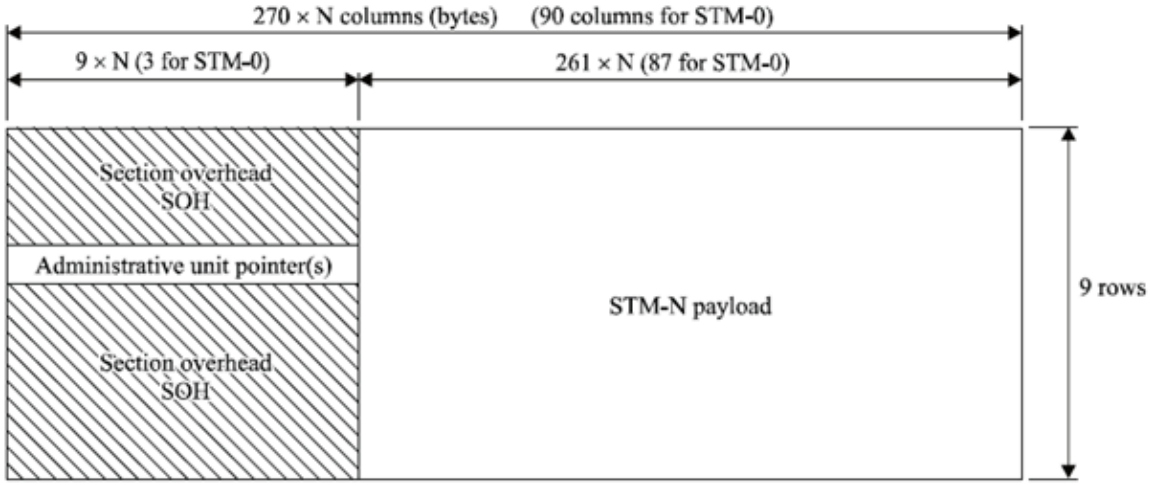


Figura 7 - Estrutura do quadro STM
Fonte: ITU-T G.707/Y.1322(2007, p.11)

O cabeçalho de Seção (SOH) carrega informações para alinhamento de quadro, manutenção, cálculo de desempenho e executa uma variedade de facilidades de gerência e administração e é composto por:

- Cabeçalho de seção de regeneração (RSOH) – carrega informações que podem ser utilizadas em um regenerador ou repetidor. Transporta informações de supervisão, alarme, manutenção e gerencia, e também possibilita ao transporte de um canal de serviço. É composto por 27 bytes em cada quadro STM-1, sendo os seis primeiros bytes utilizados para alinhamento e identificação de quadro.

- Cabeçalho de seção de multiplexação (MSOH) - carrega informações utilizadas somente na seção de multiplex, onde o STM-1 é desmontado. Transporta informações de supervisão, alarme, manutenção, gerencia e comutação para caminho reserva, e também possibilita ao transporte de um canal de serviço. É composto por 35 bytes em cada quadro STM-1.

O ponteiro de unidade administrativa (AU-*Pointer*) indica o inicio da carga útil dentro do quadro e é formado pelos primeiros nove bytes da quarta linha, e estão associados ao MSOH.

A área de carga útil (*Payload*) é onde a informação será transportada.

Funcionamento

Segundo Soares Neto (2000), o funcionamento da SDH está baseado nos princípios da multiplexação síncrona direta, multiplexando vários canais das hierarquias PCM ou PDH, formando sinais com taxas superiores a 155 Mbps. Os tributários plesincronos são mapeados em um container síncrono padrão, que é o elemento básico do STM-1, e bytes para supervisão, chamados de *Path Overhead* (POH), são adicionados à área de carga útil para formar um container virtual (VC), este podendo ser de ordem superior ou inferior, que controla o caminho percorrido. A cada container virtual também são adicionados ponteiros para indicar seu inicio dentro do quadro, formando assim as unidades tributárias (TUs) que fazem a adaptação do VC na camada de via. A multiplexação de várias unidades tributárias dá origem aos chamados grupos de unidade tributária (TUG), e estes TUGs inseridos em containers virtuais de ordem superior, e adicionando-se ponteiros, formam a unidade administrativa (AU), responsável por indicar o local de inicio do container virtual e também realizar a justificação por bytes quando necessário. Logo um agrupamento de unidades administrativas, denominado AUG (grupo de unidade administrativa), gera um sinal STM. A formação de um sinal STM-n segue a estrutura de multiplexação conforme Figura 8.

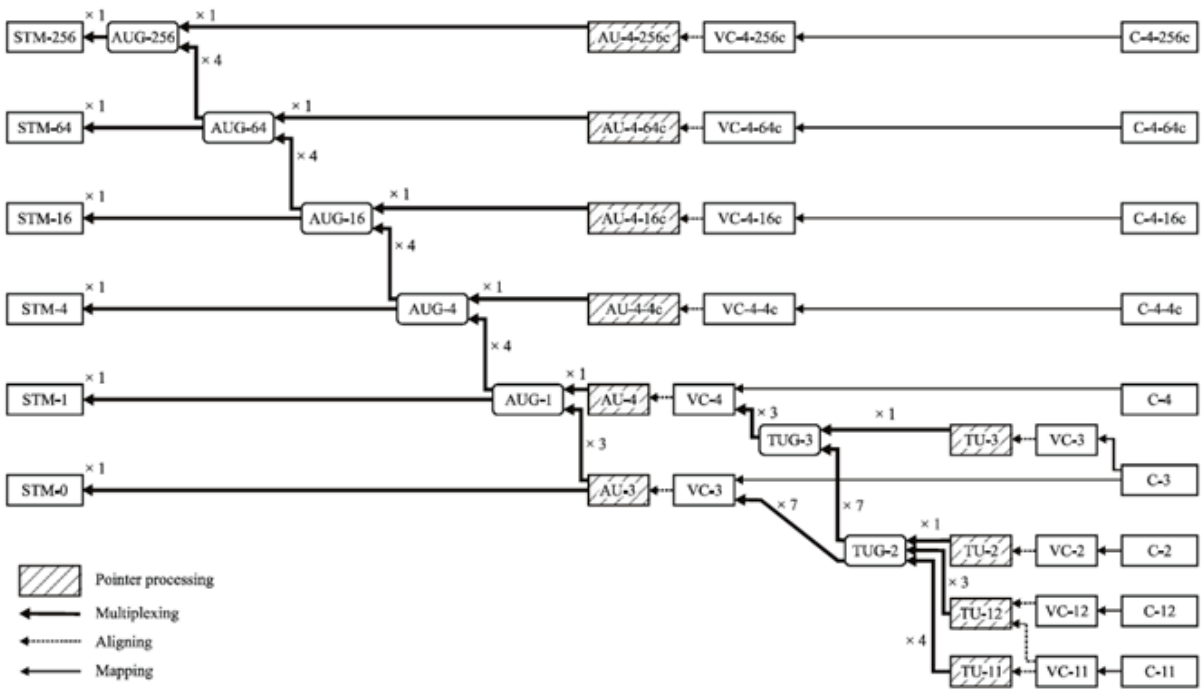


Figura 8 – Estrutura de multiplexação para obtenção de STM-n
Fonte: ITU-T G.707/Y.1322 (2007, p.8)

Sinais tributários individuais podem ser multiplexados diretamente em um sinal SDH de taxa superior, sem a necessidade de estágios de multiplexação intermediários. Portanto, os Elementos de Rede da SDH podem ser interconectados diretamente, resultando em uma economia no custo e nos equipamentos utilizados, principalmente quando comparado com a rede quase síncrona (PDH). Além disso, podem ser utilizados em redes de longa distância, rede local e intracentral, tornando possível uma infraestrutura de rede de telecomunicações unificada. Com a rede de SDH, todas as alocações de banda e o roteamento da transmissão podem ser controlados a partir de um ponto central, simplificando o re-roteamento e reaproveitamento dos circuitos (SOARES NETO, 2000).

2.5.5 CWDM e DWDM

2.5.5.1 DWDM (*Dense Wavelength Division Multiplexing*)

DWDM (*Dense Wavelength Division Multiplexing* ou WDM densa) é uma tecnologia WDM com espaçamento que varia de 12,5 GHz a 200 GHz. Sua padronização segue a Recomendação G.694.1 (*Spectral grids for WDM applications: DWDM frequency grid*) da ITU-T (FERNANDES, 2003).

A quantidade de canais pode variar de 16 a 128, entre os comprimentos de onda de 1500 nm e 1600 nm, apresentam alta capacidade de transmissão por canal, podendo sua taxa de transmissão variar de STM-1 (155 Mbits/s) a STM-64 (10 Gbits/s), alcançando até 1Tbps na transmissão de dado. Utiliza fibra monomodo e é aplicado principalmente em ligações ponto-a-ponto, onde é possível que cada sinal transmitido esteja em taxas ou formatos diferentes, ampliando a capacidade de transmissão do sistema, pois multiplexando vários comprimentos de onda utiliza melhor a banda disponível da fibra.

Atualmente as bandas de frequência ópticas mais utilizadas em sistemas DWDM são:

- S - Band (*Short Band*) - vai de 1450 nm a 1500 nm.

- C - Band (*Conventional Band*) - vai de 1530 nm a 1570 nm;
- L - Band (*Long Band*) - está na faixa de 1570 nm a 1625 nm;

2.5.5.2 CWDM *(Coarse Wavelength Division Multiplexing)*

O CWDM (*Coarse Wave Division Multiplex* ou WDM Amplo) é uma tecnologia WDM de baixa densidade e seu princípio de funcionamento é o mesmo do WDM. Sua padronização segue a Recomendação G.694.2 (*Spectral Grids for WDM Applications e CWDM Wavelength Grid*) do ITU-T (FERNANDES, 2003).

A informação é agrupada de 4 a 16 canais, dependendo da fibra óptica adotada no projeto, entre os comprimentos de onda de 1271 nm a 1611 nm, e a distância entre os canais é de 20 nm. Sua taxa de transmissão pode variar de E3 (34 Mbit/s) a STM-16 (2,5 Gbit/s), cobrindo distâncias de até 80 km. Possui tolerância de seleção de comprimento de onda e elevada qualidade de serviço. Utiliza lasers sem refrigeração como transmissores e é desnecessária a presença de amplificadores ópticos. Isso faz com que seja preferível o uso do CWDM em redes metropolitanas, devido a seu custo acessível.

Outra característica dos sistemas CWDM é que estes possuem flexibilidade suficiente para serem empregados em conexões ponto-a-ponto. Também suportam tráfego Ethernet e interconexão de SANs (*Storage Area Networks*).

Atualmente as bandas de frequência ópticas mais utilizadas em sistemas CWDM são:

- O - Band (*Original Band*) - vai de 1260 nm a 1360 nm;
- E - Band (*Extended Band*) - está na faixa de 1360 nm a 1460 nm;
- C - Band (*Conventional Band*) - vai de 1530 nm a 1570 nm.

2.5.6 Arquitetura OSI

Para padronizar o desenvolvimento de produtos para redes de dados foi elaborado um modelo aberto, de arquitetura modular, para satisfazer requerimento de clientes para a capacidade de comunicação remota, este teve como modelo o *OSI (Open System Interconection)* desenvolvido pelo ISO *(International Organization for Standadization)* no início da década de 1980 (ROCHA, 2011).

Com este modelo fabricantes podem desenvolver hardware e software capaz de se comunicar com sistemas de outros desenvolvedores. Um sistema aberto serve de base para redes de curta, média ou longa distância (TRONCO, 2011).

Até o início dos anos 1990, a indicativa era de que o modelo OSI seria padrão de fato para comunicação de dados, mas isso acabou não acontecendo e o modelo OSI nunca foi utilizado em alguma aplicação e deve ser tratado como modelo de referência (FOROUZAN, 2004).

2.5.6.1 Camada Física

Neste nível os protocolos fazem a codificação/decodificação dos símbolos e caracteres em sinais elétricos enviados ao meio físico. A função desta camada é garantir que um bit transmitido como “1” seja entendido pelo receptor como bit “1” e não como “0”. Com isso o meio físico transmite a sequência de bit através do canal de comunicação (PINHEIRO, 2005).

2.5.6.2 Camada de Enlace de Dados

A sequência de bits recebida ou transmitida do meio físico, na camada de Enlace de Dados, é transformada em uma linha livre de erros de transmissão, para que essa informação seja utilizada no nível de rede. A camada enlace é dividida em

dois sub níveis, o superior faz o controle lógico do enlace e o inferior faz o controle de acesso ao meio (PINHEIRO, 20005).

2.5.6.3 Camada de Rede

O controle da operação da rede de um modo geral é feito pela camada de rede. As principais funções são o roteamento dos pacotes entre fonte e destino, o controle de congestionamento e contabilização do número de pacotes ou bytes utilizados pelo usuário, com a finalidade de tarifação. Nesta camada é executado o roteamento dos pacotes entre fonte e destino, principalmente quando há diferentes caminhos para conectar entre si dois nós da rede (PINHEIRO, 2005).

2.5.6.4 Camada de Transporte

Na camada de Transporte é o primeiro nível que faz a conexão fim a fim, isto é, um programa que está em um equipamento conversa diretamente com o programa similar do equipamento destino sem necessidade de conversar com o nó vizinho. Nesta camada é segmentado os dados no tamanho adequado para encaminhar para o nível de rede (PINHEIRO, 2005)

A camada de transporte fornece:

- Mensagem de segmentação: aceita uma mensagem da camada de (sessão) acima dela, divide a mensagem em unidades menores (se não já pequena o suficiente) e passa as unidades menores para a rede camada. A camada de transporte na estação de destino remonta a mensagem.
- Mensagem de confirmação: fornece confiável de mensagens de ponta a ponta entrega com confirmações.
- Mensagem de controle de tráfego: informa a estação de transmissão "*back-off*" quando nenhum buffer de mensagem está disponível.

- Sessão multiplex: multiplexa vários fluxos de mensagens, ou sessões em um único link lógico e mantém controle sobre que mensagens pertencem (MICROSOFT, 2013).

2.5.6.5 Camada de Sessão

Na camada sessão os diálogos entre processos de aplicação são sincronizados. Nesta é fornecido mecanismos de estruturação dos circuitos de aplicação. Neste nível ocorre a quebra de um pacote com o posicionamento de uma marca lógica ao longo do diálogo. Uma sessão pode ser aberta entre duas estações para permitir a um usuário se conectar em um sistema remoto ou transferir um arquivo entre essas estações. Os protocolos desse nível tratam de sincronizações na transferência de arquivos (PINHEIRO, 2005).

2.5.6.6 Camada de Apresentação

Para assegurar que a informação seja transmitida de forma que seja entendida pelo receptor é utilizada a camada de apresentação, nela são convertidos os dados recebidos da Aplicação em formato a ser encaminhado na transmissão do dado. Por exemplo, uma aplicação pode gerar uma mensagem em ASCII mesmo que a estação interlocutora utilize outra forma de codificação (como EBCDIC). A camada de apresentação também é responsável por outros aspectos da representação dos dados, como criptografia e compressão de dados (PINHEIRO, 2005).

2.5.6.7 Camada de Aplicação

É a camada que fornece ao usuário uma interface que permite acesso a diversos serviços de aplicação, convertendo as diferenças entre diferentes fabricantes para um denominador comum. Por exemplo, em uma transferência de arquivos entre máquinas de diferentes fabricantes pode haver convenções de nomes diferentes, formas diferentes de representar as linhas, e assim por diante (PINHEIRO, 2005).

2.5.7 TCP/IP

Desenvolvido no inicio dos anos 1970 pelo DARPA (*Defense Advanced Resarch Projects Agency*) o TCP/IP (*Transmission Control Protocol/ Internet Protocol*), também conhecido como *Internet Protocol Suite*, é um conjunto de protocolos constituído de cinco camadas: física, enlace de dados, rede, transporte e aplicação (BRANDINO, 1998).

O protocolo TCP/IP é constituído de módulos interativos, cada módulo tem uma função diferente, mas não são necessariamente interdependentes. O TCP/IP possui protocolos relativamente independentes que podem ser misturados e combinados de acordo com as necessidades do sistema, enquanto que o modelo OSI especifica quais funções pertencem a cada uma de suas camadas (FOROUZAN; FEGAN, 2008).

Como o TCP/IP é um sistema aberto não existe um órgão regulador responsável por ele. Porém organismos como o IAB (*Internet Activites Board*) possuem grupos de trabalho que realizam pesquisas na área. Qualquer pessoa pode sugerir um novo padrão ou alteração do protocolo através de uma RFC (*Request for Comments*), especificações que detalham o conjunto de padrões para comunicação entre computadores, como convenções de interconexão, roteamento, tráfego e etc. (BRANDINO, 1998).

2.5.7.1 Camada Aplicação

Diferente do modelo OSI cada aplicativo tem um padrão de estrutura no modelo TCP/IP, nesta camada são definidos os protocolos de aplicativos TCP/IP e como os programas host estabelecem uma interface com os serviços de camada de transporte para usar a rede. Os principais protocolos que operam na camada aplicação são HTTP, SMTP, FTP, SNMP, SSH, DNS e o Telnet (MICROSOFT, 2013).

2.5.7.2 Camada Transporte

Realiza o gerenciamento de sessão de comunicação entre computadores host. Define o status da conexão e nível de serviço usado durante o transporte de dados. Principais protocolos TCP, UDP e RTP (MICROSOFT, 2013).

2.5.7.3 Camada Internet

Empacota dados em datagramas IP, que contêm informações de endereço de origem e de destino usadas para encaminhar datagramas entre hosts e redes. Executa o roteamento de datagramas IP. Protocolos IP, ICMP, ARP e RARP (MICROSOFT, 2013).

2.5.7.4 Camada Interface de Rede

Especifica os detalhes de como os dados são enviados fisicamente pela rede, inclusive como os bits são assinalados eletricamente por dispositivos de hardware que estabelecem interface com um meio da rede, como cabo coaxial, fibra óptica ou

fio de cobre de par trançado. Protocolos Ethernet, *Token Ring*, FDDI, X.25, Retransmissão de Quadros, RS-232 e v.35 (MICROSOFT, 2013).

A Figura 9 compara as principais características dos modelos OSI e TCP/IP:

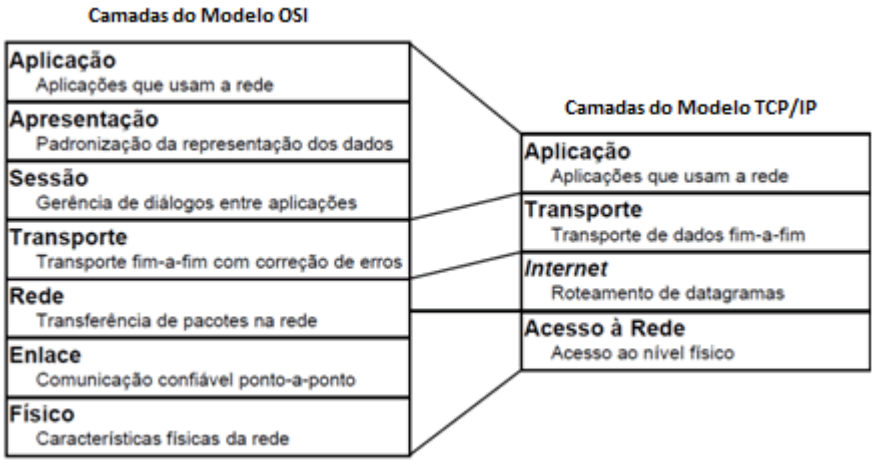


Figura 9 - Comparativo entre camada OSI e TCP/IP
Fonte: Adaptado de Porto da Silva (2009, p. 3).

2.5.8 MetroEthernet

Segundo Carissimi at al (2009), a tecnologia Ethernet, baseada no padrão IEEE 802.3, utiliza o meio compartilhado para um meio comum, inicialmente com 10 Mbps, é baseada em topologia física do tipo HUB e lógica do tipo barramento. Para segmentos que necessitam de maior capacidade foi desenvolvida a *Fast Ethernet* (100 Mbps), *Gigabit ethernet* (Gbps) e a 10 *giga bit Ethernet* (10 Gbe). Pode trafegar por SDH, MPLS (*Multiprotocol Label Switching*) e DWDM. Para redes metropolitanas (MAN) e longa distância (WAN) foi desenvolvido a rede Metro Ethernet.

Basicamente uma rede Metro Ethernet é uma rede Ethernet que interconecta dois ou mais computadores geograficamente instalados dentro de uma MAN. Pode ser utilizados por empresas para conectar escritórios e datacenters. As especificações do Metro Ethernet seguem os padrões do MEF (*Metro Ethernet Forum*), organização sem fins lucrativos, formada em 2001, para prover Redes de Serviço Ethernet, focada nas operadoras.

As principais vantagens do Metro Ethernet são custo menor da interface Ethernet em relação a interfaces SDH, suporta largura de banda superior a 10 Gbps e pode ser

facilmente conectado a rede do cliente devido ao uso de Ethernet nas corporações e residências (BEZERRA, 2013).

2.5.9 MPLS

O *Multiprotocol Label Switching* (MPLS) é uma tecnologia de encaminhamento de pacotes que funciona basicamente com a adição de um rótulo nos pacotes a serem encaminhados (TANENBAUM, 2003).

É uma tecnologia utilizada em infraestrutura de rede e tem o objetivo de solucionar os problemas das redes de computadores como velocidade, escalabilidade, gerenciamento de qualidade de serviço (QoS), a necessidade de engenharia de tráfego e ajuda na formação de VPN baseadas em IP. O MPLS é padronizado pelo IETF - *Internet Engineering Task Force* através da RFC-3031 e opera entre a camada 2 e 3 do modelo OSI, sendo assim considerada uma camada intermediaria (OLIVEIRA; LINS; MENDONÇA, 2012).

Tem como ideia base combinar técnicas simples e robustas de encaminhamento na camada de rede, e técnicas de comutação rápida, eficientes e escaláveis na camada de ligação de dados. Em MPLS as funções de Controle e de Transporte de dados são separadas. As funções de controle são realizadas em software, e baseiam-se em protocolos de encaminhamento convencionais e em protocolos de sinalização adequados aos requisitos da arquitetura. Já as funções de transporte são realizadas em hardware, e baseiam-se em técnicas de comutação de etiquetas (ROCHA, 2011).

2.5.9.1 Componentes MPLS

Segundo Tude e B. Filho (2013) os principais componentes de um MPLS são:

- *Label*

Label (rótulo) é um identificador de comprimento curto e definido que é usado para identificar uma FEC, tendo geralmente significado local. É composto de 32 bits e possui quatro campos conforme a Figura 10.

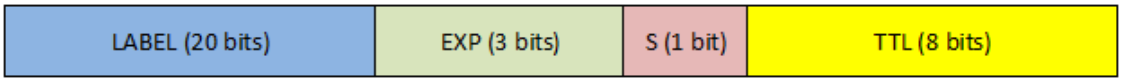


Figura 90 - Estrutura do Label MPLS
Fonte: Adaptado de Tanenbaum (2003, P.443).

- *Label* é responsável por fornecer o valor do *label* MPLS.
- EXP define a classe de serviço a que um pacote pertente.
- S (*stack*) utilizado para enfileiramento caso o pacote receba mais de um *label*.

O empilhamento de labels é utilizado para criar túneis MPLS, para que os *labels* de uma operadora não entrem em conflito com os *labels* utilizados por clientes privados.

- TTL (*Time to Live*) tem a função de contar por quantos roteadores o pacote passou. Caso o pacote ultrapasse 255 roteadores TTL é descartado para evitar loop.

- *Foward Equivalence Class (FEC)*

A *Foward Equivalence Class* (FEC) é a representação de um grupo de pacotes que tem os mesmo requisitos para o seu transporte. Para todos os pacotes neste grupo é fornecido o mesmo tratamento na rota até o seu destino.

- *Label Edge Router (LER)*

São roteadores de borda (entrada e saída) responsáveis por inserir ou remover o cabeçalho MPLS, atribuir o pacote a uma classe (FEC) e também pelo encaminhamento e controle do pacote.

- *Label Switching Router (LSR)*

O LSR é um nó do MPLS. Ele recebe o pacote de dados, extrai o *label* do pacote e o utiliza para descobrir na tabela de encaminhamento qual a porta de saída e o novo rótulo a ser atribuído ao pacote.

- *Label Distribution Protocol (LDP)*

É um conjunto de procedimentos pelo qual um LSR informa outro das associações entre *Label*/FEC que ele fez.

- *Label Switching Path (LSP)*

No MPLS a transmissão de dados ocorre em caminhos chaveados a rótulo (LSPs). LSPs são uma sequência de rótulos em cada e todos os nós ao longo do caminho da origem ao destino. LSPs são estabelecidos antes à transmissão dos dados ou com a detecção de um certo fluxo de dados.

- *Label Switching Forward Tables (LSFT) ou LIB (Label Information Base).*

Tabelas de encaminhamento dos comutadores de rótulo. Estas tabelas são responsáveis pelo processo de encaminhamento de pacotes e são mantidas pelos LSRs.

- *Componente de Controle*

Responsável por distribuir informações de roteamento entre os LSRs que compõe um domínio MPLS e também pelos algoritmos utilizados por estes roteadores para converter estas informações em tabelas de encaminhamento, mantendo a LIB sempre atualizada.

- *Componente de Encaminhamento*

Responsável pelo encaminhamento dos pacotes utilizando um algoritmo de troca de rótulos, também cria e mantém a tabela LIB.

2.5.9.2 Funcionamento

Um rótulo, utilizado para representar uma FEC, é associado a cada caminho (LSP); Em cada ponto de entrada da rede, um roteador de entrada (ILER) examina o pacote para determinar o LSP e adiciona um header MPLS antes do Pacote; A cada LSR pelo qual o pacote passa, os rótulos são trocados, pois cada rótulo representa um índice na tabela de encaminhamento do próximo roteador. Sendo assim, quando um pacote rotulado chega, o roteador procura em sua LIB pelo índice representado pelo rótulo. Ao encontrar este índice o roteador substitui o rótulo de entrada por um rótulo de saída a que pertence o pacote. Depois de completada a operação (OLIVEIRA; LINS; MENDONÇA, 2012).

2.5.10 xDSL

Segundo Carissimi at al (2009), o gasto na implantação de um terminal telefônico novo está associado com a instalação física que vai da casa do cliente ao DSLAM (*Digital Subscriber Line Access Multiplexer*) ou a Central Telefônica mais

próxima. Esse investimento feito pelas operadoras ao longo dos anos gerou a necessidade de lançar novos serviços agregados à concessão de serviços de telecomunicação.

O DSL é comumente escrito com um x inicial (por exemplo, xDSL) para coletivamente representar a família das tecnologias. A tecnologia de xDSL, enquadrado no Serviço de Comunicação Multimídia (SCM), é um dos tipos mais importantes da nova tecnologia para fornecimento de serviços digitais. Atualmente, a solução ocupa a liderança no acesso em banda larga, fato que se deve à rápida disponibilização de serviços à alta capilaridade do sistema telefônico (BOLZANI, 2004).

Vantagens da DSL:

- Pode-se manter sua conexão à Internet aberta e ainda usar a linha telefônica para chamadas de voz;
- A velocidade é muito maior do que a de um modem comum de linha discada, até 56kbits/s;
- A conexão DSL não requer necessariamente uma fiação nova: ela pode usar a linha telefônica já existente;
- As companhias que oferecem o serviço DSL atualmente estão fornecendo o modem juntamente com a instalação.

Desvantagens da DSL:

- Quanto mais distante da estação de operação do provedor, pior é a conexão DSL;
- As taxas de *downstream* são melhores que *upstream* tendo em vista o lado do cliente;
- O serviço não está disponível em qualquer lugar, necessidade de ponto fixo é uma desvantagem se comparado com outros serviços móveis.

As tecnologias de xDSL mais utilizadas são a *Asymmetric Digital Subscriber Line* (ADSL), e *Very-high-bit-rate digital subscriber line* (VDSL).

2.5.10.1 ADSL

Durante anos a rede telefônica funcionou apenas para serviço de voz. A maior taxa de transferência era de 56 Kbps. Para trafegar dados na rede a solução foi aumentar a frequência de transmissão. Do ponto de vista do assinante, o ADSL fornece a habilidade de enviar e receber informações digitais em alta velocidade. Como é dito no nome, o serviço é assimétrico, assimetria na taxa de transferência. O downstream, termo que se refere ao fluido do tráfego para o usuário, é otimizado para o tráfego ser superior a taxa de upstream, que é o fluido a partir do usuário. A taxa de transmissão ADSL na direção do assinante é de até 8 Mbit/s, no sentido contrário até 640 kbit/s (COMER, 2007).

O ADSL é padronizado pelos órgãos *ANSI (American Nation Standards Institute)* e pelo *ITU(International Telecommunication Union).*

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.DMT)
- ITU G.992.2 (G.Lite)

No ADSL a faixa de frequência de transmissão nos pares de cobre é dividida em três canais:

- Serviço telefônico convencional de voz (0-4 kHz);
- Tráfego upstream, dados originados no cliente e transmitidos para a rede;
- Tráfego downstream, dados originados na rede e transmitidos para o cliente.

Na Figura 11 é demonstrado como é dividido os canais de frequência:

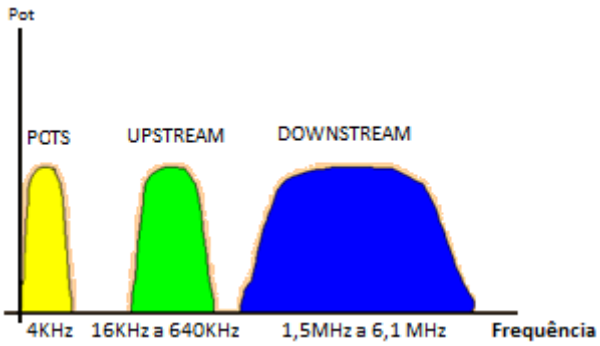


Figura 11 - Distribuição de frequências
Fonte: Adaptado de Gonçalves da Silva (2006, p. 1)

O limite para o ADSL é de 5460 metros, mas para proporcionar a velocidade de até 8 Mb/s na direção do cliente e 640 Kbps no sentido oposto.

2.5.10.2 ADSL2 e ADSL2+

A necessidade de maior taxa de transferência levou ao desenvolvimento do conjunto de padrões ADSL2 e ADSL2+, que permitem alcançar taxas de bits superiores a 10 Mbits/s (BERNAL FILHO, 2013).

ADSL2 e ADSL2+ também são padronizados pelo ITU:

- ITU G.992.3
- ITU G.992.4
- ITU G.992.5

O ADSL2 apresenta vantagens como detecção de falhas e medição de desempenho da conexão. Medição de ruído de linha, atenuação em ambas as extremidades do enlace. Outras vantagens ocorrem na parte operacional, pois o ADSL2 e ADSL2+ permite o monitoramento da conexão, conseguindo gerenciar a qualidade do serviço prestado (TEIXEIRA, 2013).

O ADSL2 também apresenta:

- Partida Rápida: permite que o tempo de inicialização de mais de 10 segundos do ADSL seja reduzido pra menos de 3 segundos;
- Transmissão de dados também na banda de Voz, adicionando 256 kbits/s na banda *upstream* (TEIXEIRA, 2013).

No caso do ADSL2+ a largura de banda de *downstream* é duplicada, possibilitando taxas de bits de até 20 Mbit/s em linhas telefônicas com distâncias de até 1,5 km entre a central e o usuário final. Outra vantagem do ADSL2+ é que este permite a operação conjunta na mesma infraestrutura, do ADSL e do ADSL2 (TEIXEIRA, 2013).

Comparando o ADSL2+ com o ADSL2, pode-se observar o novo padrão para a banda de *downstream* de 1,1 MHz (552 kHz para ADSL2 Lite) para 2,2 MHz. O resultado é um aumento significativo nas taxas de bits *downstream* em linhas telefônicas mais curtas. A taxa de bits *upstream* do ADSL2+ é aproximadamente 1 Mbit/s, dependendo das condições do enlace (TEIXEIRA, 2013).

2.5.10.3 VDSL e VDSL2

Os esforços para padronizar o VDSL começaram em 1995. Os órgãos internacionais de padronização ITU, ETSI e ANSI (T1E1.4) desenvolveram projetos simultâneos com essa finalidade. Em 1997, um grupo de operadoras que associadas ao *Full-Service Access Network* (FSAN) especificou o requisitos fim-a-fim para VDSL (BERNAL FILHO[1], 2013)

Padronização VDSL e VDSL2:

- ITU G.993.1
- ANSI T1E1.4
- ITU G.993.2

Assim como a transição do ADSL para o ADSL2 no VDSL foi utilizado o aumento do espectro para chegar ao VDSL2. O objetivo do VDSL2 é aumentar o desempenho em acessos mais longos comparado com o VDSL1. Para isso foi utilizado a faixa entre 25 kHz a 138 kHz (BERNAL FILHO[1], 2013).

As taxas de transmissão do VDSL1 são de 52 megabits por segundo (Mbps) de *downstream* e 16 megabits por segundo (Mbps) de *upstream* com distância máxima de 1200 metros, mas pode alcançar taxas de até 100 Mbps (BERNAL FILHO[1], 2013).

2.5.10.4 Modem ADSL

Conhecido também como “transceptor”, ele é o ponto em que a rede do usuário ou computador se conecta com a linha DSL. O modem pode operar como roteador, estabelecendo conexão lógica com o *BRAS (Broadband Remote Access Server)* ou como *Bridge* quando não é feito controle de rota, havendo apenas uma rota para os dados. (TYSON, 2013).

2.5.10.5 Divisores de Potência

São os divisores e filtros colocados na residência do usuário e na estação telefônica, permitem a separação do sinal de voz da chamada telefônica do tráfego de dados ADSL (BERNAL FILHO, 2013).

2.5.11 VOIP

Surgido em 1995 em Israel, a tecnologia de Voz sobre IP (VoIP) é uma aplicação de telefonia que permite a comunicação entre duas partes em uma rede de comutação de pacotes (Internet), convertendo o sinal de áudio analógico em dados digitais. As ligações VoIP podem ser realizadas ou recebidas através de um celular ou computador com *softphone* instalado, um telefone com adaptador ATA (Adaptador Telefônico Analógico), telefone IP ou um PABX com ramais (ZAPPAROLI, 2013).

O fornecimento de VoIP por uma operadora pode se enquadrar de duas formas distintas, como serviço de Valor Adicionado (art. 61, LGT) ou Serviço de Telecomunicações (art. 60, LGT). Como a ANATEL não regulamenta uso de tecnologias, somente serviço de telecomunicação, em caso de ligação entre computadores, não há caracterização de serviço de telecomunicação e sim Serviço de Valor Adicionado (SVA), desta forma não há regulamentação. Provedor que possui somente o servidor e não oferece link não necessita de licença. No caso de uma ligação entre VoIP e telefonia fixa ou móvel, a operadora VoIP a provedora de VoIP deve fornecer infraestrutura e capacidade de transmissão e recepção de informações, neste caso é um Serviço de Telecomunicação necessitando, assim, de regulamentação (ANATEL, 2013).

A vantagem do VoIP em relação a telefonia fixa convencional é que a rede não é hierárquica como a PSTN, não possui plano de numeração, é uma rede plana em que a distância geográfica não tem relevância (AMPERNET, 2013)

A telefonia VoIP pode oferecer várias conveniências agregadas, como mobilidade, o número funciona em qualquer lugar do mundo, flexibilidade, podendo

utilizar vários tipos de aparelhos para realizar as ligações, e a economia, pois ligações VoIP para VoIP não tem custo, e VoIP para telefone fixo ou celular as tarifas são inferiores a telefonia tradicional. Para o uso corporativo as principais vantagens são a redução de custos de ligações internas da empresa, interurbanas, internacionais, custo zero em ligações por meio VoIP e gerenciamento online de custeio e despesas (BARBARIOLE, 2013)

As principais desvantagens da telefonia VoIP são referentes a qualidade do serviço pois há perda de pacote em caso de congestionamento de rede, atraso de pacote gerando eco e sobreposição de sinal com a voz entrecortada e muitas vezes inteligível. Além disso, diferentemente da telefonia convencional o VoIP depende da energia elétrica para funcionar, e na maioria dos casos não disponibiliza ligação para números de emergência como 190 e 193 (BARBARIOLE, 2013).

2.5.11.1 H.323

A padronização do caminho do fluxo de dados de áudio e vídeo entre ligações VoIP é dada pelo protocolo H.323. O padrão H.323, criado pelo ITU especifica o uso de áudio, vídeo e dados em comunicações multimídia. Originalmente ele foi desenvolvido para vídeo conferências, ele ainda fornece compartilhamento de dados e aplicativos de voz como o VoIP. O H.323 incorpora um conjunto de protocolos desenvolvidos para uso específico (VALDES, 2013).

O padrão H.323 é completamente independente dos aspectos relacionados à rede. Dessa forma, podem ser utilizadas quaisquer tecnologias de enlace, também não há restrição quanto à topologia (SOUZA, 2013).

2.5.11.2 SIP

O Protocolo de Iniciação de Sessão (SIP) é um protocolo de aplicação, que utiliza o modelo “requisição-resposta”, similar ao HTTP, para iniciar sessões de comunicação interativa entre usuários. O SIP, que teve origem em meados da

década de 1990, é um protocolo menor e mais eficiente que o H.323. Padronizado pela *(Internet Engineering Task Force)* IETF. (RFC 3261, 2002) (VALDES, 2013).

O protocolo SIP estabelecer chamadas e conferências através de redes via Protocolo IP. O estabelecimento, mudança ou término da sessão é independente do tipo de mídia ou aplicação que será usada na chamada; uma chamada pode utilizar diferentes tipos de dados, incluindo áudio e vídeo. O SIP leva os controles da aplicação para o terminal, eliminando a necessidade de uma central de comutação (SOUZA, 2013).

2.5.11.3 MGCP

Proposto pelo grupo de trabalho IETF recomendação RFC 2705, o MGCP (*Media Gateway Control Protocol*) é utilizado para controlar as conexões (chamadas) nos *Gateway* presentes nos sistemas VoIP. O MGCP implementa uma interface de controle usando um conjunto de transações do tipo comando – resposta que criam, controlam e auditam as conexões (chamadas) nos Gateways. É baseado no paradigma Mestre/Escravo no qual o MGC (*Media Gateway Controller*), ou controlador de mídia, é o mestre e o MG (*Media Gateway*), escravo. Dessa forma, o MG manipula as funções de mídia, como conversão de sinais TDM, e o MGC gerencia as funções de sinalização de chamada (PETERS, 2008).

2.5.11.4 Megaco / H.248

O protocolo MeGaCo (*Media Gateway Control*) foi criado em um grupo de trabalho do IETF e do ITU-T. O texto da definição do protocolo é o mesmo para o *Draft* IETF (*Internet Engineering Task Force*) e a recomendação H.248, e representa uma alternativa ao MGCP e outros protocolos similares (OLIVEIRA, 2013).

É um protocolo complementar ao SIP e H.323, constituído por três elementos: *Media Gateway Controller* (MGC), *Media Gateway* (MG), e *Signalling Gateway* (SG). O H.248 foi desenvolvido para ser utilizado para controlar Gateways com um

equipamento ou distribuídos (vários equipamentos). Sua plataforma aplica-se a *gateway* (GW), controlador multiponto (MCU) e unidade interativa de resposta audível (IVR). Possui também interface de sinalização para diversos sistemas de telefonia, tanto fixa como móvel. O SG é um tipo de MG especializado em converter a sinalização SS7 para a rede IP (OLIVEIRA, 2013).

O MeGaCo/H.248 separa fisicamente o plano de controle, MGC (também conhecido como *Softswitch*), do plano de conexão. O MGC é responsável por trocar as sinalizações e mensagens com as outras redes e protocolos, converter as mensagens para os comandos do MeGaCo/H.248 e encaminhar na rede IP para os MGs, controla também a existência das entidades lógicas no MG (OLIVEIRA, 2013).

3 DESENVOLVIMENTO

3.1 CGR-NOC E ÁREAS RELACIONADAS

O NOC (*Network Operation Center*), também conhecido como CGR (Centro de Gerência de Rede), é o coração de toda empresa de telecomunicações, nele são concentrados todos os sistemas de gerência com objetivo de monitorar todas as plataformas de tecnologia.

De forma genérica o NOC pode ser comparado a um hospital, onde os analistas são os médicos e a rede é o paciente, se o paciente esta doente os médicos realizam um diagnostico para identificar qual a causa da doença, sendo constatada a causa é aplicado assim o tratamento adequado. Da mesma forma sempre que ocorre um problema na rede é realizada uma análise para identificar qual a causa raiz do problema seja por lógica, por processo de eliminação ou tentativa e erro, identificada a causa raiz é aplicada a melhor solução para que a rede esteja operacional novamente. Este processo de diagnóstico e solução é denominado *troubleshooting*.

O principal objetivo do NOC é garantir a alta disponibilidade da rede garantindo que os serviços oferecidos aos clientes estejam sempre disponíveis e com alto grau de qualidade.

Para entendermos melhor como o NOC funciona precisamos entender como funciona uma empresa de telecomunicações do ponto de vista operacional. Utilizaremos como base uma empresa de telecomunicações genérica, atuante no mercado brasileiro e que disponibiliza aos seus clientes serviços de dados e telefonia fixa.

As áreas Engenharia e Operações de qualquer empresa de telecomunicações é responsável por toda a administração de sua rede, compreende o planejamento, instalação, operação diária e manutenção de todas as infraestruturas físicas e lógicas da rede. É dividida em três áreas principais: Engenharia, Implantação e Operações.

A Engenharia é responsável pelo planejamento e infraestrutura de toda a rede, tem como o objetivo garantir o crescimento e inovação de toda a planta. Esta desenvolve todos os projetos a serem comissionados que vai desde um circuito para um cliente até a expansão territorial em uma nova cidade. A Engenharia é dividida em Acesso, Transmissão, Comutação, Dados, Infraestrutura e Sistemas de Rede.

A Implantação é responsável pelo crescimento e expansão da rede, é ela quem executa os projetos criados pela Engenharia. Esta é dividida em Rede Externa e Equipamentos.

A Implantação de Rede Externa é responsável pela instalação dos cabos metálicos e fibras ópticas, canalizações e caixas subterrâneas, que permite que os produtos e serviços oferecidos pela empresa saiam dos equipamentos e cheguem até os clientes, sejam eles casas, prédios ou indústrias. Sua construção, quando subterrânea, depende do uso das ruas e calçadas, quando aérea depende do uso dos postes das distribuidoras de energia elétrica. A Implantação de Equipamentos é responsável pela instalação de novos equipamentos na rede, proporcionando expansão técnica da capacidade das redes de voz e dados.

A Operação é responsável pelo funcionamento da rede e, consequentemente, pelos serviços oferecidos aos clientes. Monitora em tempo real os equipamentos e tem foco na qualidade dos serviços. Realiza a manutenção da rede, em parceria com as Regionais. Dividida em Configuração, Centro de Operações, Centro de Operações Corporativo, Centro de Gerência de Rede e Suporte Especializado.

A equipe de Configuração é responsável pela configuração de circuitos e de novos clientes nos equipamentos da rede.

O Centro de Operações (CO) filtra as reclamações de clientes residenciais que foram abertas pelo CRM, realizada testes em conjunto com os técnicos das Regionais na casa do cliente, caso a falha não seja resolvida no CO o caso é enviado para o CGR analisar, da mesma forma quando é constatada que uma falha é massiva, ou seja, falhas que afetam aos serviços de vários clientes em comum.

O Centro de Operações Corporativas (COC) realiza as mesmas ações que o CO, porém tem foco somente em clientes corporativos.

A equipe de Gestão de Relacionamento com o Cliente, mais conhecida como CRM (do inglês, *Customer Relationship management*), recebe as ligações dos

clientes através do call-center, seja para contratação ou encerramento de serviços, atualizações de planos ou para reportar qualquer problema nos serviços oferecidos.

As Regionais são divididas geograficamente e realizam as instalações executadas em conjunto com a Implantação, operação e manutenção em conjunto com o CO, COC e CGR.

Os setores CRM e Regionais não fazem parte da Engenharia e Operações.

A equipe de Suporte Especializado presta suporte a todas as áreas técnicas da empresa, também é dividida em Acesso, Transmissão, Comutação, Dados, Infraestrutura e Sistemas de Rede.

O CGR-NOC é dividido de acordo com as tecnologias e aplicações: Acesso, Comutação, Transmissão, Dados e Infraestrutura. Desta forma cada área fica responsável pelo monitoramento e manutenção de uma parte da rede.

Acesso é responsável pelo monitoramento e manutenção dos equipamentos que utilizam as tecnologias V5.2, H248 e xDSL, a maioria dos equipamentos desta tecnologia são chamados de DSLAM (Multiplexador de Acesso a Linha do Assinante), são os últimos equipamentos antes do cliente.

Transmissão monitora todos os equipamentos das tecnologias PDH, SDH, CWDM, DWDM e MetroEthernet. Portanto deve monitorar os meios de transmissão entre os armários de rua, entre sites, indoors, estações switch, e entre cidades. Normalmente entre cidade são utilizados enlaces de alta capacidade e de longa distância, estes são chamados de Backbone, a maior parte dos equipamentos utilizados para esta finalidade são de tecnologia DWDM e SDH.

Comutação monitora as centrais telefônicas, utilizam tecnologias V5.2 e H248. É responsável por monitorar as rotas de interconexão com outras operadoras e sinalização entre centrais telefônicas. Também é responsável pelo monitoramento da infraestrutura das estações switch, pois todas as centrais telefônicas ficam nestas instalações.

Dados monitora os equipamentos que utilizam tecnologia IP, ATM e MetroEthernet. Os equipamentos de Dados são utilizados como concentradores e são na maioria switchs, roteadores, agregadores e BRAS.

Infraestrutura monitora os sistemas de eletricidade, refrigeração, incêndio e sistema de segurança de todas as instalações onde há equipamentos instalados.

Para manter o controle das diversas falhas que ocorrem diariamente na rede é necessário o armazenamento das informações das falhas ocorridas e o

troubleshooting realizado. Para isto é utilizado um sistema de gerenciamento de incidentes que armazena estas informações e gera um número para este incidente que é comumente chamado de *Trouble Ticket*, no sistema o operador entram com diversas informações como alarmes gerados, descrição da falha, designador que define nome de equipamentos, placas e circuitos, localidade, e o troubleshooting realizado. Estas informações ficam armazenadas em seu histórico que são atualizadas pelo operador a cada nova ação realizada, e podem ser consultadas mesmo após o encerramento do incidente, basta procurar pelo número do *Trouble Ticket* ou por uma palavra chave como nome do armário.

Quando um cliente entra em contato com a operadora reclamando falha em seus serviços é atendido pelos operadores do CRM, é gerado um protocolo de atendimento em um sistema semelhante ao utilizado pelo CGR-NOC, porém só é utilizado pelo CRM, CO e Regionais. É verificado se a falha do cliente esta associada a alguma falha massiva que já esteja sendo tratada pelo CGR, as falhas massivas são sinalizados à equipe do CRM pelo sistema de gerenciamento de incidentes através das informações que foram adicionadas ao *Trouble Ticket*. Se constatado que é a falha é isolada são realizados diversas verificações e testes iniciais junto com o cliente seguindo uma lista de procedimentos, este processo é chamado de *Check List*. Se após este processo a falha continue o protocolo de atendimento é passado para o Centro de Operações. Os operadores do CO realizam testes em conjunto com os técnicos da Regional nas instalações da operadora e se necessário na casa do cliente. Se mesmo após os testes não for identificado a causa da falha o CO realiza a abertura de um Trouble Ticket que é repassado para o CGR-NOC, a grande maioria dos casos isolados são corrigidos ainda no CO.

No CGR-NOC a análise é iniciada pela equipe de Acesso, como o CO já realizou os testes entre a casa do cliente e a instalação da empresa a equipe de Acesso verifica as configurações dos equipamentos e realizam testes de hardware, as falhas isoladas que chegam ao NOC são resolvidas após corrigir algum parâmetro de configuração da porta do cliente ou mesmo após trocar a porta depois de constatado o defeito.

As falhas massivas são descobertas de duas formas, a primeira é pelo CRM quando identifica que há um número anormal de reclamações para um armário ou região, quando isto acontece o CRM envia um e-mail para o CGR com a relação dos armários reclamados. A segunda é por meio dos alarmes gerados pelos

equipamentos que são monitorados pelo CGR. Desta forma o CGR abre um *Trouble Ticket* e sinaliza ao CRM, assim a novas reclamações geradas são associadas a falha massiva, eliminando o tempo que seria gasto pelo CRM realizando *check list* com os clientes. Quando um e-mail do CRM chega ao CGR informando sobre falhas massivas este e-mail é analisado pelo supervisor do CGR e o caso é enviado para a equipe responsável. Quando não identificado para onde deve ir o incidente é enviado para a equipe de Acesso que verifica se a falha esta relacionada aos seus equipamentos, se for necessário serão realizados testes em conjunto com outras equipes, se não for constatada a falha o incidente é passado para a equipe de Transmissão que realizada a analise em sua rede, da mesma forma se não localizar o defeito o incidente é repassado para a equipe de Comutação de a falha for de voz ou de Dados se a falha for Internet. Em qualquer uma das equipes em último caso quando o defeito não é encontrado é realizado o acionamento do Suporte Especializado que realiza novas verificações de equipamentos e realiza testes mais apurados.

3.2 EQUIPAMENTOS DE REDE

3.2.1 Equipamentos de Transmissão

Switch

A função de um Switch é enviar os dados aos seus destinos através do endereço MAC de cada equipamento. Opera na camada de enlace de dados (Camada 2 do modelo OSI) (PIRES, 2006).

3.2.1.1 ECI

A *Electronics Corporation of Israel* (ECI) foi fundada em 1961 e tem sede em Israel.

Seus equipamentos suportam soluções C/DWDM, SDH, PDH e serviços de Dados (*Ethernet, Fast Ethernet, Gigabit Ethernet*, ATM) (ECI, 2006).

XDM-100

O XDM-100 possui 4 Us de altura e pode atingir a taxa equivalente a 2.5Gbps (STM-16) por anel (até 6 anéis STM-16 podem ser abertos), possui todas as proteções de tributários de um equipamento de grande porte. Normalmente é utilizado em redes metro ou regionais.

A Figura 12 apresenta um XDM-100.

Figura 10 - Shelf do XDM-100
Fonte: ECI (2006)

O XDM-100 é uma plataforma de multi-Service de SDH com funcionalidades TDM e

Ethernet. Além disso, o XDM-100 pode ser configurado como uma plataforma CWDM, permitindo assim a expansão da capacidade sobre a mesma fibra.

O XDM-100 pode ser utilizado para construir topologias em anel, cadeia, ponto a ponto e *mesh*, opera com STM1/4/16 *Add / Drop* ou Terminal. Possui

granularidade: VC12, VC3 & VC4, Layer1/2 – Ethernet over SDH com funcionalidades LCAS, GFP, VCAT e MPLS.

O XDM-100 é composto por 4 slots de agregado que podem ser configurados sinais SDH ópticos e elétricos (STM-1, STM-4 e/ou STM-16). Existem também 8 slots para tributários, que podem ser ocupados com E1, E3, STM-1o/e, STM-4 e STM-16, além das placas de dados camada 1/2 e MPLS. A Figura 13 apresenta o Bayface do XDM-100.

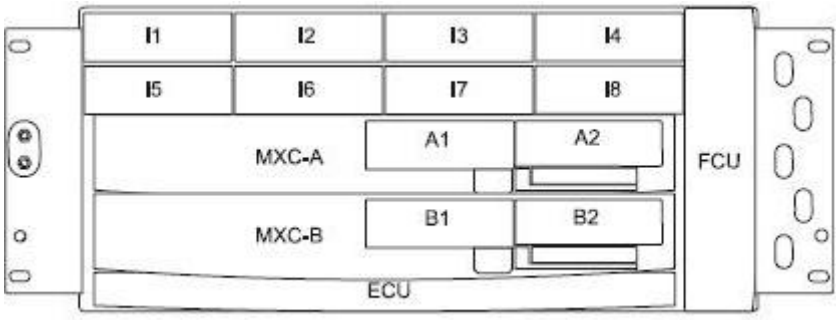


Figura 11 - Bayface do XDM-100
Fonte: ECI (2006)

XDM-1000

O XDM-1000 é uma plataforma MSPP preparada para operar como SDH, plataforma de dados (incluindo MPLS) e C/DWDM. O equipamento também está preparados para ser totalmente integrado a uma rede de dados através da funcionalidade MPLS. Para “transformar” o XDM em uma plataforma C/DWDM, basta adicionar tranponders, filtros, amplificadores, etc. (ECI, 2006). A Figura 14 apresenta um XDM-1000.

Figura 12 - Shelf do XDM-1000
Fonte: ECI (2006)

O sistema de gerência enxerga o XDM como uma única plataforma, mesmo quando ele é configurado como C/DWDM, SDH e plataforma de dados. Uma solução tradicional implica na utilização de pelo menos duas plataformas, e em certos casos, de fornecedores diferentes.

No XDM-1000 existem 23 slots disponíveis, distribuídos da seguinte forma: 11 slots para placas com interfaces elétricas (as quais são acessadas no Cage superior, M1 até M11), 23 slots para placas com interfaces ópticas (I1 até I12 e M1 até M11), dois para a controladora e dois para as matrizes. O XDM-1000 pode operar com capacidade de matriz de 30G, 60G e 120G, além de poder agregar plataforma C/DWDM.

A Figura 15 mostra o Bayface do XDM-1000.

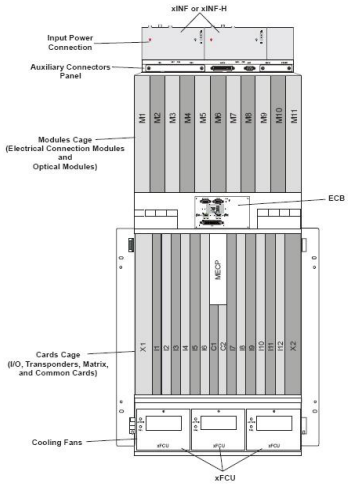


Figura 13 - Bayface do XDM-1000
Fonte: ECI (2006)

Interfaces ópticas utilizadas nos XDM

Mais conhecidos com SFP (*small form-factor pluggable*), são as interfaces ópticas para conexão de taxas de 155 Mbps (STM-1), 622 Mbps (STM-4), 2.5Gbps (STM-16), 10Gbps (STM-64/ethernet) e 1Gbps (ethernet). Existem também as SFPs coloridas, ou seja, com frequência fixa sintonizada no valor desejado pelo cliente tanto para CWDM como para DWDM. Devem ser instalados nos módulos ópticos. Observar com cuidado a etiqueta de identificação para ter certeza do tipo de interface, tanto com relação a taxa de transmissão quanto com relação ao comprimento de onda (850, 1310 ou 1550 nm) e a capacidade de transmissão (short haul e long haul), no caso deste último, atenuadores podem ser necessários para evitar a queima de uma interface. A Figura16 mostra um exemplo de SFP.

Figura 14 - Exemplo de SFP
Fonte: ECI (2006)

Modelos de SFP utilizados pelos equipamentos ECI:

- OTR64_S5: Módulo óptico short haul em 1550 nm para conexão de taxas de 10 Gbps em padrão SDH. Deve ser instalado no módulo OMTX10_S.
- OTR16_S3: Módulo óptico short haul em 1310 nm para conexão de taxas de 2.5 Gbps em padrão SDH. Deve ser instalado no módulo OMSC16_4.
- OTR4_S3: Módulo óptico short haul em 1310 nm para conexão de taxas de 622 Mbps em padrão SDH. Deve ser instalado no módulo SIO1_4.
- OTR1_S3: Módulo óptico short haul em 1310 nm para conexão de taxas de 155 Mbps em padrão SDH. Deve ser instalado no módulo SIO1_4.
- OTGBE_SX: Módulo óptico short haul em 850 nm para conexão de taxas de 1 Gbps em padrão ethernet. Deve ser instalado no módulo MCS10, MCS5 e/ou MCSM.

- OTGBE_LX: Módulo óptico short haul em 1310 nm para conexão de taxas de 1 Gbps em padrão ethernet. Deve ser instalado no módulo MCS10, MCS5 e/ou MCSM.

3.2.1.2 Huawei

A Huawei *Technologies* é sediada na cidade de Shenzhen na China e a segunda maior fornecedora de equipamentos de telecomunicações do mundo, foi fundada em 1988.

Optix Metro 1000

O Optix Metro 1000 é um equipamento da plataforma SDH com suporte a TDM e serviços Ethernet. Para serviços Ethernet opera em pequena escala onde convergem os serviços de várias portas *Fast Ethernet* em uma porta *Giga Ethernet*. O Metro 1000 tem dimensões de 436 mm (W) x 293 mm (D) x 86 mm (H), e consumo máximo de 82W de potência, tem capacidade máxima de 3 STM－4 e 6 STM－1 de entrada e saída e suporta até 80×E1, 14×FE (*Layer 2 Switch*) e 9×E3. Opera com multi proteção para ATM-VP-*ring* e SDH *Protection* (HUAWEI, 2005). A Figura 17 apresenta um Optix Metro 1000 e a Figura18 o Bayface do Optix Metro.

Figura 15 - Optix Metro 1000
Fonte: Huawei (2005)

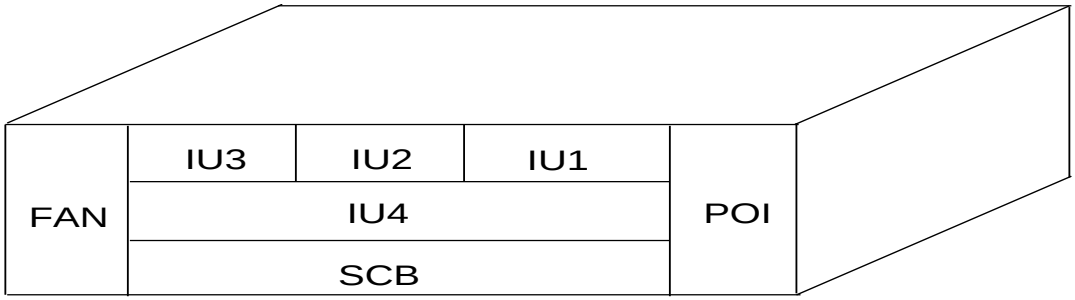


Figura 16 - Bayface do Optix Metro 1000
Fonte: Huawei (2005)

As placas do Metro 1000 são classificadas em unidades PDH, SDH, Ethernet, SCB, PIU, Módulo de energia e FAN.

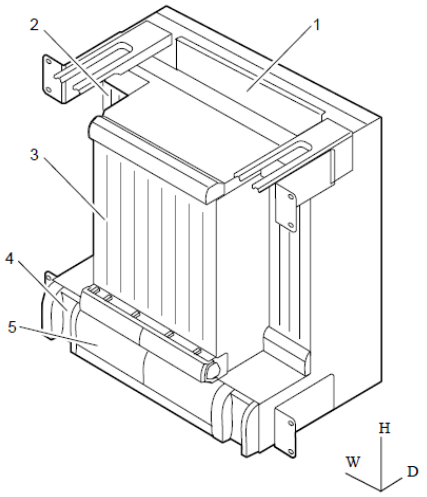
OptiX OSN 2500

O OSN 2500 tem capacidades de 2.5Gbit/s ou 622Mbit/s, herda todos os recursos da tecnologia MSTP que é a plataforma de transporte *multi-service* baseado em SDH, esta tecnologia herda as habilidades de proteção SDH, suportando PDH, SDH, Ethernet, ATM, entre outros serviços. O OSN 2500 é compatível com redes SDH tradicional e MSTP, e suporta soluções SDH, PDH, DDN (*Data Direct Networks*), Ethernet, WDM, ATM, IMA(*Inverse Multiplexing for* ATM), e RPR (*Router Processor Redundancy*), ESCON(*Enterprise Connection Systems*), FICON(*Fibre Connetion*), FC(*Fiber Connector*) e DVB-ASI (*Digital Video Broadcast-Asynchronous Serial Interface*) (HUAWEI, 2005).

A Figura 19 apresenta um subrac do OptiX OSN 2500 e a Figura 20 a estrutura do OptiX OSN 2500.

Figura 17 - Sub-rack do OptiX OSN 2500

Fonte: Huawei (2006)



1. Area de interfaces auxiliar.
2. Area de placas de interface.
3. Area de placa de Processamento.
4. Area da PIU.
5. Area Fan.

Figura 18 - Estrutura do Optix OSN 2500
Fonte: Huawei (2006)

O OSN 2500 possui 8 slot para placas de interfaces e 10 slots para placas de processamento, conforme Figura 21.

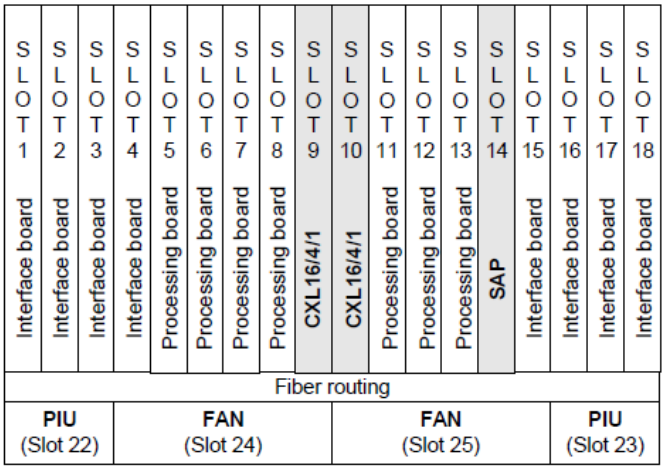
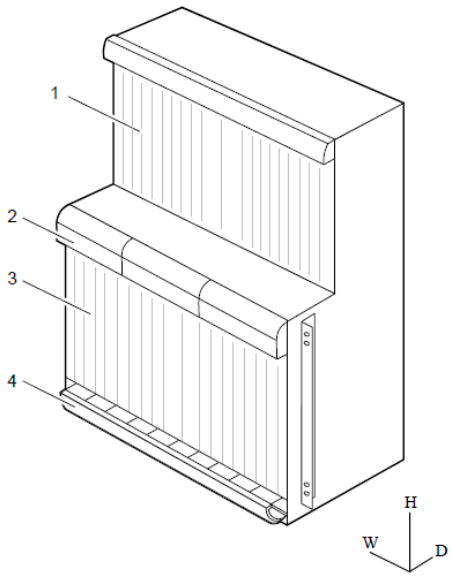


Figura 19 - Bayface do OSN 2500
Fonte: Huawei (2006)

OptiX OSN 3500

O OSN 3500, Figura 22, tem capacidades de 10 Gbit/s ou 2,5 Gbit/s, herda todos os recursos da tecnologia MSTP. É compatível com redes SDH tradicional e MSTP, e suporta soluções SDH, PDH, DDN, Ethernet, WDM, ATM, IMA, e RPR, ESCON, FICON, FC e DVB-ASI (HUAWEI, 2006). A Figura 23 apresenta a estrutura do OptiX OSN 3500.

Figura 20 - Sub-rack do OptiX OSN 3500
Fonte: Huawei (2006)



1. Area de placas de interface.
2. Area Fan.
3. Area de placa de Processamento.
4. Area distribuição de fibras.

Figura 21 - Estrutura do Optix OSN 3500
Fonte: Huawei (2006)

O subrack do OSN 3500, Figura 24, é dividido em duas camadas, A camada superior tem 16 slots para placas de interface, a camada inferior possui 15 slots para placas de processamento.

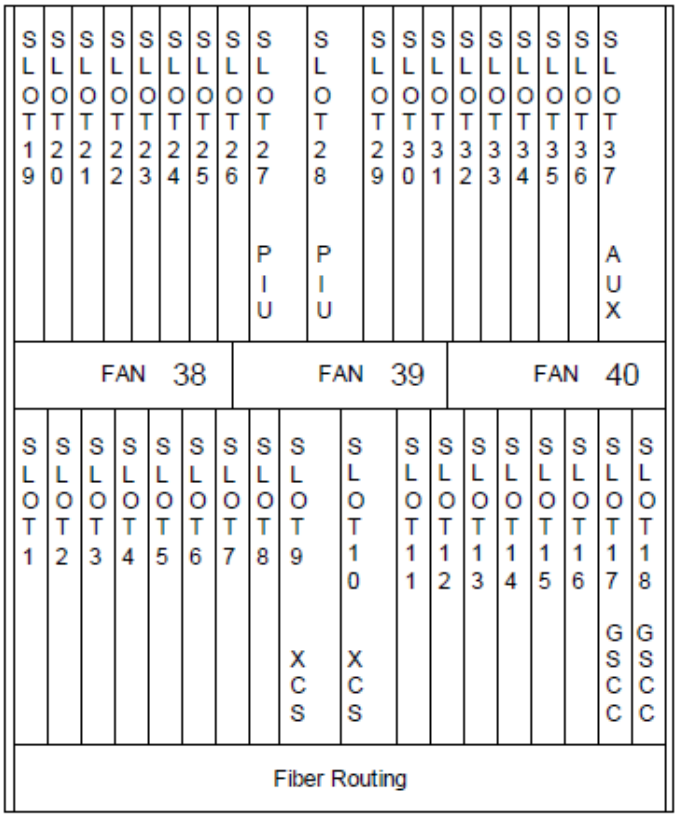


Figura 22 - Bayface do OSN 3500
Fonte: Huawei (2006)

A maioria das placas utilizadas no OptiX OSN 2500 e OptiX OSN 3500 são intercambiáveis, portanto podem ser utilizadas nos dois elementos. As placas são classificadas em unidades PDH, SDH, processamento de dados, placas *Cross-connect* e SCC e placas Auxiliares.

3.2.1.3 Datacom

A DATACOM iniciou suas atividades em outubro de 1998 e é de origem nacional.

Seus equipamentos suportam soluções Metro Ethernet oferecendo tecnologias 10 Gigabit Ethernet, Gigabit Ethernet, Fast Ethernet e suporte para comunicação ótica ou elétrica. Também suportam soluções de Transmissão em 10G(STM-64), transportando múltiplos canais TDM e SDH com disponibilidade de interfaces tributárias como E1, E3, STM-1, STM-4, STM-16, *Fast Ethernet e Gigabit Ethernet*.

DM3000

O switch possui 1U de altura, para instalação em racks 19 polegadas. Possuem opções de modelos voltados para aplicações *Layer2* e *Layer3*, oferece fontes *hot-swap* (podem ser trocadas sem desligar o equipamento), redundantes AC/DC *fullrange*. As portas SFP disponíveis permitem a utilização de módulos mini-GBIC com diferentes alcances e tipos de fibra.

A construção de Virtual LANs no DmSwitch pode utilizar até 4.096 VLANs, oferece funcionalidade de *double tagging* (Q-in-Q). É possível definir VLANs por protocolo, por endereço MAC e por IP-subnet, com possibilidade de *overlap* de portas nas VLANs *port-based*, além de configuração dinâmica usando o protocolo GVRP.

Utiliza mecanismos de proteção *Spanning Tree*, RSTP, MSTP, ERPS e EAPS específico para proteção da ordem de milissegundos em anéis Ethernet. Através das funcionalidades de *link aggregation* é possível agrupar portas físicas formando portas lógicas, com balanceamento de carga automático e recuperação com tempos típicos de sub-200ms.

Os switches DM3000 possuem 24 interfaces elétricas 10/100Base-X e 4 interfaces óticas 1000Base-X ou 10/100/1000Base-T(Combo), todas as suas interfaces utilizam SFPs (DATACOM, 2013). A Figura 25 apresenta um switch Metro Ethernet DM3000.

Figura 23 - Switch Metro Ethernet DM3000
Fonte: Datacom (2013).

3.2.1.4 Tellabs

A Tellabs Inc. iniciou suas atividade em 1975 na cidade de Chicago nos Estados Unidos, oferece produtos IP e Ethernet, gerenciamento de rede e soluções para rede ótica.

Tellabs 7345 Switch Agregação Ethernet

O Tellabs 7345 é um switch Layer2, suporta serviços Ethernet, banda larga, serviços de dados e acesso a Internet, portanto é muito utilizado em redes Metro-Ethernet.

O Tellabs 7345 tem capacidade de até 40 Gbit/s, suporta aplicações *Layer2* e *Layer3* incluindo MAC (*Media Access Network*) *Address*, VLAN (*Virtual Local Area Network*), ID e DSCP (*Differentiated Services Code Point*). Utiliza mecanismos de proteção MSTP (*Multiple Spanning Tree Protocol*) e RSTP (*Rapid Spanning Tree Protocol*) (TELLABS, 2011).

Shelf Tellabs 7345

O Shelf do Tellabs 7345, Figura 26, possui dimensões de 88.5 mm x 480 mm x 215.9 mm para instalação de racks de 19 polegadas, possui 7 slots para instalação de placas, Figura 27, (TELLABS, 2011).

Figura 24 - Shelf do Tellabs 7345
Fonte: Tellabs (2011)

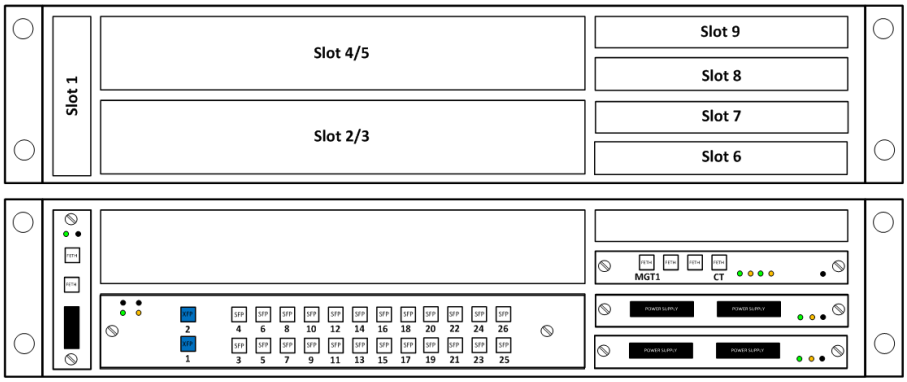


Figura 25 - Shelf Tellabs 7345 e suas placas
Fonte: Tellabs (2011)

Tellabs 6325 Edge Node

O Tellabs 6325 possui capacidade de até 2.5Gbit/s (STM-16) e proporciona facilidade MSPP (*Multi-Service Provisioning Platform*) oferecendo serviços tradicionais como SDH e PDH sobre WDM e interfaces IP. Suporta proteções do tipo SNC e MSP1+1. O equipamento possui interfaces STM-16, STM-4, STM-1 (ótica ou elétrica), E1 (2 Mbit/s), *Gigabit Ethernet, Fast Ethernet* e módulos WDM que geram até 8 canais CWDM e 8 canais DWDM, associando os dois módulos é possível gerar até 15 canais WDM por *Shelf*. O *Shelf* (SC2), Figura 28, possui apenas 1U de altura e capacidade para 4 placas de tráfego (TELLABS, 2006). A Figura 29 apresenta o Bayface do Tellabs 6325.

Figura 26 - Shelf SC2 do Tellabs 6325
Fonte: Tellabs (2006)

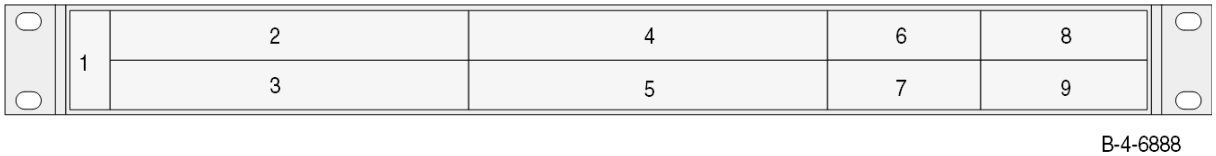


Figura 27 - Bayface do Tellabs 6325
Fonte: Tellabs (2006)

Tellabs 8860 Smart Router

O *Smart Router* Tellabs 8860, Figura 30, é um roteador baseado em recursos Ethernet, IP e MPLS, suporte simultâneo para aplicações *multi-service* em redes de acesso e agregação. Suporta aplicações SDH, ATM, Frame Relay, Ethernet, VLAN, Metro-Ethernet, TDM, PPP e HDLC. Realiza roteamento IP.
O Tellabs 8860 tem capacidade de 360 Gbps *full duplex*, possui 19 slots que suporta até 3 controladoras SCCs (*Switch and Control Card*), 16 placas de linha ULCs (*Universal Line Cards*) contendo até 4 módulos de linha PLM (*Physical Line Modules*) ou 16 placas de linha LCAs (*Line Card Adapters*) cada uma contendo até 2 placas de linha Ethernet ELCs (*Ethernet Line Cards*), o equipamento possui dimensões 549 x 889 x 295 mm (TELLABS, 2012).

Figura 28 - Tellabs 8860 Smart Router
Fonte: Tellabs (2012)

3.2.1.5 Padtec

A empresa Padtec é de origem nacional, fornece soluções para redes de longa distância, redes metropolitanas e redes de acesso, além de ser a primeira

fabricante da América Latina de sistemas de transmissão baseados na tecnologia WDM.

LightPad i1600G

A plataforma LightPad, Figura 31, realiza o transporte óptico de múltiplos serviços. Possui arquitetura que realiza o transporte de qualquer serviço através de interfaces transparentes ao tipo de protocolo. Os serviços são transportados diretamente sobre DWDM, ou multiplexados através de ODU e SDH sobre um único comprimento de onda. Possui até 160 canais a 2,5 Gb/s, 10 Gb/s ou a 40 Gb/s, tudo em um único sistema DWDM. Incorpora a camada de Rede de Transporte Óptico (OTN, G.709) suportando a crescente demanda de banda (Tb/s por fibra em enlaces DWDM) e serviços faixa larga de 2,5 Gb/s e 40 Gb/s nas tecnologias SDH, Ethernet, ATM e IP (PADTEC, 2010).

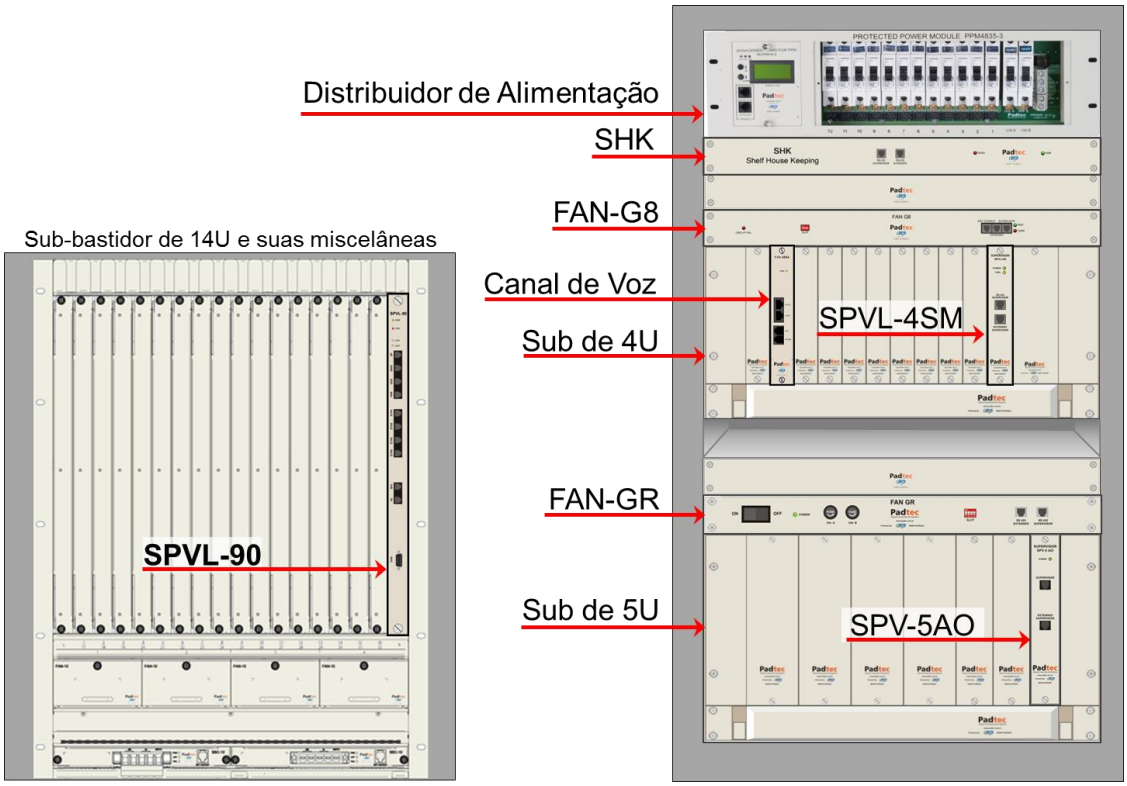


Figura 29 - Bastidor LightPad i1600G
Fonte: Padtec (2010)

3.2.2 Equipamentos de Acesso

DSLAM (*Digital Subscriber Line Access Multiplexer*)

O multiplexador de acesso a linha digital do assinante concentra o tráfego de diversas linhas telefônicas e realiza conexão com a rede de dados, realiza a distribuição de conexão a internet em altas velocidades utilizando tecnologia xDSL (PIRES, 2006).

Zhone MALC

O DSLAM Zhone MALC, Figura 32, é uma plataforma de acesso *multi-service* otimizada para oferecer serviços de voz, dados e vídeo através de uma rede de acesso. O Zhone MALC possui 2 interfaces óticas *Gigabit Ethernet* e 8 interfaces elétricas STM1 / E3 / E1. Suporta serviços voz TDM utilizando interface V5.2 e GR-303 sobre E1/T1 e VOIP através dos protocolos SIP, MGCP e H.248. Suporta serviços de dados e banda larga em ATM ou IP / *Gigabit Ethernet*, e vídeo através de Vídeo IP e RF Vídeo Overlay. Suporta ADSL2+, ReachDSL, SHDSL, POTS, ISDN, T1/E1, e *Pseudo-wire* (PWE). Tem capacidade de 24 a 960 portas por *shelf*, portanto, se considerarmos que em cada porta pode ser configurado um cliente em um único DSLAM pode-se configurar até 960 clientes oferecendo serviços de voz, dados e vídeo (ZHONE, 2013).

Figura 30 - Zhone MALC
Fonte: Zhone (2013)

Zhone MXK

O DSLAM Zhone MXK, Figura 33, é uma plataforma de acesso *multi-service* otimizada para oferecer serviços de voz, dados e vídeo através de uma rede de acesso. O Zhone MXK possui 2 interfaces óticas 10Gbit Eth, 8 interfaces óticas Gigabit Eth e 24 interfaces elétricas STM1 / E3 / E1. Suporta serviços voz TDM utilizando interface V5.2 e GR-303 sobre E1/T1 e VOIP através dos protocolos SIP, MGCP e H.248. Suporta serviços de dados e banda larga em ATM ou IP / *Gigabit Ethernet*, e vídeo através de Vídeo IP e RF *Vídeo Overlay*. Suporta EFM, VDSL, VDSL2, ADSL, ADSL2, ADSL2+, POTS, metro Wi-Fi, ISDN, T1/E1, e *Pseudo-wire* (PWE). Trabalha com proteções LACP, EAPS, e MSTP. Tem capacidade de 3.600 assinantes GPON 100 Mbps ou 360 assinantes de 1G Ethernet por *shelf* (ZHONE, 2013).

Figura 31 - Zhone MXK
Fonte: Zhone (2013)

Keymile Milegate 2500/2510

O MileGate 2500/2510, Figura 34, é projetado para fornecer serviços de dados e voz e serviços NGN em escritórios centrais, espaço de co-instalação, bem como em armários de rua. Possui interfaces ótica 10 GbE e 1 GbE, e interfaces elétrica STM-1, STM-4 e E1.

O sub-bastidor oferece 21 slots para placas, dos quais 20 podem ser equipados com placas de linha. Suporta serviços voz TDM utilizando interface V5.2 sobre E1/T1 e EoS, VOIP através dos protocolos SIP e H.248. Suporta serviços de dados e banda

larga em ou IP-DSLAM e Ethernet Switch. Trabalha com proteções RSTP e STP. Dependendo da seleção de placas de linha é possível ter até 1.280 interfaces de ADSL2+. (KEYMILE, 2013)

Figura 32 - Keymile Milegate 2500/2510
Fonte: Keymaile (2013)

3.2.3 Equipamentos de Dados

Roteador

O roteador é um dispositivo de rede que realiza o encaminhamento de pacotes de dados entre redes diferentes e fornece um meio inteligente de transferência de pacotes de uma rede para outra. Cada pacote de dados possui um endereço de destino, o roteador lê a informação de endereço e em seguida consulta a tabela de roteamento ou encaminhamento e assim direciona o pacote para a rede seguinte até que o mesmo chegue ao seu destino. Opera de camada de rede (Camada 3 do modelo OSI) (TITTEL, 2003).

BRAS (*Broadband Remote Access Server*)

O Servidor de Acesso Remoto de Banda Larga é um dispositivo, concentrador de tráfego de equipamentos como DSLAM, desta forma agrega as sessões de usuário da rede de acesso. Realiza o gerenciamento e autenticação de clientes, concentração e distribuição do tráfego de assinantes de banda larga e conectividade

com a Internet. Opera na camada de enlace de dados e na camada de rede (Camada 2 e Camada 3 do modelo OSI) (TITTEL, 2003).

Cisco 7600 Internet Router

O Cisco 7600, Figura 35, é um equipamento de roteamento IP / MPLS, possui interfaces de até 10 Gbps e capacidade de até 720 Gbps em um único *shelf* ou 40 Gbps de capacidade por slot.

O Cisco 7600 tem recursos de redundância lógicos como HSRP (*Hot Standby Router Protocol*), balanceamento de carga de Layer3 e tecnologia Cisco *EtherChannel* para fornecer proteção de nível superior, oferece QoS e segurança ACL (*Access Control List*). Os estados são sincronizados entre o processador ativo e *backup, upgrades* de software podem ser realizados enquanto o roteador está ativo sem comprometer o seu funcionamento. Cartões de linha não são reinicializados no caso de falhas de processos (CISCO, 2013).

Figura 33 - Cisco Catalyst 7600
Fonte: Cisco (2013)

Cisco ASR 9000

O roteador Cisco ASR 9000, Figura 36, oferece alta capacidade de transporte em redes Ethernet para aplicações como serviços de banda larga, IPTV e distribuição de vídeo, voz sobre IP (VoIP), serviços de VPN de negócios, serviços de atacado, e aplicações móveis, tais como o transporte de *backhaul*. É projetado para

trabalhar com de tecnologias de acesso como DSL, GPON, Ethernet, cabo e móvel. Tem recursos de redundância lógicos como HSRP (*Hot Standby Router Protocol*) e resiliência de rede com software inteligente para proteger contra a falha de ligação de rede e falhas de nó, possui balanceamento de carga de *Layer3* e tecnologia Cisco *EtherChannel* para fornecer proteção de nível superior, oferece QoS e segurança ACL (*Access Control List*). Os estados são sincronizados entre o processador ativo e backup, upgrades de software podem ser realizados enquanto o roteador está ativo sem comprometer o seu funcionamento. Cartões de linha não são reinicializados no caso de falhas de processos(CISCO, 2013).

Figura 34 - Cisco ASR 9000
Fonte: Cisco (2013)

Juniper MX960 – *Universal Edge Router*

O MX960, Figura 37, opera com sistema operacional Junos OS, é otimizado para roteamento e comutação avançada de rede para serviços Ethernet e fornecer suporte para interfaces de *multi-service* Frame Relay e ATM. Possui alta capacidade e suporta até 240 Gbps por slot, suporta serviços VPN, serviços *multiplay* de banda larga de NGN e Internet de alto tráfego para *Datacenter internetworking*. O roteador possui 14 slots que podem ser preenchidas com até 12 placas DPCs (*Dense Port Concentrators*) ou MPCs (*Modular Port Concentrators*), 6 placas FPCs (*Flexible PIC*

Concentrators) e 2 placas controladoras SCBs (*Switch Control Boards*) (JUNIPER, 2013).

Figura 35 - Juniper MX960
Fonte: Juniper (2013)

Juniper ERX310 Broadband Services Router

O ERX310, Figura 38, é um BRAS, é utilizado para prover acesso à Internet de banda larga, IPTV, vídeo sob demanda, voz sobre IP (VoIP), jogos online, e uma série de aplicações interativas. Suporta aplicações em MPLS, BGP4, IS-IS, OSPF e RIP, tem capacidade de comutação de 10 Gbps, dois slots dedicados para módulos de linha, e suporta interfaces OC12c/STM4 e interfaces *Ethernet Gigabit* (JUNIPER, 2013)

Figura 36 - Juniper ERX310
Fonte: Juniper (2013)

Ericsson SmartEdge 1200 – Multi-Service Edge Router (MSER)

O SE-1200, Figura 39, é projetado é otimizado para oferecer serviços de classe de operadora, tais como vídeo, voz, dados e entrega de conteúdo interativo.

Ele consolida e simplifica a borda da rede do provedor de serviços pela convergência de funcionalidades Ethernet agregação, BRAS e IP /. Os recursos do SE-1200 permitem a operação eficiente da rede e inclui o provisionamento de banda larga dinâmica, gestão de tráfego, a minimização do tempo de inatividade da rede e alocação dos níveis adequados de QoS por usuário, por aplicativo. Suporta mais de 750 mil assinantes em um único rack (ERICSSON, 2013)

Figura 37 - Ericsson SmartEdge 1200
Fonte: Ericson (2013)

3.2.4 Equipamentos de Comutação

Nortel Switch DMS-100

A Central Telefônica DMS-100, Figura 40, é uma Sistema Multiplex Digital (DMS), é utilizada na prestação de serviços e ligações locais para a Rede Pública de Telefonia Comutada (PSTN). Suporta aplicações POTS (*Plain Old Telephone Service*), ISDN (*Integrated Services Digital Network*) e MDC (*Meridian Digital Centrex*), realiza a gestão de mobilidade para sistemas de telefonia celular, serviços de negócios sofisticados, como distribuição automática de chamadas (ACD). Fornece funções de Rede Inteligente (AIN, CS1-R, ETSI INAP).

Figura 38 – Nortel Switch DMS-100
Fonte: Nortel (2002)

Nortel Communication Server 1000

O Nortel CS 1000, Figura 41, é um sistema de comunicação distribuída IP, oferece conexões de chamadas telefônicas e serviço de gerenciamento de conexão. Possui Servidor de Sinalização que realiza serviços de controle de chamada, como registro de terminais IP, tradução de endereços de IP e controle de banda, simplifica o plano de discagem de rede. Suporta protocolos de comunicação TDM, H.248, H.323v4, SIP, 802.1p/q, DiffServ, SNMP, DHCP, RTP, RTCP, VPIM e mais de 650 recursos de telefonia de classe mundial. Suporta até 86 000 dispositivos TDM e quantidade ilimitada de dispositivos IP (NORTEL, 2008).

Figura 39 – Nortel DMS-1000E

Fonte: Nortel (2008)

Huawei C&C08 Switching System

A central telefônica C&C08, Figura 42, é sistema de comutação, é muito utilizados em interconexão com centrais tandem, *gateway*, locais, redes privadas e redes comerciais e encaminhamento de chamadas para Rede Pública de Telefonia Comutada (PSTN) e rede IP, suporta aplicações ISDN (*Integrated Services Digital Network*), MDC (*Meridian Digital Centrex*) (Huawei, 2006).

Figura 40 – Huawei C&C08
Fonte: Huawei (2006)

3.3 TOPOLOGIAS DE REDES DE TRANSMISSÃO

As topologias de rede podem ser das formas mais variadas possíveis, portanto são projetadas conforme as suas aplicações e conforme a disponibilidade de recursos.

Na sequência veremos algumas topologias utilizadas empregando-se os equipamentos de transmissão que vimos, lembrando que todas podem variar de acordo com as suas aplicações.

3.3.1 Topologia Para Elementos de Transmissão ECI

Na topologia da Figura 43, os elementos de transmissão são XDM-100 e XDM-1000 do fabricante ECI. Todas as conexões entre os elementos são físicas, desconsiderando as conexões internas que citaremos posteriormente.

No armário os DSLAMs de serviços de dados e voz são separados para demostrar que os serviços são diferentes, porém podemos ter os dois serviços no mesmo DSLAM, porém em serviços separados.

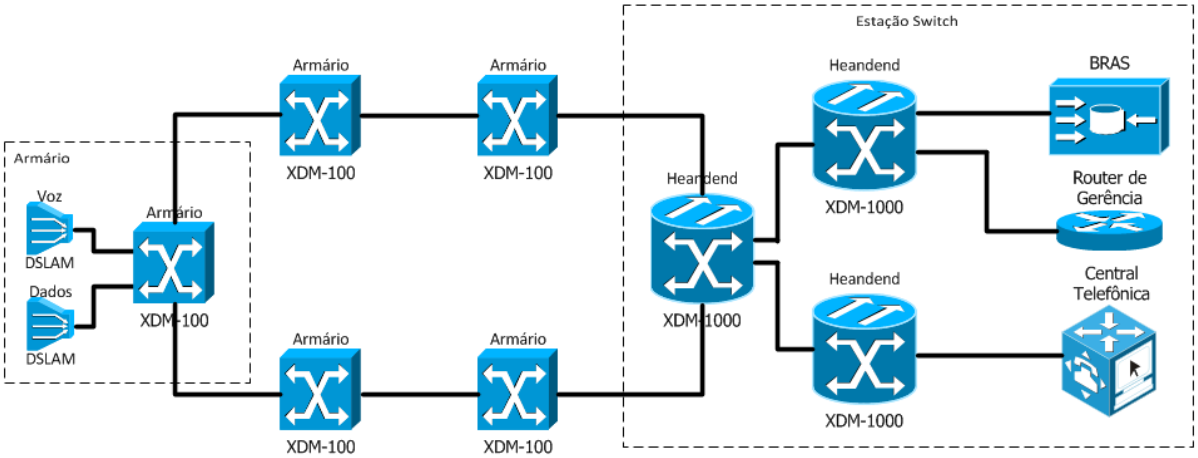


Figura 41 – Topologia física com elementos de transmissão ECI
Fonte: Autoria Própria.

Para os equipamentos da ECI, os serviços de dados e de voz por H248 são configurados em serviços Ethernet em rede MPLS. Na topologia MPLS (*Multi Protocol Label Switching*), é criada conexão lógica entre as placas MCSM quando for

entre armários e conexão lógica entre as placas MCS10 e MCSM quando for entre o headend e armário, esta conexão lógica é chamada de MOT (*MPLS over Tranport Port*). Nos exemplos a seguir temos três serviços Ethernet diferentes, um para serviço de dados, Figura 44, um para serviço de gerência de todos os equipamentos do anel, Figura 45 e outro para serviço de voz utilizando protocolo H248 (Figura 46). Nota-se que cada serviço termina em uma placa MCS10 diferente na estação switch, pois haverá uma conexão lógica diferente sempre que os serviços forem configurados em slots diferentes mesmo que sejam no mesmo elemento ou em elementos diferentes.

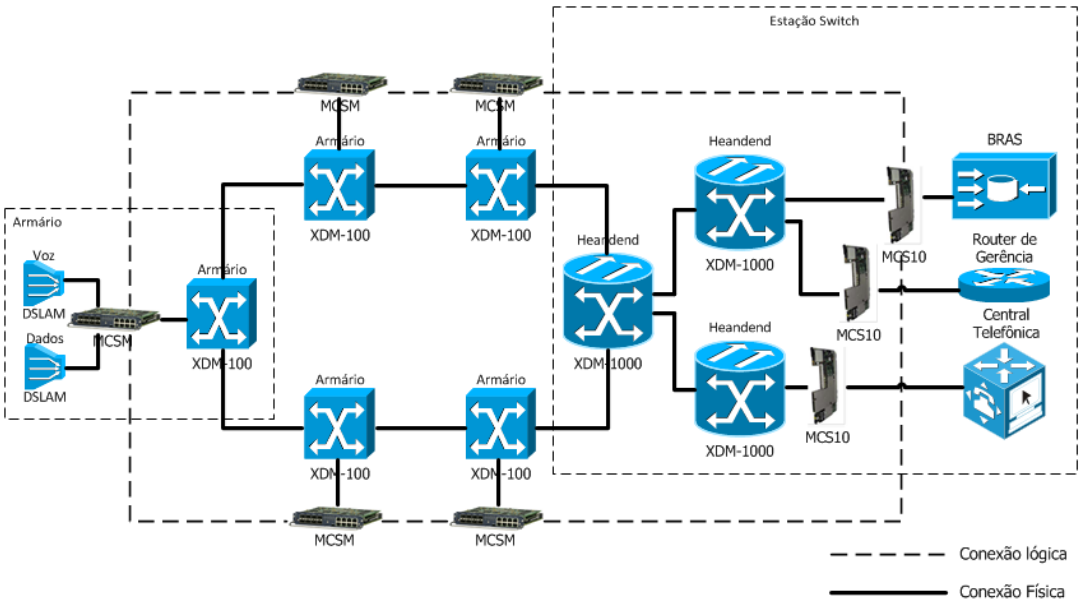


Figura 42 – Topologia lógica MPLS para serviços Ethernet de dados
Fonte: Autoria Própria.

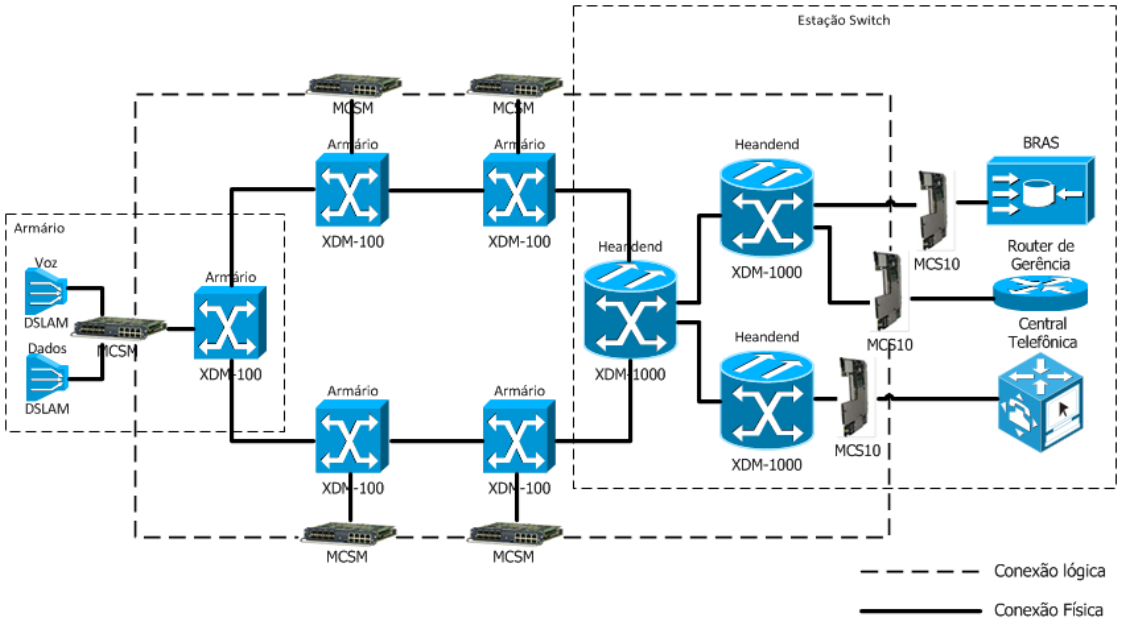


Figura 43 – Topologia lógica MPLS para serviços Ethernet de gerência
Fonte: Autoria Própria.

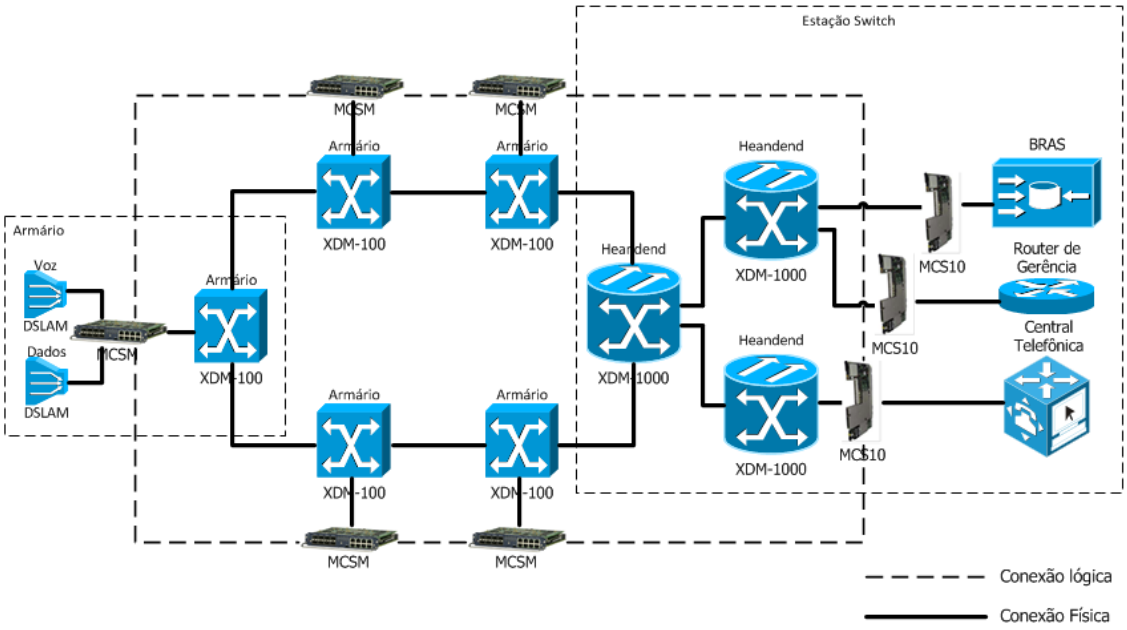


Figura 44 – Topologia lógica MPLS para serviços Ethernet de voz por H248
Fonte: Autoria Própria.

3.3.2 Topologia Para Elementos de Transmissão Huawei e Datacom

Nesta topologia, Figuras 47 e 48, os elementos da Metro1000, OSN2500, OSN 3500 da Huawei são utilizados para serviços de voz por protocolo V5 e o

elemento Datacom DM3000 é utilizado par serviços de dados e de gerência, os dois equipamentos ficam juntos dentro do mesmo armário.

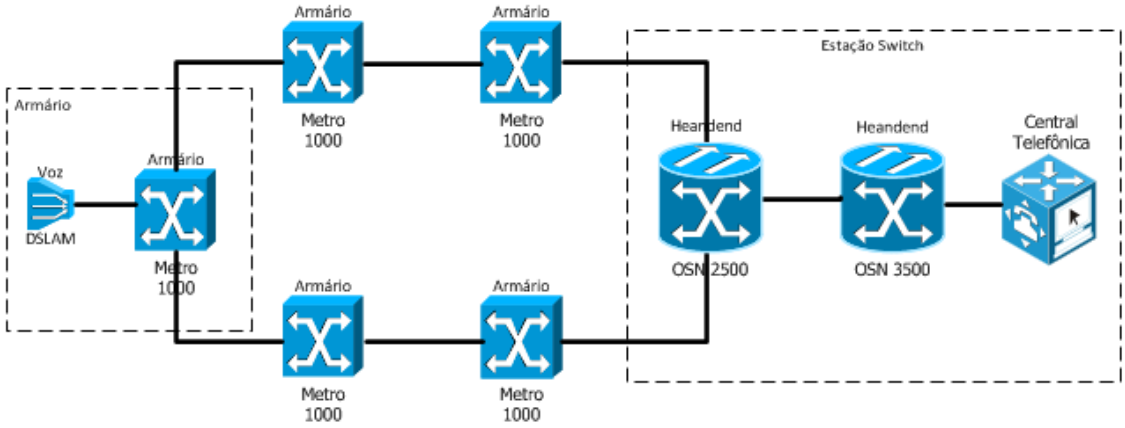


Figura 45 – Topologia física com elementos de transmissão Huawei
Fonte: Autoria Própria.

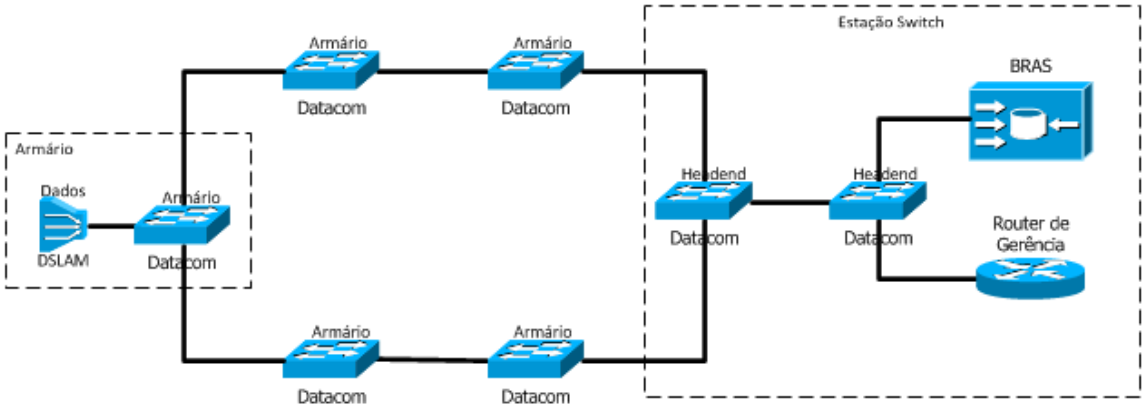


Figura 46 – Topologia física com elementos de transmissão Datacom
Fonte: Autoria Própria.

3.3.3 Topologia Para Elementos de Transmissão Tellabs

Nesta topologia, Figura 49, os equipamentos Tellabs 6325 e 7345 são conectados entre eles, havendo uma conexão lógica entre os elementos 7345 do anel e o 8860 do *headend*. Quando o DSLAM de voz utilizar protocolo V5 será conectado ao elemento 6325, caso o DSLAM de voz utilize protocolo H248, o mesmo será conectado ao elemento 7345 conforme o exemplo abaixo:

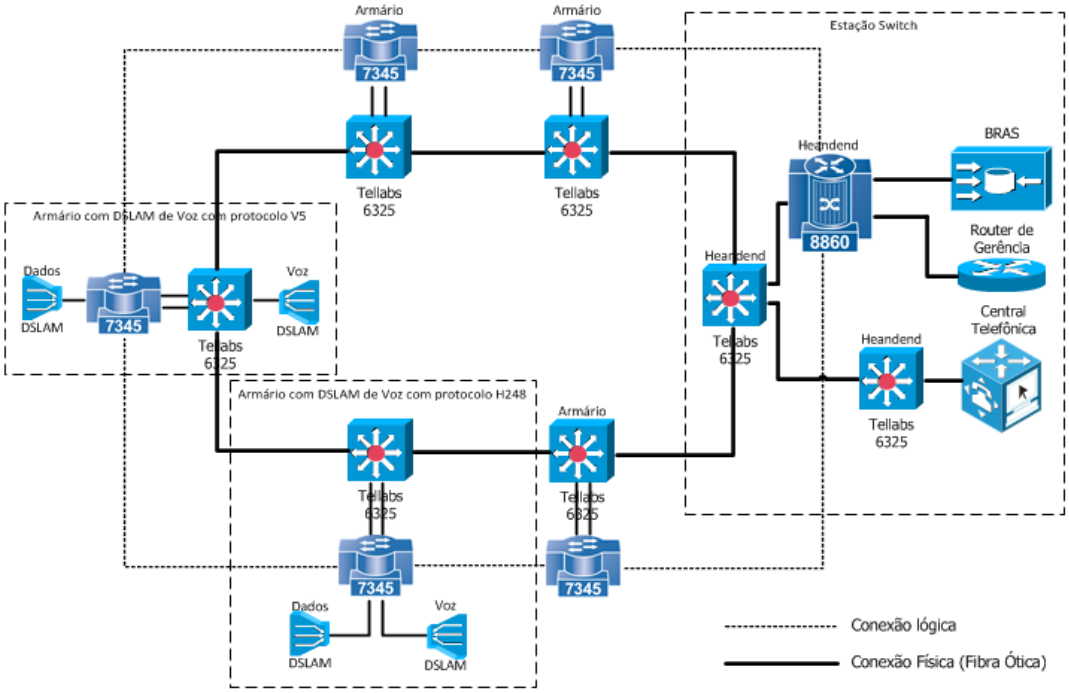


Figura 47 – Topologia física e lógica utilizando elementos de transmissão Tellabs
Fonte: Autoria Própria.

As conexões entre o 6325 e 7345 são realizadas conforme a Figura 50.

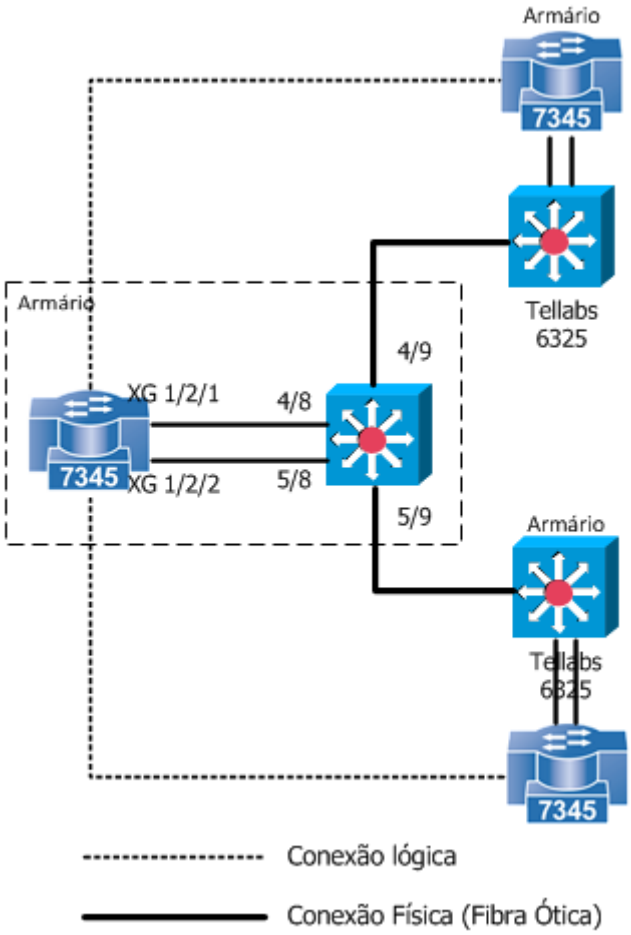


Figura 48 – Conexões entre os elementos Tellabs 6325 e 7345
Fonte: Autoria Própria.

No elemento 7345 as interfaces são mapeadas pelo tipo de interface e posição, por exemplo, a XG 1/2/1, o XG indica o tipo de interface utilizada, XG para 10 Giga e Gi para 1 Giga, na sequência temos os números 1/2/1 que indicam Shelf / Slot / porta, portanto a interface 10 Giga esta no *shelf* 1, slot 2, porta 1.

No elemento 6325 as interfaces são mapeadas de forma mais simplificada, por exemplo, a posição 4/8 indica Slot / Interface, portanto slot 4, porta 8. As placas do slot 4 e 5 são OMCs portanto as interfaces 4/9 e 5/9 são as interfaces de linha e são conectadas as fibras óticas que conectam aos outros armários.

3.3.4 Conexões Internas

Há várias conexões entre os elementos nas instalações físicas nos armários e nas estações switch. No esquema da Figura 51, vemos as conexões internas dos armários.

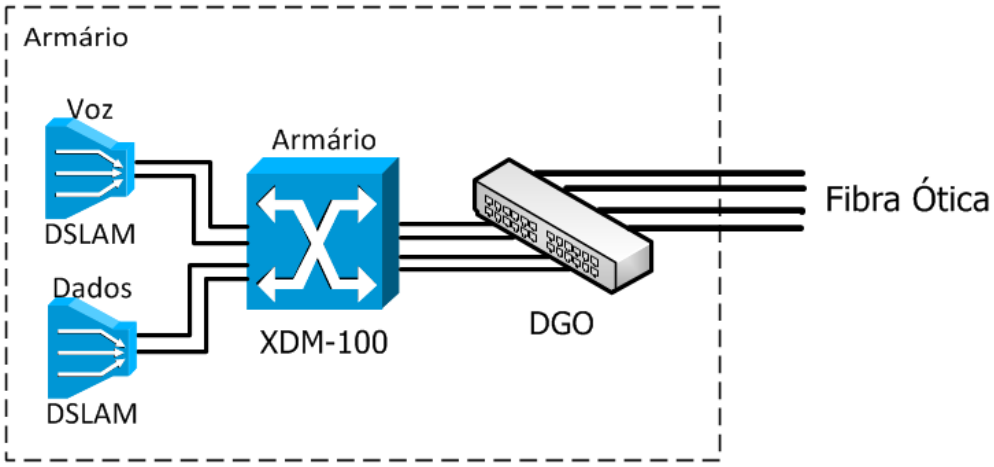


Figura 49 – Conexões internas de um armário
Fonte: Autoria Própria.

Há um DGO (Distribuidor Interno Ótico) que recebe as fibras óticas dos armários vizinhos, um par de cada armário vizinho, sendo um Tx (Transmissão) e outro Rx (Recepção). As conexões entre o DGO e o SDH e entre o SDH e os DSLAMs é realizadas por cordões óticos ou cabos elétricos.

Na estação switch o DGO (Distribuidor Interno Ótico), Figura 52, recebe as fibras óticas vindo dos armários. As conexões internas entre *headends* e outros elementos de rede é realizado por cordões óticos ou cabos elétricos, porém sempre que as conexões foram por cordões óticos haverá passagem por um DIO (Distribuidor Interno Ótico), e sempre que utilizar cabos elétricos haverá passagem por um DID (Distribuidor Intermediário Digital).

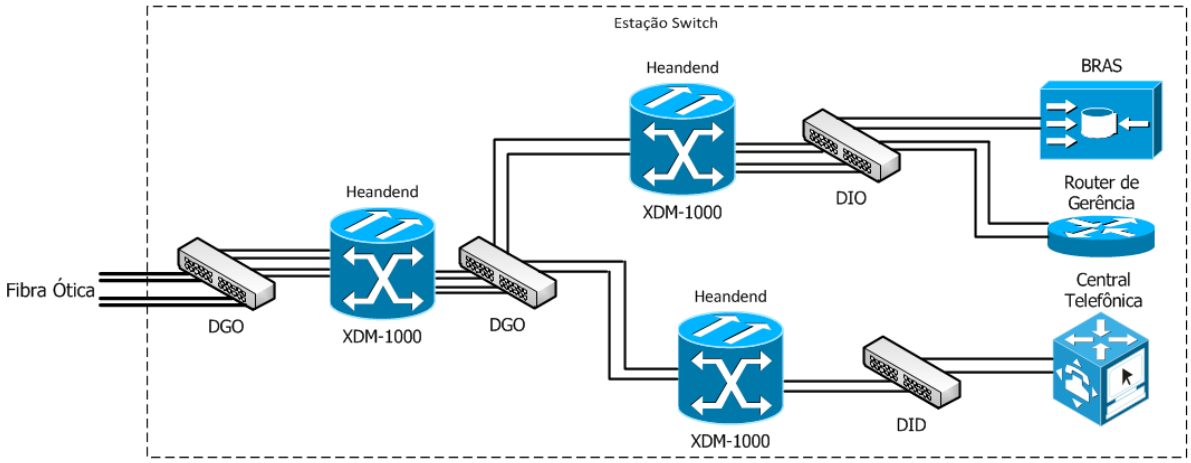


Figura 50 – Conexões internas na estação switch
Fonte: Autoria Própria.

3.4 TIPOS DE FALHAS EM REDES DE TRANSMISSÃO

Alarmes são avisos enviados pelo sistema de detecção de falhas ao sistema de gerência da rede alertando sobre a ocorrência de falhas e defeitos. Os alarmes podem ser de falhas de comunicação, controle de transmissão e recepção ótica, falha de serviço, temporização e sincronismo, equipamentos e hardware, entre outros.

Os alarmes também são classificados por severidade, e vão do mais importante ao menos relevante, pode ser Crítico (*Critical*), Majoritário (*Major*), Minoritário (*Minor*) e Advertência (*Warning*).

Em redes SDH alguns alarmes podem ocorrer em diversos níveis, como na seção de regeneração (RS), seção de multiplexação (MS), e níveis de alta ordem (HO) e baixa ordem (LO). Na maioria dos casos, os alarmes são eliminados da mesma forma em todos os níveis, portanto o *troubleshooting* deve começar pelas ordens mais altas.

Listaremos alguns dos alarmes mais comuns dentre os equipamento da rede de transmissão, a maioria dos alarmes são comuns a diversos equipamentos, porém lembramos que muitos fabricantes possuem alarmes específicos para seus equipamentos.

3.4.1 Alarmes de Transmissão

SIA (*Alarm Indication Signal*)

SIA indica que ocorreu uma falha antes do equipamento que gerou este alarme, ou seja, há outro alarme existente no equipamento anterior a ele em uma rede.

DEG (*Degraded*)

O alarme indica que há taxa de erro de bits de entrada (BER), é maior do que o limite configurado.

EXC (*Excessive Errors*)

O alarme EXC é um alarme de limiar que indica que a taxa de erro de bits (BER) na estrutura do sinal de entrada é maior do que o limiar configurado.

LOA (*Loss of Alignment*)

O alarme LOA indica uma perda de alinhamento na concatenação do sinal de entrada.

LOD (*Loss of Data*)

O alarme indica que o não foi detectado perda de comunicação óptica, porém não foi detectado nenhum sinal de dados.

LOF (*Loss of Frame*)

O alarme LOF indica que nenhum alinhamento de quadro foi detectado na entrada de sinal. O extremo do link pode causar esse alarme. Esta é uma das principais causas do alarme, tal como o receptor não consegue reconhecer quaisquer dados das fibras. Este alarme é detectado ao nível RS. Ambas as falhas na fonte (transmissor) e a taxas de erros (BER) extremamente altas podem gerar alarmes de LOF.

LOM (*Loss of Multiframe*)

Este alarme é acionado quando for detectada perda de sincronização no byte H4 (Bits 7, 8) de uma sequência de superquadro. Este alarme pode ser gerado por uma placa defeituosa ou equipamento de teste ligado que não suporta *multiframe*.

LOMC (*Loss of Multiframe – Concatenated*)

O alarme de LOMC indica uma perda de alinhamento *multiframe* relacionado com circuitos concatenados.

LOP (*Loss of Pointer*)

O alarme de LOP indica que foram recebidos ponteiros inválidos devido a uma falha de equipamento, incompatibilidade no mapeamento do sinal ou problema de sincronismo.

LOS (*Loss of Signal*)

O alarme de LOS indica uma perda significativa no nível do sinal ótico recebido. Esta falha pode ser causada por uma fibra danificada ou desconectado, ou por um defeito óptico no transmissor ou no receptor.

Loss of Synchronization

Este alarme indica perda de sincronização na interface. Possui potência na Rx da interface, porém sem carga útil.

Signal Failure

Este alarme indica falha na interpretação do sinal pela interface. Possui potência na Rx da interface, porém sem carga útil.

PLM (*Payload Label Mismatch*)

O alarme de PLM indica uma incompatibilidade no rótulo do sinal de carga. Tal como acontece com o UNEQ ou alarmes TIM, a causa para este alarme pode ser uma conexão errada (perda de *cross* conexão ou uma fibra cruzada).

RAI (*Remote Alarm Indication*)

Um alarme de RAI indica uma condição de falha de sinal na ponta remota. Quando o alarme é detectado é enviado um código *upstream* de uma rede digital, tal como um sinal de notificação que ocorreu uma falha *downstream*.

RDI (*Remote Defect Indication*)

Um alarme de RDI indica uma condição de falha remota, defeito distante mais próximo á outra extremidade.

SSF (*Server Signal Fail*)

O alarme SSF indica uma falha na função de adaptação, devido a um alarme de SIA ou LOP.

TIM (*Trace Identifier Mismatch*)

O alarme de TIM indica uma incompatibilidade do *label* identificador, é causado pelo provisionamento incorreta do *label* identificador ou por conexão incorreta. Este alarme é obtido comparando os bytes (J0/J1/J2) esperados com os bytes recebidos.

UAT (*Unavailable Time*)

O alarme UAT indica 10 SES consecutivos (*severely errored seconds*). Indica indisponibilidade de um link ou circuito.

UNEQ (*Unequipped*)

O alarme de UNEQ indica que foi detectado um sinal de circuito não configurado. Este erro pode ser causado por uma desconexão de circuito ou falha de cross-conexão.

Auto Negotiation (AN) Failure

Indica uma falha de sincronização e comunicação no processo de auto negociação entre a interface do SDH e um dispositivo cliente como um switch ou roteador. Quando o processo de AN está habilitado, ele é ativado automaticamente sempre que cabos estão conectados nas interfaces.

Encapsulation Mismatch

O alarme de incompatibilidade de encapsulamento indica que a encapsulamento GFP / HDLC não é suportado pelo tipo de encapsulamento configurado para o hardware.

Header Mismatch

O alarme de incompatibilidade de cabeçalho indica um desalinhamento entre o cabeçalho esperado e a extensão de cabeçalho recebido na camada de GFP. Este alarme normalmente indica um problema de interoperabilidade com outros equipamentos.

Link Down

O alarme de Link Down indica um link Ethernet que está em *down* ou perda de comunicação (conforme definido na norma IEEE 802.3). Este alarme pode ser resultado de falha no processo de auto negociação, perda de sinal sobre a ligação resultante a partir de fibras ou cabos desconectados, ou uma falha de hardware.

LFD (*Loss of Frame Delineation*)

O alarme LFD indica uma perda de delineação de quadro na camada GFP.

Loopback Alarm

Indica que um loopback lógico esta ativo para a interface alarmada.

3.4.2 Alarmes de Serviços

Service Degraded

O alarme de Serviço Degradado indica degradação no sinal em tráfego. Este alarme também pode indicar que um circuito por onde o serviço esta trafegando está degradado ou taxando erro.

Service Failed

O alarme de falha de serviço indica que ambos os caminhos principais e de proteção não estão transmitindo o tráfego do circuito.

3.4.3 Alarmes de Equipamentos

Card Failure / Unit Problem

Indica que a placa tem uma falha geral de hardware. Este alarme é gerado quando há alguma falha de funcionamento da placa comprometendo suas aplicações.

Card Out / Unit missing / Replacement Unit Missing / Transceiver Response Fail

Estes alarmes indica que a placa atribuída não está mais em seu slot. Acontece quando a placa é atribuída, mas fisicamente não está presente no compartimento do slot ou quando a placa já não é mais reconhecida pelo equipamento.

High Temperature

O alarme de alta temperatura indica que a temperatura do material é superior a 65°C.

Low Temperature

O alarme de alta temperatura indica que a temperatura do material é inferior a 0°C.

Type Mismatch / Mismatch Equipment

O alarme de tipo incompatível de placa indica que a placa errada foi inserida no slot. Este alarme ocorre quando o tipo de placa inserida no slot e o tipo de placa configurado no equipamento não são os mesmos. Estes dois valores devem ser idênticos.

Algumas das placas dos equipamentos XDM da ECI geram um BIT *Code (Built-In Test*), que é um código específico gerado pela placa alarmada indicando em qual módulo interno ocorreu o erro, a partir do BIT *Code* o fabricante realiza o reparo da placa.

BIT *Degraded*

O alarme BIT *Degraded* indica uma falha de equipamento que pode afetar a sua funcionalidade. Além do alarme, se o equipamento estiver protegido, ele executa uma interrupção para o modo protegido. Este alarme pode ser resultado de problema na placa ou as conexões com as placas matrizes HLXC / XIO estão defeituosas.

BIT *Failed*

O alarme de BIT *Failed* indica uma falha de equipamento, é mais grave que um alarme de BIT *Degraded*. Este alarme pode ser resultado de problema na placa ou as conexões com as placas matrizes HLXC / XIO estão defeituosas.

Program Fail

Indica que o software não está funcionando corretamente na placa controladora, ou o sistema não foi capaz de atualizar o banco de dados da placa para a memória da placa.

High Rx Power

O alarme de alta potência de Rx indica que a potência recebida é superior ao valor máximo permitido.

High Tx Power

O alarme de alta potência de Tx indica que a potência transmitida é superior ao valor máximo permitido.

Low Rx Power / Signal Degraded / Out of Frame

O alarme de baixa potência de Rx e sinal degradado indicam que a potência recebida é inferior ao valor mínimo permitido.

Low Tx Power

O alarme de baixa potência de Tx indica que a potência transmitida é menor do que o valor mínimo permitido.

Power Feed / Power Problem / Relay Alarm

Estes alarmes indicam falha na alimentação elétrica do equipamento.

3.4.4 Alarmes de Gerência

NE Disconnected / NE Unavailable / NE Fault / NE Communication Fault

Indica perda de comunicação do elemento de rede com o servidor de gerência.

Gateway NE Communication Fault

Indica perda de comunicação do elemento de rede gateway com o servidor de gerência.

3.4.5 Alarmes de Temporização e Sincronismo

Primary Timing Source Not Active / Loss of Time Input

Indica que a fonte principal de sincronismo não esta ativa, presumivelmente devido a uma falha da fonte primária, estará operando pela fonte secundária.

Timing Generator (TG) Holdover / Holdover Syncronization

Indica que o gerador de temporização e sicronismo não tem referência de temporização disponível para sincronização, e está entrando em um estado *holdover* (o último *clock* válido). Este alarme pode ser consequente ao alarme de *Primary Timing Source Not Active*.

3.5 SISTEMAS DE GERÊNCIA

O sistema de gerenciamento de rede, abreviado para NMS (*Network Management System*), possui as funções de gerência dos elementos de rede, gerenciamento de alarme e falhas, monitoramento de performance, gerenciamento de configuração, gerenciamento de VC's de alta / baixa ordens, operações de manutenção, gerenciamento de segurança, gerenciamento de cross-conexões e circuitos do elemento em questão. Como todos os sistemas de gerência de rede, é necessário um servidor dedicado e um servidor backup, para proteção do principal. É utilizado também um servidor EMS (*Element Management Systems*), um Sistema de Gerenciamento de Elementos.

3.5.1 ECI

O sistema de gerenciamento de rede utilizado pelos equipamentos ECI é o LightSoft NMS, Figura 53, desenvolvido pela própria ECI, abaixo temos a janela principal da gerência com uma janela dedicada para alarmes e outra para topologia:

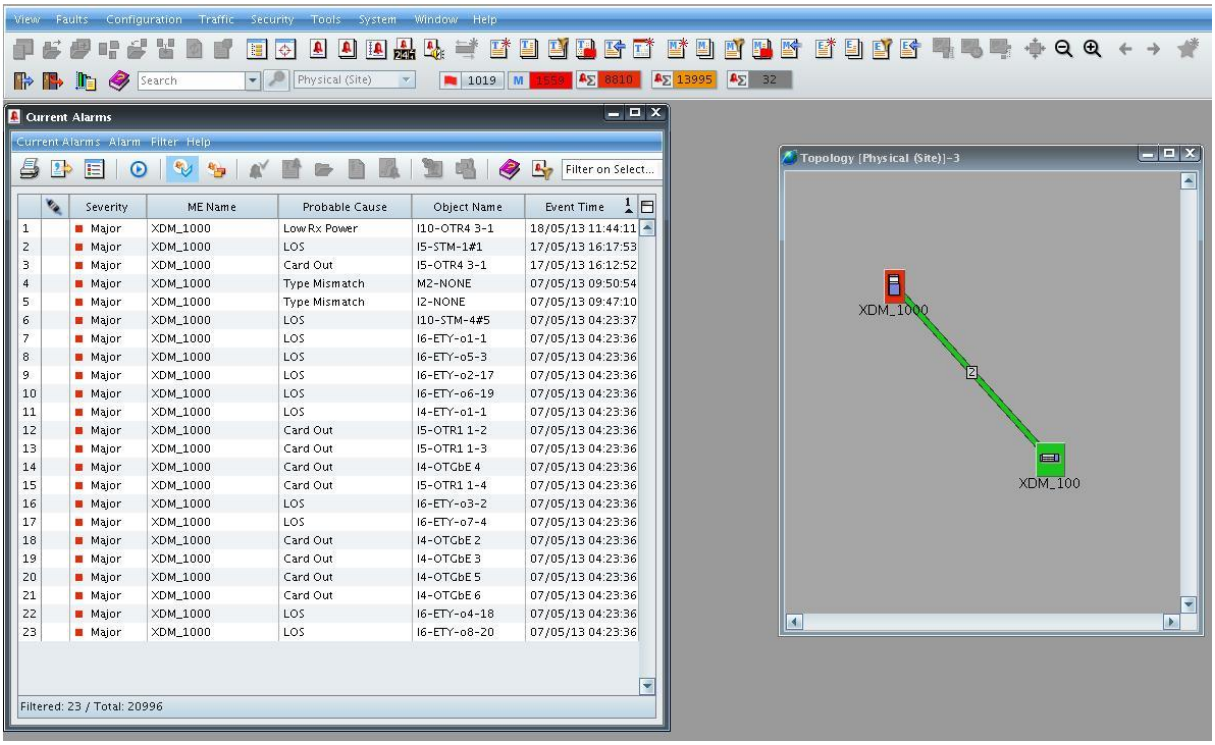


Figura 51 – Gerência LightSoft ECI
Fonte: Autoria Própria.

Como exemplo de interação com a gerência será citado a verificação de alarmes nos elementos de rede e nos links entre os elementos, conforme as imagens na sequência.

Nas Figuras 54 e 55, após clicar com o botão direito do mouse no elemento e clicar em *Current alarms* é aberta a janela de alarmes do elemento:

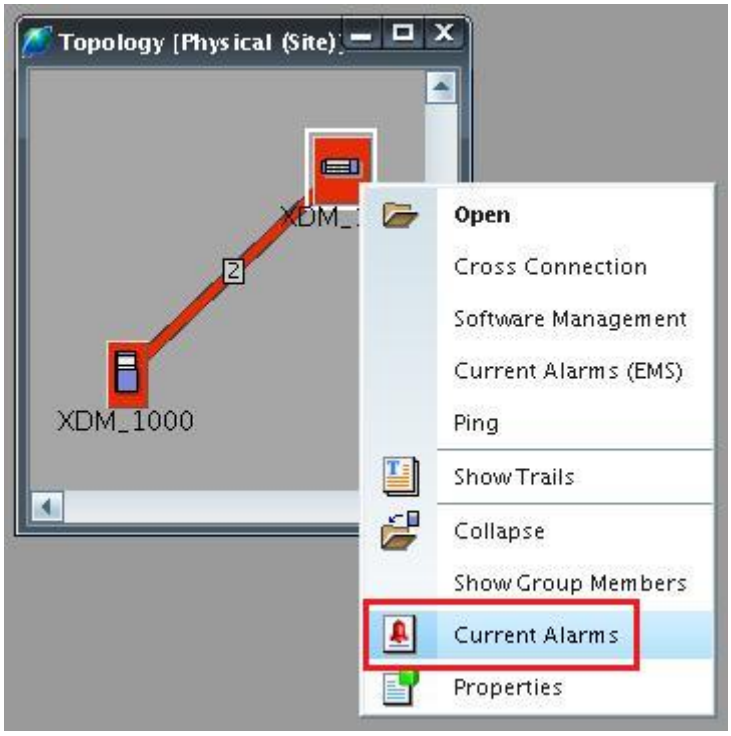


Figura 52 – Abrindo os alarmes do elemento
Fonte: Autoria Própria.

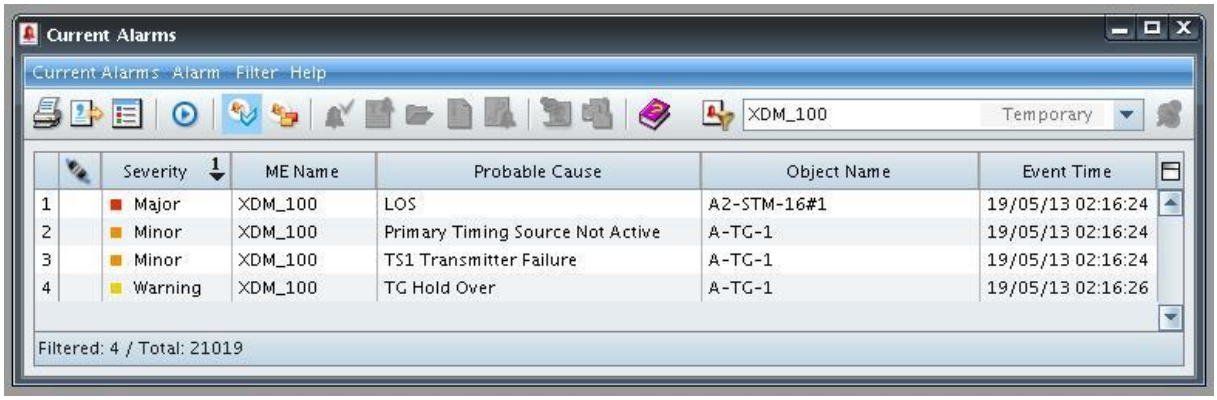


Figura 53 – Visualizando alarmes do elemento
Fonte: Autoria Própria.

Nas Figuras, 56 e 57, após clicar com o botão direito do mouse no link entre os elementos e clicar em *Expand* é aberta janela com as conexões entre os elementos, clicando com o botão direito no link e em seguida em *Current Alarms* é aberta a janela de alarmes do link desejado:

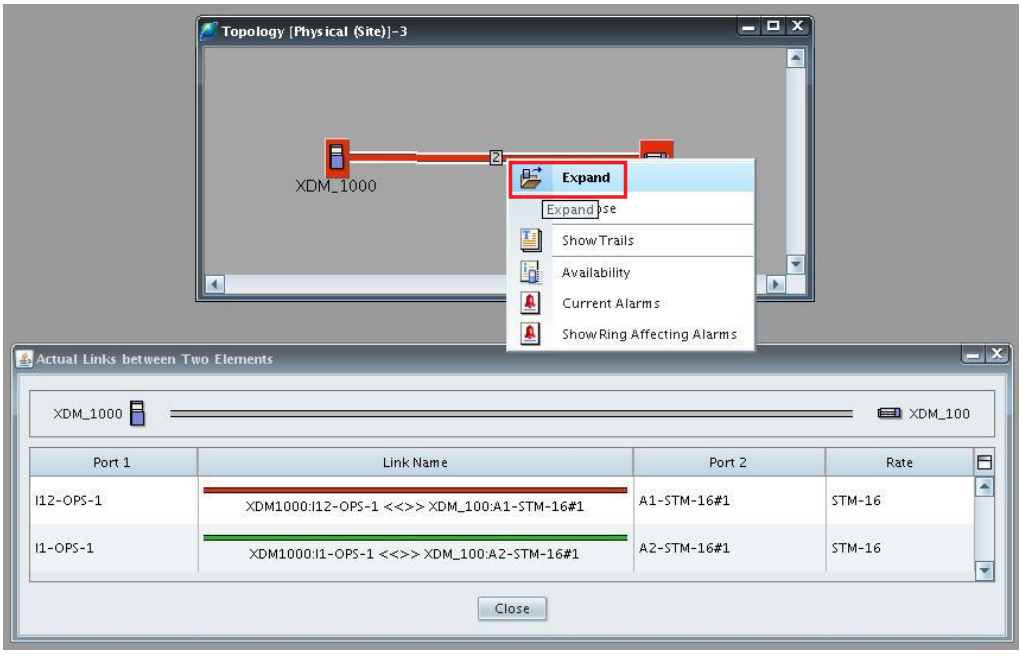


Figura 54 - Abrindo o link
Fonte: Autoria Própria.

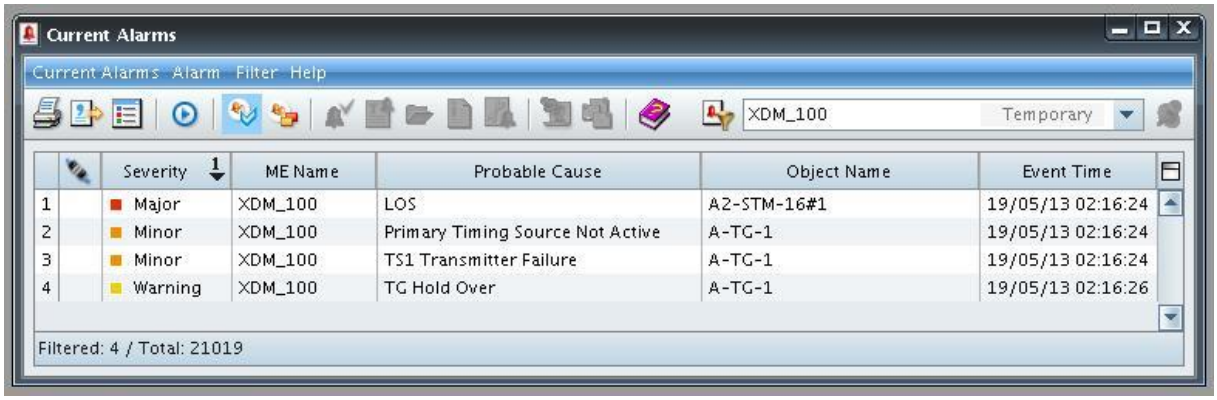


Figura 55 – Visualizando alarmes do link
Fonte: Autoria Própria.

3.5.2 Huawei

O sistema de gerenciamento de rede utilizado pelos equipamentos da Huawei é o Optix iManager T2000, a seguir tem-se a janela principal da gerência, Figura 58, com uma aba dedicada para topologia e outra aba, Figura 59, para alarmes:

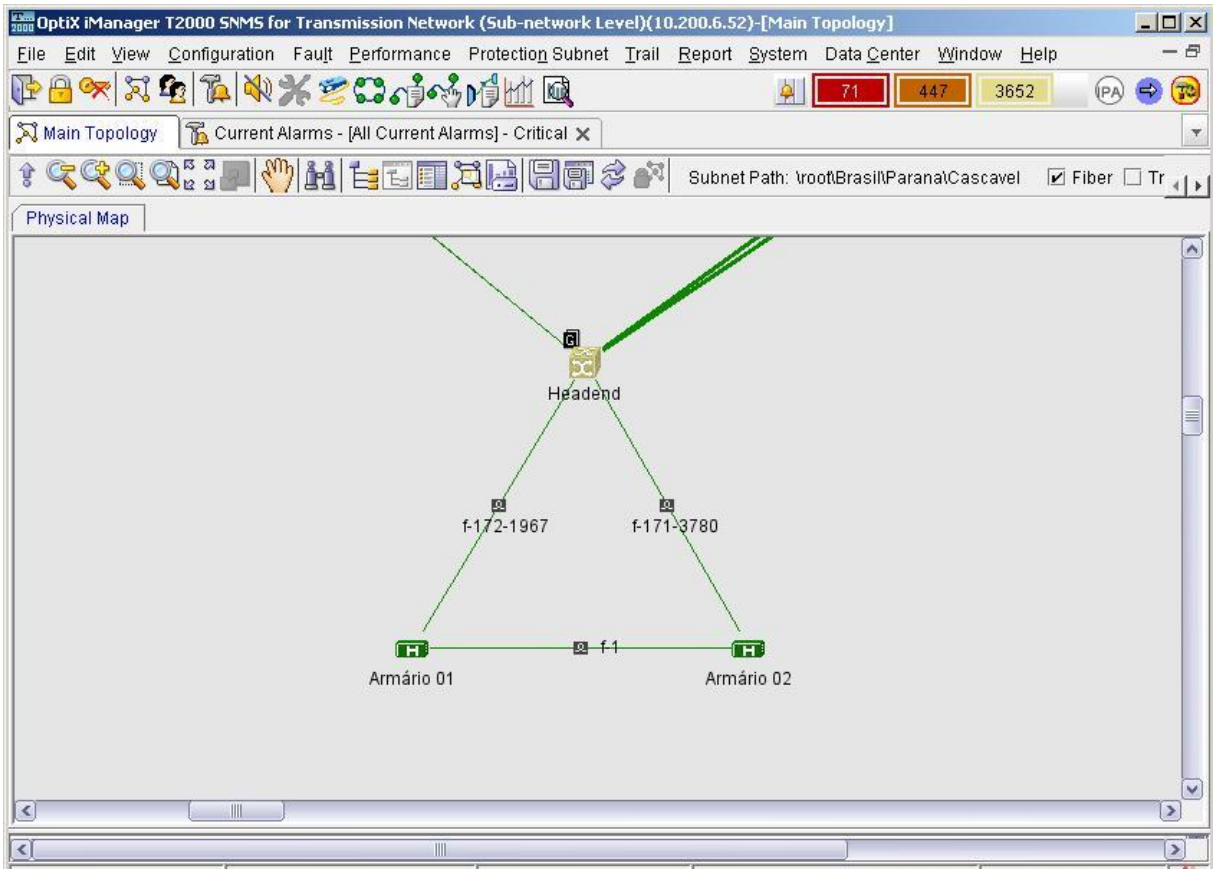


Figura 56 - Gerência Optix iManager T2000
Fonte: Autoria Própria.

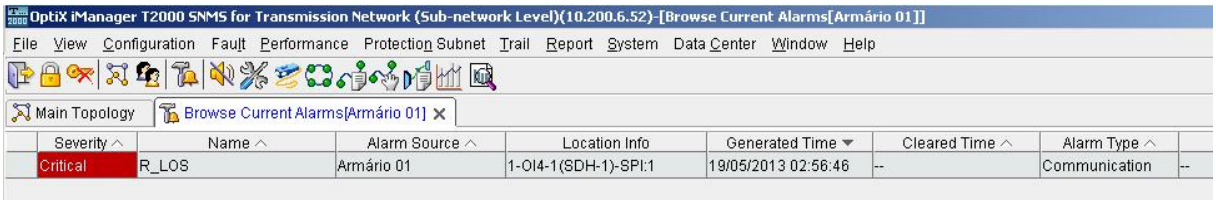


Figura 57 – Aba de alarme
Fonte: Autoria Própria.

Como exemplo de interação com a gerência será citado a verificação de alarmes nos elementos de rede e nos links entre os elementos.

Nas imagens abaixo após clicar com o botão direito do mouse no elemento e clicar na opção *Fault* seguido de *Browse Current alarms* é aberta a janela de alarmes do elemento, Figura 60, e na Figura 61 a visualização do alarme do elemento:

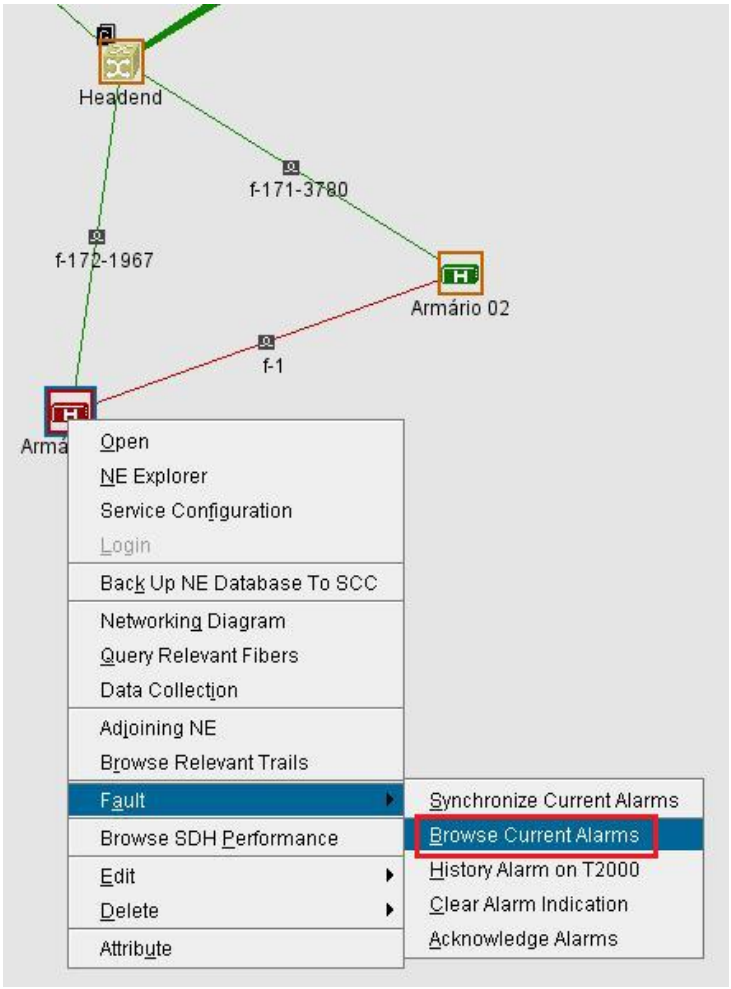


Figura 58 - Abrindo alarmes do elemento
Fonte: Autoria Própria.

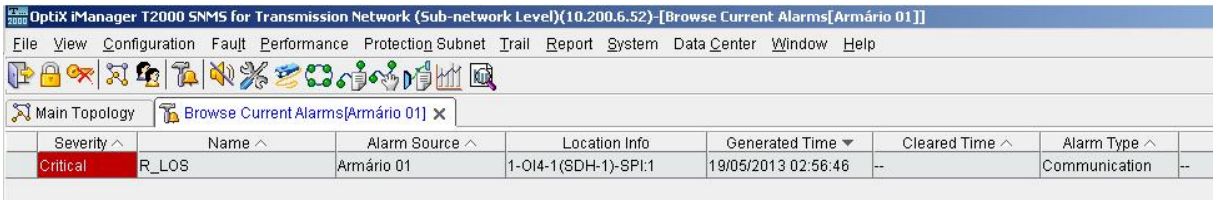


Figura 59 – Visualizando alarmes do elemento
Fonte: Autoria Própria.

Clicando duas vezes no link entre os elementos é aberta uma janela com as conexões entre os elementos e clicando com o botão direito no link e em seguida em *Browse Current Alarms*, Figura 62 , é aberta a janela de alarmes do link desejado, Figuras 63 e 64:

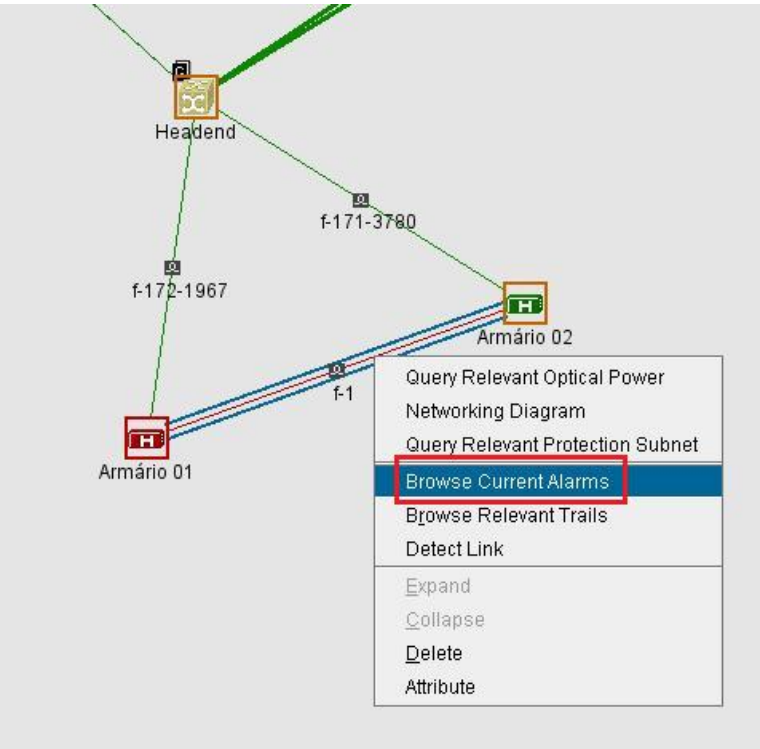


Figura 60 - Abrindo os alarmes do link
Fonte: Autoria Própria.

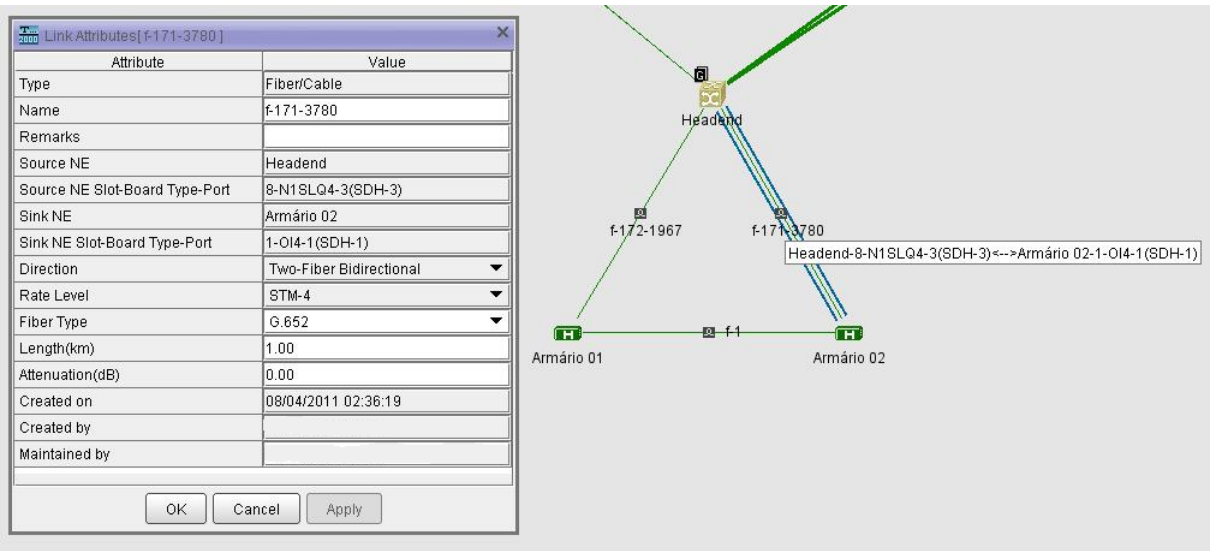


Figura 61 - Verificando o link
Fonte: Autoria Própria.

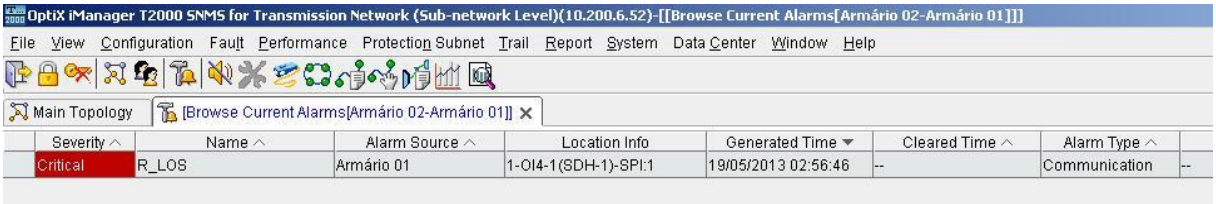


Figura 62 – Visualizando alarmes do link
Fonte: Autoria Própria.

3.5.3 Tellabs

O sistema de gerenciamento de rede utilizado pelos equipamentos da Tellabs é o Tellabs 8000 INM (*Intelligent Network Manager*), Figura 65 que é dividido em opções de construção de rede, criação e gerenciamento de circuitos e serviços, gerenciamento de falhas, monitoramento de performance e gerenciamento de segurança.

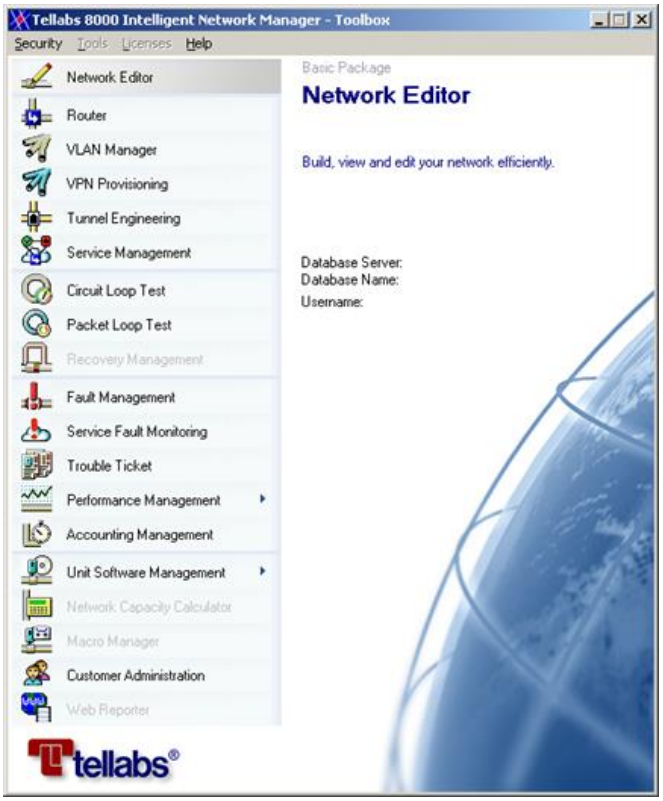


Figura 63 – Gerência Tellabs 8000 INM (Intelligent Network Manager)
Fonte: Autoria Própria.

Na opção *Fault Management,* Figura 66 tem-se as funções de monitoramento de alarmes e falhas, nesta função temos uma janela dedicada para topologia e outra para alarmes, Figura 67:

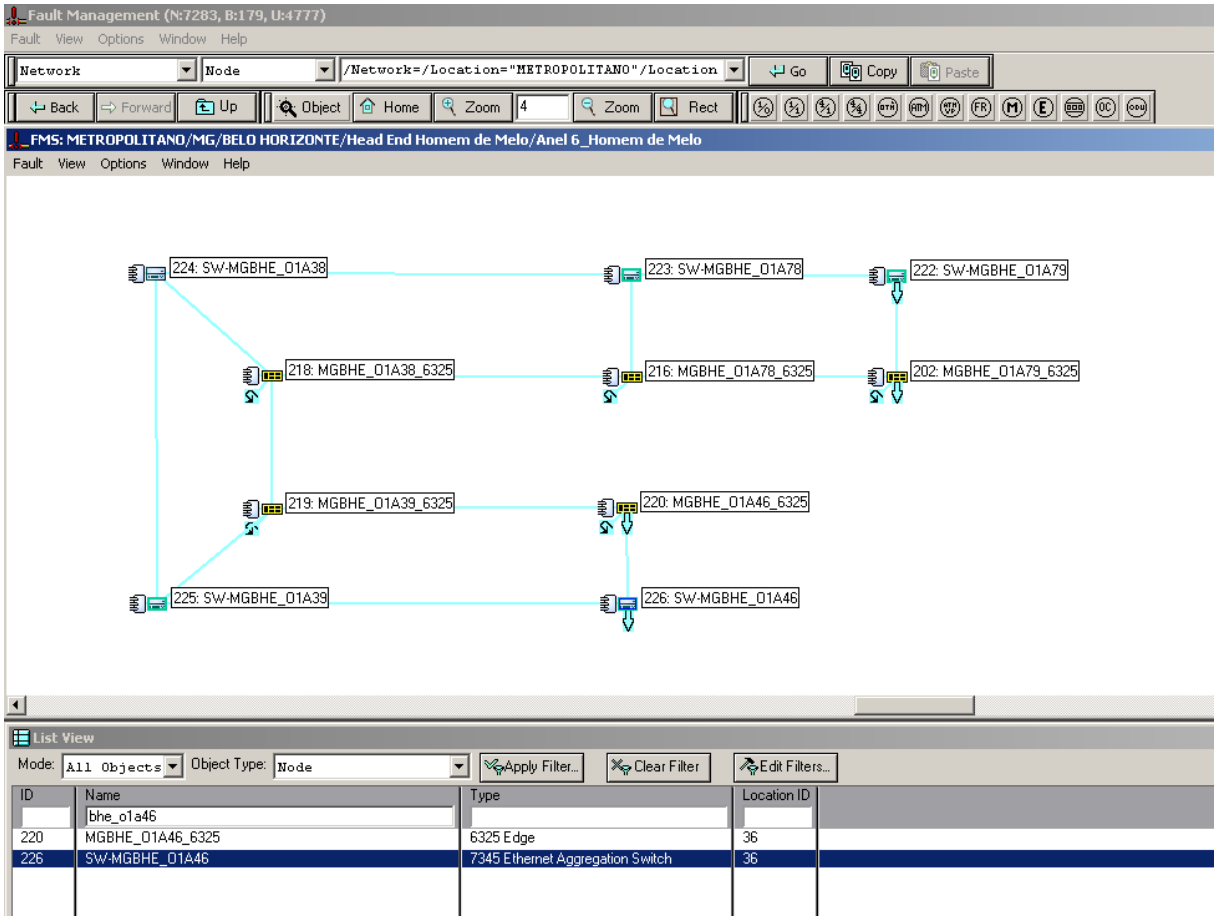


Figura 64 – Fault Management
Fonte: Autoria Própria.

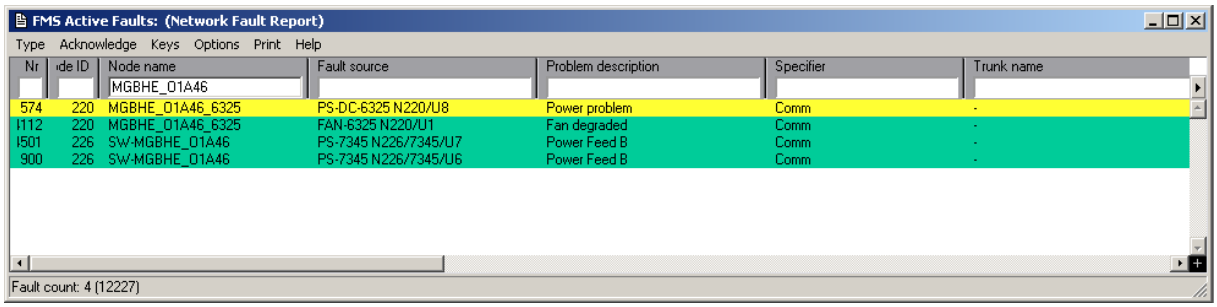


Figura 65 – Janela de alarmes ativos
Fonte: Autoria Própria.

Como exemplo de interação com a gerência será citado a verificação dos elementos de rede e dos links entre eles.

Clicando duas vezes no elemento desejado, Figura 68, é aberta uma janela com as informações das placas utilizadas e da posição do elemento na rede com seus elementos vizinhos, Figura 69:

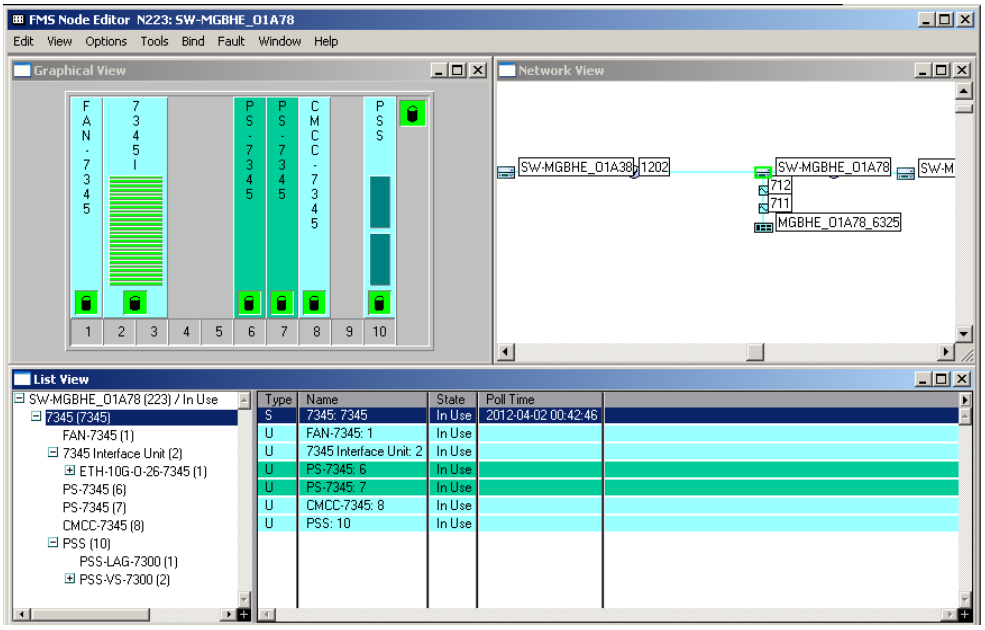


Figura 66 – Verificando o elemento Tellabs 7345
Fonte: Autoria Própria.

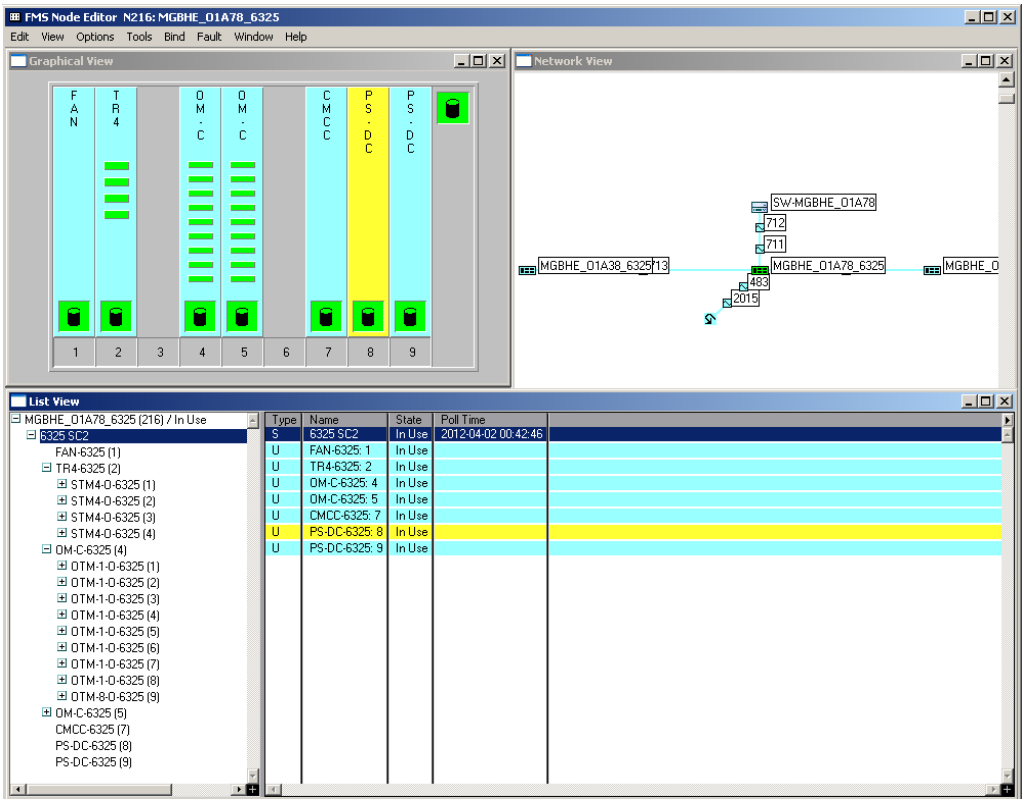


Figura 67 – Verificando o elemento Tellabs 6325
Fonte: Autoria Própria.

Clicando duas vezes no link entre os elementos é possível verificar por quais interfaces estão conectados, Figuras 70 e 71:

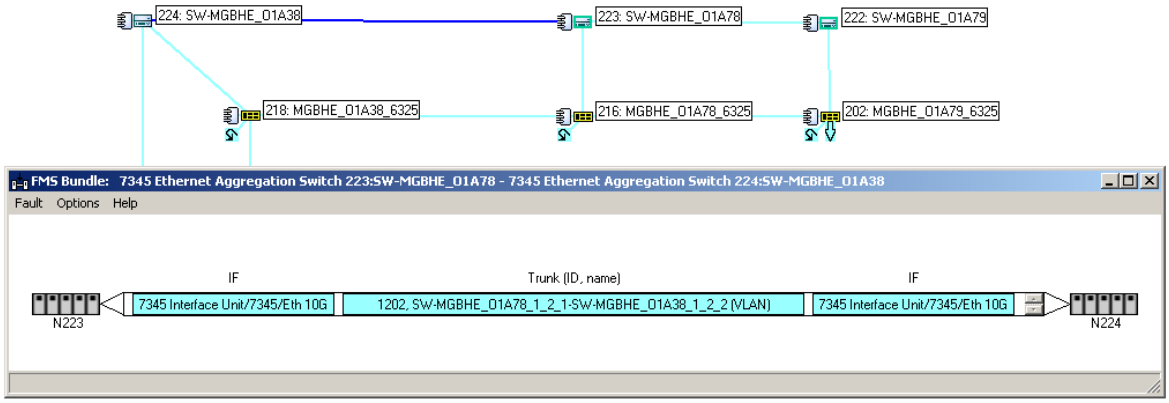


Figura 68 – Verificando os links entre os elementos Tellabs 7345
Fonte: Autoria Própria.

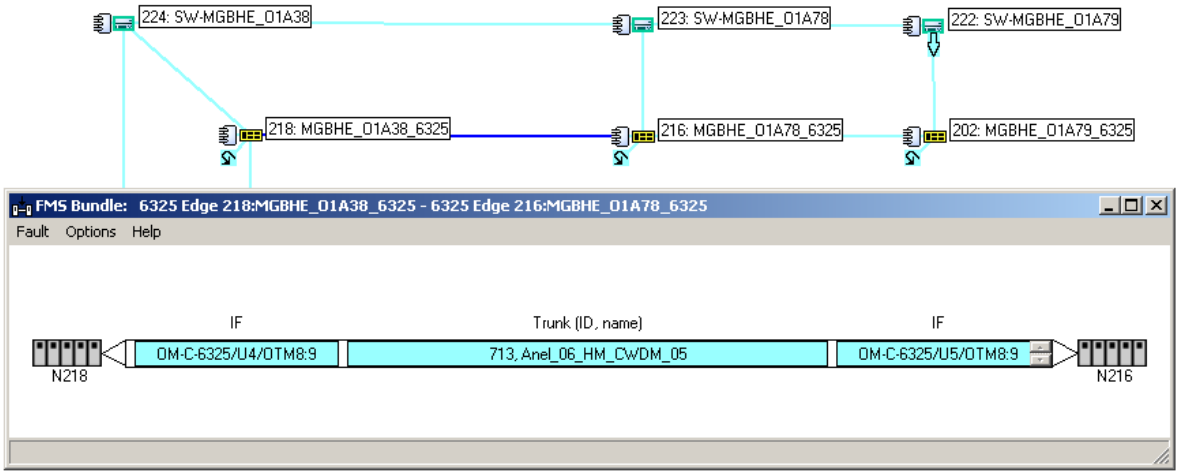


Figura 69– Verificando os links entre os elementos Tellabs 6325
Fonte: Autoria Própria.

3.5.4 Datacom

O sistema de gerenciamento de rede utilizado pelos equipamentos Datacom é o DmView. Na Figura 72 tem-se a janela principal da gerência:

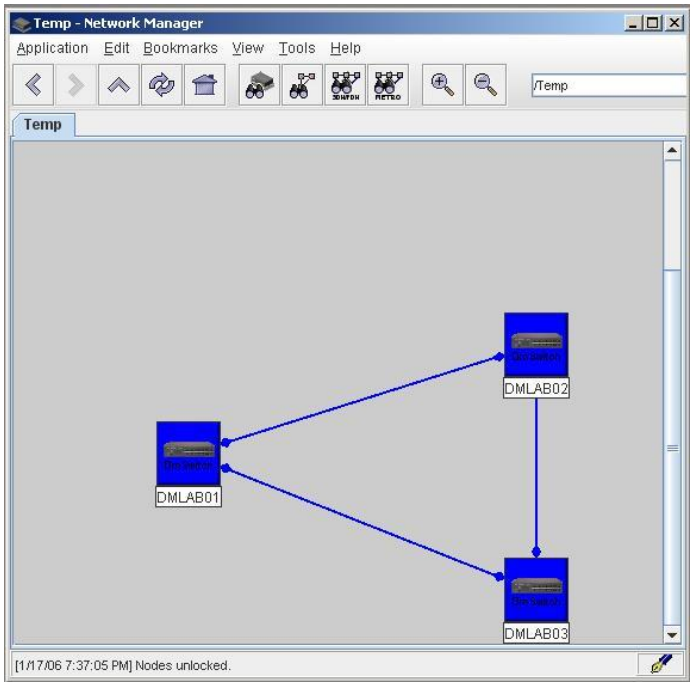


Figura 70 – Gerência DmView
Fonte: Autoria Própria.

Clicando duas vezes no elemento desejado é aberta uma janela com as informações como nome e IP do elemento e interfaces utilizadas, Figura 73:

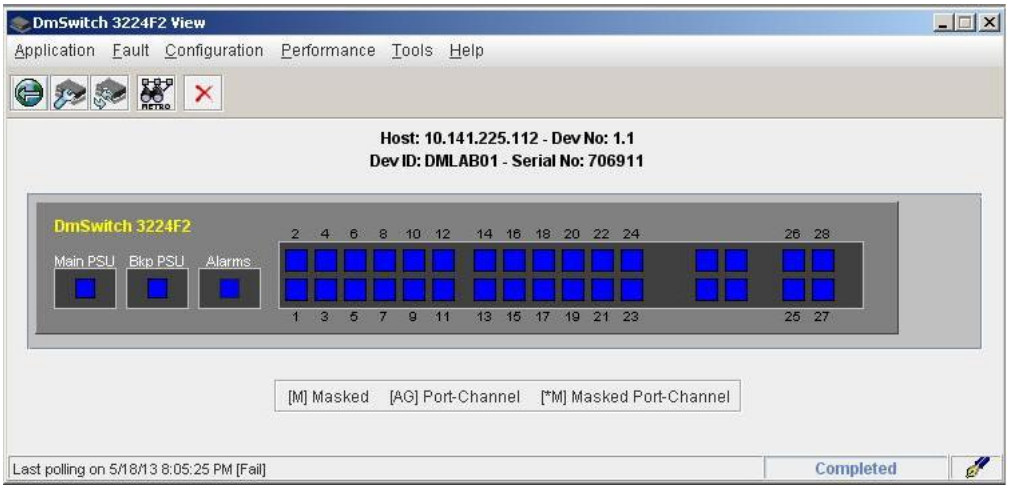


Figura 71 – Verificando o elemento
Fonte: Autoria Própria.

Clicando duas vezes no link entre os elementos é possível verificar por quais interfaces estão conectado, Figura 74:

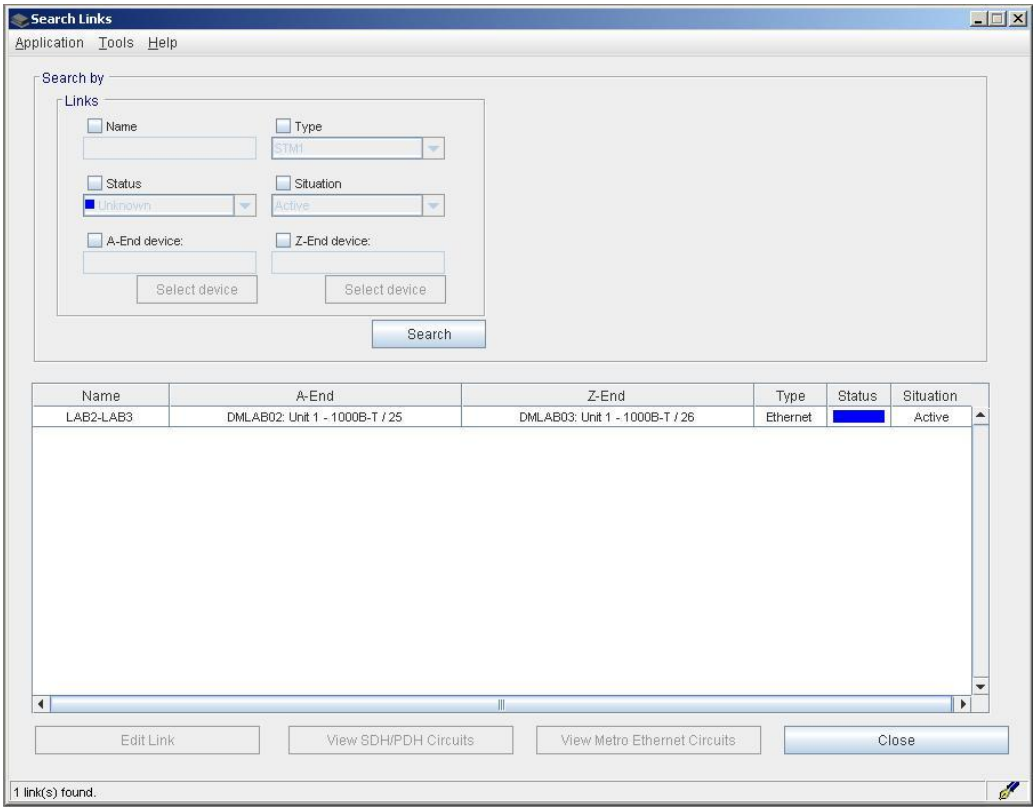


Figura 72 – Verificando os links entre os elementos
Fonte: Autoria Própria.

4 CONCLUSÃO

Durante todo o processo de produção do documento o mesmo foi aplicado no CGR-NOC de uma Operadora de Telecomunicações e foi submetido à análise de colaboradores que já trabalhavam na área, e de colaboradores que acabaram de ingressar no setor, neste processo recebemos várias sugestões, dos colaboradores mais antigos, de vários tópicos que poderiam ser adicionados ao trabalho e identificamos as principais dificuldades dos colaboradores mais novos, melhorando os assuntos abordados. Enfrentamos muitas dificuldades na coleta de informações sobre os equipamentos, pois a maioria dos fabricantes disponibilizam os manuais somente para os seus clientes, neste processo tivemos auxílio da Operadora que disponibilizou os documentos.

Ao concluir o Tutorial o mesmo foi disponibilizado em formato PDF em um servidor de livre acesso a todos os colaboradores do setor, portanto os objetivos propostos foram atingidos uma vez que todas as informações necessárias para a realização de *troubleshooting* foram disponibilizadas em um único documentado de livre acesso a todos os colaboradores do setor.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES-ANATEL. **Serviço de voz sobre IP**. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao&codItemCanal=1216>. Acesso em: 15 mai.. 2013.

ALENCAR, Marcelo Sampaio de. **Telefonia Digital**. São Paulo: Érica, 1998.

AMPERNET. **Telefonia VoIP**. Disponível em: < http://www.ampernet.com.br/telefonia-voip.php>. Acesso em: 15 mai. 2013.

B. FILHO, Huber. **Asynchronous Transfer Mode (ATM).** Teleco Telecomunicações Inteligentes: 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialatm/default.asp>. Acesso em: 20 dez. 2013

BARBARIOLE, Luciana Fontes. **TELEFONIA IP I: Vantagens e Desvantagens do VoIP**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialteliporg1/pagina_4.asp >. Acesso em: 20 mai. 2013.

BERNAL FILHO, Huber. **ADSL2 e ADSL2+: Os novos padrões ADSL**. Disponível em: < http://www.teleco.com.br/tutoriais/tutorialadsl2/pagina_1.asp>. Acesso em: 03 abr. 2013.

BERNAL FILHO[1], Huber. **VDSL e VDLS2: A EVOLUÇÃO DOS PADRÕES xDSL**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvdsl/pagina_3.asp>. Acesso em: 20 abr. 2013.

BEZERRA, Jerônimo A. **Fundamentos de Carrier Ethernet**. Disponível em: <http://www.pop-ba.rnp.br/pub/WTR2012/Programacao/02-WTR2012-CarrierEthernet-Jab.pdf>. Acesso em: 05 abr. 2013.

BOLZANI, Caio A. M. **Residências Inteligentes**. São Paulo: Editora Livraria da Física, 2004.

BRANDINO, Luiz W. **APOSTILA TCP/IP**. 1998. Disponível em: <http://www.wandreson.com/download/training-networking-tcpip.pdf>. Acesso em: 23 abr. 2013.

CARISSIMI, A. da Silva.; ROCHOL, Juergen; GRANVILLE, Lisandro Z. **Redes de computadores: Volume 20 da Série Livros didáticos informática UFRGS**. Porto Alegre: Bookman, 2009.

COMER, Douglas E.; DROMS, Ralph E. **Redes de Computadores e Internet**. Porto Alegre: Bookman, 2007.

CEREDA, Ronaldo Luiz Dias. **ATM o Futuro das Redes**. São Paulo: Makron Books, 1997.

CISCO. **Cisco 7600 Series Routers.** Disponível em: <http://www.cisco.com/en/US/products/hw/routers/ps368/index.html>. Acesso em: 09 dez. 2013.

_____. **Cisco ASR 9000 Series Aggregation Services Routers**. Disponível em <http://www.cisco.com/en/US/products/ps9853/index.html>. Acesso em 09 DEZ. 2013.

DATACOM. **DM3000 - Switch Metro & Enterprise Ethernet Series**. Disponível em: <http://www.datacom.ind.br/new/pt-br/node/940>. Acesso em: 01 fev.2013.

ECI. **XDM-100 – Product Line**, 2006. Acesso Restrito.

ERICSSON, **SmartEdge 1200 - Multi-Service Edge Router (MSER).** Disponível em <http://www.ericsson.com/ourportfolio/products/se1200>. Acesso em: 10 fev. 2013.

FERNANDES, Luiz Felipe de Camargo, **Tutoriais Redes Opticas**. Teleco Inteligência em Telecomunicações: 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialwdm/default.asp>. Acesso em: 12 abr. 2013.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. São Paulo: Bookman, 2004.

FOROUZAN, Behrouz A.; FEGAN, Sophia C. **Protocolo TCP/IP**. 3. Ed. Porto Alegre: AMGH, 2008.

GONÇALVES DA SILVA, Sérgio. **Estudo de Enlace de Transmissão da Tecnologia ADSL**. Disponível em < http://www.teleco.com.br/pdfs/tutorialenlaceadsl.pdf >. Acesso em 15 Jun. 2013.

GONZAGA, Diaulas Hedin. **Interfaces V5**. Teleco Inteligência em Telecomunicações:2004. Disponível em < http://www.teleco.com.br/pdfs/tutorialinterface.pdf>. Acesso em: 03 abr. 2013.

HUAWEI, **C&C08 Switching System**, 2006. Acesso Restrito.

_____. **OptiX OSN 1000 - Hardware Description ISSUE 1.00**, 2005. Acesso Restrito.

_____. **OptiX OSN 2500 - Hardware Description ISSUE 1.30**, 2006. Acesso Restrito.

_____. **OptiX OSN 3500 - Hardware Description ISSUE 1.10**, 2006. Acesso Restrito.

ITU-T G.707/Y.1322, **Recommendation G.707/Y.1322,** Disponível em: <http://www.itu.int/rec/T-REC-G.707-200701-I/en>, Acesso em: 22 mar. 2013.

ITU-T Recommendation, **ITU-T Recommendation series structure.** Disponível em: <http://www.itu.int/en/ITU-T/publications/Pages/structure.aspx>, Acesso em: 22 mar. 2013.

JUNIPER. **Juniper ERX310 Broadband Services Router**. Disponível em: <http://www.juniper.net/br/pt/products-services/routing/e-series/erx310/>. Acesso em: 10 fev. 2013.

_____. **MX960 Universal Edge Router**. Disponível em: <http://www.juniper.net/br/pt/products-services/routing/mx-series/mx960/>. Acesso em: 10 fev. 2013.

KEYMILE. **MileGate 2500/2510 for CO applications**. Disponível em: <http://www.keymile.com/en/products/milegate/milegate_system_family/System_Family.html>. Acesso em: 07 fev. 2013.

MICROSOFT. **O Modelo TCP/IP**. Disponível em: <http://technet.microsoft.com/pt-BR/library/cc786900(v=ws.10).aspx>. Acesso em: 03 abr. 2013.

NASCIMENTO, Marcelo Brenzink do; TAVARES, Alexei Correa. **Tecnologia de Acesso em Telecomunicações**. São Paulo, 2002.

NORTEL. **Nortel Communication Server 1000**, 2008. Acesso Restrito.

_____. **Nortel Switch DMS-100**, 2002. Acesso Restrito.

OLIVEIRA, Júlio César Mondadori de. **MeGaCo: Conheça o protocolo de sinalização de Mídia Gateways VoIP.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmegaco/default.asp>. Acesso em: 5 Ago. 2012.

OLIVEIRA, José Mario Alexandre Melo de.; LINS, Rafael Duarte.; MENDONÇA, Roberto José Lopes. **Redes Mpls- Fundamentos e Aplicações.** São Paulo: Brasport, 2012.

PADTEC. **Descrição dos Produtos da Plataforma LightPad i1600G**, 2010. Acesso Restrito.

PETERS, James. **Fundamentos de VOIP.** Porto Alegre: Artmed, 2008.

PINHEIRO, José Mauricio dos Santos. **Rede Telefônica Comutada**. Projeto de redes: 2005. Disponível em: <http://www.projetoderedes.com.br/tutoriais/tutorial_rede_telefonica_comutada_01.php>. Acesso em: 8 dez. 2012.

PIRES, João J. O. . **Sistemas e Redes de Telecomunicações**. Disponível em: <https://dspace.ist.utl.pt/bitstream/2295/161140/1/SRT_2006.pdf>. Acesso em: 29 abr. 2013.

ROCHA, Adriano Santos. **Estudo Básico do MPLS (Multi Protocol Label Switching).** Disponível em:< http://www.teleco.com.br/tutoriais/tutorialmplseb1/default.asp>. Acesso em: 17 Fev. 2013.

SOARES NETO, Vicente. **Telecomunicações, Redes de Alta Velocidade, Sistemas PDH e SDH**. São Paulo: Érica, 2000.

SOUZA, Wendley. **Protocolos VOIP**. Disponível em:<http://www.brasilescola.com/informatica/protocolos-voip.htm>. Acesso em: 7 Ago. 2013.

TANENBAUM, Andrew S., **Redes de Computadores,** Rio de Janeiro: Campus, 2003.

TELLABS. **Tellabs 6325 Edge Node - Hardware Installation Manual**, 2006. Acesso Restrito.

_____. **Tellabs 7345 Ethernet Aggregation Switch Node - Hardware Installation Manual**, 2011. Acesso Restrito.

_____. **Tellabs 8860 Smart Router - Hardware Installation Manual, 2012**. Acesso Restrito.

TEIXEIRA, Damázio. **ADSL e ADSL2: As Tecnologias da Internet na Telefonia Fixa.** Disponível em: < http://www.teleco.com.br/tutoriais/tutorialadsltec/default.asp>. Acesso em: 26 Out. 2013.

TITTEL, Ed. **Teorias e Problemas de Redes de Computadores**. Porto Alegre: Bookman, 2003.

TRONCO, Tania Regina. **Redes de Nova Geração**. São Paulo: Érica, 2011.

TUDE, Eduardo; B. FILHO, Huber. **MPLS**. Teleco Inteligência em Telecomunicações. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmpls/pagina_3.asp>. Acesso em: 20 jun. 2013.

VALDES, Robert. **Como funciona o VoIP**. Disponível em: <http://informatica.hsw.uol.com.br/voip3.htm>. Acesso em: 20 jun. 2013.

WIKIPÉDIA. **Redes de Telecomunicações**, Disponível em: <http://pt.wikipedia.org/wiki/Rede_de_telecomunica%C3%A7%C3%B5es>. Acesso em 08 dez. 2012.

ZAPPAROLI, Agenor. **Voz sobre IP - VoIP - O Começo**. Disponível em: <http://www.agenorzapparoli.com.br/index.php?p=ahistoria.html>. Acesso em 23 Jun. 2013.

ZHONE. **MALC 319, MALC 719, MALC 723**. Disponível em: <http://www.zhone.com/products/dslam/MALC/>. Acesso em: 07 fev. 2013.

_____. **MXK 319, 819, 823**. Disponível em: <http://www.zhone.com/products/dslam/MXK/>. Acesso em: 07 fev. 2013.

APÊNDICE A - Tutorial de Tratamento de Falhas em Redes de Transmissão

O Tutorial é dividido em duas partes:

- **Lista de Procedimentos**

A lista de procedimentos descreve passo a passo como verificar as informações nos equipamentos e é especifico por fabricante.

Estão descritos:

- Como verificar os parâmetros e configurações dos equipamentos, suas placas e interfaces (óticas e elétricas);
- Verificação, alteração, exclusão, criação e testes de serviços;

- **Tratamento de falhas**

Em tratamento de falhas estão descritos passo a passo os procedimentos de análise, detecção e correção de falhas. Estão descritos de forma genérica para que sejam utilizados para qualquer equipamento.

Foi subdividido por tipos de falhas:

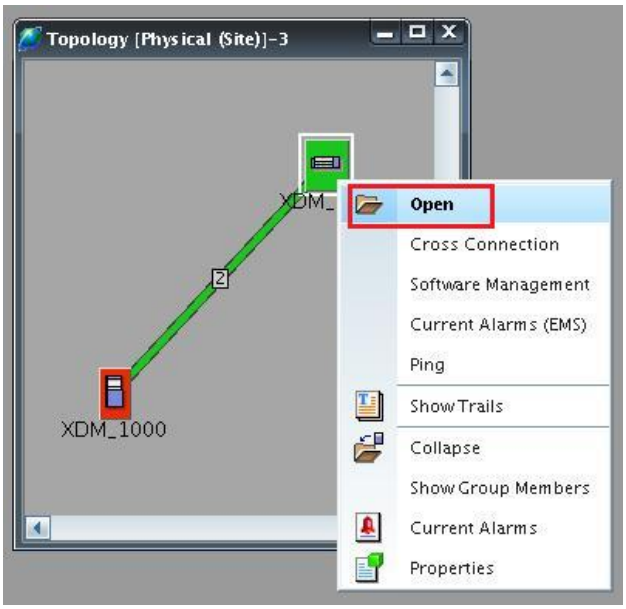
- Falhas de Transmissão;
- Falhas de Equipamentos;
- Falha de Gerência;
- Falha de Temporização e Sincronismo;
- Falhas de serviços.

LISTA DE PROCEDIMENTOS

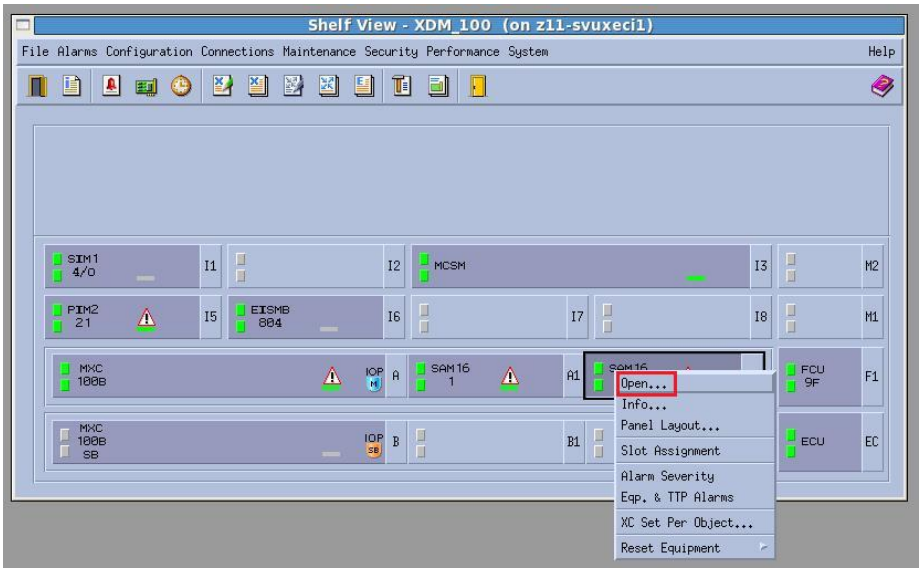
Procedimento de verificação de potência ótica nos equipamentos

- ECI

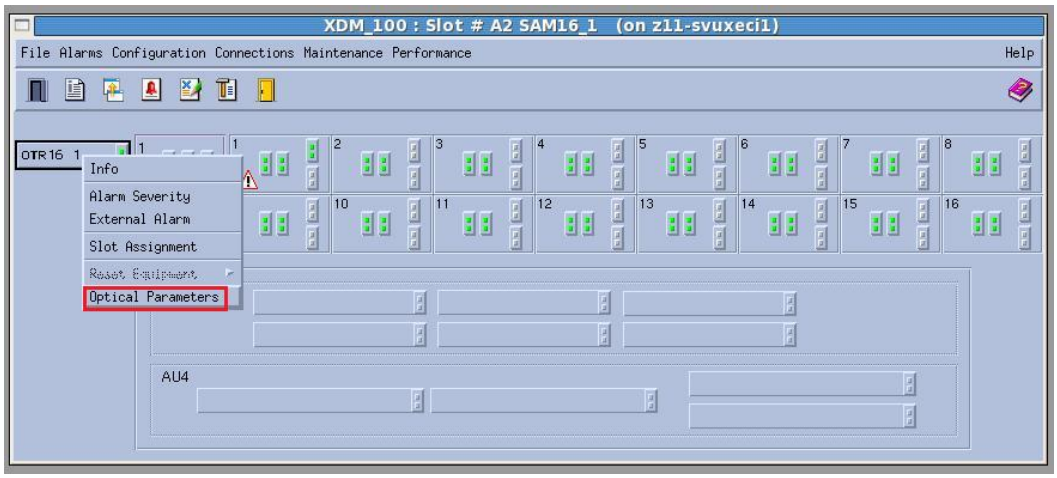
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open conforme a seguir:



2° Passo: Após abrir o elemento selecione a placa que deseja verificar, clique com o botão direito do mouse e em seguida selecione a opção Open:



3° Passo: Após abrir a placa selecione a interface ótica SFP, clique com o botão direito do mouse e em seguida selecione a opção Optical Parameters:

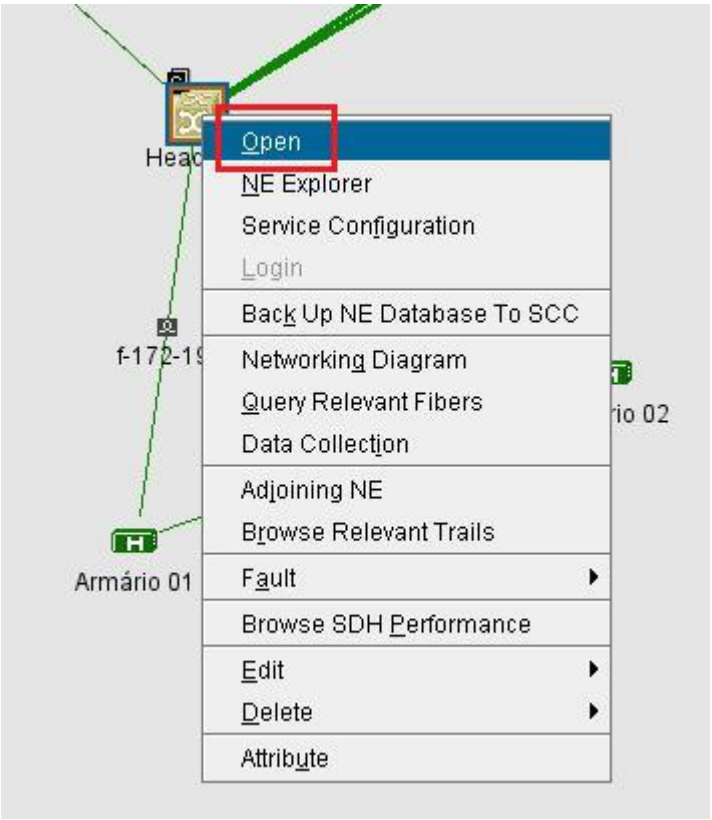


4° Passo: Abrirá uma janela com as informações de potências de RX e de TX, corrente consumida e temperatura do laser.

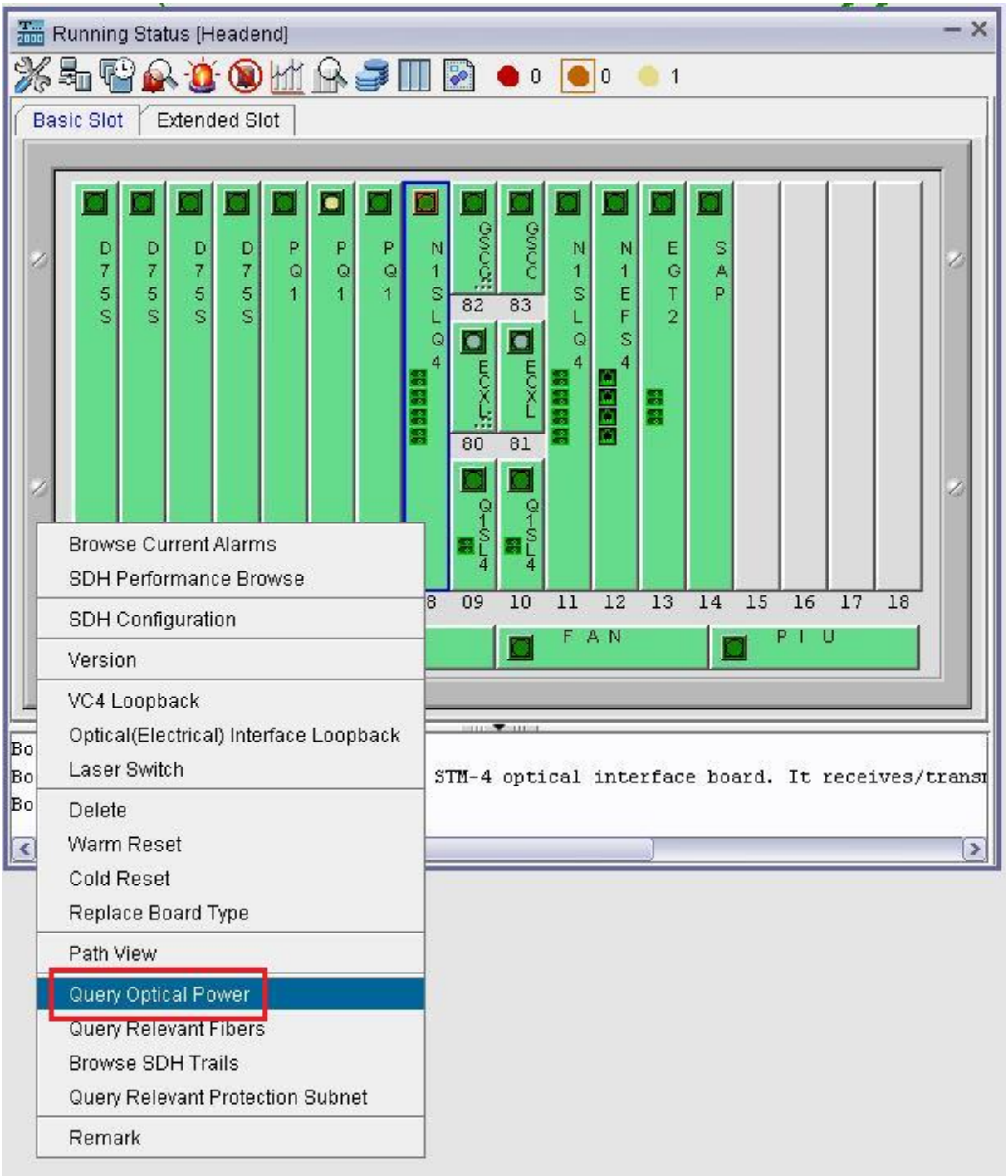
Há também as informações de limiares de potências máximas e mínimas de TX e RX, históricos máximos e mínimos de potências de RX e de TX, corrente consumida e temperatura do laser.

- Huawei

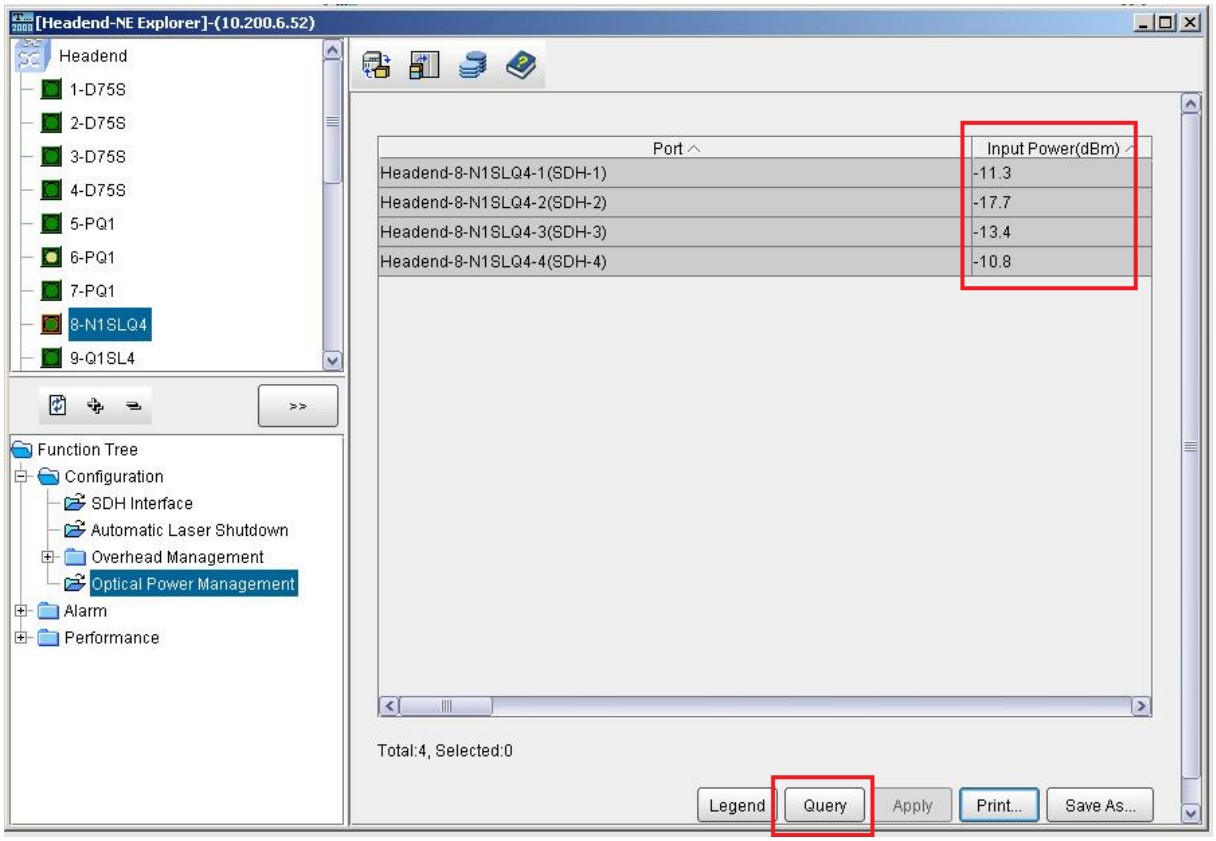
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



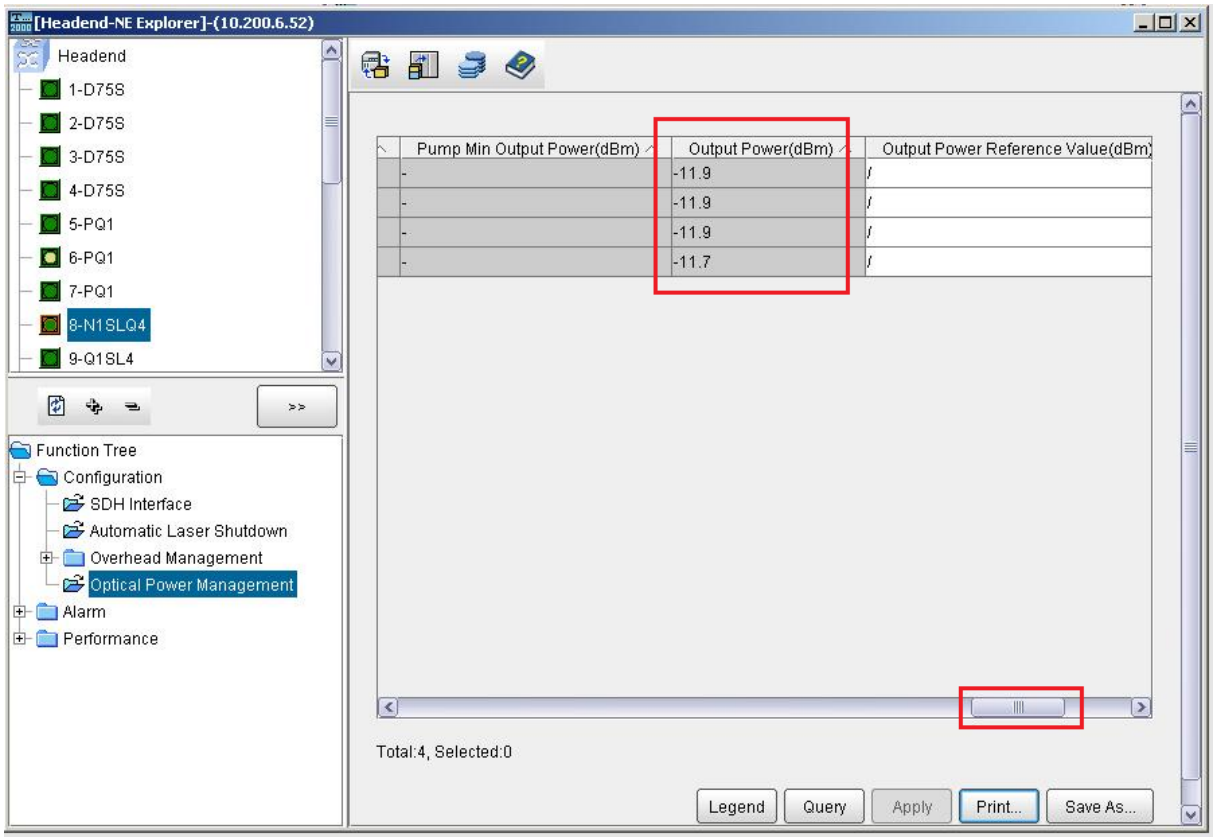
2° Passo: Após abrir o elemento selecione a placa que deseja verificar, clique com o botão direito do mouse e em seguida selecione a opção Query Optical Power:



3° Passo: Abrirá uma janela com as informações de potências de Input Power (RX) e de Output Power (TX). Clique no botão Query para atualizar as informações:



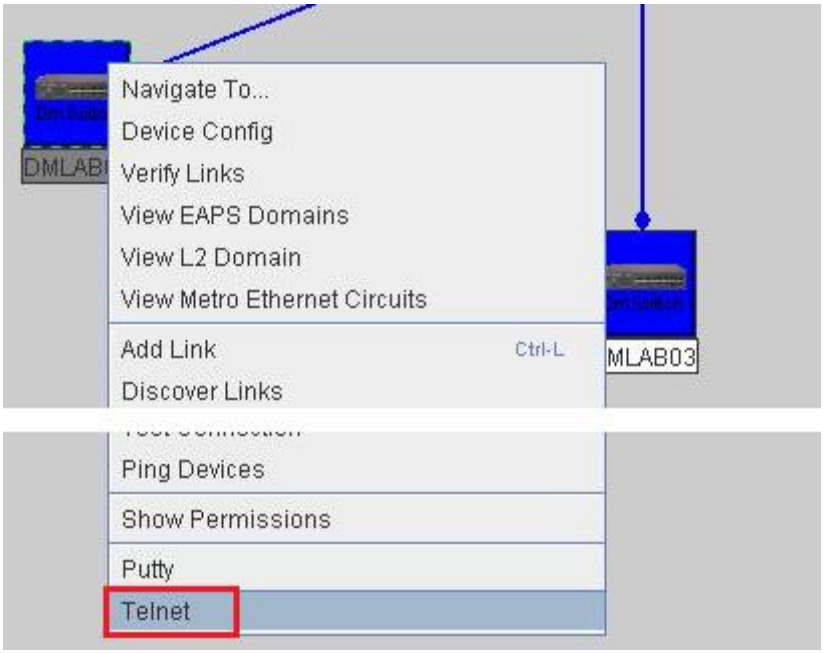
Deslize a barra até localizar as informações de TX:



- Datacom

O Datacom DM3000 não possui leitura de potência ótica, porém podemos verificar o status dos links.

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Telnet:

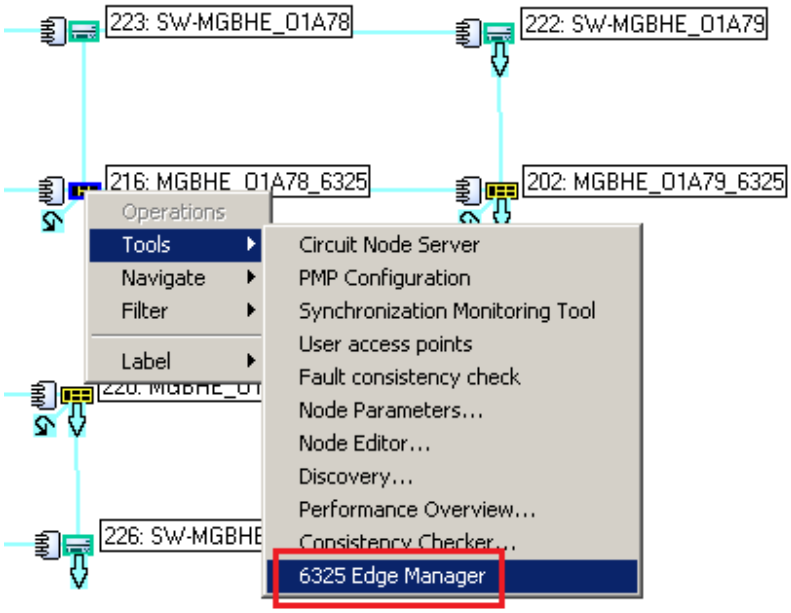


2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. execute o comando “show interfaces table configuration”, aparecerão as informações de estado das portas, status dos links e configurações de auto-negociação, capacidade e modo de taxa da interface:

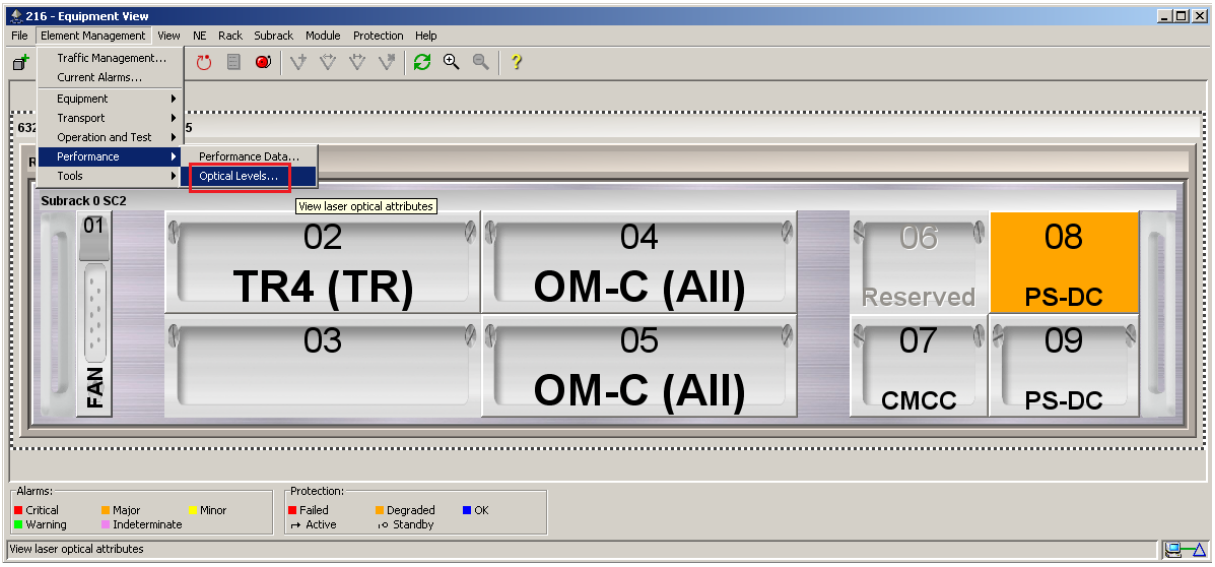
```
DMLAB01#show interfaces table configuration

                Port    Link   Auto       Speed       Duplex     Flow
 Port           State   Status Neg     Cfg  Actual  Cfg  Actual  Ctrl    Pvid
================================================================================
 1/ 1           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 2           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 3           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 4           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 5           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 6           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 7           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 8           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/ 9           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/10           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/11           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/12           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/13           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/14           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/15           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/16           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/17           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/18           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/19           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/20           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/21           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/22           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/23           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
 1/24 D2BH      ENABLE  UP     ON      100  100     AUTO FULL    NONE    698
 1/25 RT:M      ENABLE  UP     ON      100  1000    AUTO FULL    NONE    1
 1/26 RT:M      ENABLE  UP     ON      100  1000    AUTO FULL    NONE    1
 1/27 D2BH      ENABLE  UP     ON      100  1000    AUTO FULL    NONE    1
 1/28           DISABLE DOWN   ON      100          AUTO HALF    NONE    1
================================================================================
                    spacebar->toggle screen  ESC->exit
DMLAB01#
```

- Tellabs 6325 Edge Node

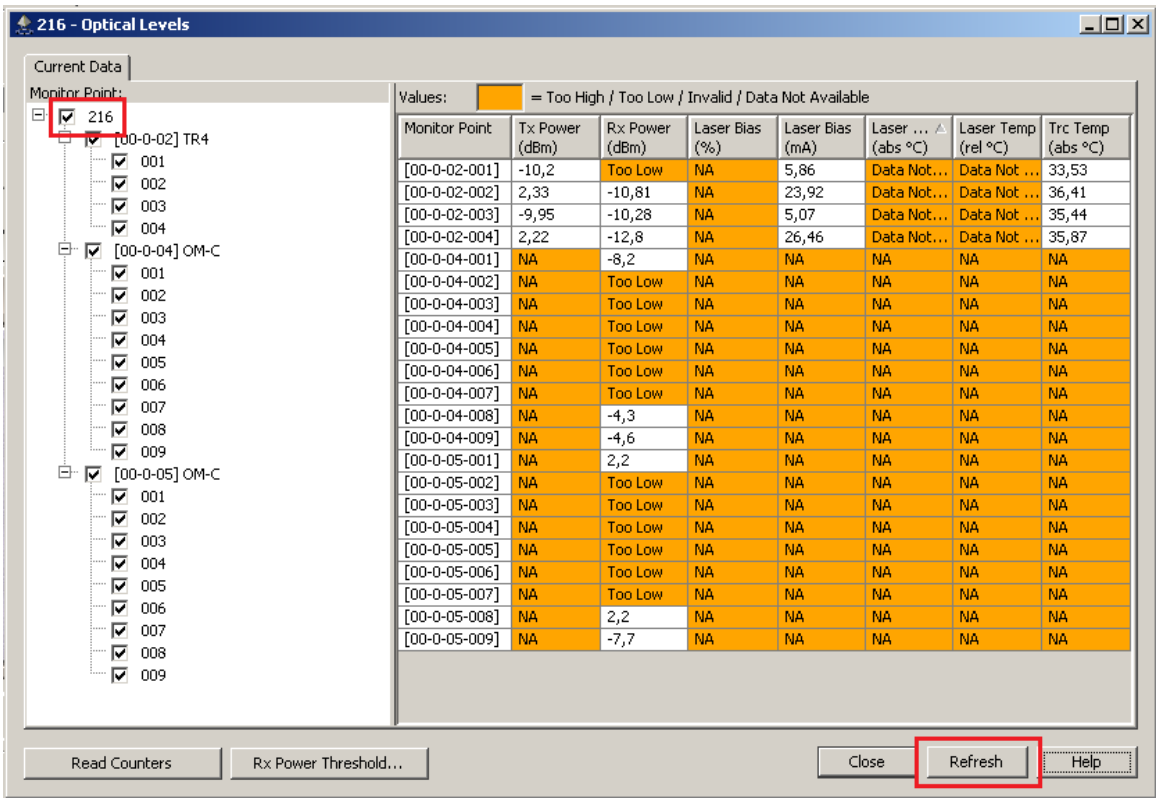
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e 6325 Edge Manager:



2° Passo: Após abrir o elemento selecione as opções Element Management, seguido de Performance e Optical Levels:

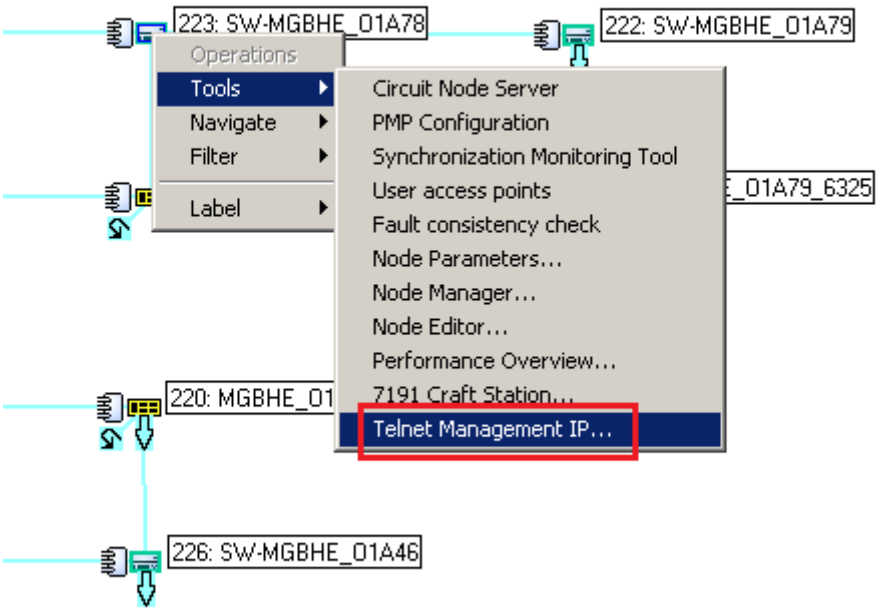


3° Passo: Após abrir a janela as informações de potências de RX e de TX, corrente consumida e temperatura do módulo, selecione o primeiro botão no canto superior esquerdo em seguida clique no botão Refresh para atualizar as informações:



- Tellabs 7345 Switch Agregação Ethernet

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e Telnet Management IP:



2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. execute o comando “show interface transceiver”, aparecerão as informações de potências de RX e de TX, tensão e corrente consumida e temperatura do módulo:

t7300-SW-MGBHE_O1A78# show interface transceiver

Port	TX Power (dBm)	RX Power (dBm)	Supply Voltage (V)	Temp (C)	Bias Current (mA)
Xg1/2/1	2.09	-13.02	3.291	40	81776
Xg1/2/2	1.59	-15.83	3.283	41	89136
Gi1/2/3	-5.62	-6.63	3.298	28	2873
Gi1/2/4	-5.51	-6.53	3.299	28	3148
Gi1/2/5	-5.55	-5.18	3.299	34	3396
Gi1/2/6	-5.55	-5.32	3.294	36	3090
Gi1/2/7	-99.00	-33.98	3.304	26	317
Gi1/2/8	-99.00	-40.00	3.273	33	112
Gi1/2/9	-99.00	-99.00	3.322	33	239
Gi1/2/10	-99.00	-99.00	3.300	25	0
Gi1/2/24	-99.00	-30.97	3.322	31	314

```
Gi1/2/25 -99.00     -99.00     3.300          25         0
Gi1/2/26 -99.00     -99.00     3.300          25         0

Serial0 up, 8 data bits, no parity, 38400 baud
```

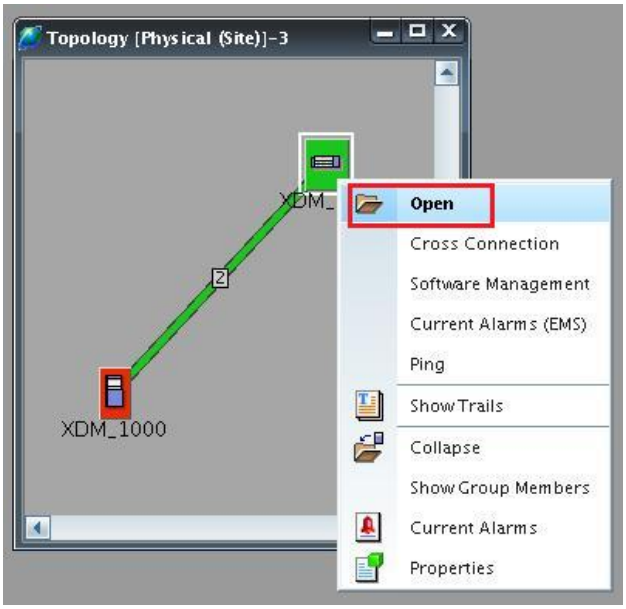
3° Passo: Execute o comando “show interface description”, aparecerão as informações de status administrativo e status operacional das interfaces, função ALS e status do laser:

```
t7300-SW-MGBHE_O1A78# show interface description

Interface    Admin    Oper              ALS Admin      Laser
                      Status   Status          State          Status
---------      ------   ------          ---------      --------
Xg1/2/1      up         up              disabled       disabled
Xg1/2/2      up         up              disabled       disabled
Gi1/2/3      up         up              disabled       disabled
Gi1/2/4      up         up              disabled       disabled
Gi1/2/5      up         up              disabled       disabled
Gi1/2/6      up         up              disabled       disabled
Gi1/2/7      down     down            disabled       disabled
Gi1/2/8      down     down            disabled       disabled
Gi1/2/9      down     down            disabled       disabled
Gi1/2/10     down     down          disabled       disabled
Gi1/2/24     down     down            disabled       disabled
Gi1/2/25     up         up              disabled       disabled
Gi1/2/26     up       down            disabled       disabled
cpu0         up        down            disabled       disabled
vlan697      up         up              disabled       disabled

 Serial0 up, 8 data bits, no parity, 38400 baud
```

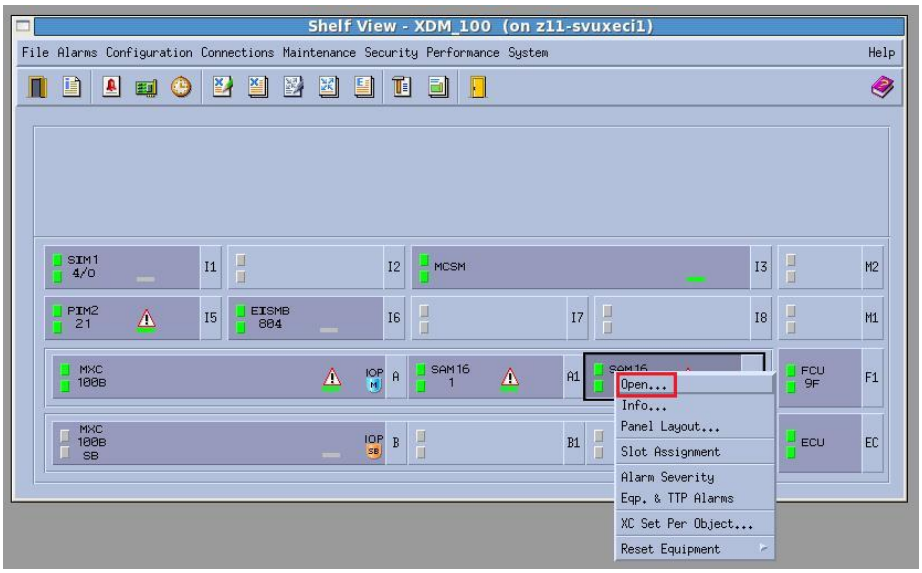
Procedimento de verificação de taxa de erro nos equipamentos

- ECI

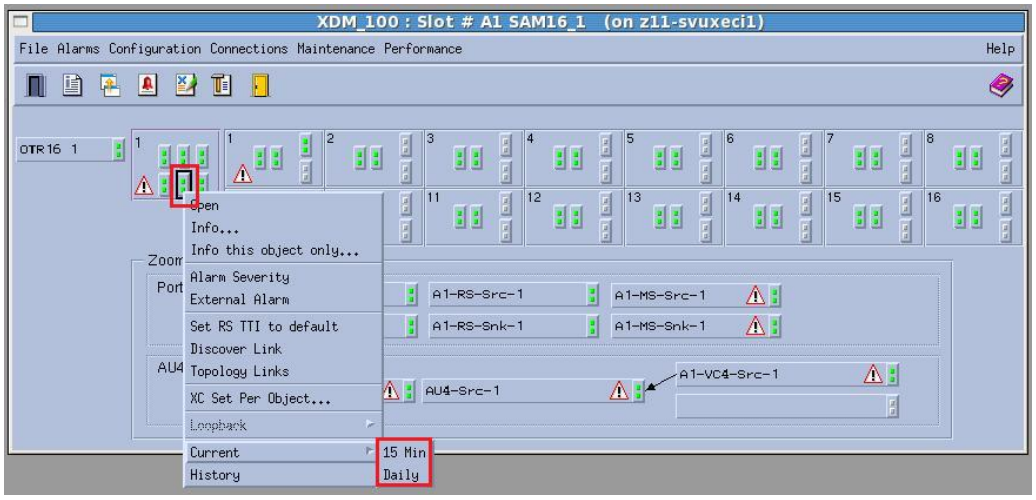
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



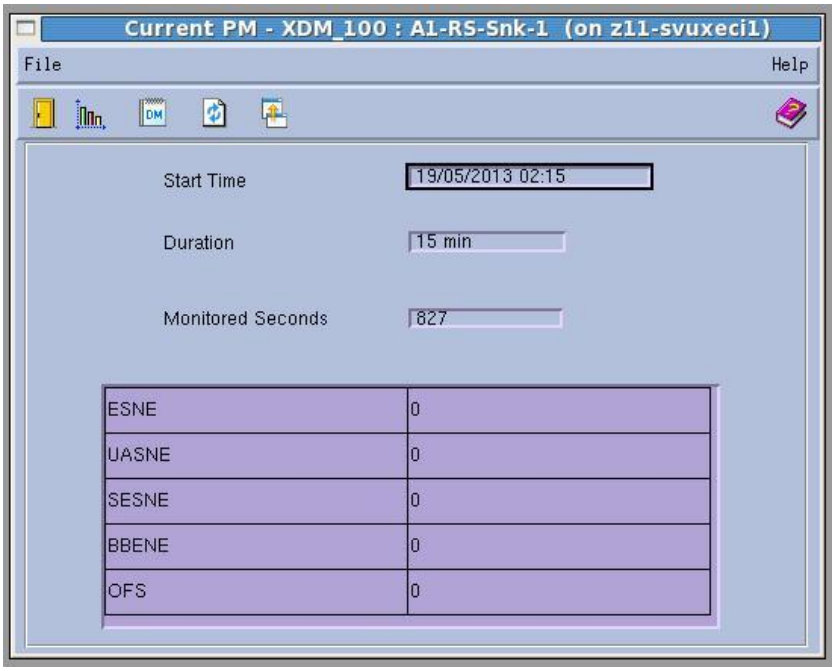
2° Passo: Após abrir o elemento selecione a placa que deseja verificar, clique com o botão direito do mouse e em seguida selecione a opção Open:



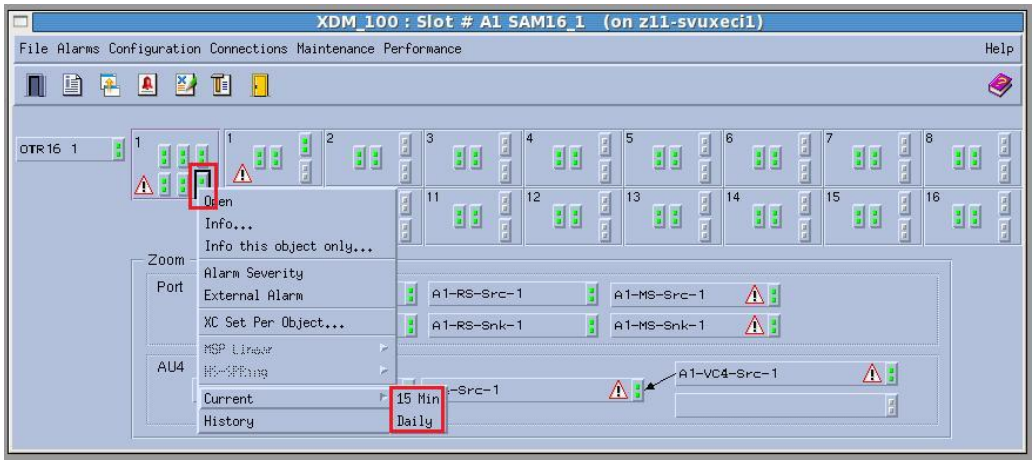
3° Passo: Após abrir a placa selecione penúltimo botão que está marcado conforme abaixo para verificar a seção de regeneração (RS), clique com o botão direito do mouse, selecione a opção Current e em seguida selecione a opção 15 Min ou Daily para as últimas 24 horas:



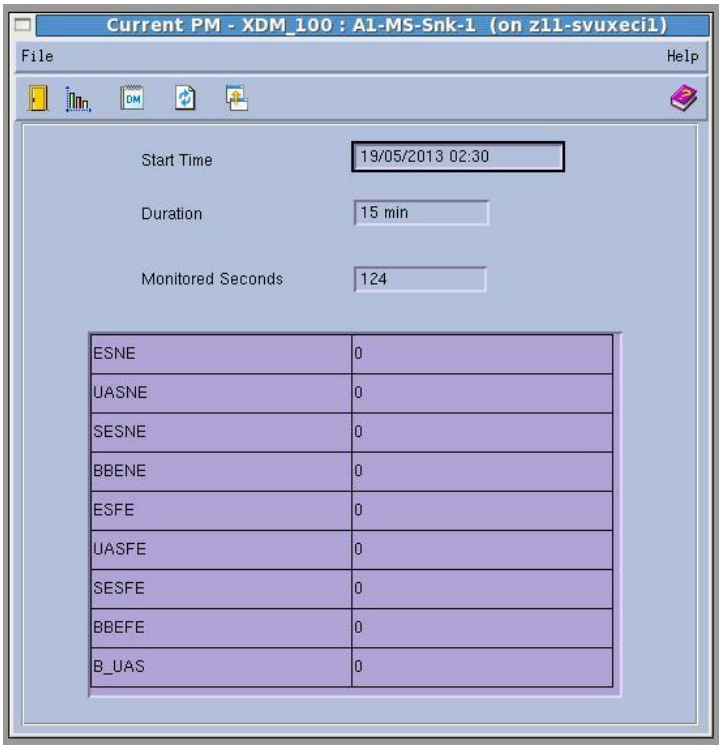
Abrirá uma janela conforme abaixo, se os valores estiverem zerados significa que a interface esta sem taxa de erro:



3° Passo: Após abrir a placa selecione o último botão que está marcado conforme abaixo para verificar a seção de multiplexação (MS), clique com o botão direito do mouse, selecione a opção Current e em seguida selecione a opção 15 Min ou Daily para as últimas 24 horas:

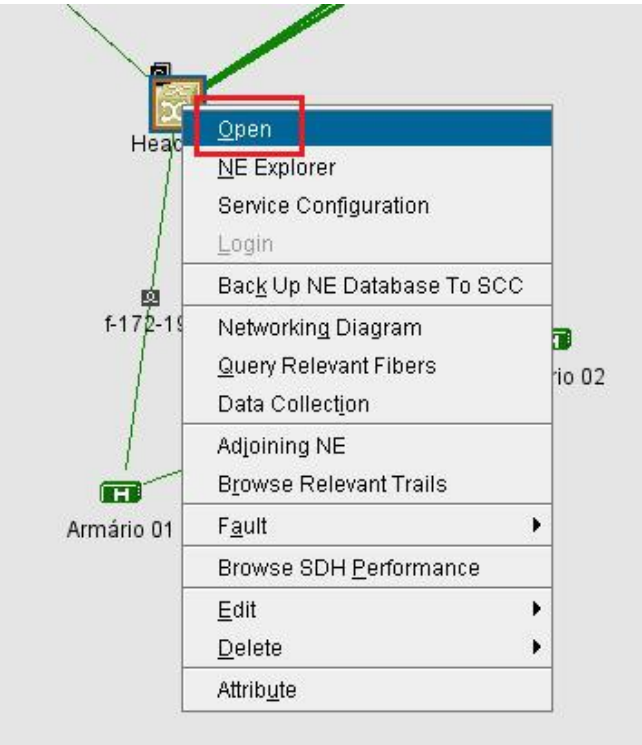


Abrirá uma janela conforme abaixo, se os valores estiverem zerados significa que a interface esta sem taxa de erro:

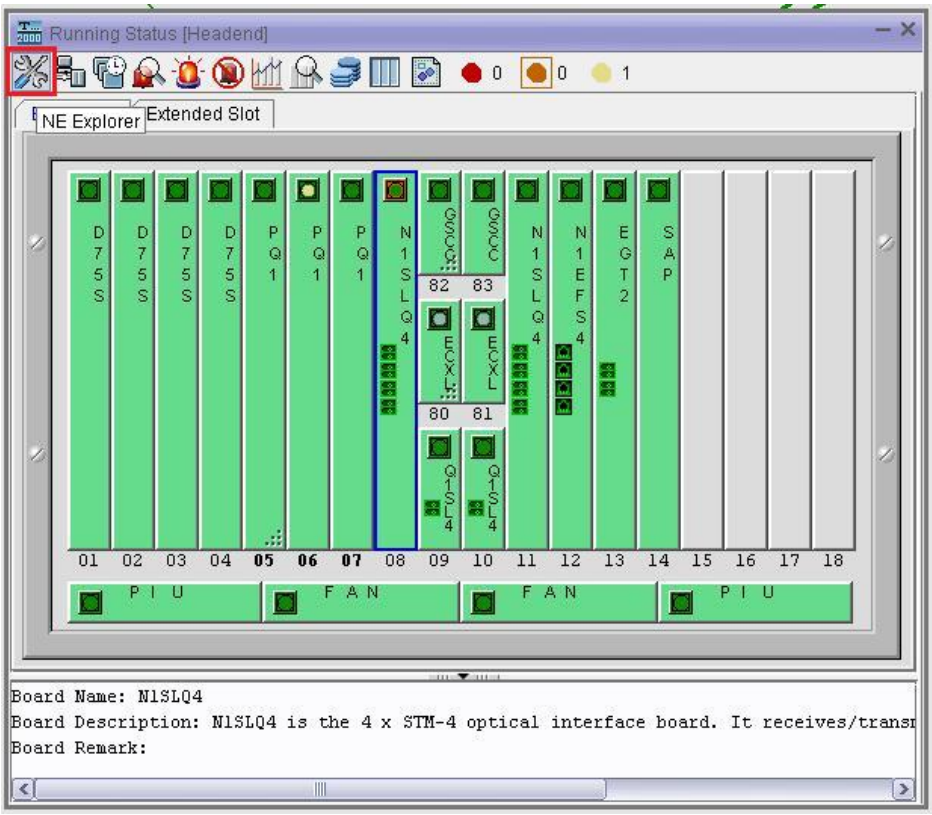


- Huawei

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:

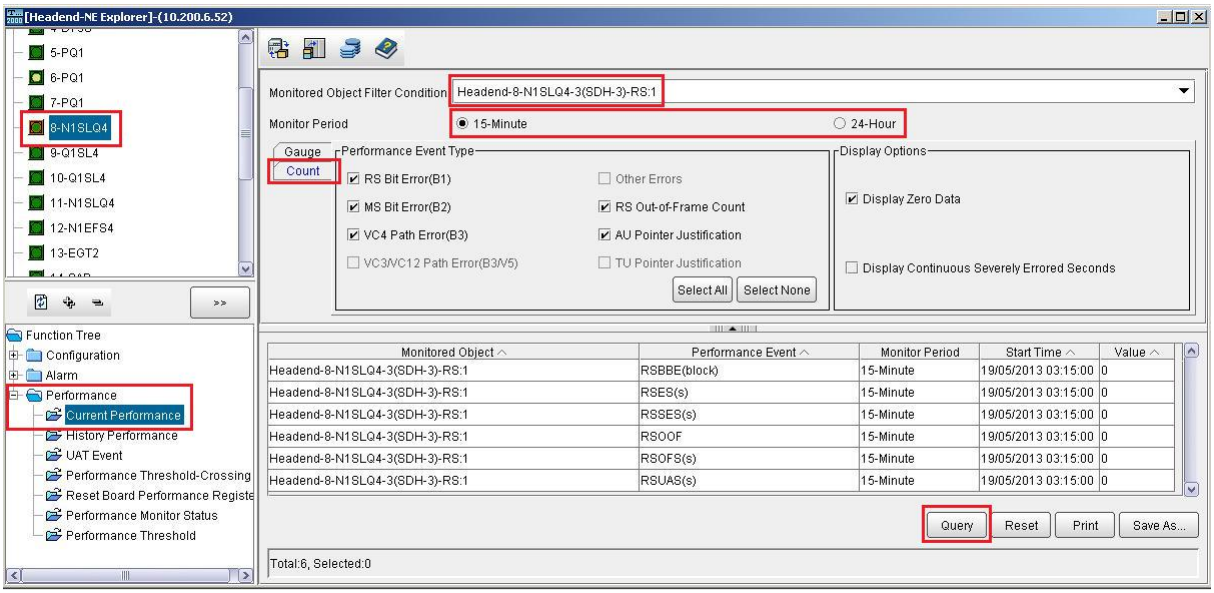


2° Passo: Após abrir o elemento clique no botão NE Explorer no canto superior esquerdo:

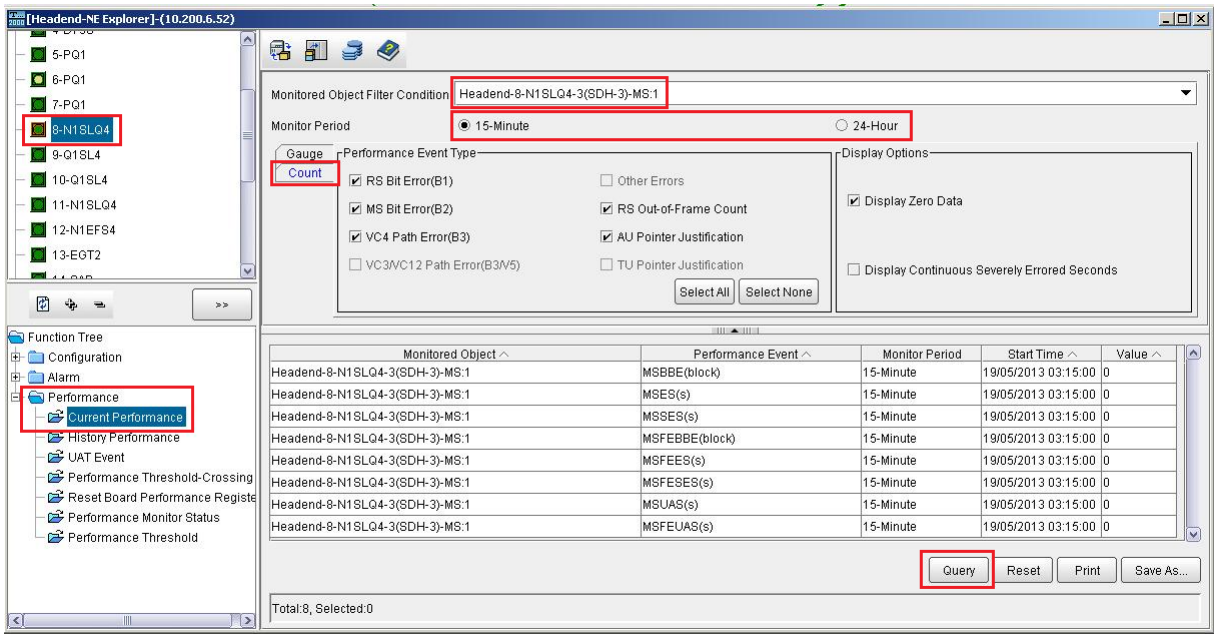


3° Passo: Após abrir a janela selecione no campo superior esquerdo a placa desejada, em seguida no campo inferior esquerdo as opções Performance e Current

Performance. Na mesma janela em Monitored Object Filter Condiction selecione a opção RS para verificar a seção de regeneração, em Monitor Period selecione 15-Minute ou 24-Hour, logo abaixo selecione a aba Count e finalmente o botão Query para atualizar os valores, se os contadores estiverem zerados significa que a interface esta sem taxa de erro:

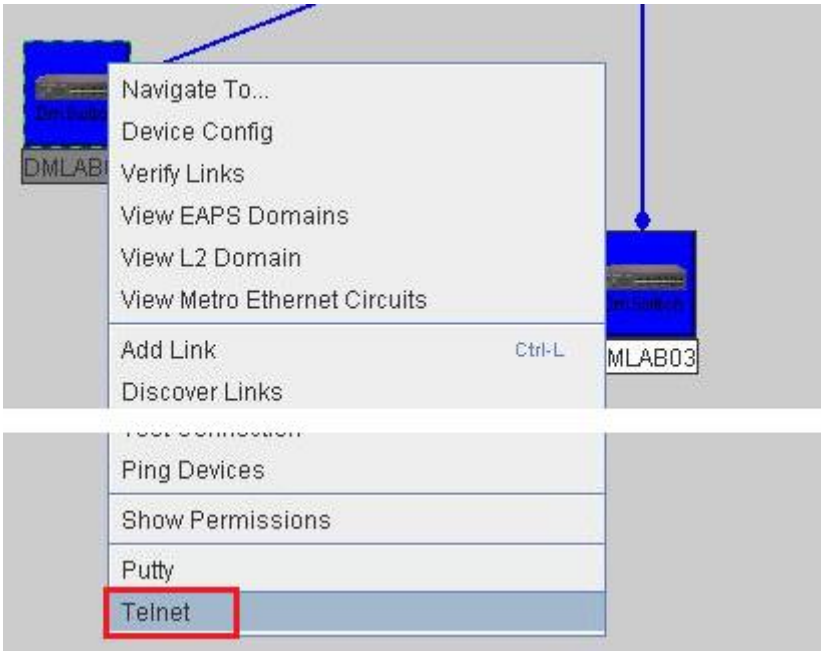


4° Passo: Após abrir a janela selecione no campo superior esquerdo a placa desejada, em seguida no campo inferior esquerdo as opções Performance e Current Performance. Na mesma janela em Monitored Object Filter Condiction selecione a opção MS para verificar a seção de multiplexação, em Monitor Period selecione 15-Minute ou 24-Hour, logo abaixo selecione o botão Count e finalmente o botão Query para atualizar os valores, se os contadores estiverem zerados significa que a interface esta sem taxa de erro:



- Datacom

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Telnet:



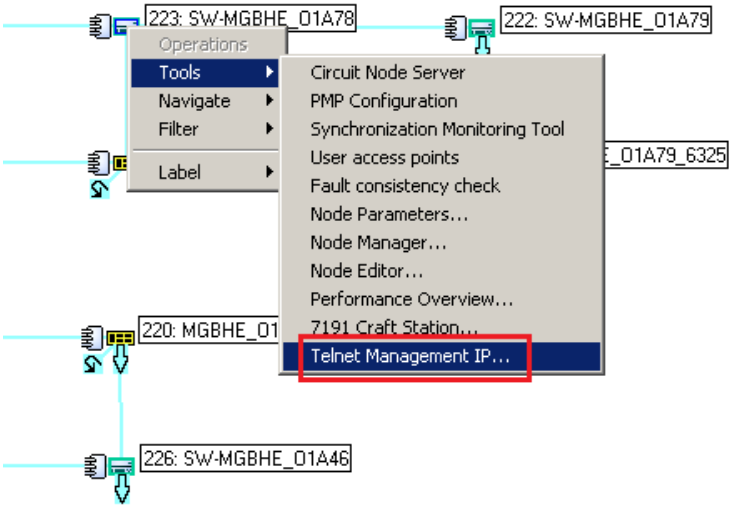
2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. execute o comando “show interfaces counters ethernet XX”, onde XX é a interface que será verificada:

```
DMLAB01#show interfaces counters ethernet 25
Eth 1/25
  Octets input                : 1088292
  Octets output               : 2068128
  Unicast input               : 5824
  Unicast output              : 6524
  Discard input               : 0
  Discard output              : 0
  Error input                 : 0
  Error output                : 0
  Unknown protos input        : 0
  QLen                        : 0
```

Se os campos Error input e Error output estiverem zerados significa que não há taxa de erro.

- Tellabs 7345 Switch Agregação Ethernet

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e Telnet Management IP:



2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. execute o comando “show interface xgigabitethernet X/X/X counters”, onde X/X/X é a interface que será verificada:

```
t7300-SW-MGBHE_O1A78# show interface xgigabitethernet 1/2/1 counters
```

Xg1/2/1
Reception Counters
HCInOctets : 774717323914
HCInUcast : 2260125596
HCInMcast : 752928
HCInBcast : 460703
Discarded Packets : 95428
Error Packets : 0
Unknown Protocol : 0

Transmission Counters
HCOutOctets : 3185340685817
HCOutUcast : 1690953516
HCOutMcast : 17086838
HCOutBcast : 1097527
Discarded Packets : 9
Error Packets : 0

Time since last discontinuity: 0

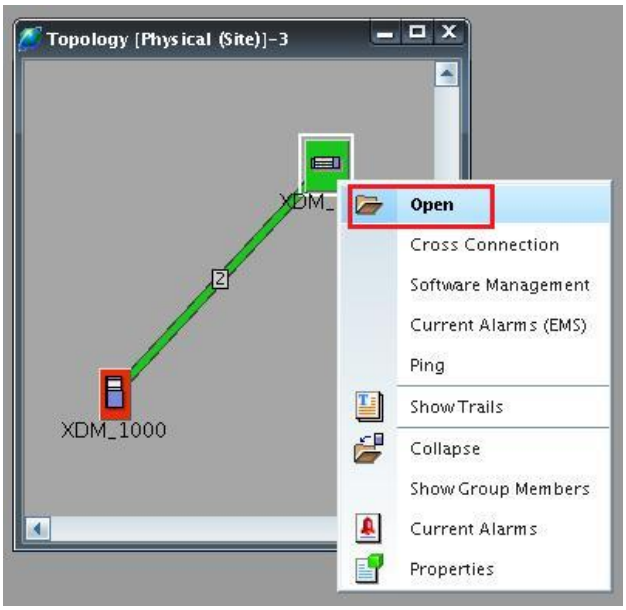
Se os campos Error Packets estiverem zerados significa que não há taxa de erro.

Procedimento para verificação de configurações de interfaces

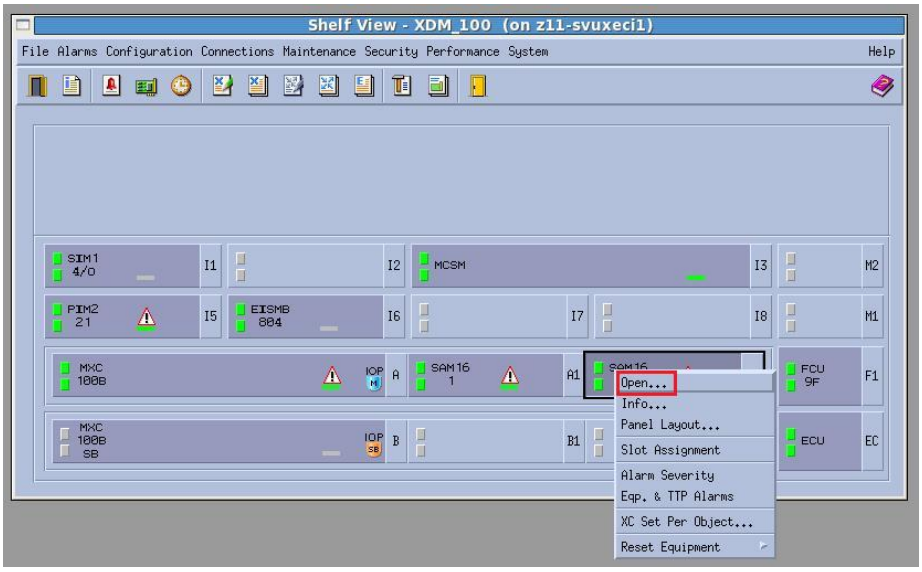
- ECI

- Verificando as configurações da SFP:

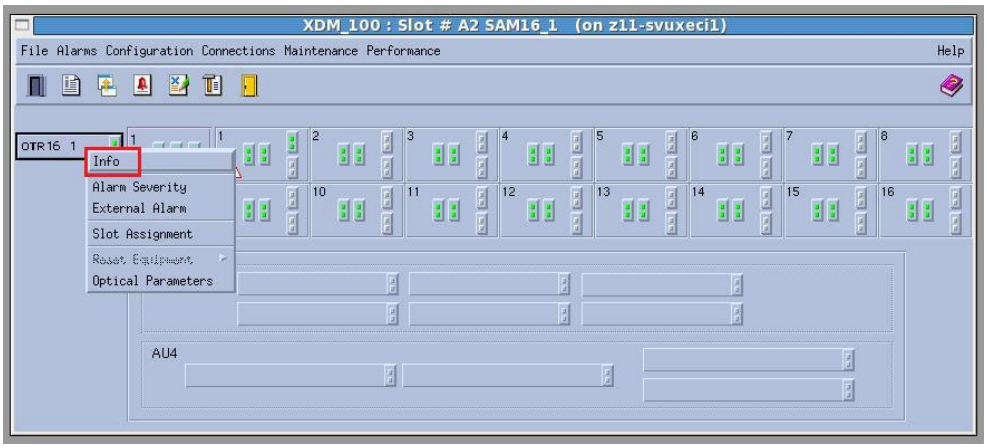
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



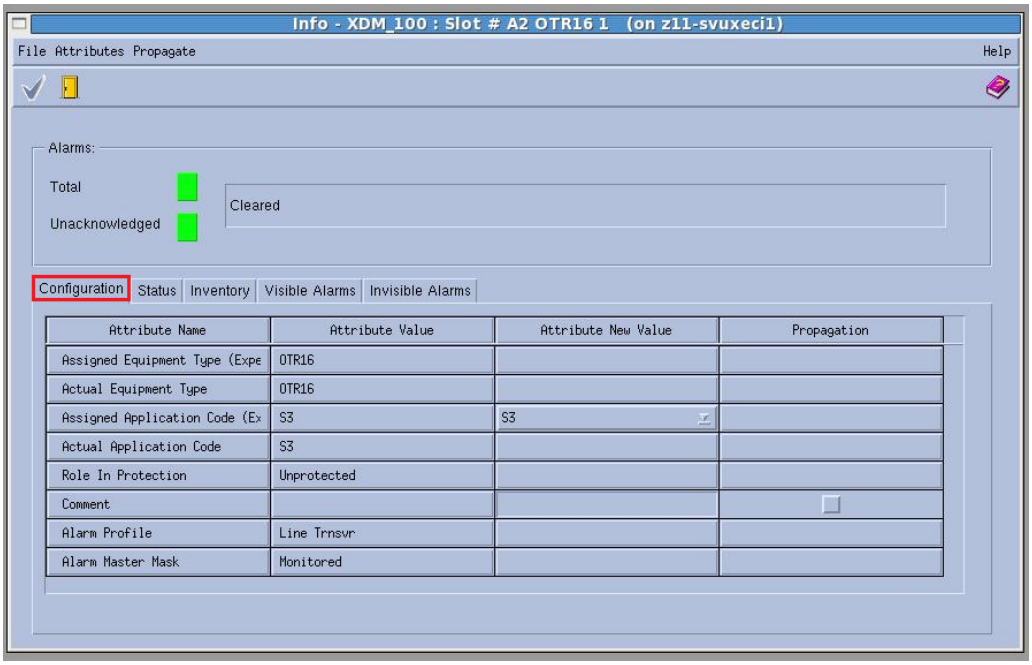
2° Passo: Após abrir o elemento selecione a placa que deseja verificar, clique com o botão direito do mouse e em seguida selecione a opção Open:



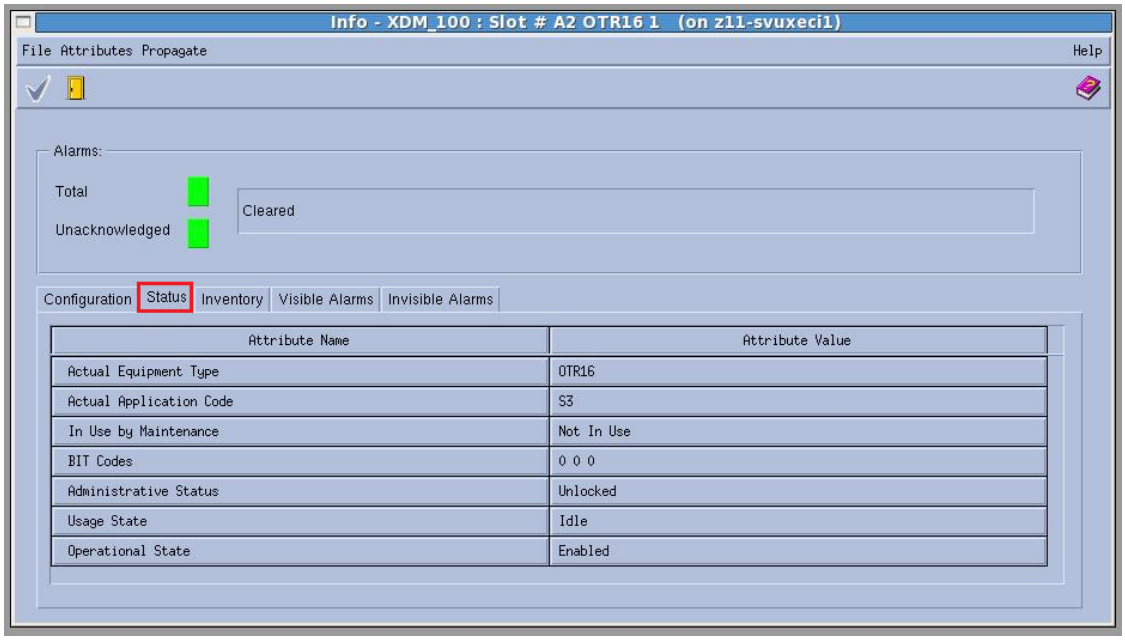
3° Passo: Após abrir a placa selecione a interface ótica SFP, clique com o botão direito do mouse e em seguida selecione a opção Info:



4° Passo: Na próxima janela selecione a aba Configuration, nela temos as informações do tipo de SFP configurado para o equipamento:



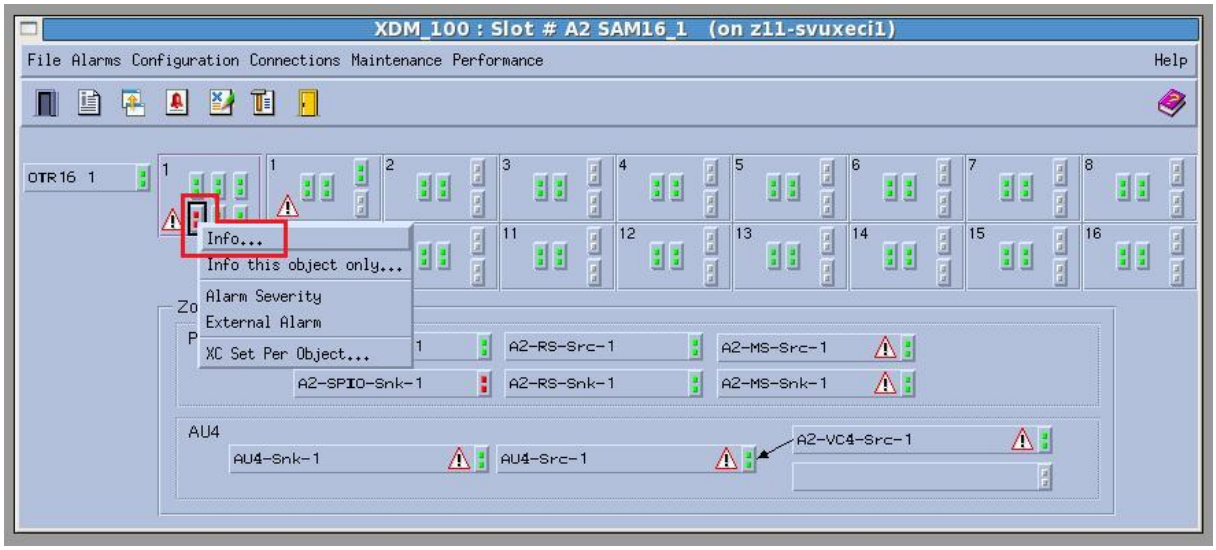
5° Passo: Selecione a aba Status, nela temos as informações do tipo de SFP que está sendo utilizada neste momento:



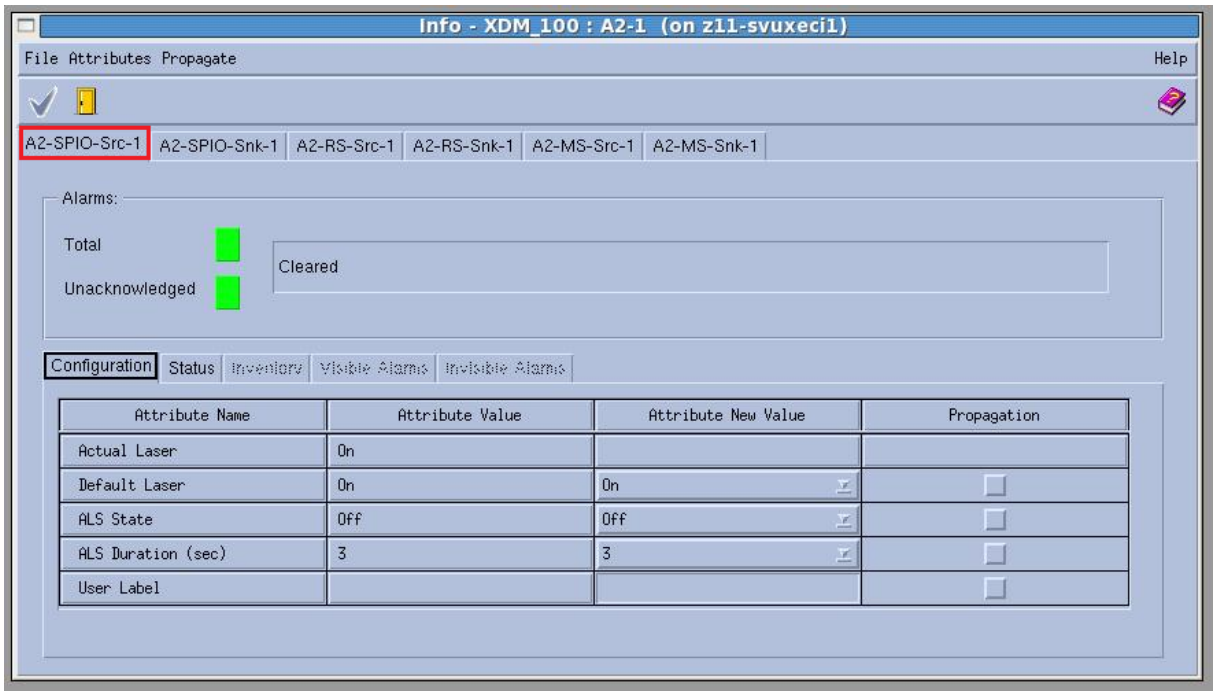
- Verificando as configurações do laser:

Seguir o 1° Passo e 2° Passo citados anteriormente.

3° Passo: Após abrir a placa selecione o botão conforme a imagem abaixo e selecione a opção Info:



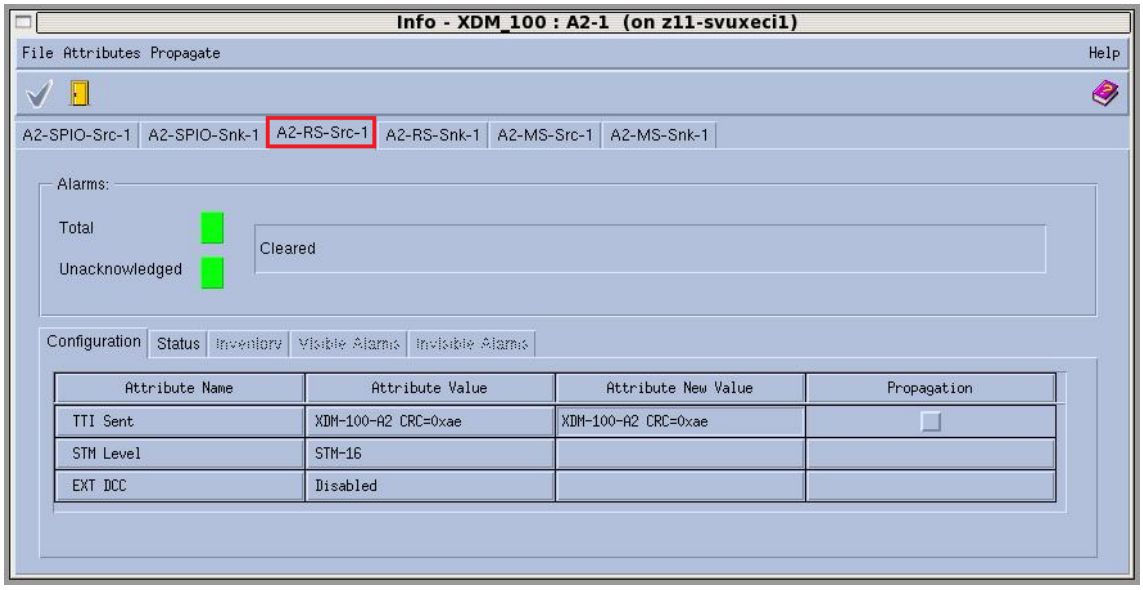
4° Passo: Selecionar a primeira aba correspondente a interface física conforme a imagem abaixo nela tem as informações do estado atual do laser e opções para habilitar de desabilitar o laser e função ALS.



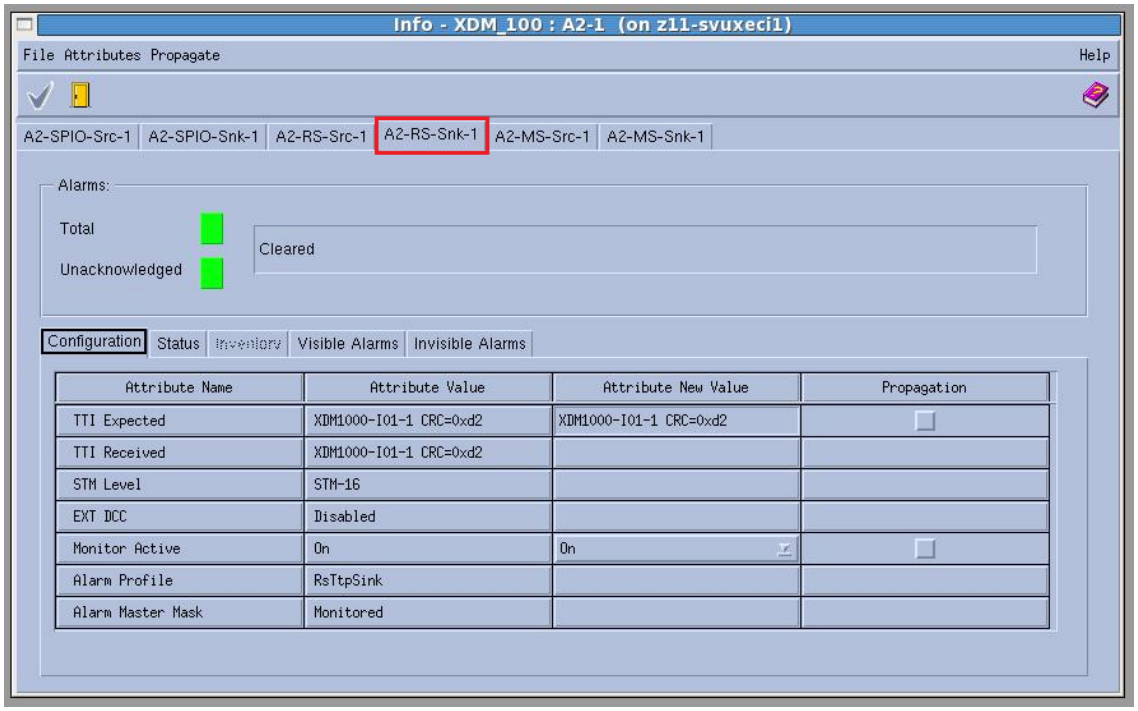
- Verificando as configurações de label identificador:

Seguir o 1° Passo, 2° Passo e 3° Passo citados anteriormente.

4° Passo: Selecionar a terceira aba correspondente a seção de regeneração (RS) conforme a imagem abaixo, nela pode ser configurado o label identificador transmitido ao elemento vizinho:



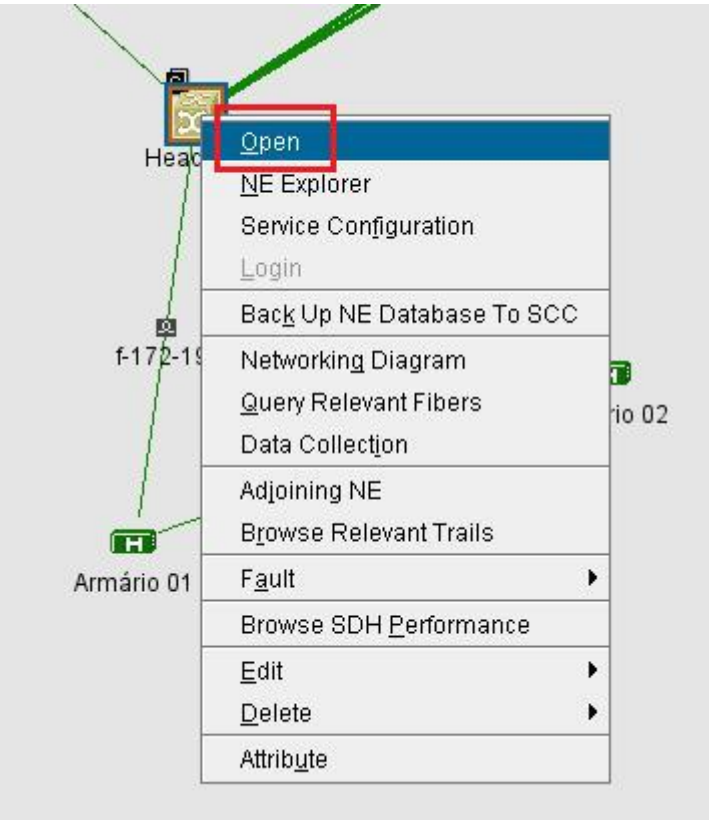
5° Passo: Selecionar a quarta aba correspondente a seção de regeneração (RS) conforme a imagem abaixo pode verificar e configurar o label identificador esperado do elemento vizinho:



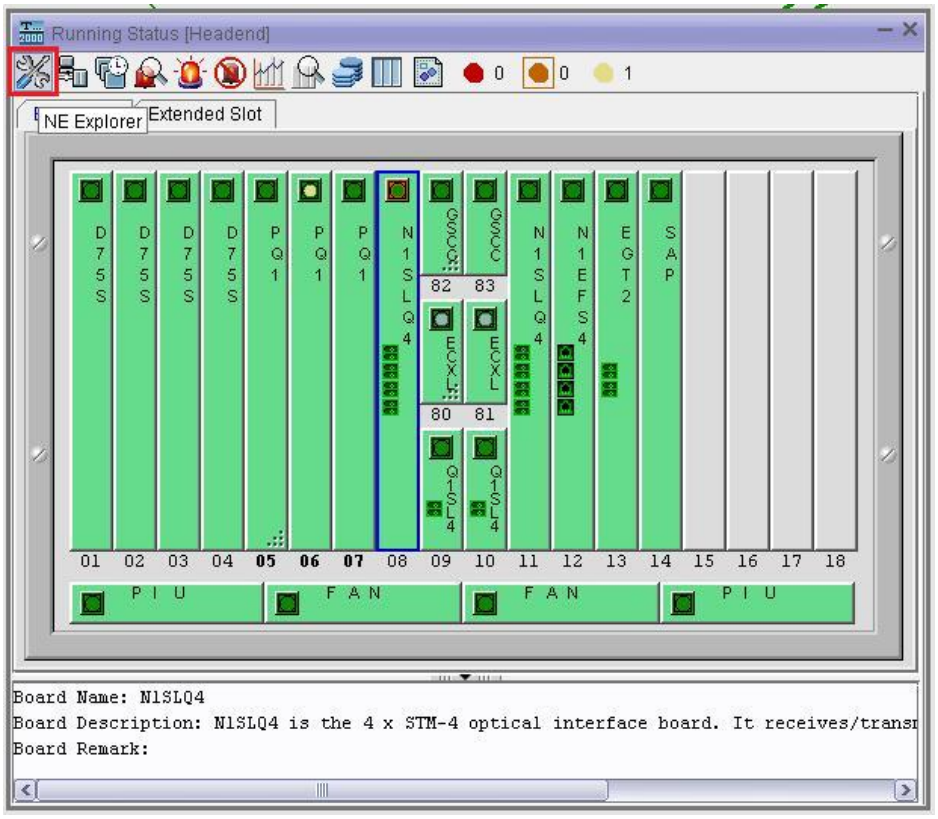
- Huawei

- Verificando as configurações do laser:

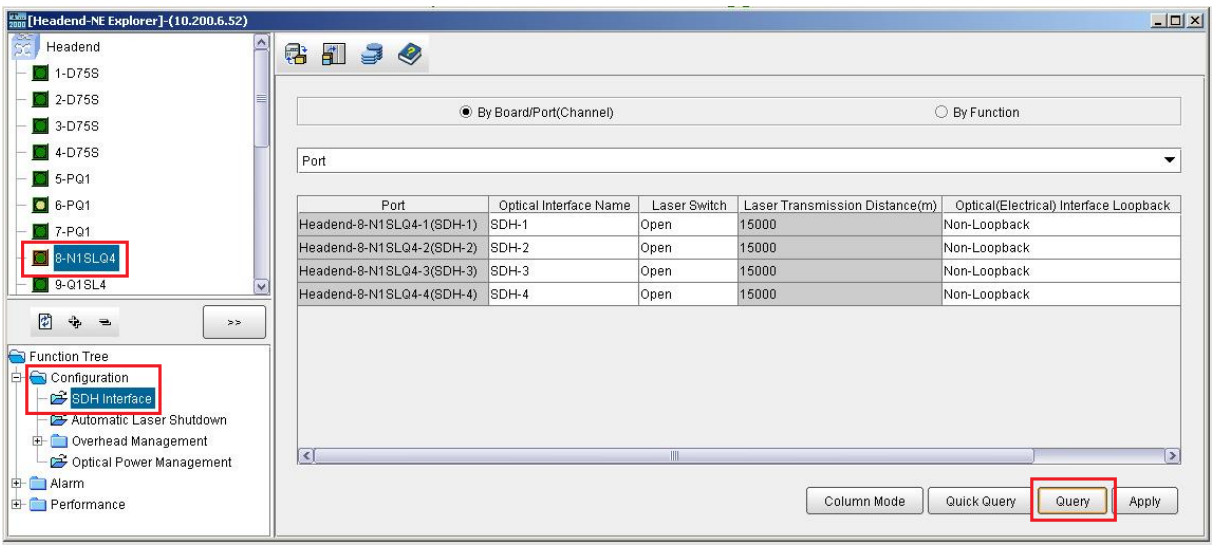
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



2° Passo: Após abrir o elemento clique no botão NE Explorer no canto superior esquerdo:



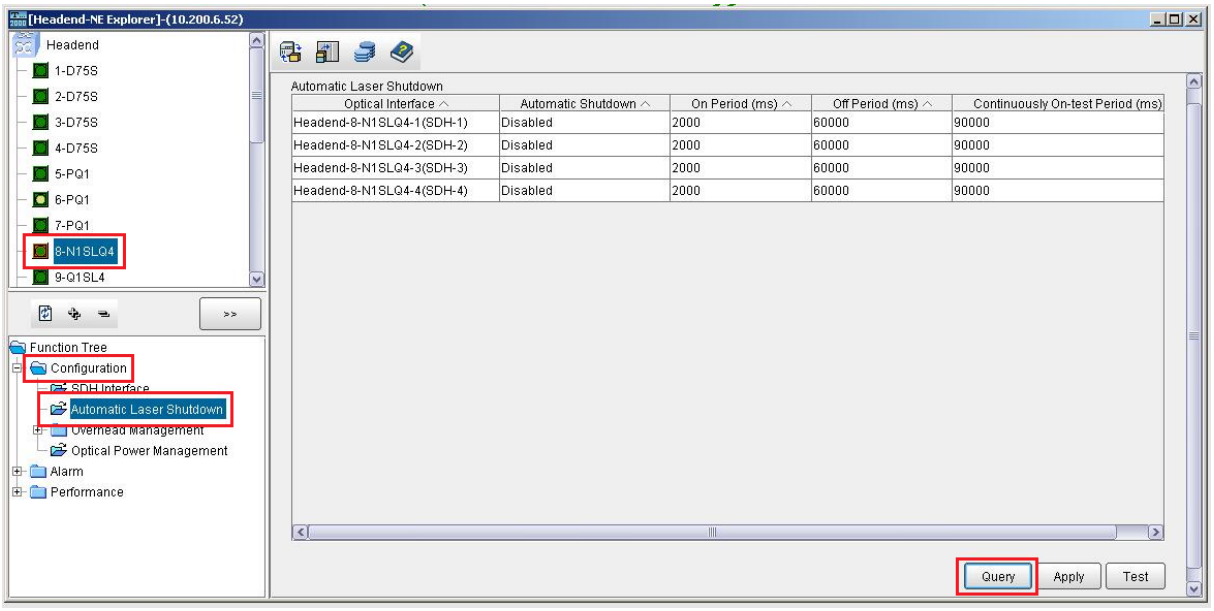
3° Passo: Após abrir a janela selecione no campo superior esquerdo a placa desejada, em seguida no campo inferior esquerdo as opções Configuration e SDH Interface, clicar no botão Query para atualizar as informações, na mesma janela têm as informações do estado atual do laser (Open para habilitado e Close para desabilitado) e de loopback:



- Verificando as configurações da função ALS:

Seguir o 1° Passo e 2° Passo citados anteriormente.

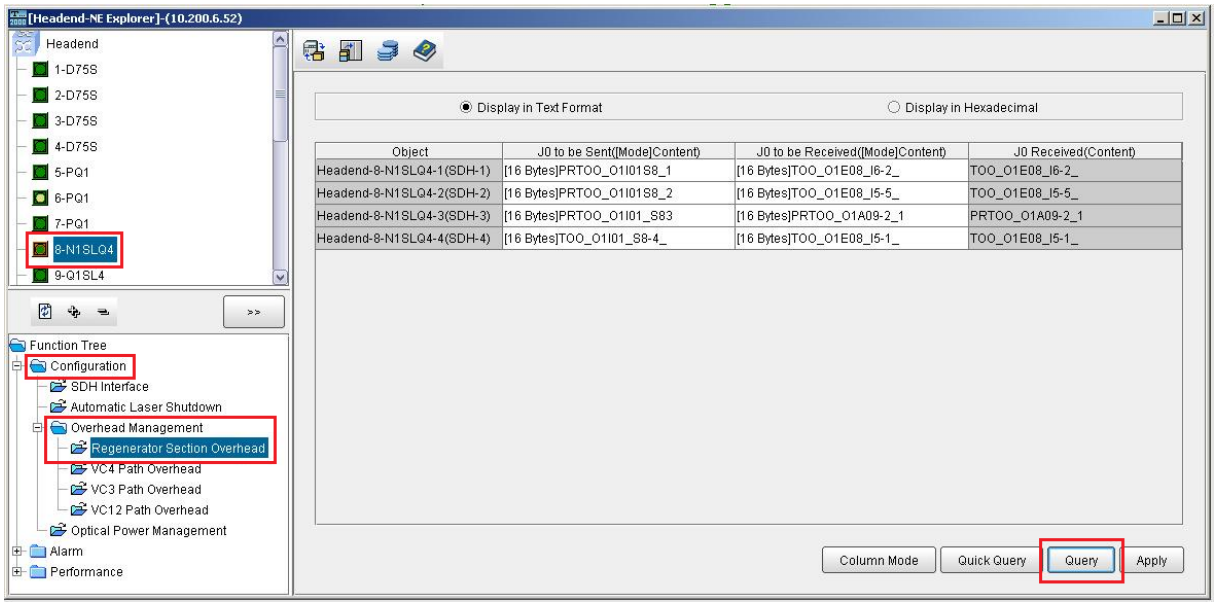
3° Passo: Após abrir a janela selecione no campo superior esquerdo a placa desejada, em seguida no campo inferior esquerdo selecione as opções Configuration e Automatic Laser Shutdown, clicar no botão Query para atualizar as informações, na mesma janela têm as informações do estado atual da função ALS:



- Verificando as configurações de label identificador:

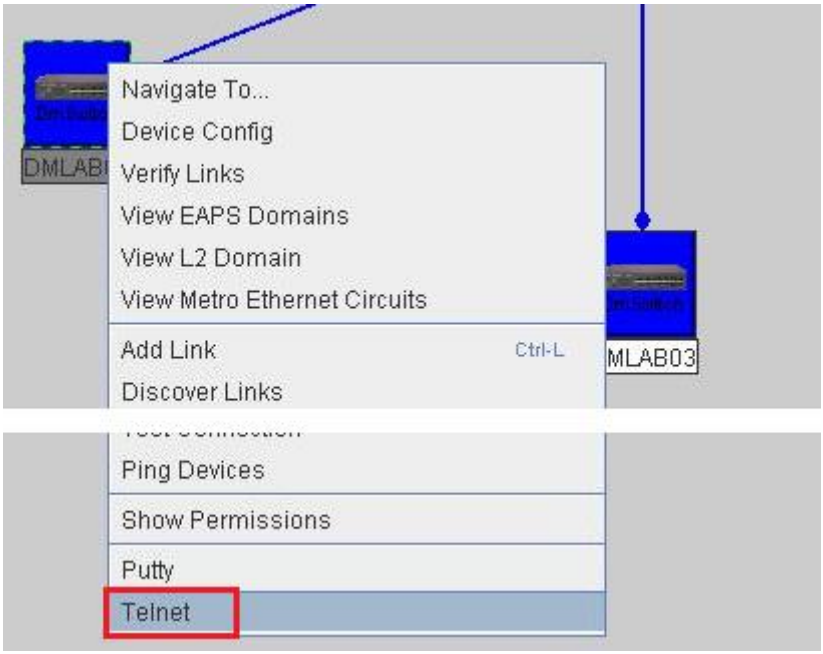
Seguir o 1° Passo e 2° Passo citados anteriormente.

3° Passo: Após abrir a janela selecione no campo superior esquerdo a placa desejada, em seguida no campo inferior esquerdo as opções Configuration, seguido da opção Overhead management e Regenerator Section Overhead, clicar no botão Query para atualizar as informações, nela temos as informações de configuração de label identificador enviado e esperado, e label identificador recebido no momento:



- Datacom

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Telnet:



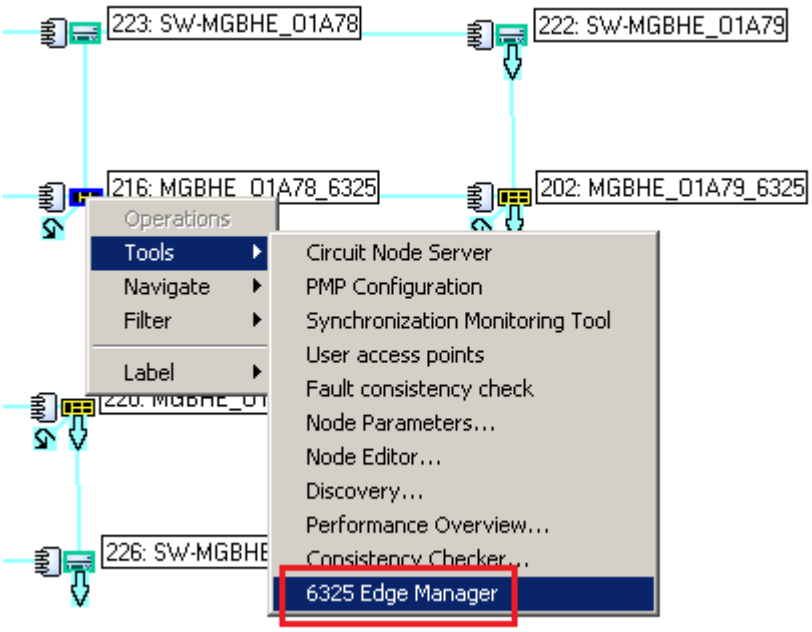
2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. execute o comando “show interfaces status ethernet XX”, onde XX é a interface que será verificada:

```
DMLAB01#show interfaces status ethernet 25
Information of Eth 1/25
Basic information:
Port type:              SFP
MAC address:            00:04:DF:10:57:C3
Configuration:
Name:                   RT:MON:D2BHE07A1001_Port26
Port admin:             Up
Speed-duplex:           Auto
Capabilities:           100M full, 1000M full
Flow-control:           Disabled
MDIX:                   Auto
Slow Protocols MAC:     Standard
LACP:                   Disabled
OAM:                    Disabled
Loopback Detection:     Enabled - Unblock hysteresis: 30 sec
Link-Flap Detection:    Enabled - Unblock hysteresis: 30 sec
Current status:
Link status:            Up
Operation speed-duplex: 1000M full
Flow control:           Disabled
MDIX:                   Normal
```

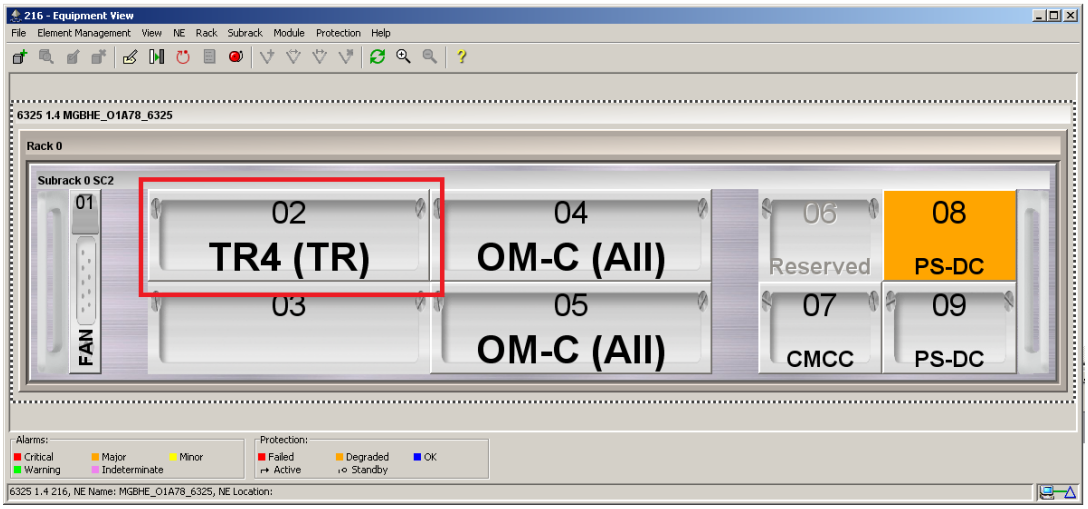
Para verificar todas as configurações do elemento executar o comando “show running-config”.

- Tellabs 6325 Edge Node

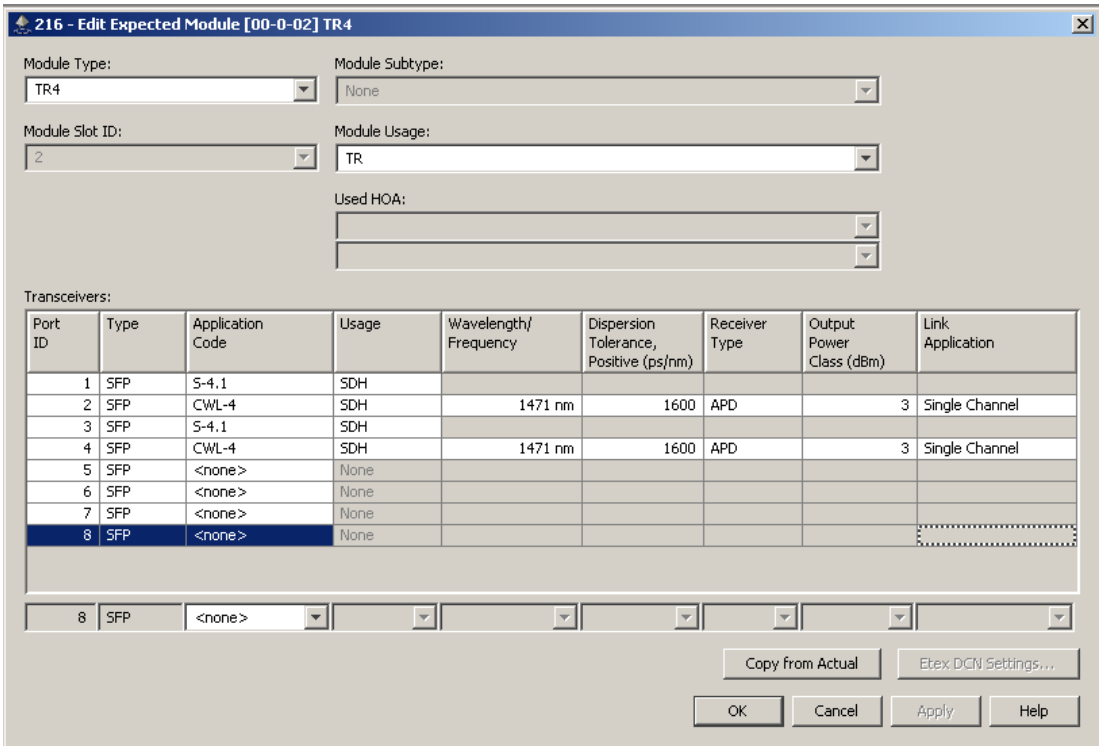
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e 6325 Edge Manager:



2° Passo: Após abrir o elemento clique duas vezes na placa TR4:



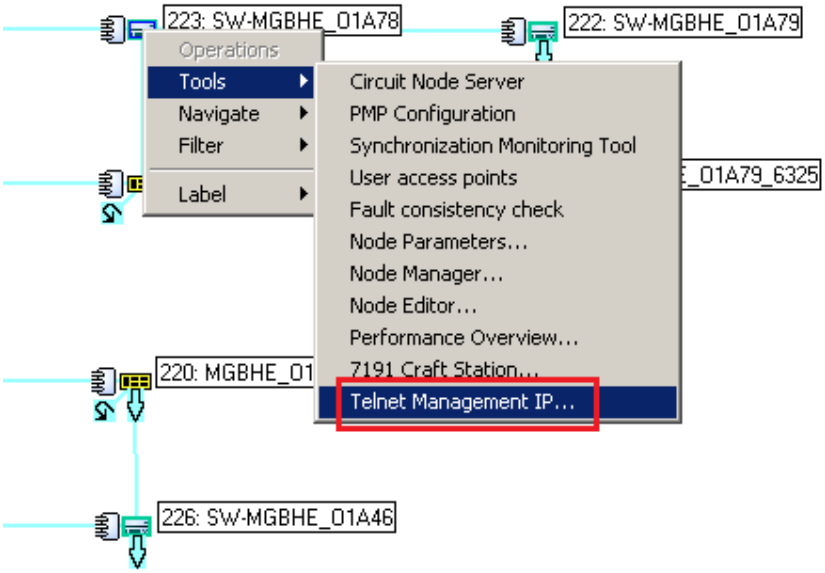
2° Passo: Irá abrir uma janela com as informações das SFPs que estão sendo utilizadas, como modelo utilizado e comprimento de onda, os outros parâmetros não são modificados:



A placa OMC é passiva, portanto não é possível alterar os parâmetros das interfaces.

- Tellabs 7345 Switch Agregação Ethernet

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e Telnet Management IP:



2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar. para verificar as configurações da interface execute o comando “show interface xgigabitethernet X/X/X”, onde X/X/X é a interface que será verificada:

```
t7300-SW-MGBHE_O1A78# show interface xgigabitethernet 1/2/1

Xg1/2/1 up, line protocol is up (connected)
Bridge Port Type: Provider Network Port

Hardware Address is 70:dd:a1:0f:61:7d
MTU  9600 bytes, No-Negotiation
Alias Name LT:CONN_TO_SW-MGBHE_O1A38_1/2/2

Operational value: Full duplex, 10 Gbps
Configured value: Full duplex, 10 Gbps
HOL Block Prevention enabled.
Operational input flow-control is off, output flow-control is off
Configured input flow-control is off, output flow-control is off

SD Set Window value: 100000 frames
SD Set Threshold value: 1 frames
SF Set Window value: 1000 frames
SF Set Threshold value: 1 frames

Link Up/Down Trap is enabled
LOS Trap is enabled
LOSYNC Trap is enabled
TRDI-E Trap is enabled
Auto-Neg Failure Trap is enabled
SF Trap is enabled
SD Trap is enabled

Discontinuity Time : 0
```

3° Passo: Para verificar as informações do módulo utilizado execute o comando “show equipment X/X/X”, onde X/X/X é a interface que será verificada:

```
t7300-SW-MGBHE_O1A78# show equipment 1/2/1
----------------------------------------------------
Location                    : Slot 1/2 SubSlot 1
Equipment                   : XFP10G
Configured Equipment        : XFP10G
Description                 : XFP10G
Class                       : module(6)
Allowed Types               : 0x0
Hardware Revision           : D3
```

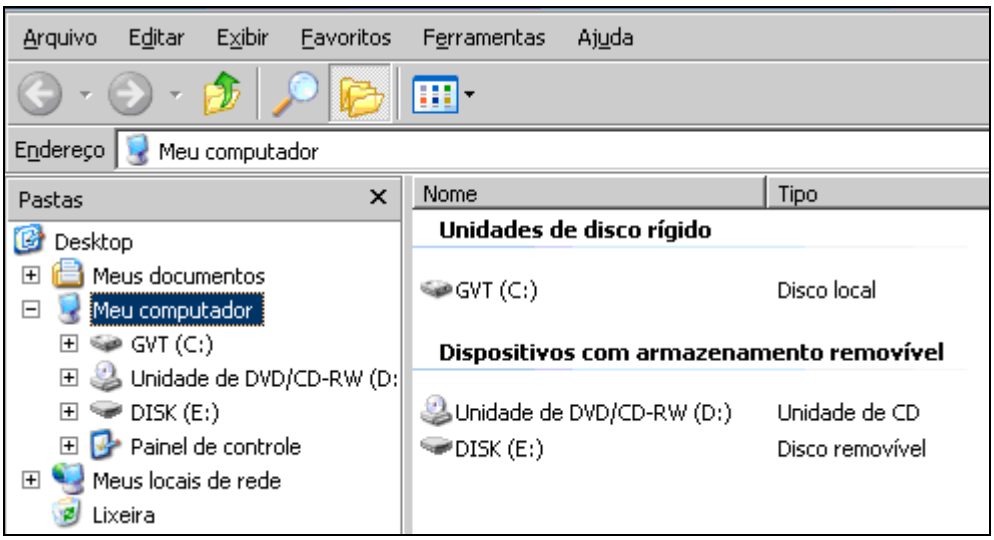
```
Firmware Revision          : NA
Software Revision          : NA
Serial Number                    : MXLL0152
Asset ID                   : NA
Manufacturing Date         : 101207
Field-Replaceable Unit     : YES
Manufacturer               : Multiplex Inc
Model                      : MXP-L6201AI3CTL3
Oper Status                      : UP
Admin Status               : UP
Act/Stby Status            : NA
Last Change                : 2000-01-04 16:58:23
Link LED Status            : Green
-----------------------------------------------------
```

Para verificar todas as configurações do elemento executar o comando “show running-config”.

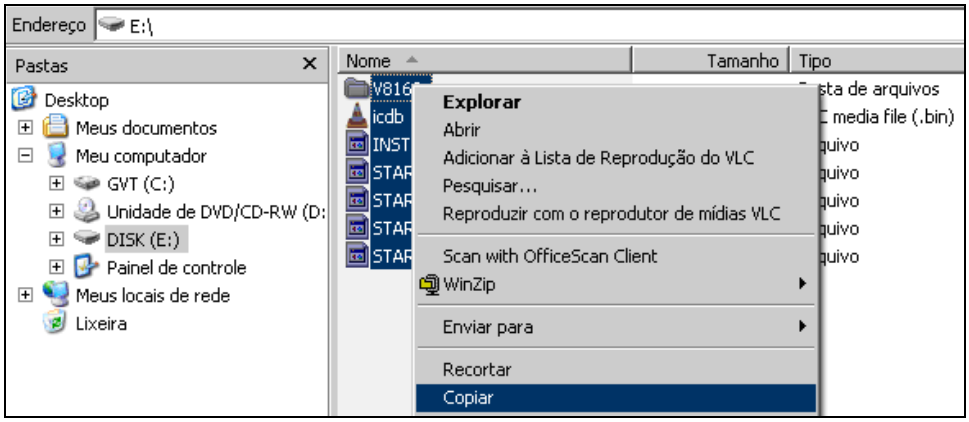
Procedimento para formatação do cartão de memória (NVM) dos equipamentos ECI

Para realizar a formatação de cartões memória (NVM) que são utilizadas nos equipamentos de transmissão do fabricante ECI (XDM100 e XDM1000) é necessário que o técnico tenha instalado em seu computador o programa “XDM FLASH PROGRAMER 7.03” e também as versões de software atualizadas que serão gravadas ou formatadas nos cartões de memória.

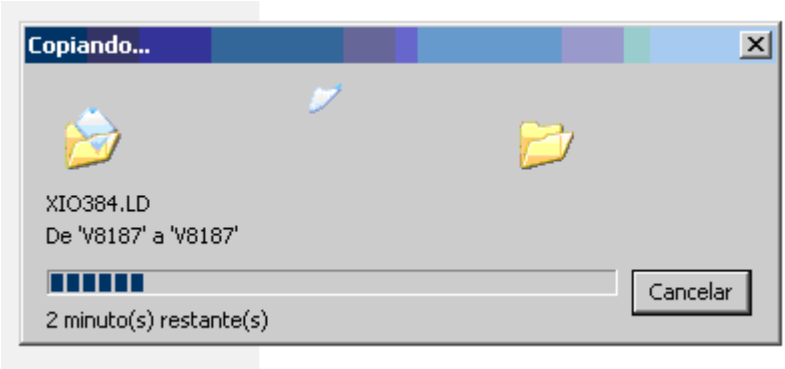
1° Passo: Inserir o cartão de memória antigo no computador através de uma interface PCMCIA ou um adaptador para cartões de memória via USB, identificar qual a unidade que foi atribuída à NVM (Disco Removível):



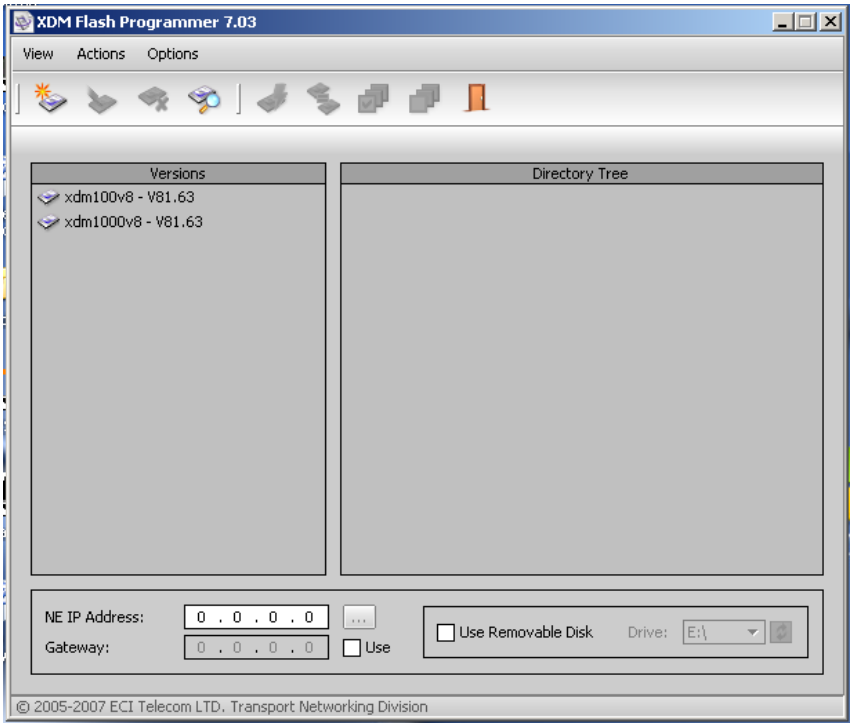
2° Passo: Copiar todos os arquivos existentes no cartão de memória:



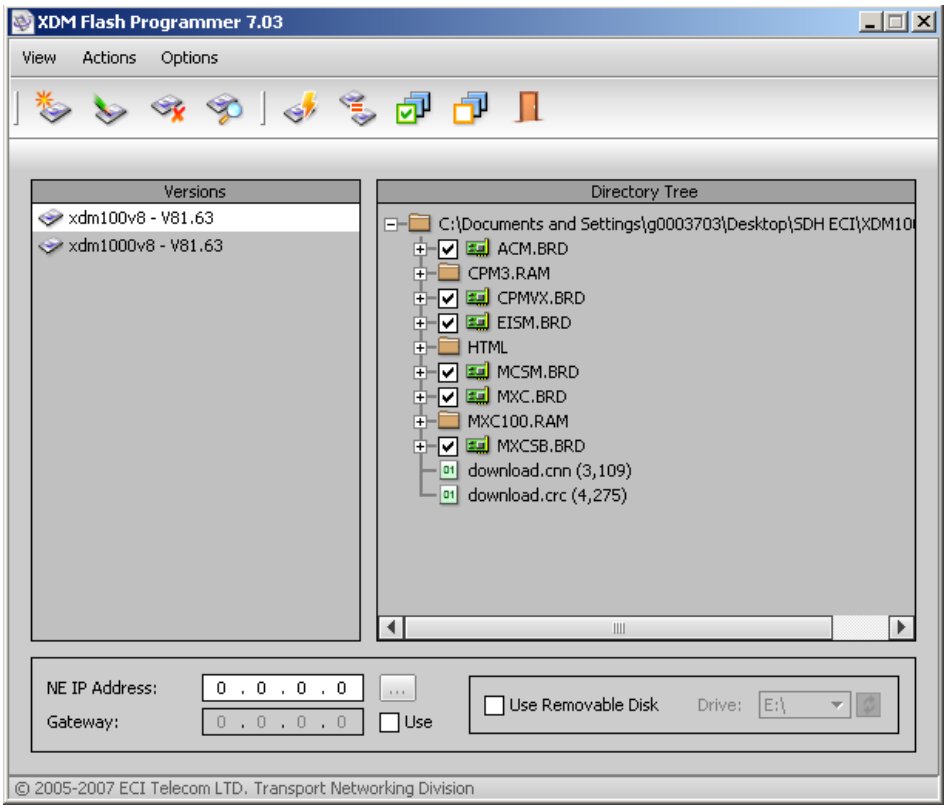
3° Passo: Criar uma nova pasta no Notebook e colar os arquivos copiados.



4° Passo: Abrir o programa “XDM FLASH PROGRAMER”:

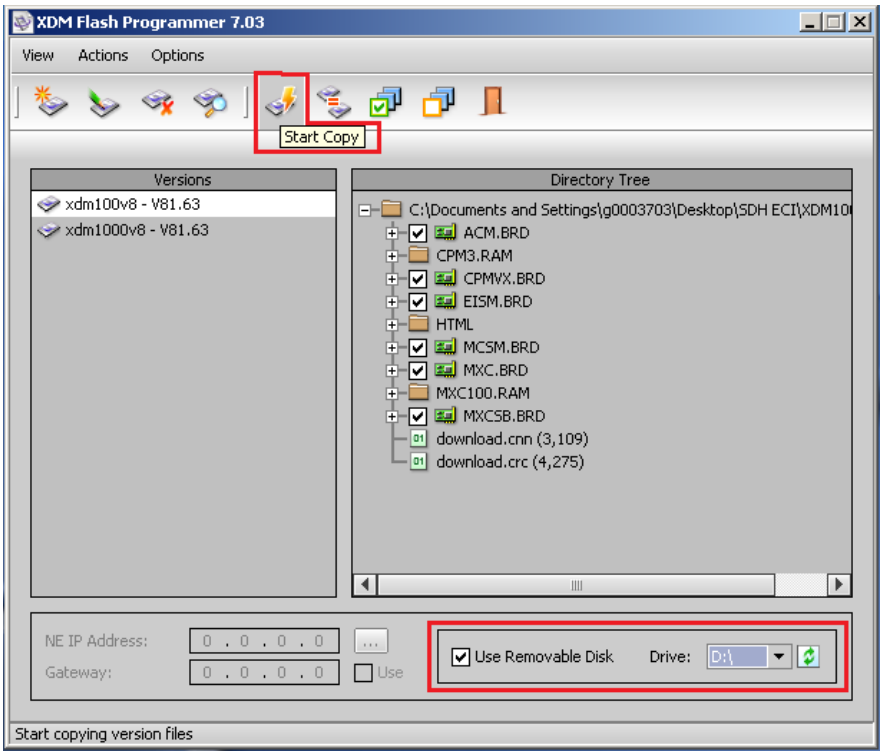


5° Passo: Escolher a versão do firmware que será utilizado, no caso de formatação para XDM-100 escolher a firmware referente ao modelo do equipamento, por exemplo, a versão de firmware xdm100v8 – v81. 63, conforme abaixo:

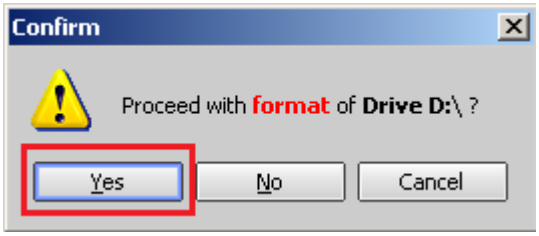


6° Passo: Inserir no computador o novo cartão de memória que será formatado, identificar qual a unidade que foi atribuída à NVM (Disco Removível):

7° Passo: Após verificar em qual drive está o cartão de memória, no programa de formatação na aba abaixo onde está localizado Use Removable Disk escolha o drive aonde o computador identificou o cartão, após selecione o botão Start copy:

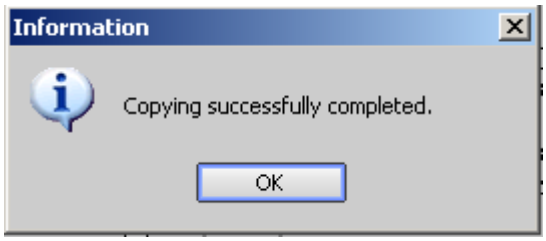


Confirme o procedimento de formatação no botão Yes.

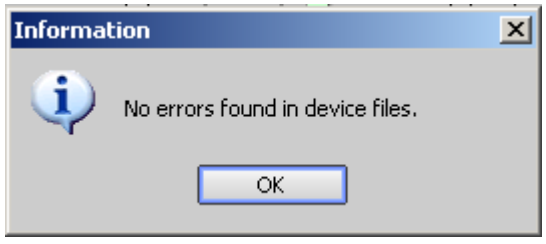


Aguarde o processo ser realizado completamente.

Após o procedimento de formatação estar completo aparecerá a mensagem de “Copyng successfully completed” em seguida click em OK:

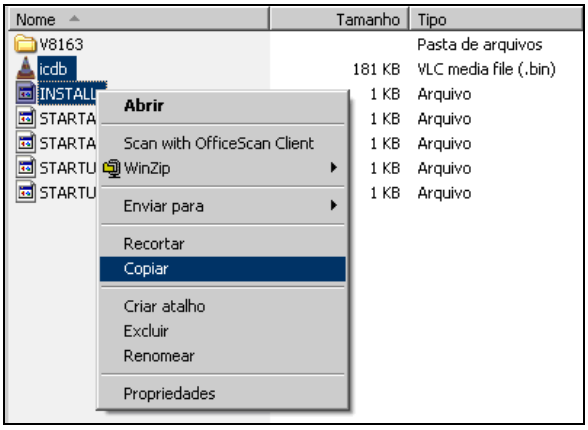


O software realizará uma verificação no cartão a procura de erros e logo em seguida enviara uma mensagem de “No errors found in device files”:

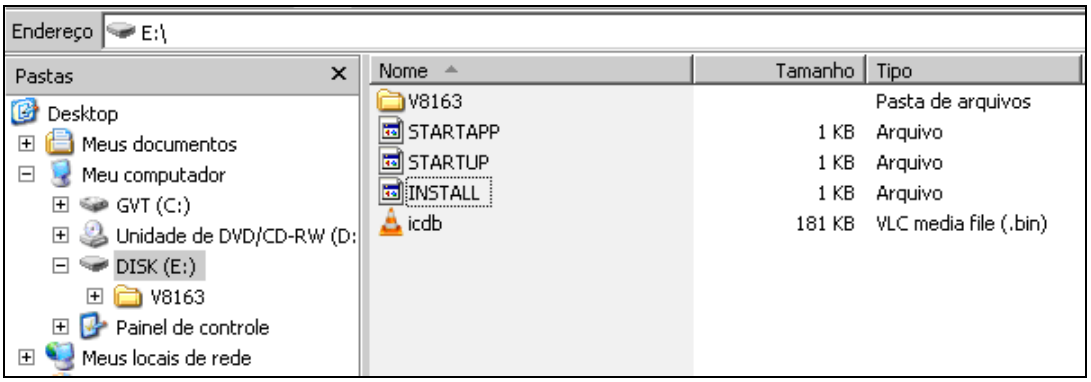


Em seguida aparecerá uma janela “Remover hardware com segurança”. Ainda não remova a NVM.

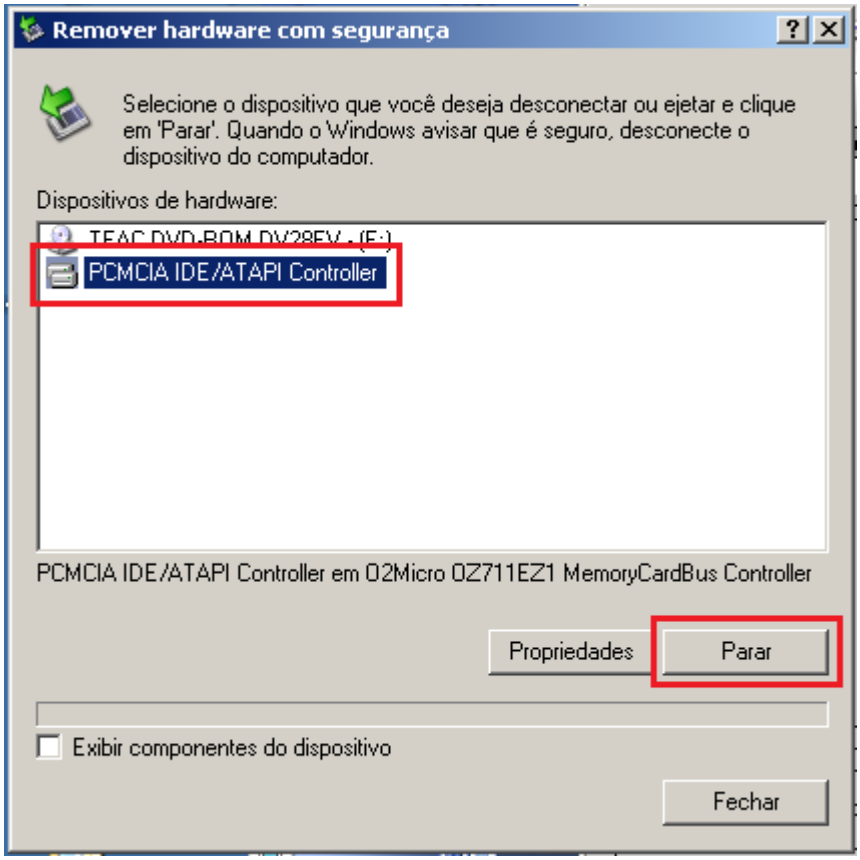
7° Passo: Copie os arquivos “icdb” e “INSTALL” que foram salvos anteriormente no computador e cole os arquivos no cartão de memória:



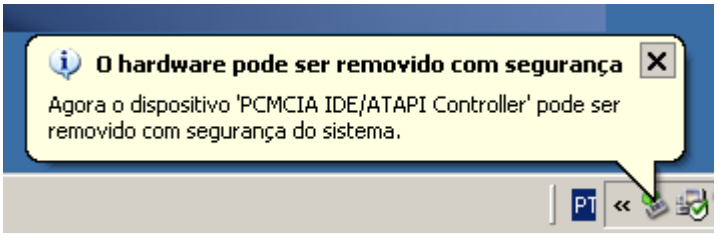
8° Passo: Certifique-se de que os arquivos com a firmware e os arquivos “icdb” e “INSTALL” estão conforme a imagem abaixo:



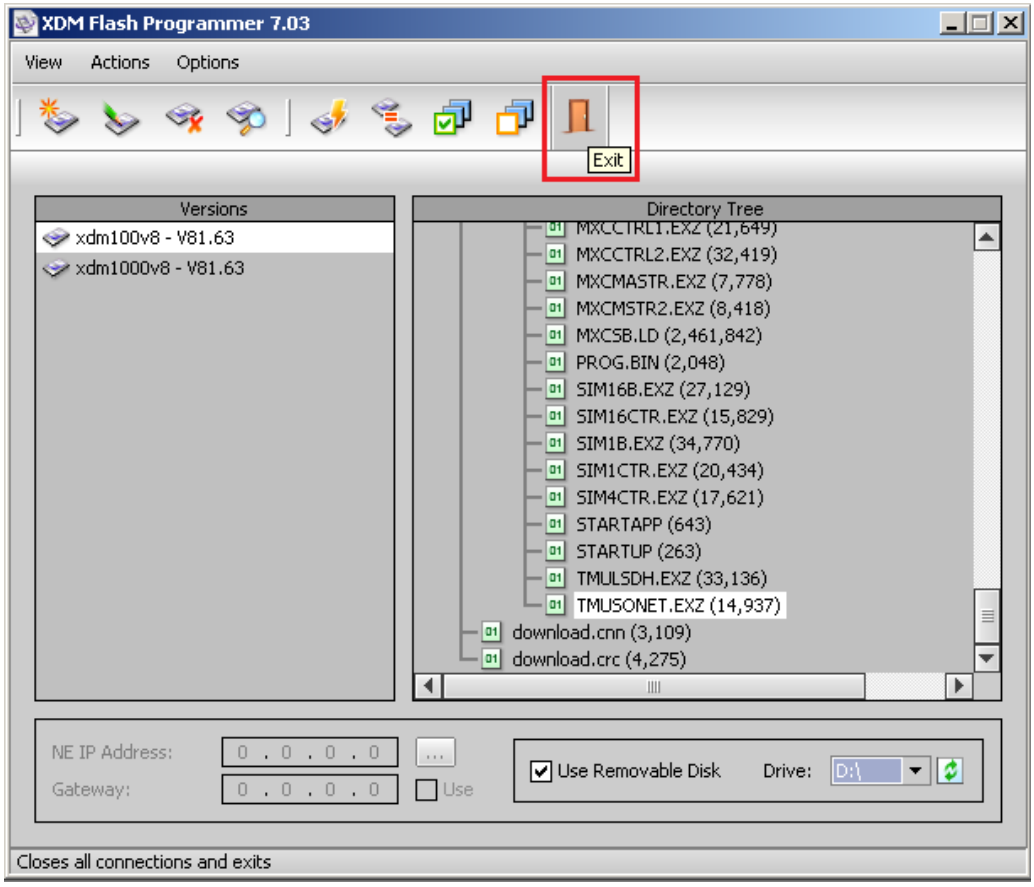
9° Passo: Realizar o procedimento de remoção de hardware do Windows selecionando o hardware que realizou o processo de formatação e clicando no botão em Parar:



9° Passo: Quando aparecer a mensagem que “O Hardware pode ser removido com segurança”, retire o cartão e insira no slot correspondente da placa controladora do XDM onde está indicado NVM.



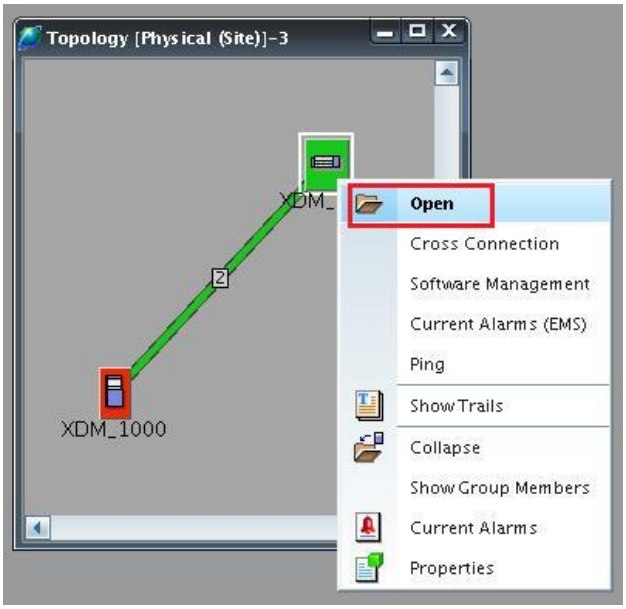
Terminado o processo click no ícone Exit para sair do aplicativo:



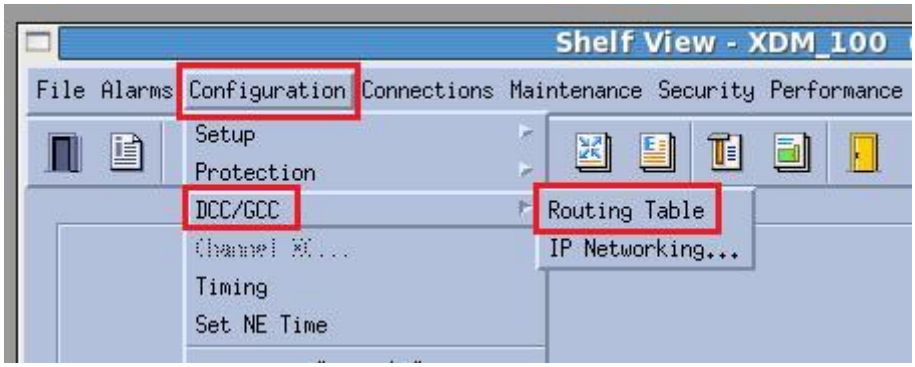
Procedimento de verificação de configurações de gerência do equipamento

- ECI

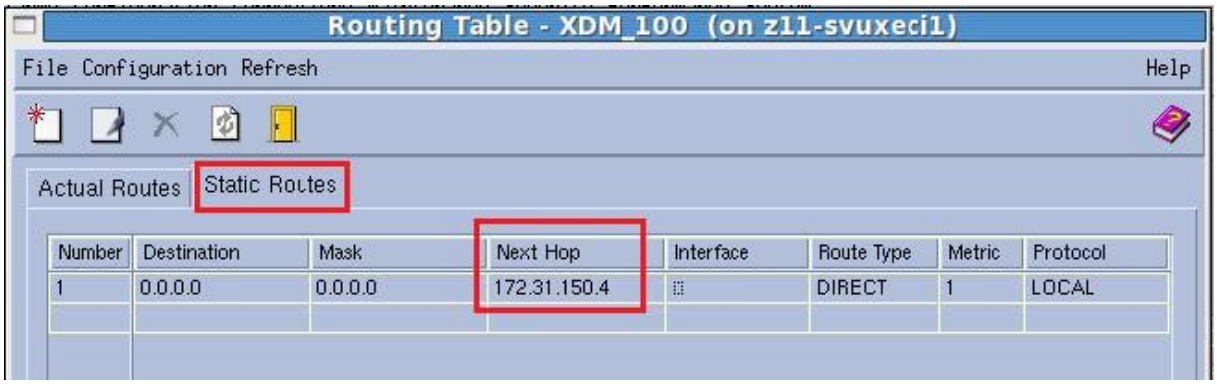
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



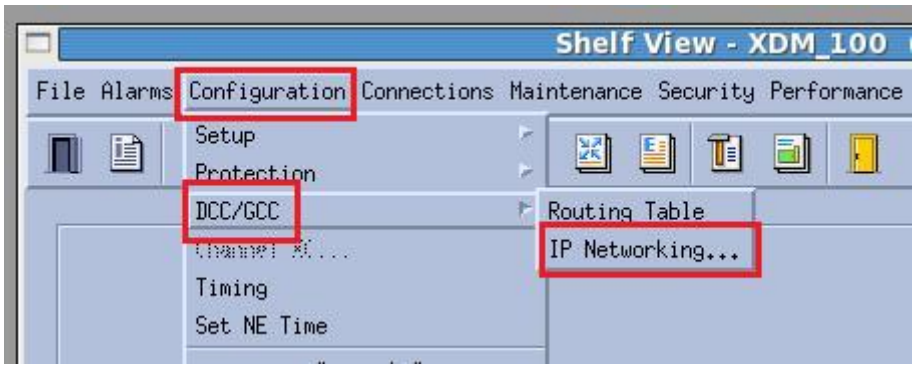
2° Passo: Após abrir o elemento selecione a opção Configuration na parte superior do elemento, em seguida clique em DCC/GCC e Routing Table:



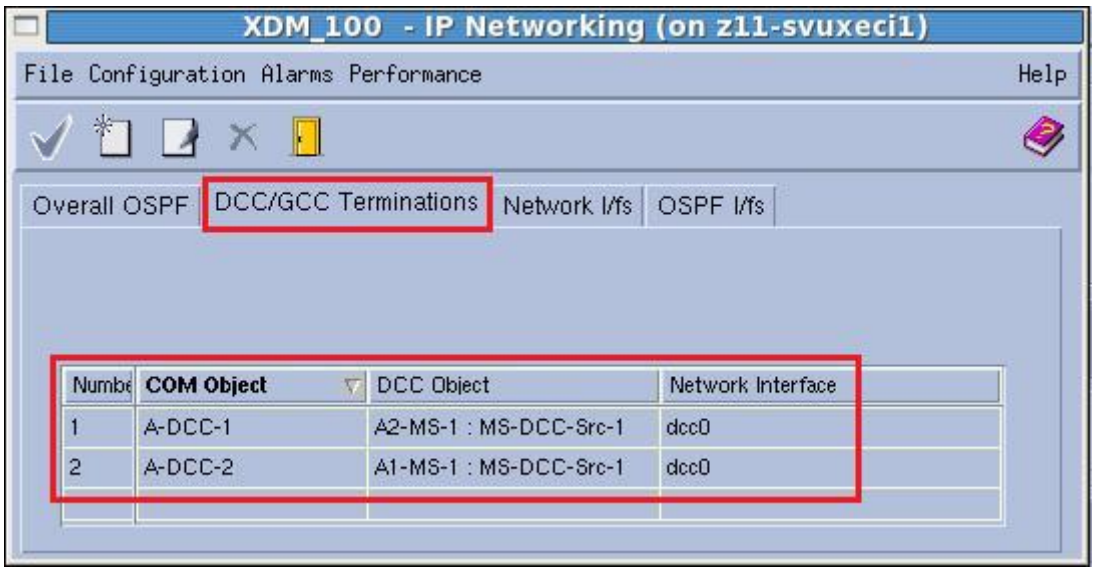
2° Passo: Abrirá uma janela, clique na aba Static Routes, abaixo na coluna Next Hop estará a o endereço IP do equipamento:



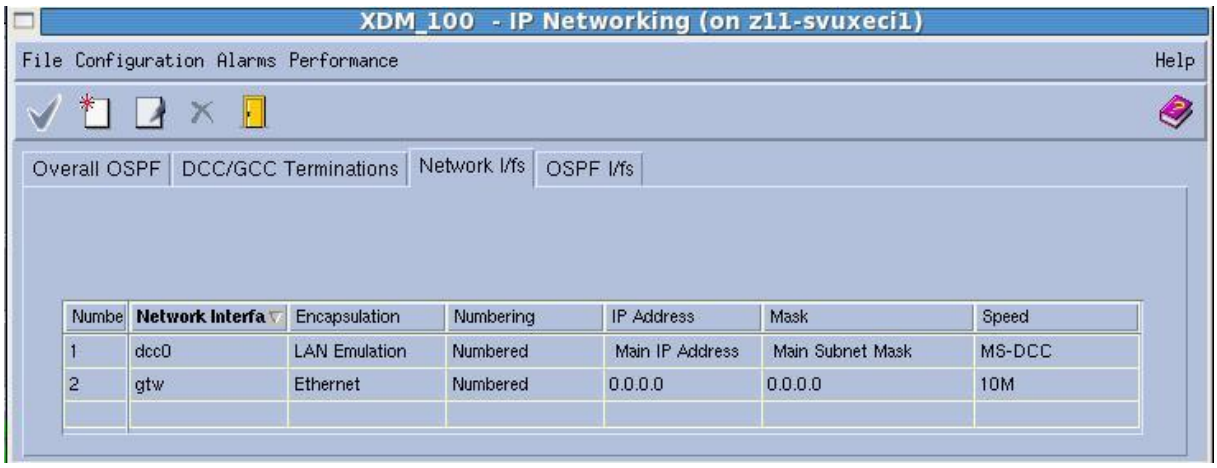
3° Passo: Novamente no equipamento clique na opção Configuration na parte superior do elemento, em seguida clique em DCC/GCC e IP Networking:



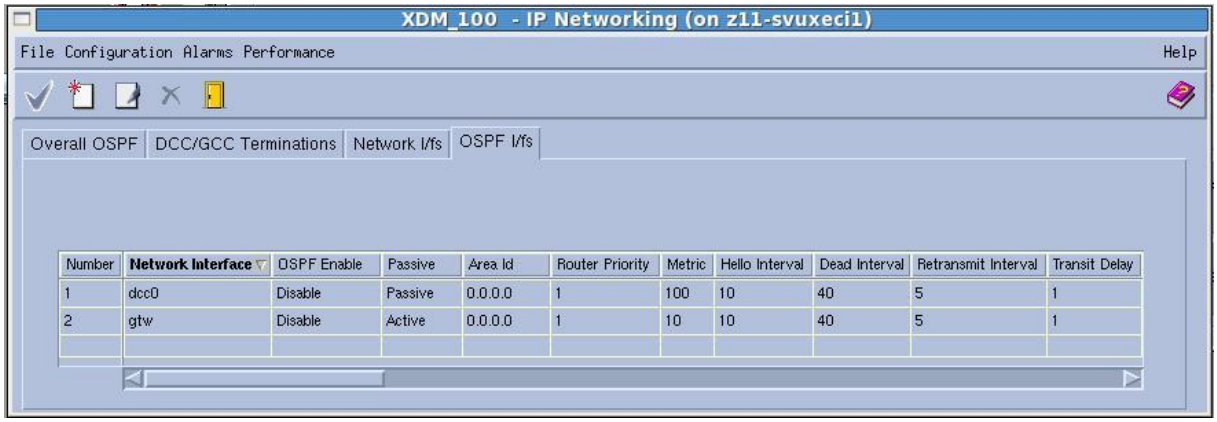
4° Passo: Abrirá uma janela, clique na aba DCC/GCC Terminations, abaixo estão as configurações de canal DCC do equipamento, tem que estar configurado para os dois lados do anel conforme abaixo:



5° Passo: Clique na próxima aba Nertwork I/fs, nela estarão as configurações de canal DCC e gateway de rede do equipamento:



6° Passo: Clique na última aba OSPF I/fs, nela estarão as configurações de canal DCC, gateway, OSPF e intervalos de comunicação:

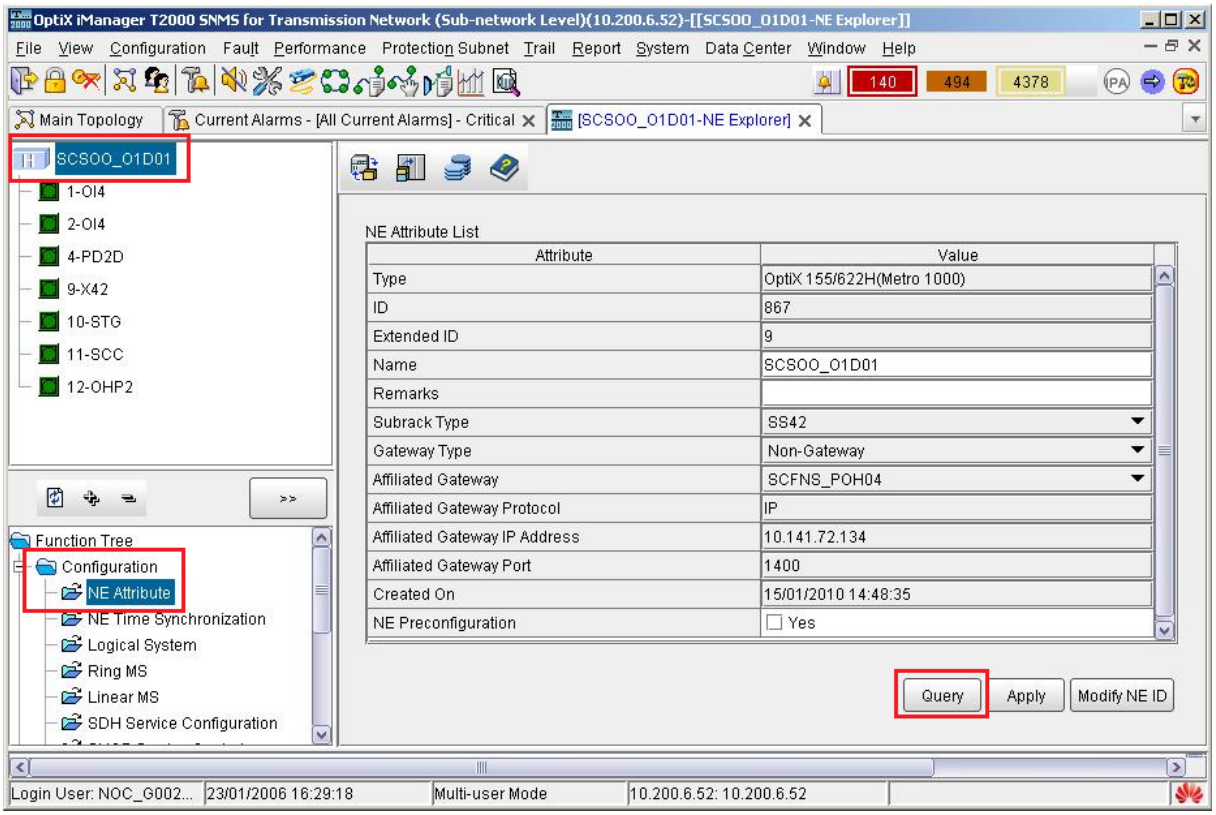


- Huawei

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:

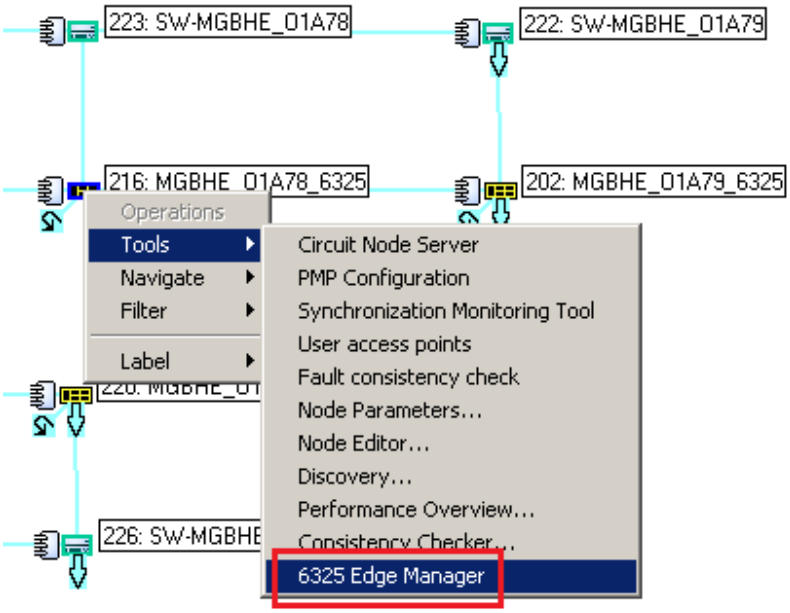
2° Passo: Após abrir o elemento clique no botão NE Explorer no canto superior esquerdo:

3° Passo: Após abrir a janela selecione o equipamento no campo superior esquerdo, em seguida no campo inferior esquerdo as opções Configuration e NE Atribute e clicar no botão Query para atualizar as informações, na mesma janela temos as informações do nome e ID do elemento, nome e IP do gateway:

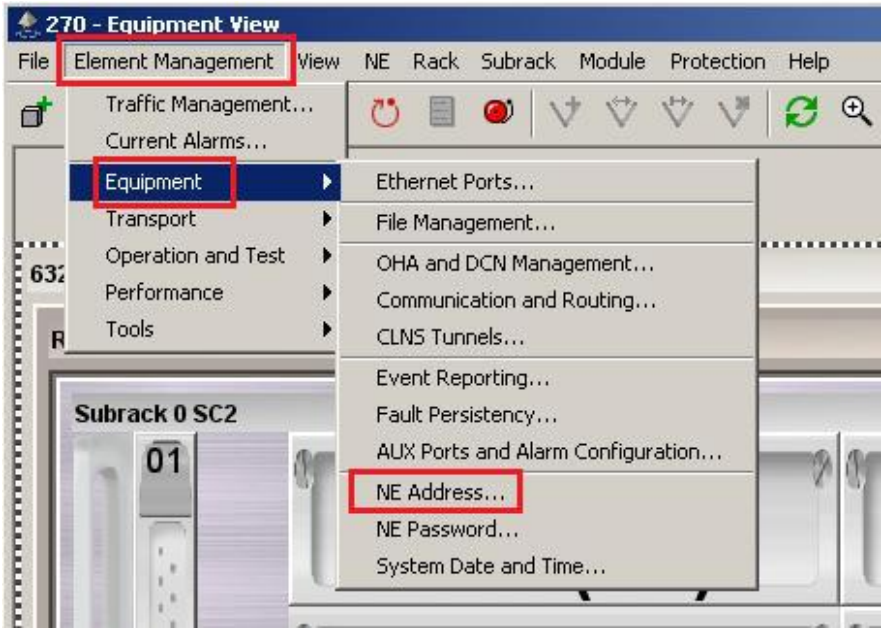


- Tellabs 6325 Edge Node

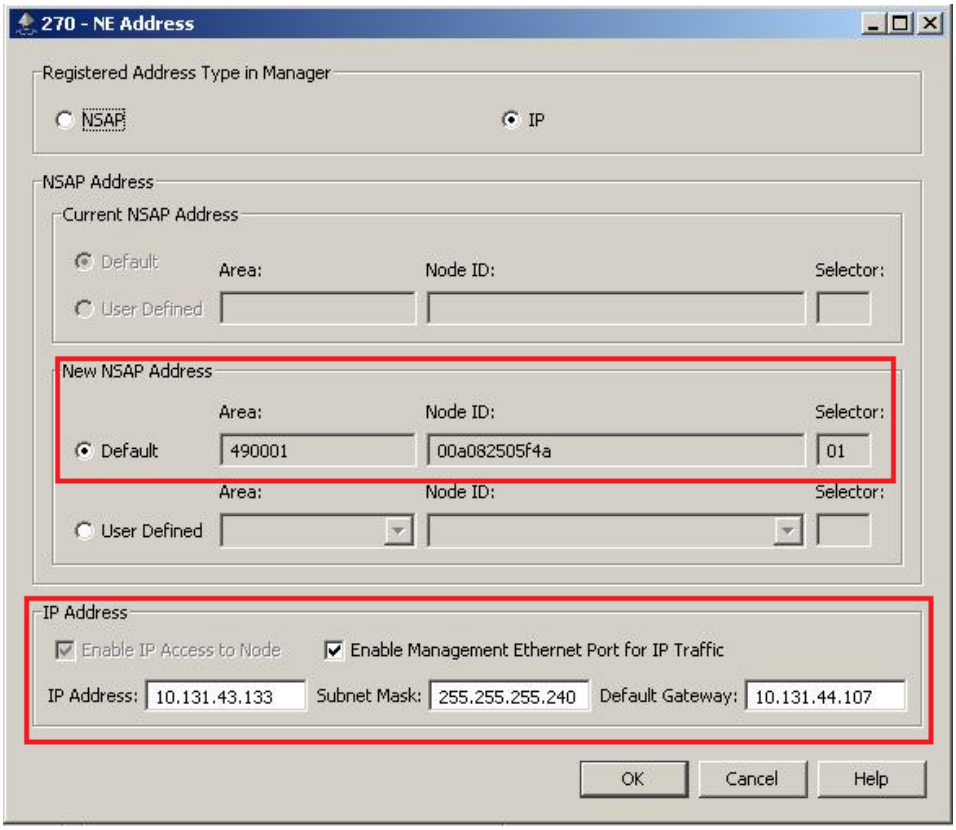
1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e 6325 Edge Manager:



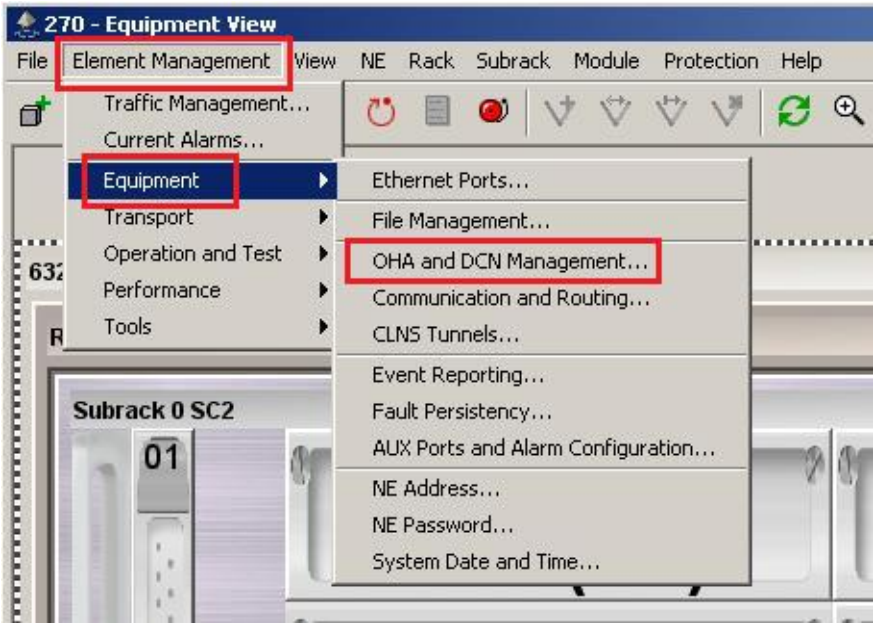
2° Passo: Após abrir o elemento selecione as opções Element Management, seguido de Equipament e NE Address:



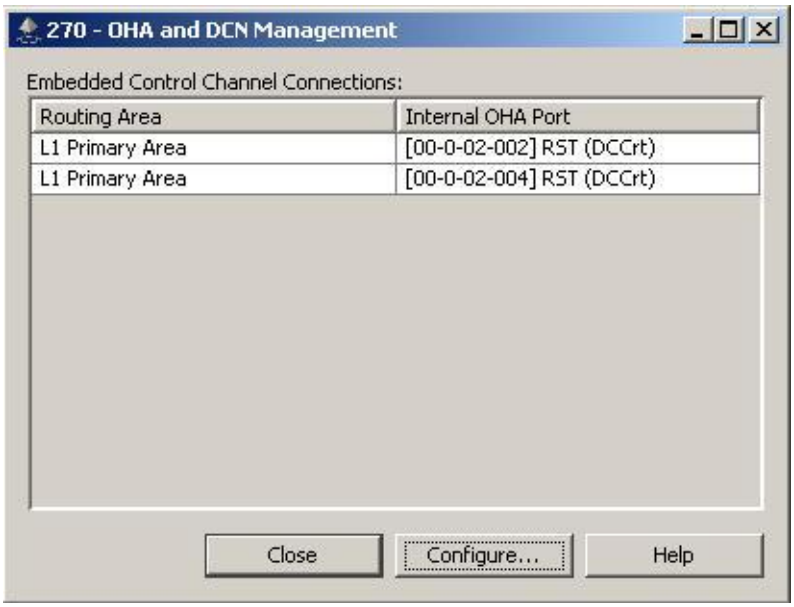
3° Passo: Abrirá uma janela com as informações de endereço NSAP do servidor de gerência, IP, mascará de rede e gateway do equipamento:



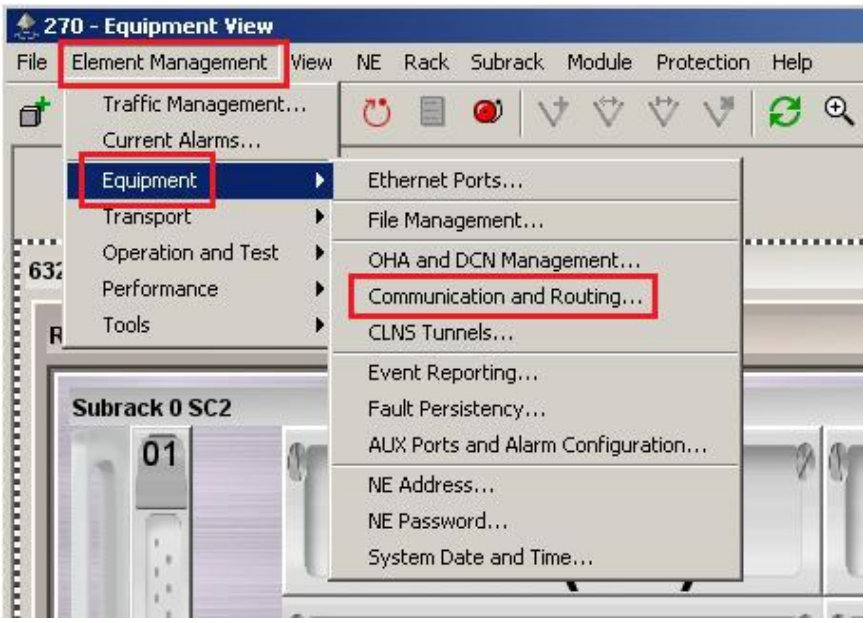
4° Passo: No elemento selecione as opções Element Management, seguido de Equipament e OHA and DCN Management:



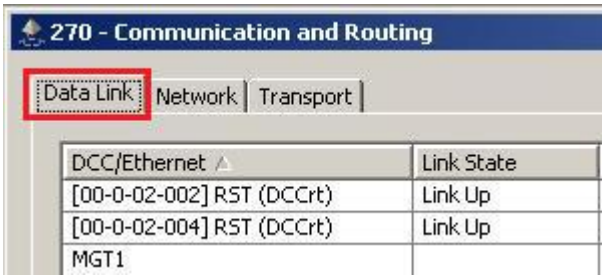
5° Passo: Abrirá uma janela com as configurações do canal DCC do equipamento, tem que estar configurado para os dois lados do anel conforme abaixo:



6° Passo: No elemento selecione as opções Element Management, seguido de Equipament e Communication and Routing:

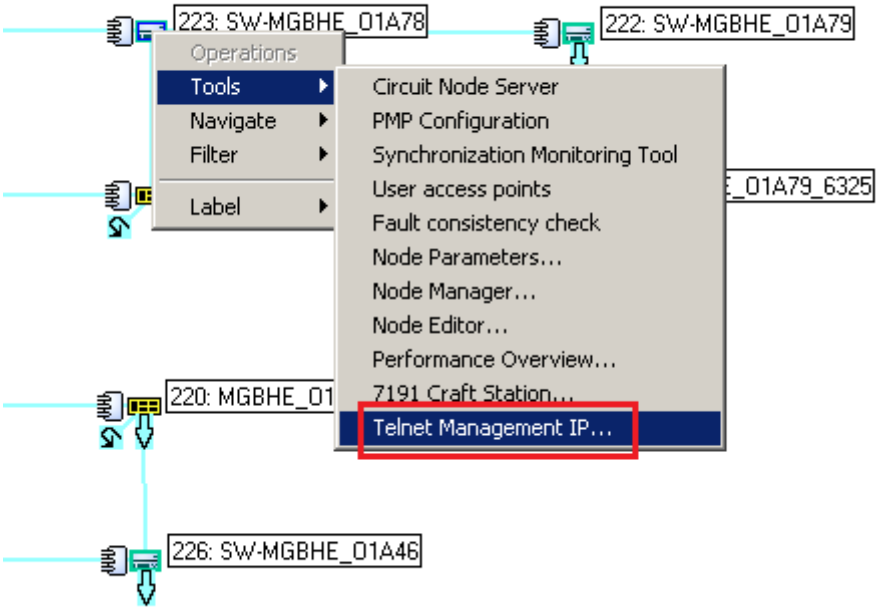


7° Passo: Abrirá uma janela, clique na aba Data Link, nela aparecerá o status de cada canal DCC:



- Tellabs 7345 Switch Agregação Ethernet

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione as opções Tools e Telnet Management IP:



2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar execute o comando “show running-config”, verifique as configurações da vlan 697, interface vlan 697, interface cpu0 e ip route:

```
vlan 697
 ports xgigabitethernet 1/2/1-2

interface vlan 697
 ip address  10.121.12.121 255.255.255.0
 no shutdown
```

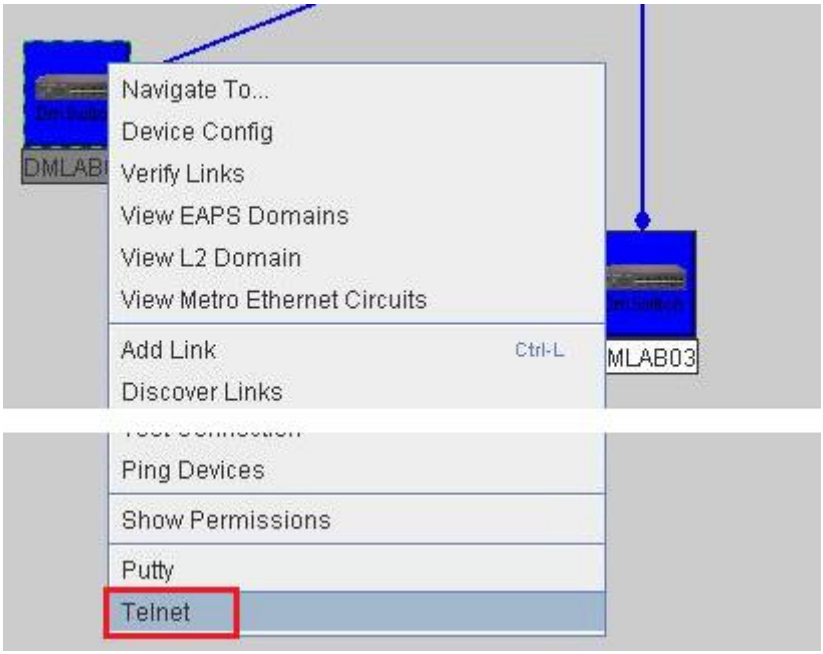
```
interface cpu0
 mtu 1500
 ip address  10.0.0.1 255.255.255.0
 no shutdown

ip route 0.0.0.0  0.0.0.0  10.121.12.254
```

3° Passo: Execute o comando “show interface description”, verifique o status das interfaces 10 Gb que estão conectadas aos elementos vizinhos, o status da cpo0 e da vlan697:

```
t7300-SW-MGBHE_O1A44# show interface description

Interface    Admin    Oper          ALS         Admin
              Status   Status        State       Status
---------    ------   ------      ---------     --------
Xg1/2/1       up       up          disabled      disabled
Xg1/2/2       up       up          disabled      disabled
Gi1/2/3       up       up          disabled      disabled
Gi1/2/4       up       up          disabled      disabled
Gi1/2/5       up       up          disabled      disabled
Gi1/2/6       up       up          disabled      disabled
Gi1/2/7      down     down         disabled      disabled
Gi1/2/8      down     down       disabled       disabled
Gi1/2/9      down     down       disabled       disabled
Gi1/2/10     down     down       disabled       disabled
Gi1/2/25      up       up          disabled      disabled
Gi1/2/26      up      down         disabled      disabled
cpu0          up      down         disabled      disabled
vlan697       up      up           disabled      disabled

 Serial0 up, 8 data bits, no parity, 38400 baud
```

- Datacom

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Telnet:



2° Passo: Irá abrir a interface CLI do equipamento, irá solicitar usuário e senha, após logar execute o comando “show running-config”, verifique as configurações da interface vlan 698, ip default-gateway e ip dns-server:

```
interface vlan 698
 name MGMT-DATACOM
 ip address 10.123.9.97/24
 set-member tagged ethernet range 1/25 1/26

ip default-gateway 10.123.9.254
ip dns-server 10.200.1.123
```

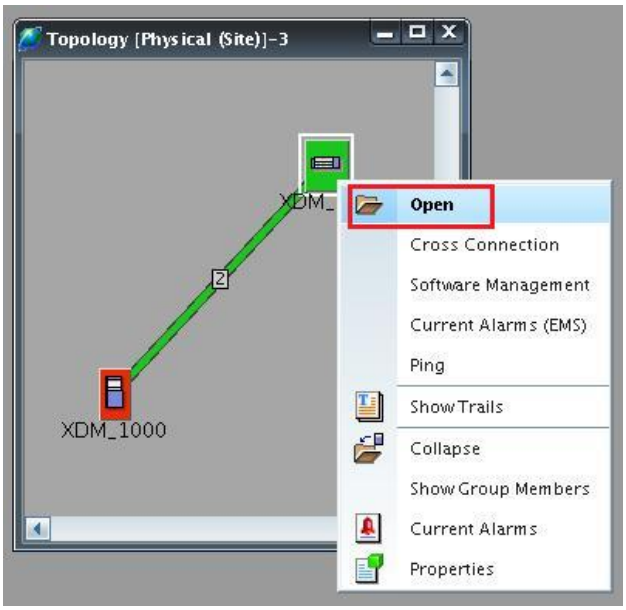
3° Passo: Execute o comando “show interfaces table configuration”, verifique o status das interfaces 25 e 26 que estão conectadas aos elementos vizinhos:

```
DMLAB01#show interfaces table configuration

                Port    Link   Auto       Speed       Duplex     Flow
 Port           State   Status Neg     Cfg  Actual  Cfg  Actual  Ctrl   Pvid
================================================================================
 1/ 1           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 2           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 3           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 4           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 5           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 6           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 7           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 8           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/ 9           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/10           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/11           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/12           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/13           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/14           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/15           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/16           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/17           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/18           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/19           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/20           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/21           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/22           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/23           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
 1/24 D2BH      ENABLE  UP     ON      100  100     AUTO FULL    NONE   698
 1/25 RT:M      ENABLE  UP     ON      100  1000    AUTO FULL    NONE     1
 1/26 RT:M      ENABLE  UP     ON      100  1000    AUTO FULL    NONE     1
 1/27 D2BH      ENABLE  UP     ON      100  1000    AUTO FULL    NONE     1
 1/28           DISABLE DOWN   ON      100          AUTO HALF    NONE     1
================================================================================
                    spacebar->toggle screen  ESC->exit
DMLAB01#
```

Procedimento de verificação de configurações de sincronismo de equipamentos SDH

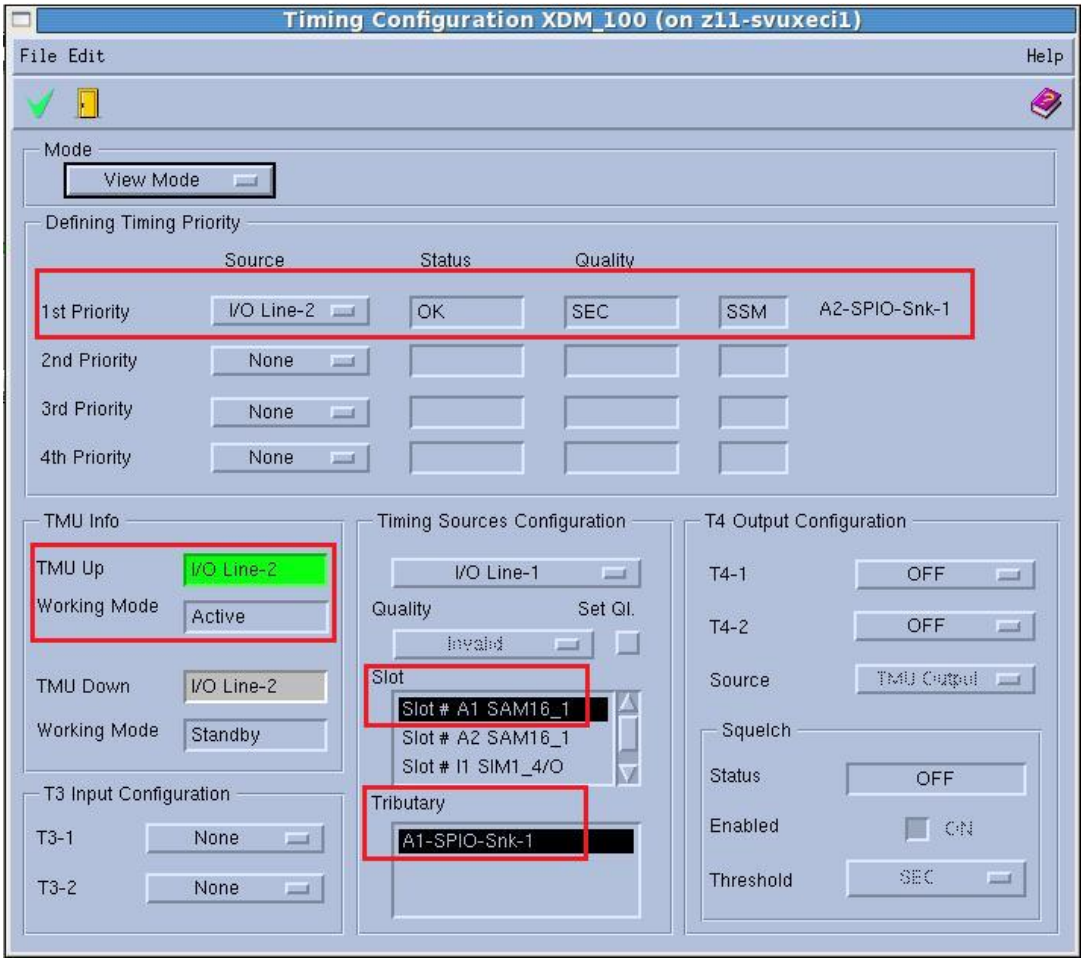
- ECI

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:



2° Passo: Após abrir o elemento selecione a opção Configuration na parte superior do elemento, em seguida clique na opção Timing:

2° Passo: Abrirá uma janela com as informações das interfaces principal e secundária configuradas para sincronismo e status de cada interface conforme abaixo:

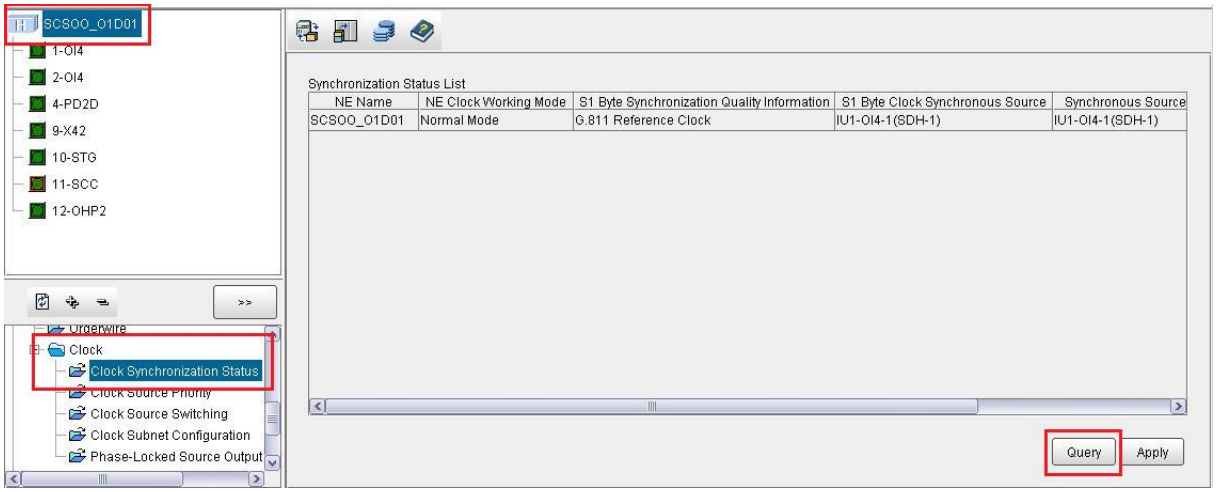


- Huawei

1° Passo: Clique com o botão direito do mouse em cima do elemento que deseja verificar, em seguida selecione a opção Open:

2° Passo: Após abrir o elemento clique no botão NE Explorer no canto superior esquerdo:

3° Passo: Após abrir a janela selecione o equipamento no campo superior esquerdo, em seguida no campo inferior esquerdo as opções Configuration Clock e Clock Synchronization Status e clicar no botão Query para atualizar as informações, na mesma janela temos as informações tipo de qualidade do Clock e interfaces primária e secundária configuradas para sincronismo do equipamento:

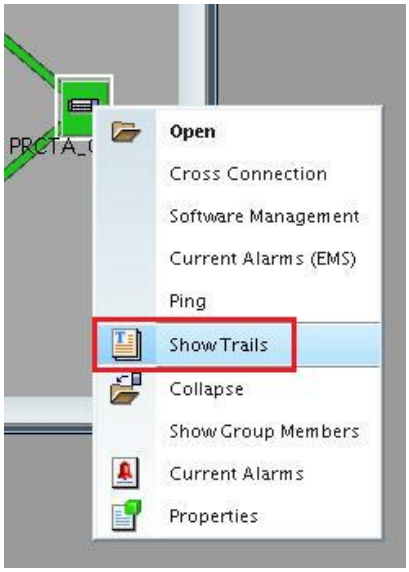


Procedimento de verificação de configurações de serviços (Dados, Voz por V5, Voz por H248 e MGMT)

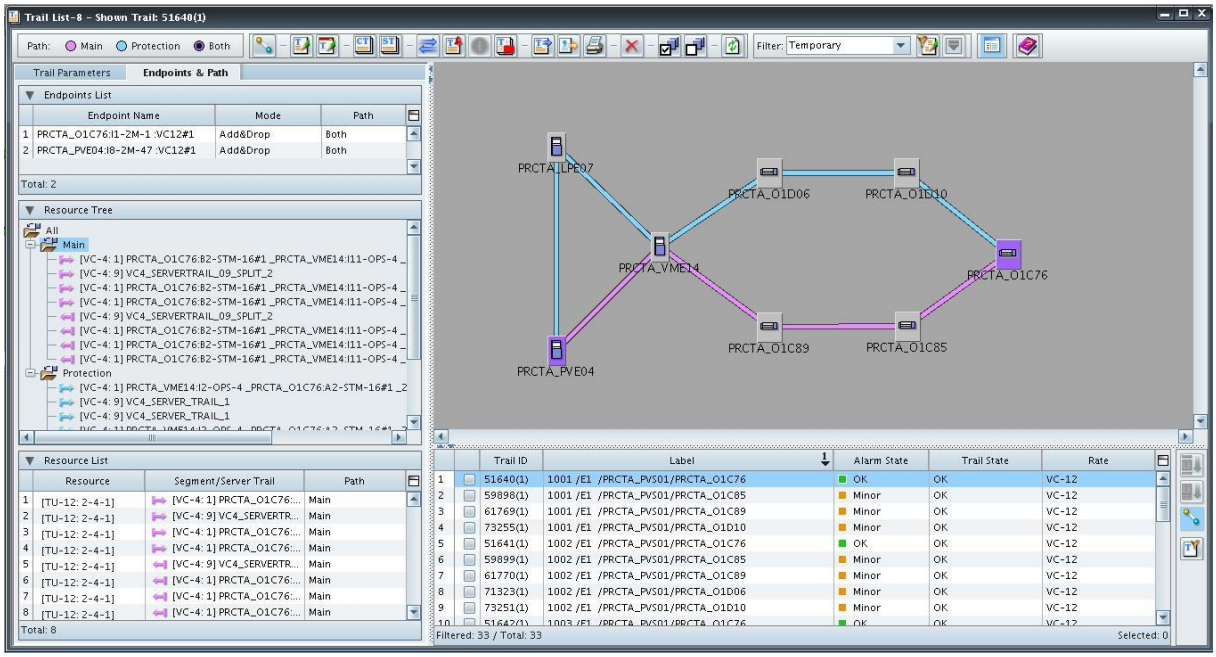
- ECI

- Verificando as configurações de serviços de Voz por V5:

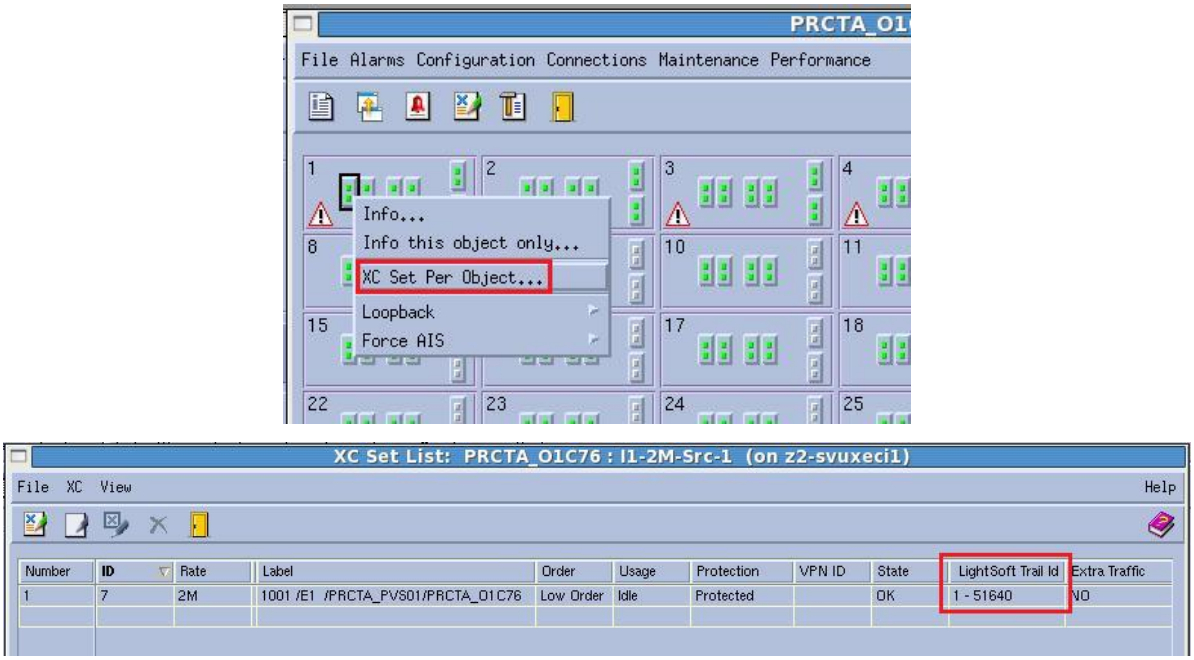
1° Passo: Selecione o elemento que deseja verificar, clique com o botão direito do mouse, após abrir a aba selecione a opção Show Trails:



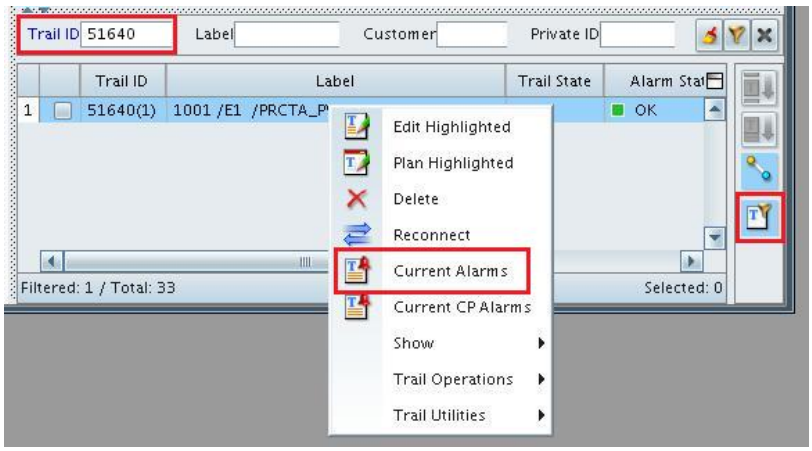
2° Passo: Abrirá uma janela listando todos os serviços SDH configurados no elemento:



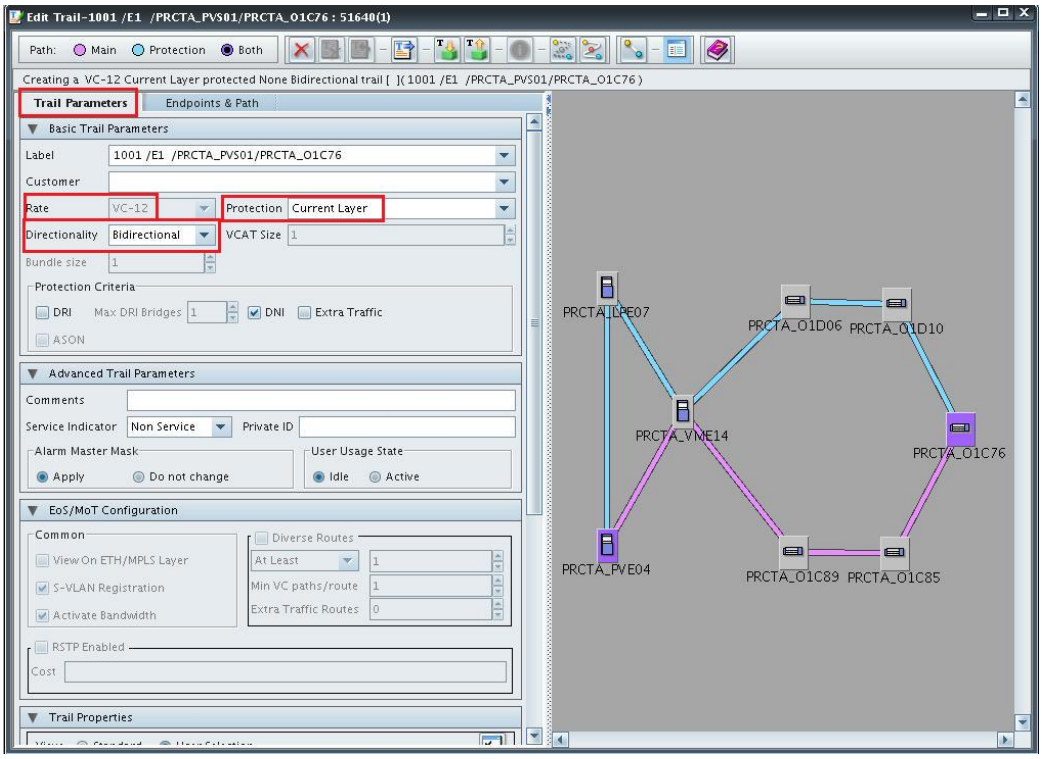
3° Passo: Para listar todos os serviços SDH configurados em uma interface abra a placa do elemento e selecione a interface tributária desejada, clique com o botão direito do mouse e selecione a opção XC Set Per Object, anote o Trail Id do circuito, conforme abaixo:



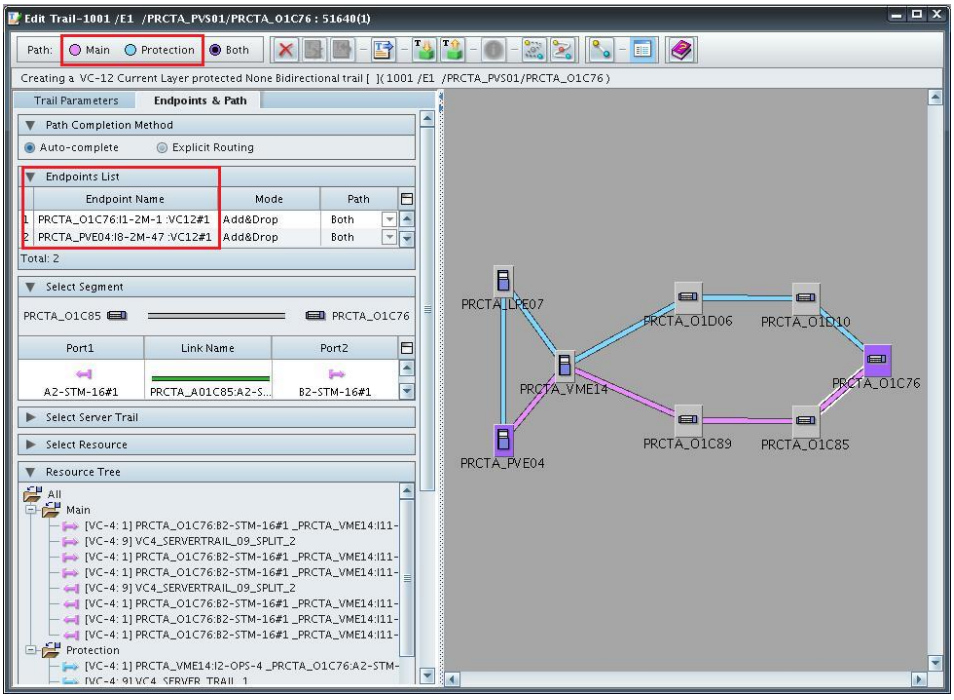
4° Passo: Na janela onde foram listados todos os serviços do elemento selecione a opção para pesquisa no canto inferior direito da janela, após abrir a barra de pesquisa insira o Trail Id anotado anteriormente. Selecione o serviço desejado e clique com o botão direito do mouse, após abrir a aba selecione a opção Current Alarms para verificar os alarmes do serviço selecionado:



5° Passo: Na aba Trail Parameters devem ser verificados a as opções Rate. Onde Rate á a taxa de transmissão, Protection é setado Current Layer para circuito protegido e Unprotected para desprotegido e Directinality é setado Bidirectional ou Unidirectional:



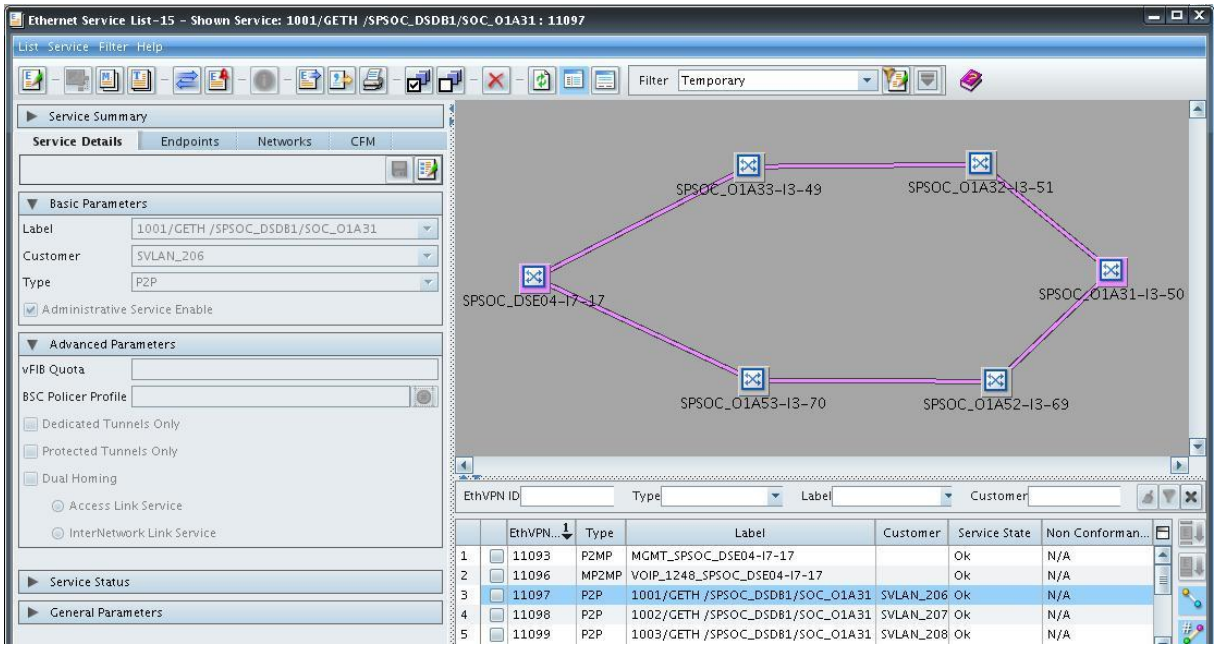
6° Passo: Selecione a aba Endpoints & Path, nela podemos verificar as interfaces onde fecham o circuito e o caminho configurado, no exemplo abaixo como o circuito é protegido o caminho principal é destacado em rosa e a proteção é destacada em azul:



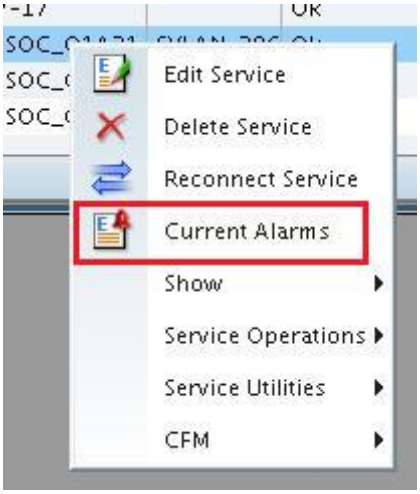
- Verificando as configurações de serviços de Dados:

1° Passo: Selecione o elemento que deseja verificar, em seguida clique no botão ETH Service List, no canto superior da tela:

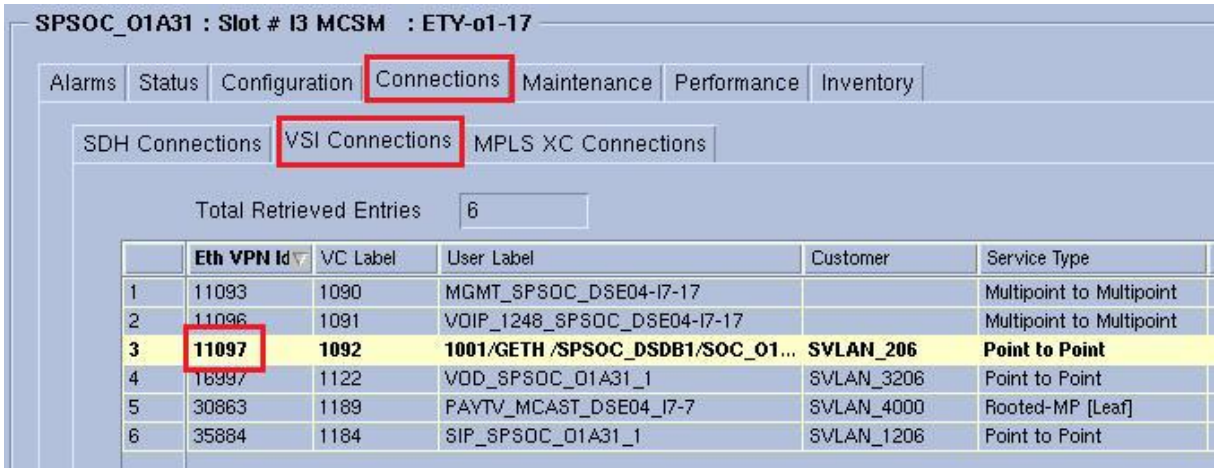
2° Passo: Abrirá uma janela listando todos os serviços Ethernet configurados no elemento:



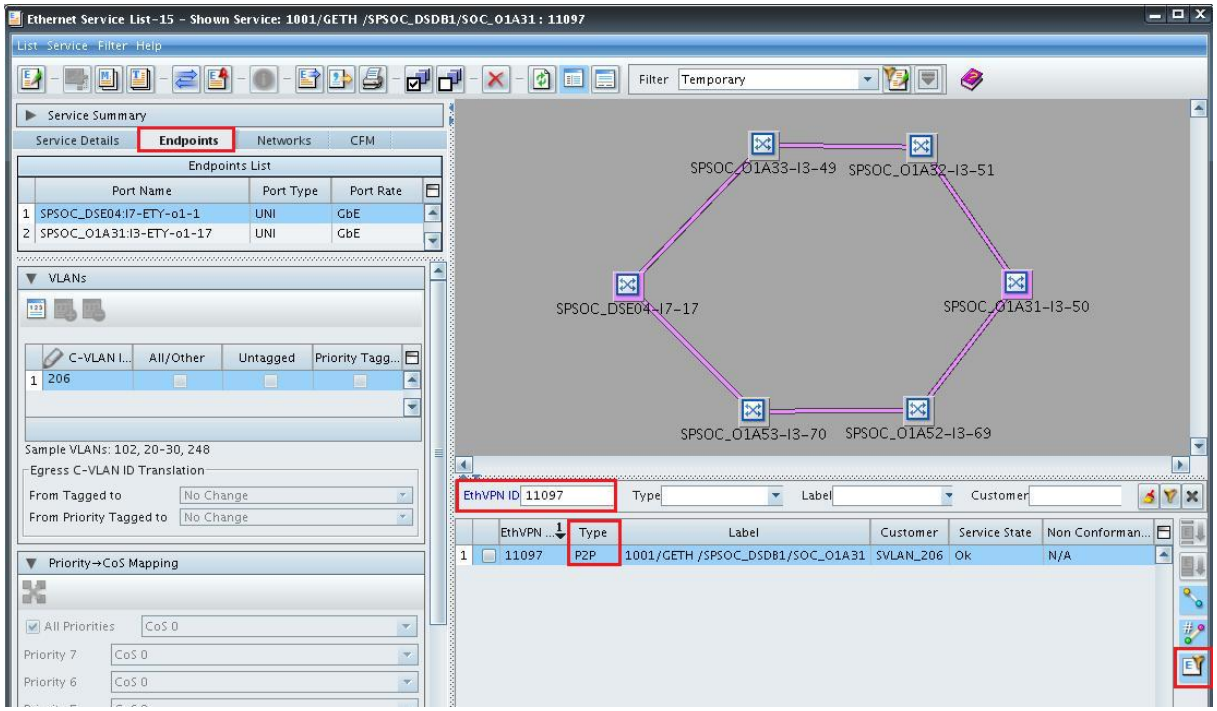
3° Passo: Selecione o serviço desejado e clique com o botão direito do mouse, após abrir a aba selecione a opção Current Alarms para verificar os alarmes do serviço selecionado:



4° Passo: Para listar todos os serviços Ethernet configurados em uma interface do elemento abra a placa MCSM do elemento e selecione a interface desejada, em seguida selecione as opções Connections e VSI Connections, se desejar verificar um serviço específico anote o Eth VPN Id conforme abaixo:



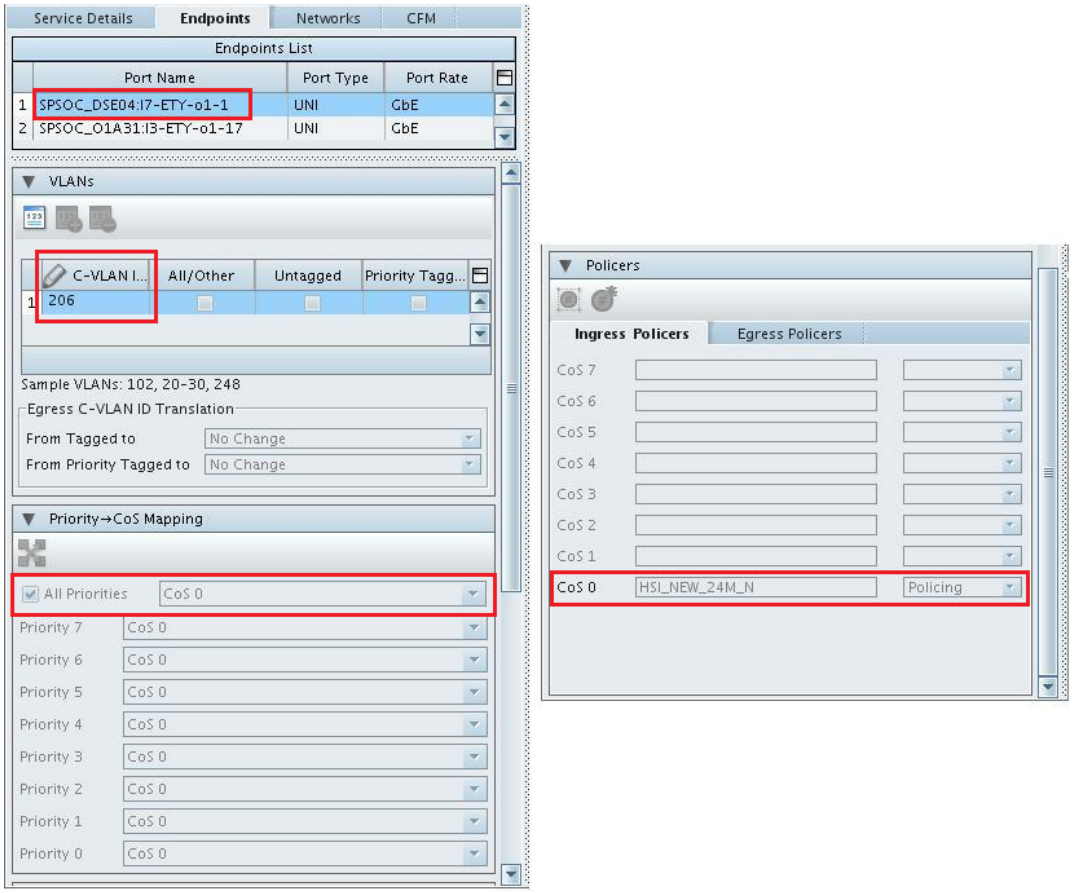
5° Passo: Na janela onde foram listados todos os serviços do elemento selecione a opção para pesquisa no canto inferior direito da janela, após abrir a barra de pesquisa insira o Eth VPN Id anotado anteriormente. Note que o serviço selecionado abaixo é ponto a ponto. Selecione a aba Endpoints para verificar as configurações do serviço:



6° Passo: Na coluna a esquerda da janela verifique os parâmetros de configurações selecionando uma das interfaces. Na interface devem estar configurados:

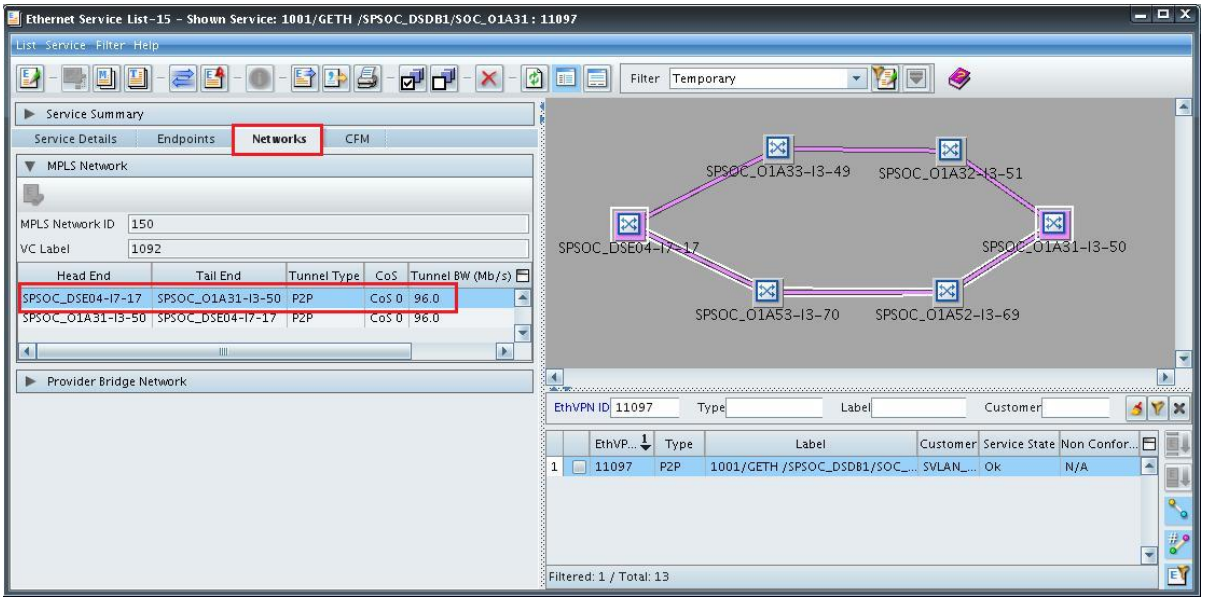
- VLAN: Deve ser o mesmo que foi configurado no DSLAM e BRAS;

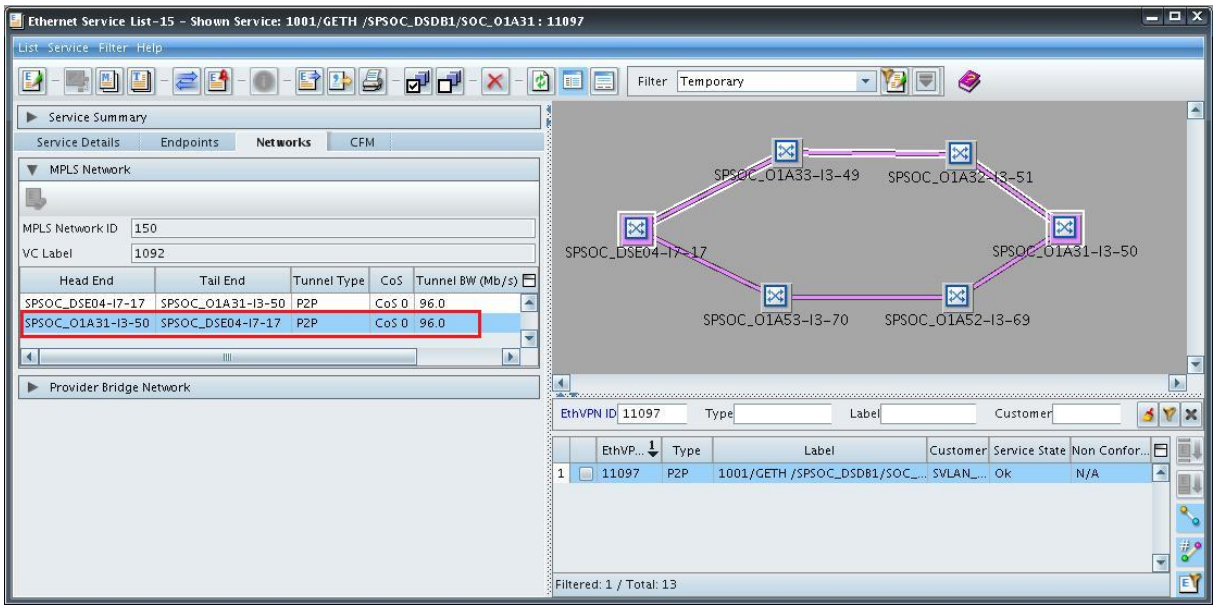
- Priority -> CoS Mapping: Selecionado opção All Priorities e CoS 0 para os serviços de Dados;
- Policers: Ingress Policers: Policing ou No Rate Limite setado na CoS 0;
  Egress Policers: No Rate Limite setado.



Após verificar os parâmetros de configurações da primeira interface verifique a segunda, deve conter as mesmas configurações.

7° Passo: Selecione a aba Networks para verificar os túneis de passagem da rede MPLS, como o serviço é ponto a ponto haverá apenas dois túneis, um de ida, do headend para o armário e outro de volta, do armário para o headend, estará em sentido anti-horário em relação ao anel, devem estar configurados na CoS 0 e com Banda de 96 Mb /s para os serviços de Dados, conforme abaixo:

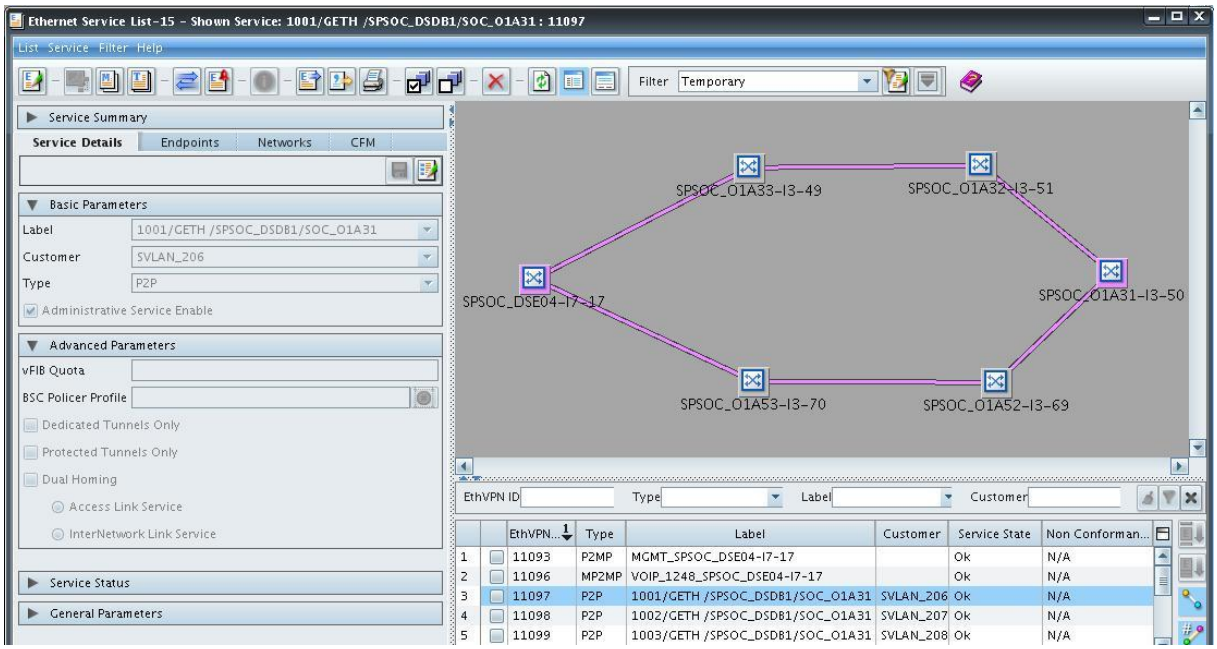




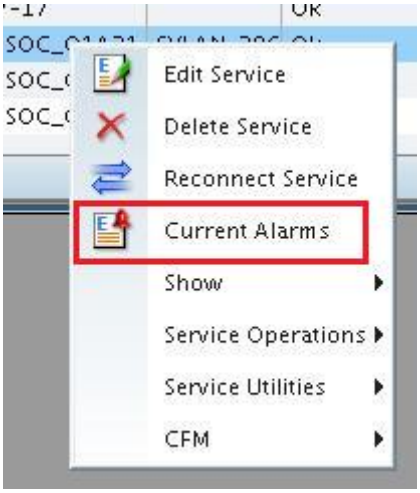
- Verificando as configurações de serviços de Voz por H248:

1° Passo: Selecione o elemento que deseja verificar, em seguida clique no botão ETH Service List, no canto superior da tela:

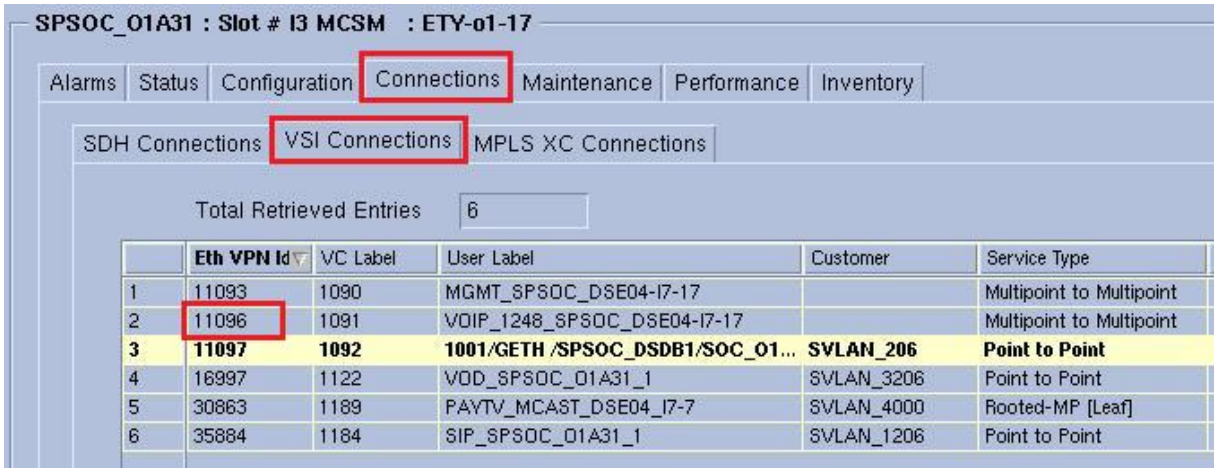
2° Passo: Abrirá uma janela listando todos os serviços Ethernet configurados no elemento:



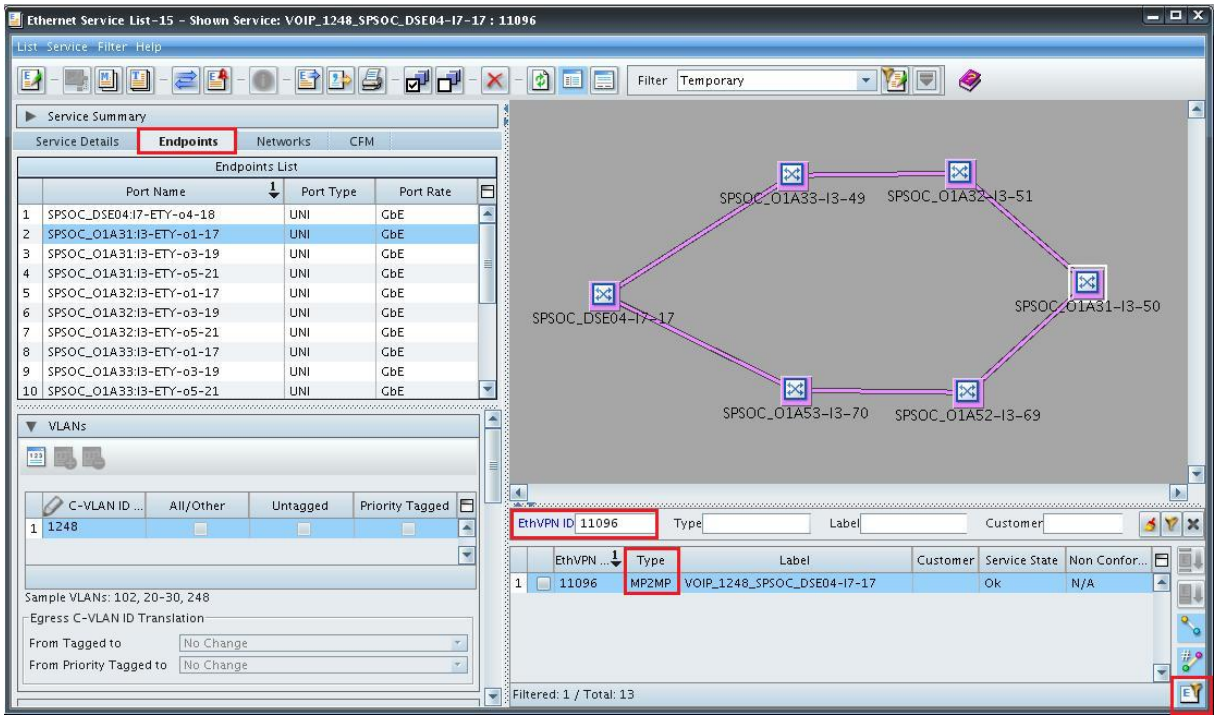
3° Passo: Selecione o serviço desejado e clique com o botão direito do mouse, após abrir a aba selecione a opção Current Alarms para verificar os alarmes do serviço selecionado:



4° Passo: Para listar todos os serviços Ethernet configurados em uma interface do elemento abra a placa MCSM do elemento e selecione a interface desejada, em seguida selecione as opções Connections e VSI Connections, se desejar verificar um serviço específico anote o Eth VPN Id conforme abaixo:



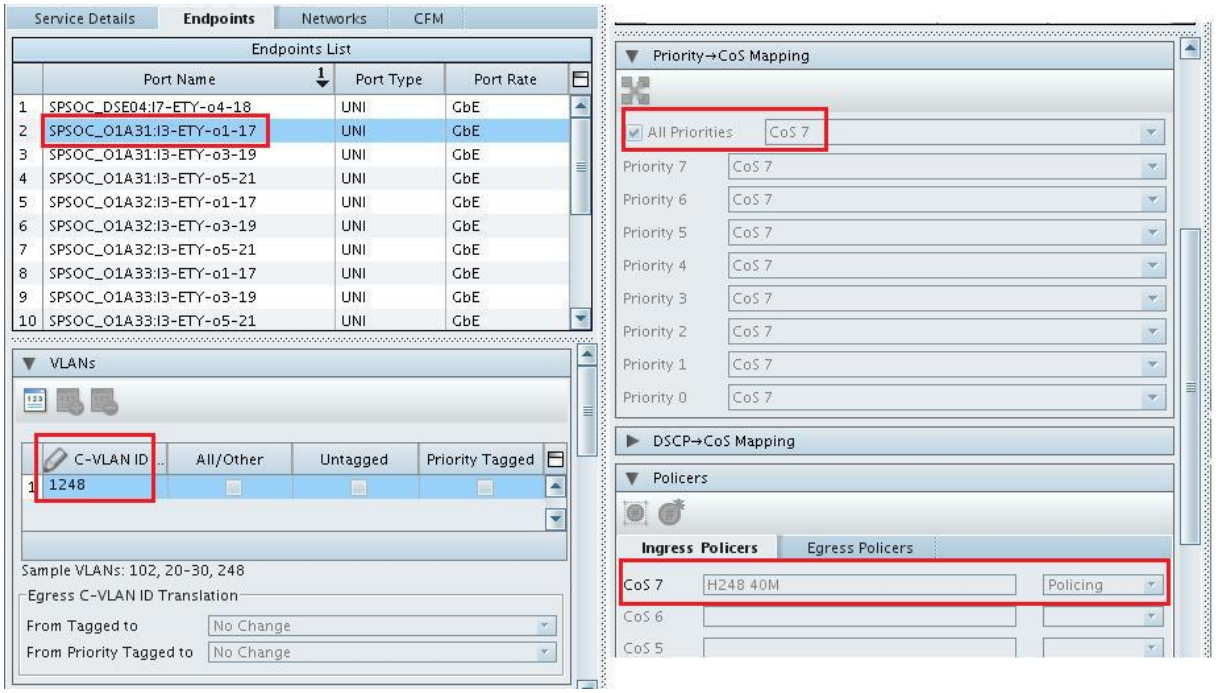
5° Passo: Na janela onde foram listados todos os serviços do elemento selecione a opção para pesquisa no canto inferior direito da janela, após abrir a barra de pesquisa insira o Eth VPN Id anotado anteriormente. Note que o serviço selecionado abaixo é MP2MP (Múltiplos Pontos para Múltiplos Pontos). Selecione a aba Endpoints para verificar as configurações do serviço:



6° Passo: Na coluna a esquerda da janela verifique os parâmetros de configurações selecionando uma das interfaces. Na interface devem estar configurados:

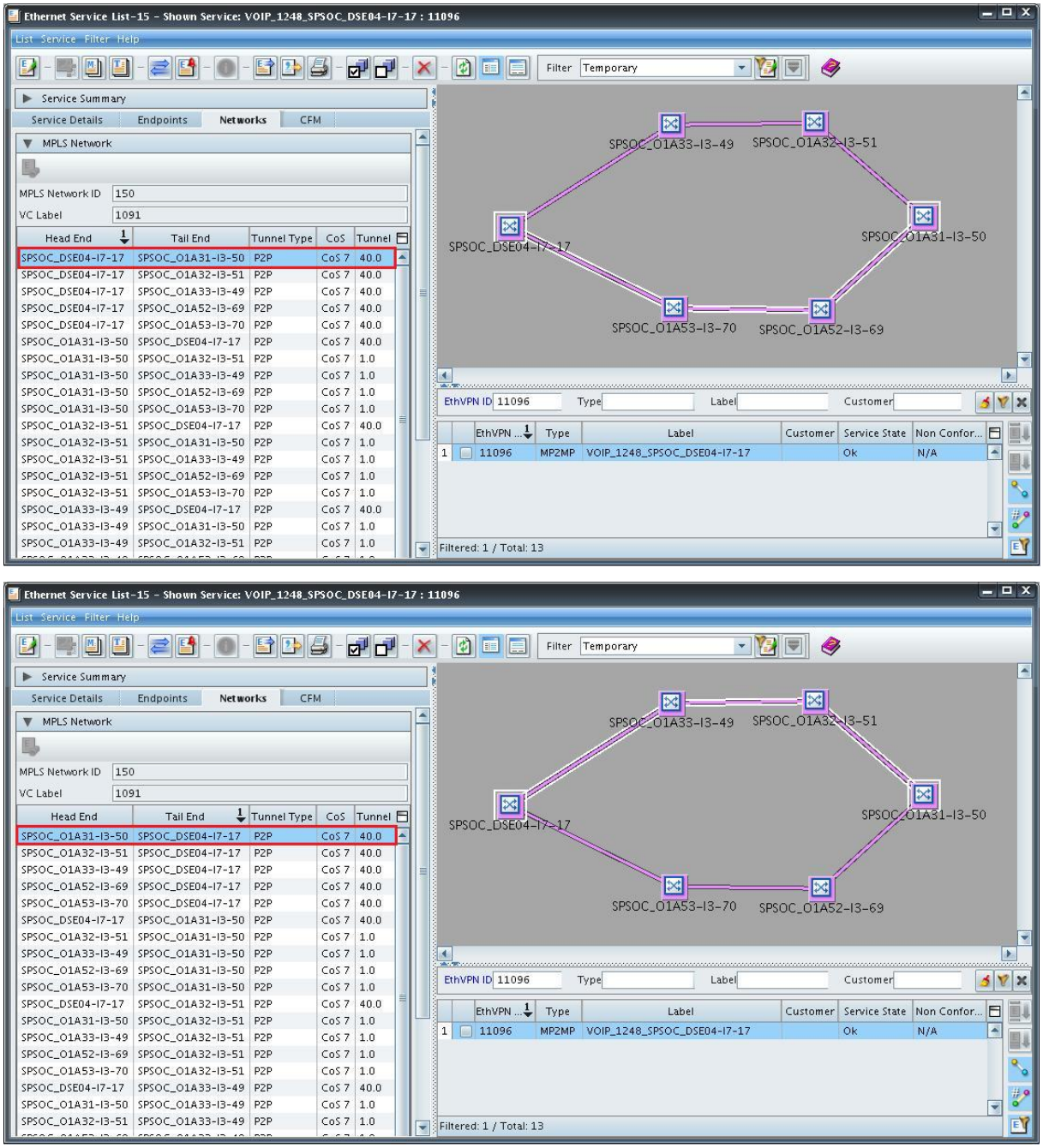
- VLAN: Deve ser o mesmo que foi configurado no DSLAM e SW-AGG, sendo 1248 ou 1249 para H248;

- Priority -> CoS Mapping: Selecionado opção All Priorities e CoS 7 para os serviços de Voz por H248;
- Policers: Ingress Policers: Policing ou No Rate Limite setado na CoS 7;
  Egress Policers: No Rate Limite setado.



Após verificar os parâmetros de configurações da primeira interface verifique todas as outras, devem conter as mesmas configurações.

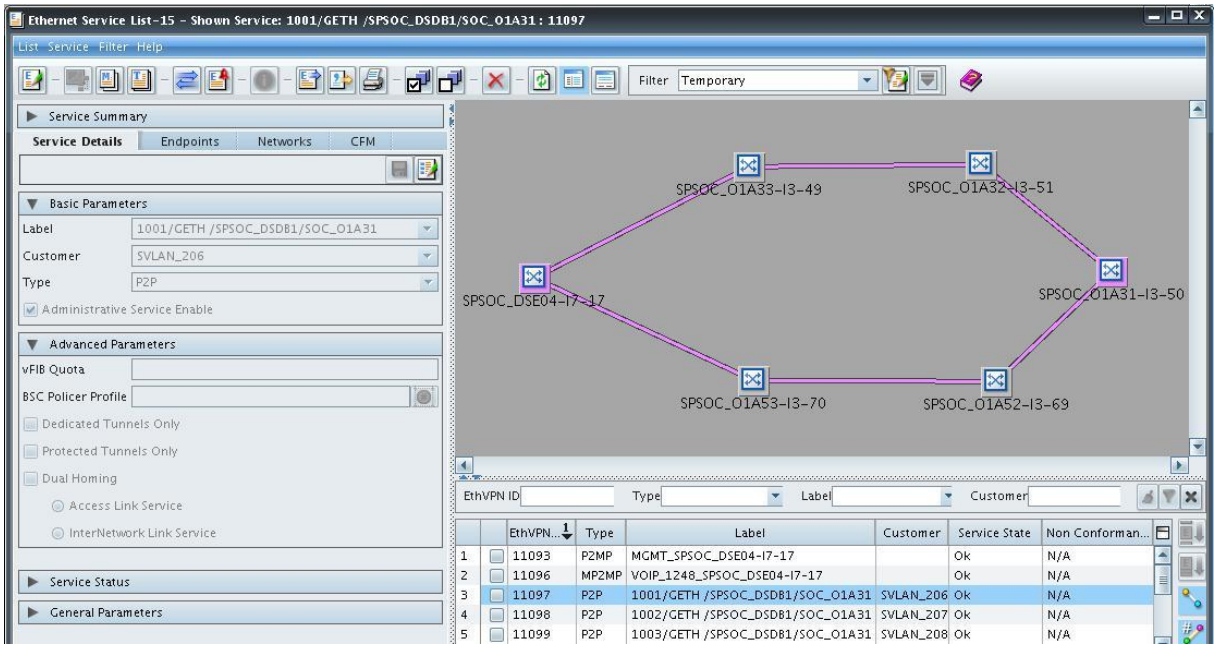
7° Passo: Selecione a aba Networks para verificar os túneis de passagem da rede MPLS, como o serviço é MP2MP haverá túneis entre todos os elementos do anel, porém que mantém o serviço ativo é o de ida, do headend para o armário e o de volta, do armário para o headend. Estará em sentido anti-horário em relação ao anel, devem estar configurados na CoS 7 e com banda de 40 Mb /s entre o headend e o armário e 1 Mb /s entre os elementos do anel.



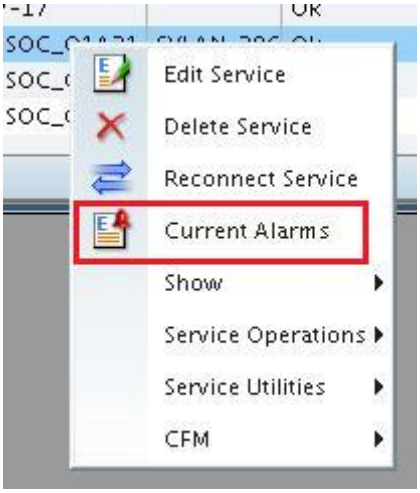
- Verificando as configurações de gerência dos DSLAMs e fontes:

1° Passo: Selecione o elemento que deseja verificar, em seguida clique no botão ETH Service List, no canto superior da tela:

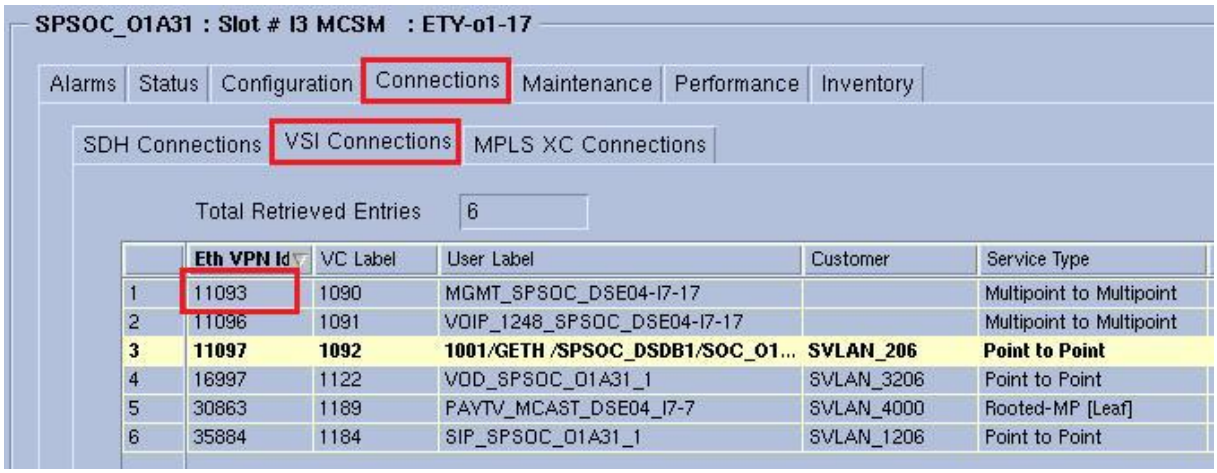
2° Passo: Abrirá uma janela listando todos os serviços Ethernet configurados no elemento:



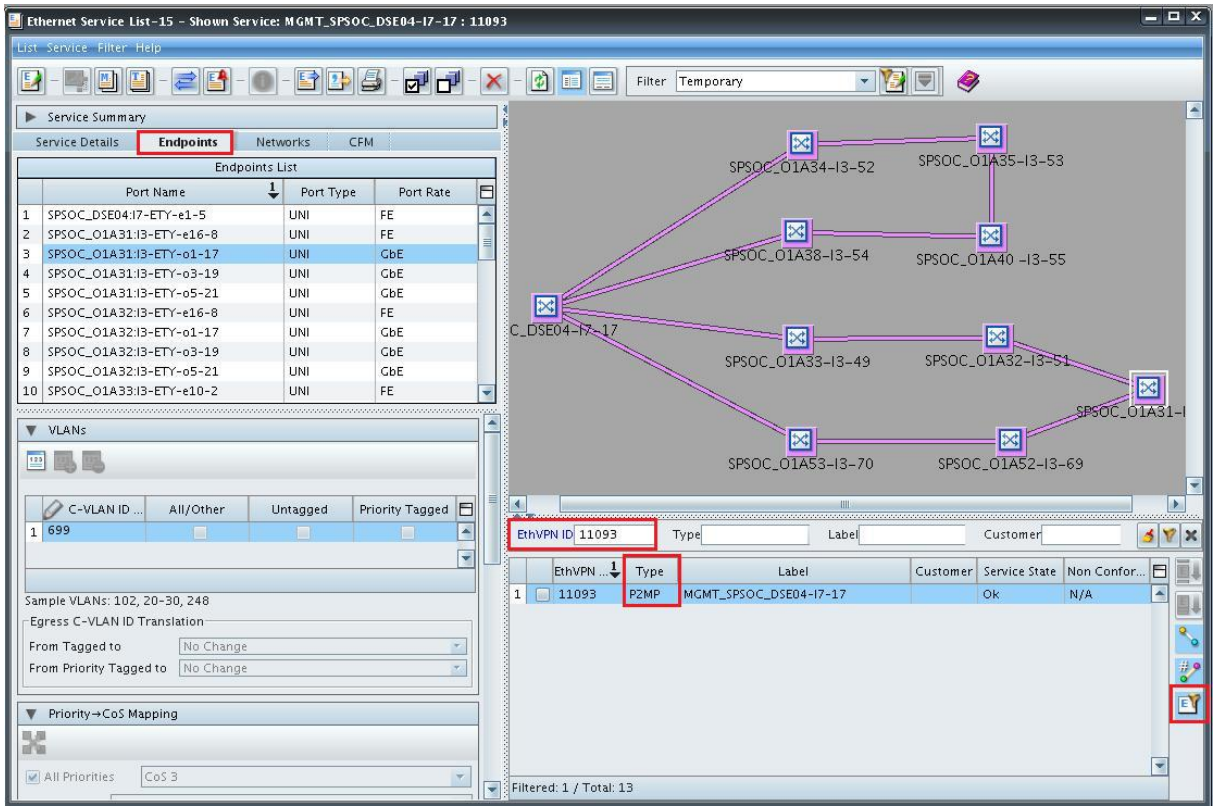
3° Passo: Selecione o serviço desejado e clique com o botão direito do mouse, após abrir a aba selecione a opção Current Alarms para verificar os alarmes do serviço selecionado:



4° Passo: Para listar todos os serviços Ethernet configurados em uma interface do elemento abra a placa MCSM do elemento e selecione a interface desejada, em seguida selecione as opções Connections e VSI Connections, se desejar verificar um serviço específico anote o Eth VPN Id conforme abaixo:



5° Passo: Na janela onde foram listados todos os serviços do elemento selecione a opção para pesquisa no canto inferior direito da janela, após abrir a barra de pesquisa insira o Eth VPN Id anotado anteriormente. Note que o serviço selecionado abaixo é P2MP (Ponto para Múltiplos Pontos). Selecione a aba Endpoints para verificar as configurações do serviço:



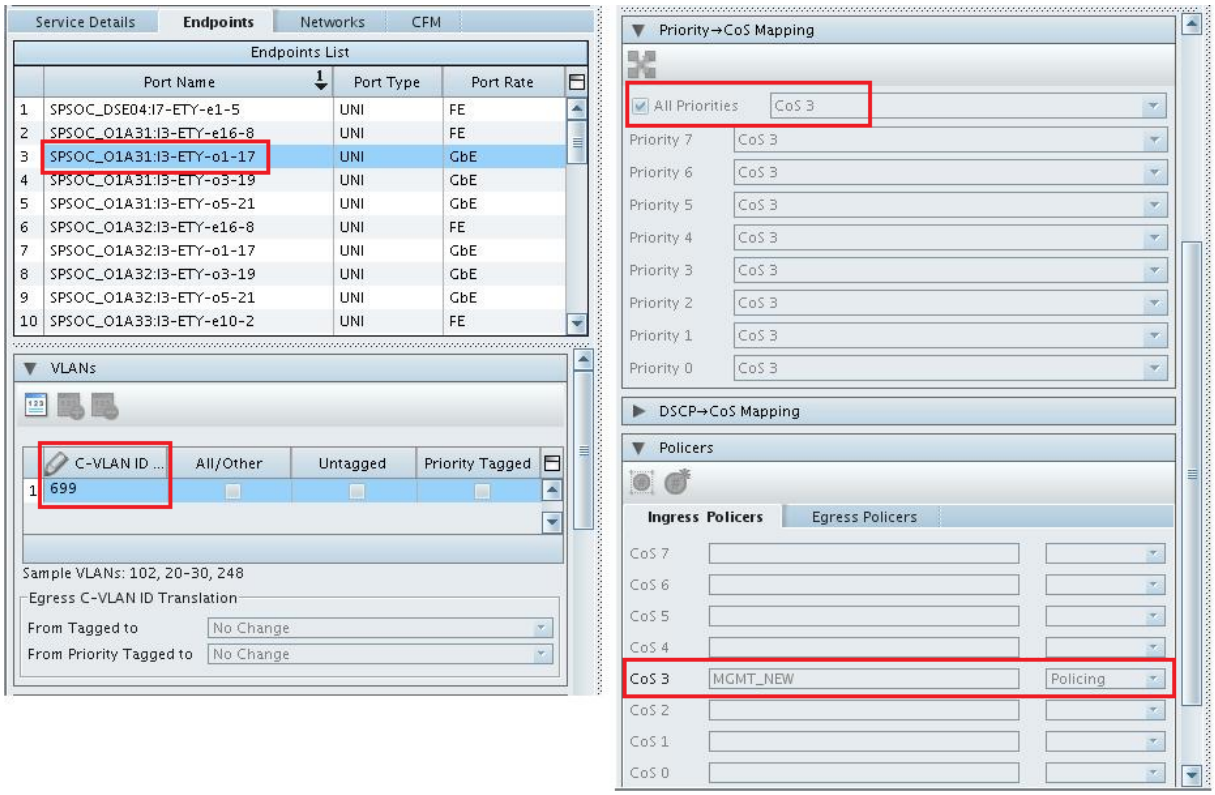
6° Passo: Na coluna a esquerda da janela verifique os parâmetros de configurações selecionando uma das interfaces. Na interface devem estar configurados:

- VLAN: Deve ser o mesmo que foi configurado no DSLAM e SW-MGMT, sendo 699, 700, 1010 para DSLAMs e 704 para fontes;

- Priority -> CoS Mapping: Selecionado opção All Priorities e CoS 3 ou CoS 4 para os serviços de MGMT;

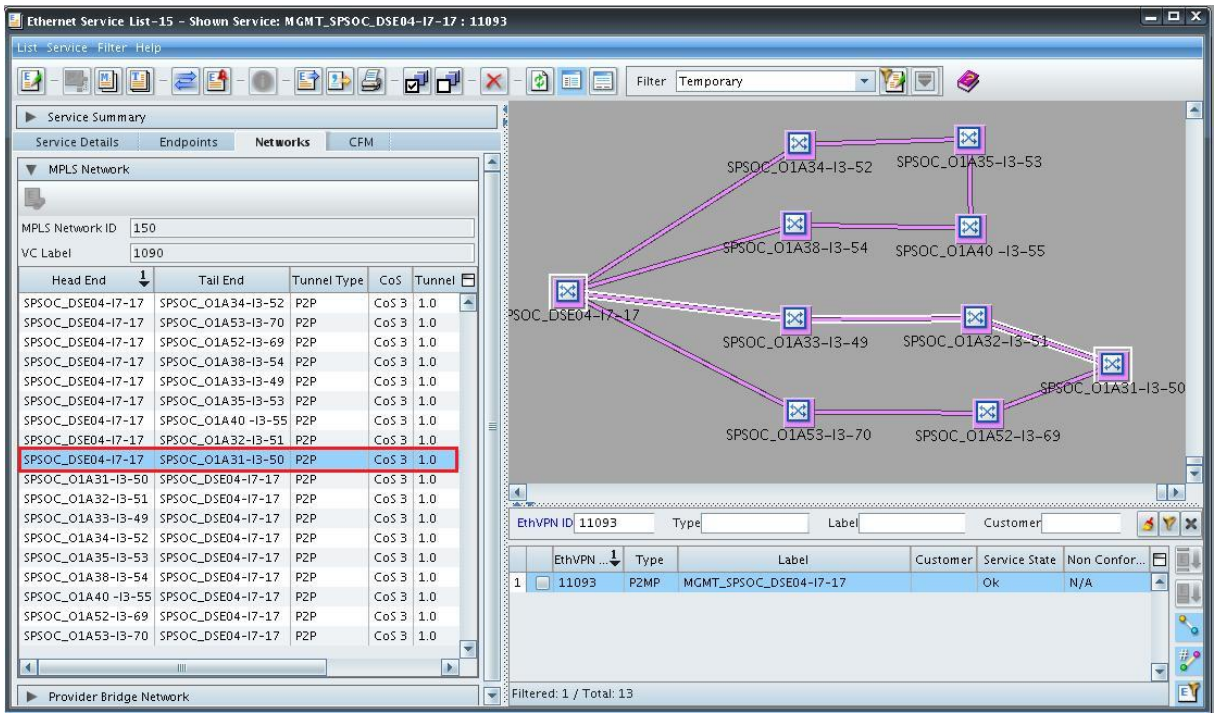
- Policers: Ingress Policers: Policing ou No Rate Limite setado na CoS 3 ou CoS 4;

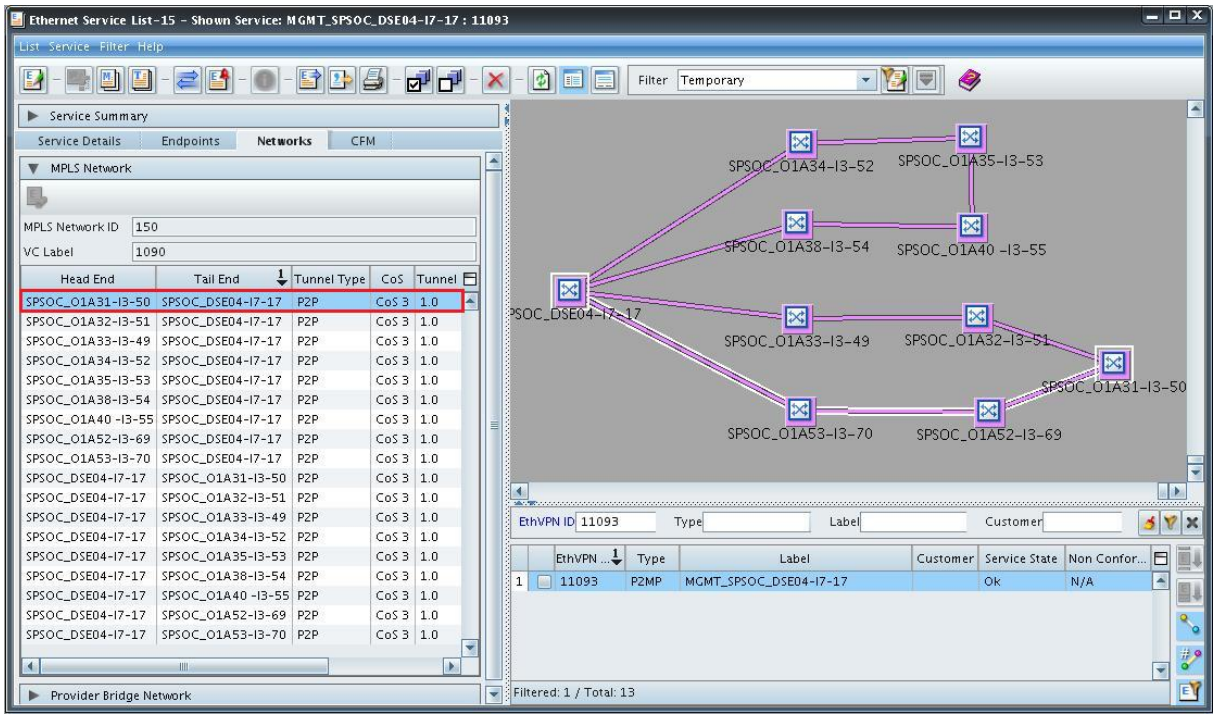
Egress Policers: No Rate Limite setado.



Após verificar os parâmetros de configurações da primeira interface verifique todas as outras, devem conter as mesmas configurações.

7° Passo: Selecione a aba Networks para verificar os túneis de passagem da rede MPLS, como o serviço é P2MP haverá túneis entre o headend e todos os elementos do anel, verificar os túneis de ida, do headend para o armário e o de volta, do armário para o headend. Estará em sentido horário em relação ao anel, devem estar configurados na CoS 3 ou CoS 4 e com banda de 1 Mb /s.

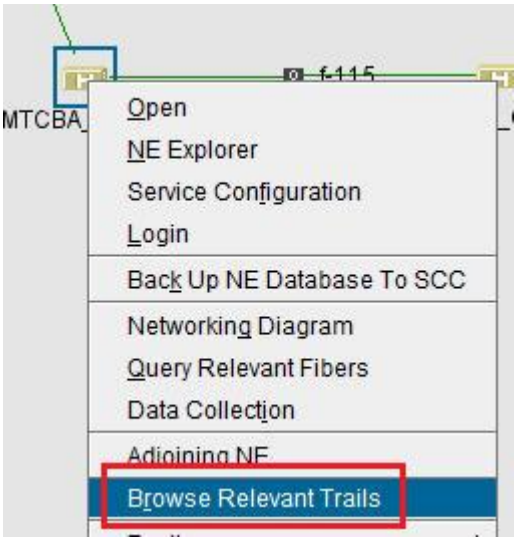




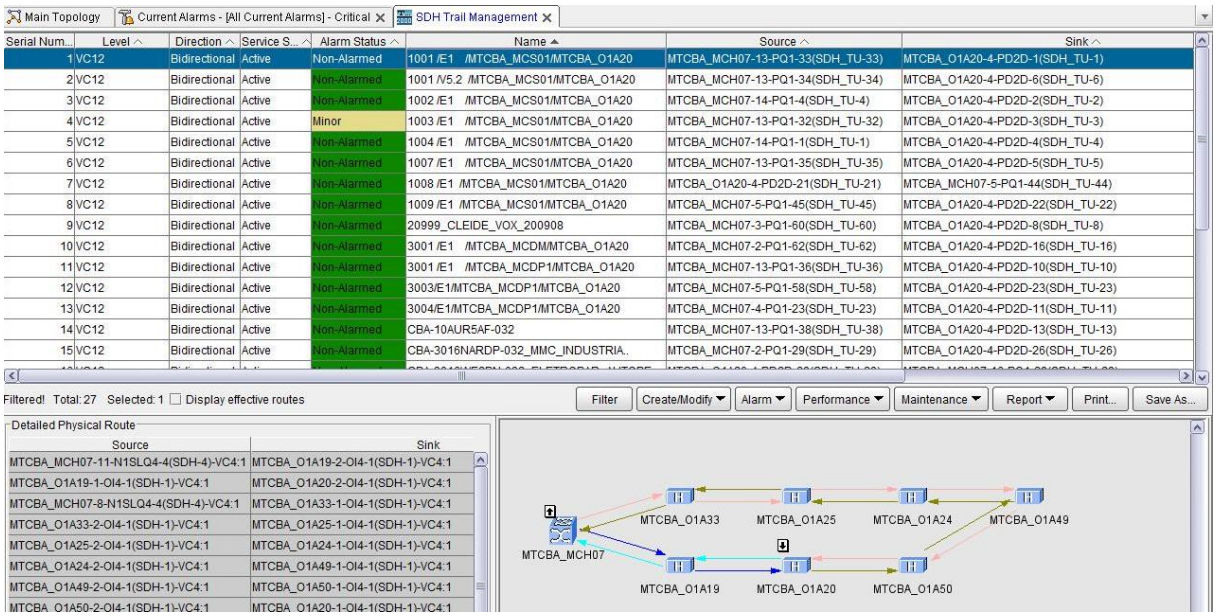
- Huawei

- Verificando as configurações de serviços de Voz por V5:

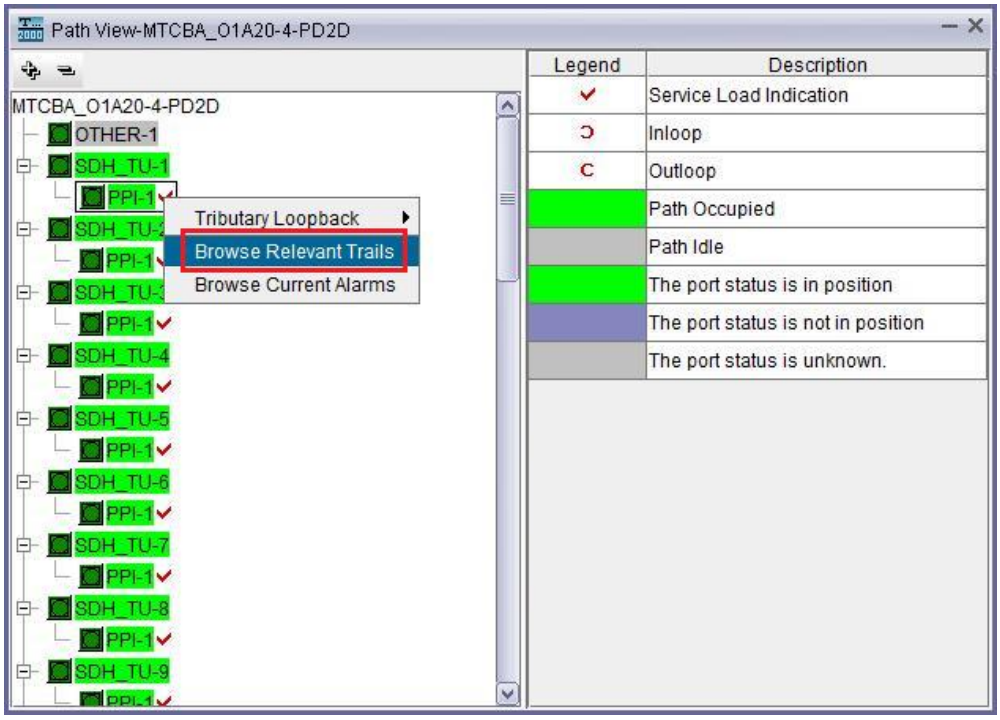
1° Passo: Selecione o elemento que deseja verificar, clique com o botão direito do mouse, após abrir a aba selecione a opção Browse Relevant Trails:



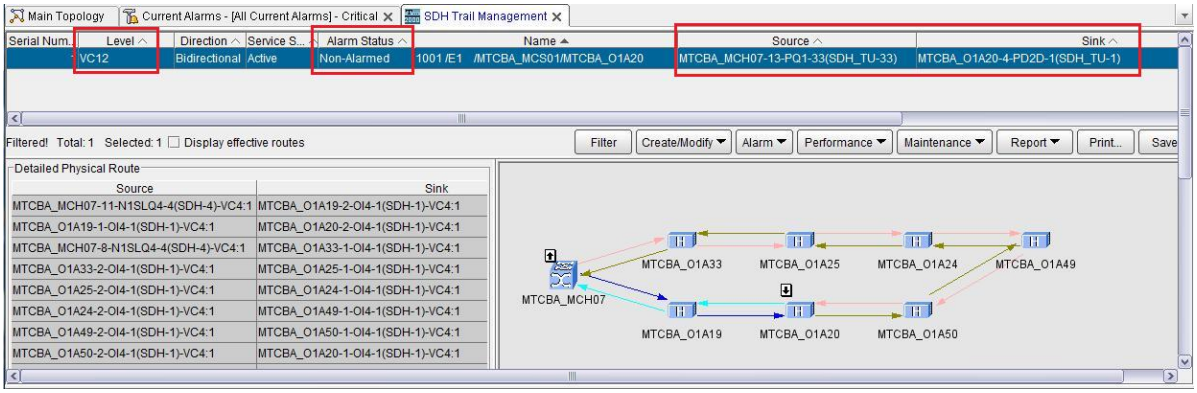
2° Passo: Abrirá uma janela listando todos os serviços SDH configurados no elemento:



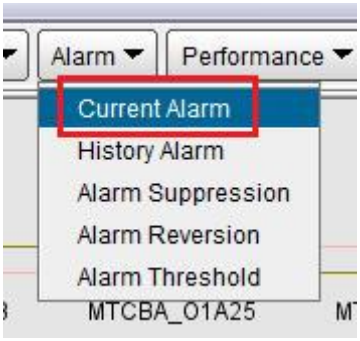
3° Passo: Para listar todos os serviços SDH configurados em uma interface abra a placa do elemento e selecione a interface tributária desejada, clique com o botão direito do mouse e selecione a opção Browse Relevant Trails, conforme abaixo:



5° Passo: Após abrir a janela pode ser verificada a taxa de transmissão do circuito em Level, se há alarmes ativos em Alarm Status e as interfaces onde fecham o circuito em Source e Sink, assim como o caminho utilizado pelo circuito:



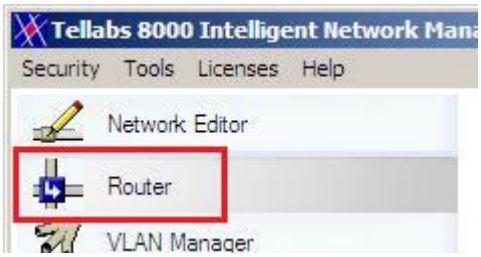
4° Passo: Selecione o serviço desejado e clique no botão alarme, após abrir a aba selecione a opção Current Alarm para verificar os alarmes ativos do serviço selecionado:



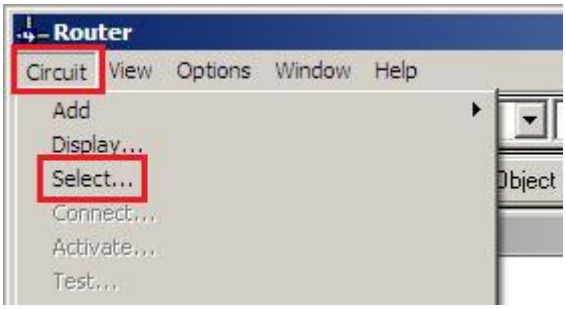
- Tellabs 6325 Edge Node

- Verificando as configurações de serviços de Voz por V5:

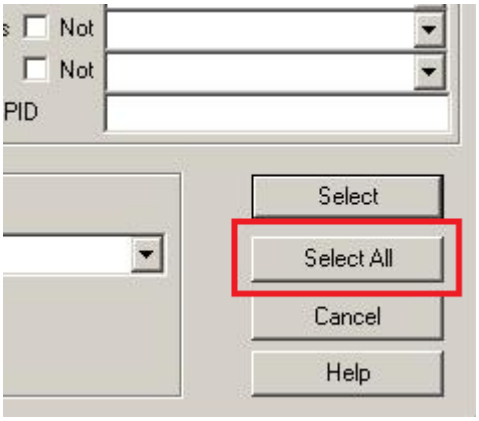
1° Passo: No ToolBox da gerência selecione a opção Router, conforme abaixo:



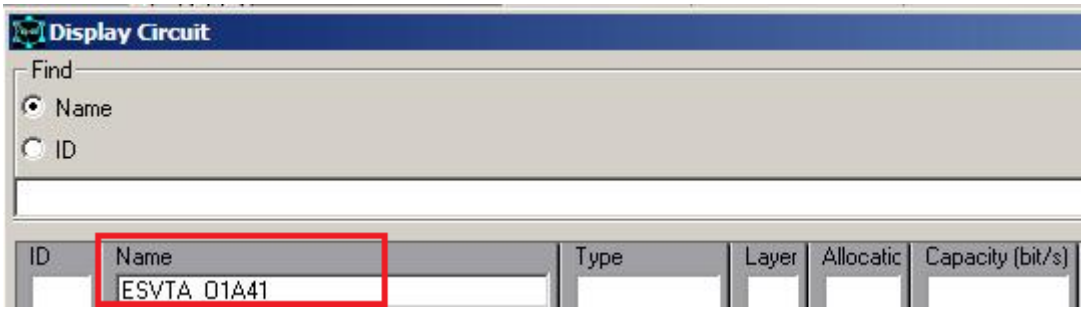
2° Passo: Abrirá uma janela, clique no botão Circuit no canto superior esquerdo da tela seguido de Select:



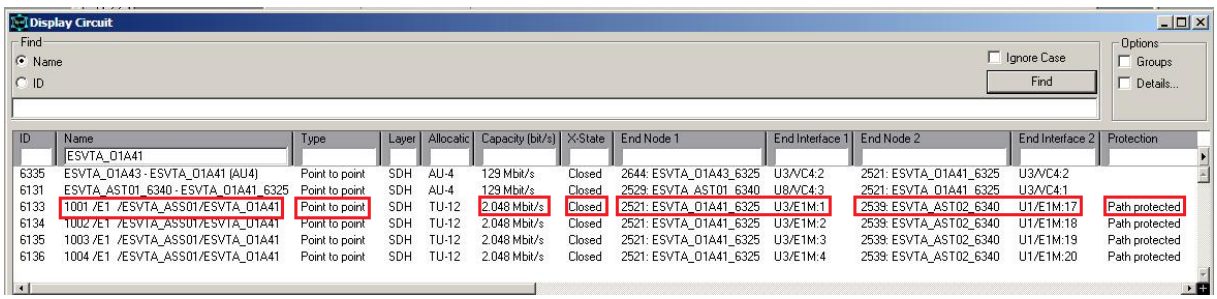
3° Passo: Na próxima janela, clique no botão Select All no canto inferior direito da tela:



4° Passo: Abrirá uma janela listando todos os serviços SDH configurados na rede, insira o nome do armário no campo name, assim serão listados apenas os circuitos do armário, também pode ser listado pelos campos End Node:



5° Passo: Abrirá uma janela listando todos os serviços SDH configurados no elemento, no circuito destacado abaixo temos as informações de tipo do circuito (P2P), capacidade (2Mb/s), estado (closed para conectado, open para desconectado), interfaces onde fecham o circuito e proteção do circuito (Patch Protected):



- Tellabs 7345 Switch Agregação Ethernet

- Verificando as configurações de serviços de Dados:

1° Passo: Após logar no equipamento execute o comando “show vlan id XXX”, onde XXX é a VLAN de serviços de dados. Devem estar adicionadas ao Member Port a porta que esta conectada ao DSLAM e as interfaces 10 Gb que estão conectadas aos elementos vizinhos, conforme abaixo:

t7300-SW-MGBHE_O1A44# show vlan id 238
Vlan database

Vlan ID : 238
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3
Untagged Ports : None
Stats Collection State : Enabled
Name : 1001-GETH-MGBHE_O1A44
Status : Permanent

2° Passo: Execute o comando “show interface name” e verifique pelas descrições das interfaces se as configurações estão coincidindo:

t7300-SW-MGBHE_O1A44# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A45_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A43_1/2/1**
Gi1/2/3 Alias Name is **DSLAM:1001-GETH-MGBHE_O1A44_VLAN238**

3° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

t7300-SW-MGBHE_O1A44# show interface description

Interface	Admin Status	Oper Status	ALS Admin State	Laser Status
Xg1/2/1	**up**	**up**	**disabled**	**disabled**

Xg1/2/2	**up**	**up**	**disabled**	**disabled**
Gi1/2/3	**up**	**up**	**disabled**	**disabled**

4° Passo: Execute o comando “show mac-address-table dynamic vlan XXX”, onde XXX é a VLAN de serviços de dados, verifique se o equipamento esta recebendo os MAC Address vindo do DSLAM, cada MAC Address recebido é um modem de cliente que esta conectado ao DSLAM:

```
t7300-SW-MGBHE_O1A44# show mac-address-table dynamic vlan 238
show mac-address-table : dynamic unicast
Vlan    Mac Address          Type     Ports
----       -----------              ----       -----
238     00:e0:4d:2f:5a:8a    Learnt   Gi1/2/3
238     00:17:d0:66:d8:c2            Learnt   Gi1/2/3
238     00:18:e7:9e:29:1c    Learnt   Gi1/2/3
238     7c:4f:b5:85:9b:85    Learnt   Gi1/2/3
238     00:17:d0:41:d9:92    Learnt   Gi1/2/3
238     84:c9:b2:ca:95:0c    Learnt   Gi1/2/3
show mac-address-table : dynamic unicast total count 6
```

5° Passo: Acesse todos os elementos do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos vizinhos foram adicionadas ao Member Port da VLAN, conforme abaixo:

```
t7300-SW-MGBHE_O1A45# show vlan id 238
Vlan database
---------------------------------------------------
Vlan ID                : 238
Member Ports           : Xg1/2/1, Xg1/2/2
Untagged Ports         : None
Stats Collection State : Enabled
Name                   : 1001-GETH-MGBHE_O1A44
Status                 : Permanent
```

6° Passo: Acessar o headend do anel e através do comando “show interface name” verifique pelas descrições das interfaces quais estão conectadas aos armários do anel e ao BRAS:

t7300-SW-MGBHE_HM01# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A42_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A46_1/2/1**
Xg1/4/1 Alias Name is LT:CONN_TO_**BRAS:SE-BHE01_1/6/3**

7° Passo: Executar o comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos do anel e a interface que esta conectada ao BRAS foram adicionadas ao Member Port da VLAN, conforme abaixo:

t7300-SW-MGBHE_HM01# show vlan id 238
Vlan database

Vlan ID : 238
Member Ports : Xg1/2/1, Xg1/2/2, Xg1/4/1
Untagged Ports : None
Stats Collection State : Enabled
Name : 1001-GETH-MGBHE_O1A44_VLAN238
Status : Permanent

8° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

t7300-SW-MGBHE_HM01# show interface description

Interface	Admin Status	Oper Status	ALS Admin State	Laser Status
---	---	---	---	---

Xg1/2/1	**up**	**up**	**disabled**	**disabled**
Xg1/2/2	**up**	**up**	**disabled**	**disabled**
Xg1/4/1	**up**	**up**	**disabled**	**disabled**

9° Passo: Execute o comando “show mac-address-table dynamic vlan XXX”, verifique se o equipamento esta recebendo os MAC Address vindo armário:

t7300-SW-MGBHE_HM01# show mac-address-table dynamic vlan 238
show mac-address-table : dynamic unicast

Vlan	Mac Address	Type	Ports
238	00:e0:4d:2f:5a:8a	Learnt	Xg1/2/1
238	00:17:d0:66:d8:c2	Learnt	Xg1/2/1
238	00:18:e7:9e:29:1c	Learnt	Xg1/2/1
238	7c:4f:b5:85:9b:85	Learnt	Xg1/2/1
238	00:17:d0:41:d9:92	Learnt	Xg1/2/1
238	84:c9:b2:ca:95:0c	Learnt	Xg1/2/1

show mac-address-table : dynamic unicast total count 6

- Verificando as configurações de serviços de Voz por H248:

1° Passo: Após logar no equipamento execute o comando “show vlan id 1248”, para verificar a VLAN correspondente ao serviço de voz, caso ela não esteja configurada verifique a VLAN 1249. Devem estar adicionadas ao Member Port da VLAN todas as portas que estão conectadas aos DSLAMs e as interfaces 10 Gb que estão conectadas aos elementos vizinhos, conforme abaixo:

t7300-SW-MGBHE_O1A44# show vlan id 1248
Vlan database

Vlan ID : 1248
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3, Gi1/2/4, Gi1/2/5
Untagged Ports : None
Stats Collection State : Enabled
Name : VLAN_H248-VLAN1248

Status : Permanent

2° Passo: Execute o comando “show interface name” e verifique pelas descrições das interfaces se as configurações estão coincidindo:

t7300-SW-MGBHE_O1A44# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A45_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A43_1/2/1**
Gi1/2/3 Alias Name is **DSLAM:1001-GETH-MGBHE_O1A44_VLAN238**
Gi1/2/4 Alias Name is **DSLAM:1002-GETH-MGBHE_O1A44_VLAN239**
Gi1/2/5 Alias Name is **DSLAM:1003-GETH-MGBHE_O1A44_VLAN240**

3° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

t7300-SW-MGBHE_O1A44# show interface description

Interface	Admin Status	Oper Status	ALS Admin State	Laser Status
Xg1/2/1	**up**	**up**	**disabled**	**disabled**
Xg1/2/2	**up**	**up**	**disabled**	**disabled**
Gi1/2/3	**up**	**up**	**disabled**	**disabled**
Gi1/2/4	**up**	**up**	**disabled**	**disabled**
Gi1/2/5	**up**	**up**	**disabled**	**disabled**

4° Passo: Execute o comando “show mac-address-table dynamic vlan 1248”, verifique se o equipamento esta recebendo os MAC Address vindo dos DSLAMs recebidos pelas portas giga, cada MAC Address recebido é um DSLAM que esta configurado para esta VLAN do armário e do anel:

t7300-SW-MGBHE_O1A44# show mac-address-table dynamic vlan 1248
show mac-address-table : dynamic unicast

Vlan	Mac Address	Type	Ports
1248	00:01:47:8b:e4:1d	Learnt	Xg1/2/2
1248	00:e0:df:5f:dc:e7	Learnt	Xg1/2/1
1248	00:01:47:b3:77:85	Learnt	Xg1/2/1
1248	00:01:47:b3:75:87	Learnt	Xg1/2/1
1248	**00:e0:df:59:ed:90**	**Learnt**	**Gi1/2/4**
1248	**00:e0:df:60:37:f3**	**Learnt**	**Gi1/2/5**
1248	00:01:47:8d:54:83	Learnt	Xg1/2/1
1248	**00:01:47:88:be:f0**	**Learnt**	**Gi1/2/3**
1248	00:e0:df:60:37:f1	Learnt	Xg1/2/1
1248	02:04:96:52:84:a2	Learnt	Xg1/2/1

show mac-address-table : dynamic unicast total count 10

5° Passo: Acesse todos os elementos do anel e através do comando “show vlan id 1248”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos vizinhos foram adicionadas ao Member Port da VLAN, conforme abaixo:

t7300-SW-MGBHE_O1A45# show vlan id 1248
Vlan database

Vlan ID : 1248
Member Ports : Xg1/2/1, Xg1/2/2
Untagged Ports : None
Stats Collection State : Enabled
Name : VLAN_H248-VLAN1248
Status : Permanent

6° Passo: Acessar o headend do anel e através do comando “show interface name” verifique pelas descrições das interfaces quais estão conectadas aos armários do anel e ao Switch Agregador:

t7300-SW-MGBHE_HM01# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A42_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A46_1/2/1**
Gi1/2/3 Alias Name is LT:CONN_TO_**SW-AGG-BHE01_2/3**

7° Passo: Executar o comando “show vlan id 1248”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos do anel e a interface que esta conectada ao SW-AGG foram adicionadas ao Member Port da VLAN, conforme abaixo:

t7300-SW-MGBHE_HM01# show vlan id 1248
Vlan database

Vlan ID : 1248
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3
Untagged Ports : None
Stats Collection State : Enabled
Name : VLAN_H248-VLAN1248
Status : Permanent

8° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

t7300-SW-MGBHE_HM01# show interface description

Interface	Admin Status	Oper Status	ALS Admin State	Laser Status
Xg1/2/1	**up**	**up**	**disabled**	**disabled**
Xg1/2/2	**up**	**up**	**disabled**	**disabled**
Gi1/2/3	**up**	**up**	**disabled**	**disabled**

9° Passo: Execute o comando “show mac-address-table dynamic vlan 1248”, verifique se o equipamento esta recebendo os MAC Address vindo do armário:

t7300-SW-MGBHE_HM01# show mac-address-table dynamic vlan 1248
show mac-address-table : dynamic unicast
Vlan Mac Address Type Ports
---- ----------- ---- -----
1248 00:01:47:8b:e4:1d Learnt Xg1/2/2
1248 00:e0:df:5f:dc:e7 Learnt Xg1/2/1
1248 00:01:47:b3:77:85 Learnt Xg1/2/1
1248 00:01:47:b3:75:87 Learnt Xg1/2/1
1248 00:e0:df:59:ed:90 Learnt Xg1/2/1
1248 00:e0:df:60:37:f3 Learnt Xg1/2/1
1248 00:01:47:8d:54:83 Learnt Xg1/2/1
1248 00:01:47:88:be:f0 Learnt Xg1/2/1
1248 00:e0:df:60:37:f1 Learnt Xg1/2/1
1248 02:04:96:52:84:a2 Learnt Xg1/2/1
show mac-address-table : dynamic unicast total count 10

- Verificando as configurações de gerência dos DSLAMs e fontes:

1° Passo: Após logar no equipamento execute o comando “show vlan id XXX”, onde XXX é a VLAN de gerência dos DSLAMs, são utilizadas as VLANs 699,700 e 1010, a VLAN 704 é utilizada para a gerência de fontes. Devem estar adicionadas ao Member Port da VLAN todas as portas que estão conectadas aos DSLAMs e as interfaces 10 Gb que estão conectadas aos elementos vizinhos. Quando a VLAN de gerência esta configurada na mesma porta da VLAN de serviço é chamado de inband, quando o DSLAM utiliza uma porta dedica para a VLAN de gerência é chamado de outband, no caso abaixo a gerência é inband:

t7300-SW-MGBHE_O1A44# show vlan id 699
Vlan database
---
t7300-SW-MGBHE_O1A44# show vlan id 700
Vlan database

Vlan ID : 700

Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3, Gi1/2/4, Gi1/2/5
Untagged Ports : None
Stats Collection State : Enabled
Name : MGMT_DSLAM_VOZ-MGBHE_O1A44
Status : Permanent
---
t7300-SW-MGBHE_O1A44# show vlan id 1010
Vlan database

Vlan ID : 1010
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3, Gi1/2/4, Gi1/2/5
Untagged Ports : None
Stats Collection State : Enabled
Name : MGMT_DSLAM-MGBHE_O1A44
Status : Permanent
---
t7300-SW-MGBHE_O1A44# show vlan id 704
Vlan database

Vlan ID : 704
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/26
Untagged Ports : Gi1/2/26
Stats Collection State : Enabled
Name : MGMT_FONTE-MGBHE_O1A44
Status : Permanent

2° Passo: Execute o comando “show interface name” e verifique pelas descrições das interfaces se as configurações estão coincidindo:

t7300-SW-MGBHE_O1A44# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A45_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A43_1/2/1**
Gi1/2/3 Alias Name is **DSLAM:1001-GETH-MGBHE_O1A44_VLAN238**

Gi1/2/4 Alias Name is **DSLAM:1002-GETH-MGBHE_O1A44_VLAN239**
Gi1/2/5 Alias Name is **DSLAM:1003-GETH-MGBHE_O1A44_VLAN240**
Gi1/2/26 Alias Name is **FONTE:MGBHE_O1A44_VLAN704**

3° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

```
t7300-SW-MGBHE_O1A44# show interface description
Interface    Admin    Oper          ALS Admin      Laser
              Status   Status            State        Status
---------    ------   ------        ---------      --------
Xg1/2/1      up       up            disabled       disabled
Xg1/2/2      up       up            disabled       disabled
Gi1/2/3      up       up            disabled       disabled
Gi1/2/4      up       up            disabled       disabled
Gi1/2/5      up       up            disabled       disabled
Gi1/2/26     up       up            disabled       disabled
```

4° Passo: Execute o comando “show mac-address-table dynamic vlan XXX”, verifique se o equipamento esta recebendo os MAC Address vindo dos DSLAMs recebidos pelas portas giga, cada MAC Address recebido é um DSLAM que esta configurado para esta VLAN do armário e do anel:

```
t7300-SW-MGBHE_O1A44# show mac-address-table dynamic vlan
700
show mac-address-table : dynamic unicast
Vlan    Mac Address         Type     Ports
----      -----------         ----     -----
700     00:e0:df:71:35:73   Learnt   Xg1/2/1
700     00:e0:df:13:7b:6c   Learnt   Xg1/2/1
700     00:e0:df:0a:bc:99   Learnt   Xg1/2/1
700     00:e0:df:08:89:cc   Learnt   Gi1/2/3
700     00:e0:df:56:df:1a   Learnt   Xg1/2/1
700     02:04:96:36:ad:7e   Learnt   Xg1/2/1
```

700 00:e0:df:70:d4:4d Learnt Xg1/2/1

t7300-SW-MGBHE_O1A44# show mac-address-table dynamic vlan 1010

show mac-address-table : dynamic unicast

Vlan	Mac Address	Type	Ports
1010	00:01:47:8b:e4:1d	Learnt	Xg1/2/2
1010	00:e0:df:5f:dc:e7	Learnt	Xg1/2/1
1010	00:01:47:b3:77:85	Learnt	Xg1/2/1
1010	00:01:47:b3:75:87	Learnt	Xg1/2/1
1010	**00:e0:df:59:ed:90**	**Learnt**	**Gi1/2/4**
1010	**00:e0:df:60:37:f3**	**Learnt**	**Gi1/2/5**
1010	00:01:47:8d:54:83	Learnt	Xg1/2/1
1010	00:e0:df:60:37:f1	Learnt	Xg1/2/1

t7300-SW-MGBHE_O1A44# show mac-address-table dynamic vlan 704

show mac-address-table : dynamic unicast

Vlan	Mac Address	Type	Ports
704	**00:e0:df:71:35:73**	**Learnt**	**Gi1/2/26**
704	00:e0:df:13:7b:6c	Learnt	Xg1/2/1
704	00:e0:df:0a:bc:99	Learnt	Xg1/2/1
704	02:04:96:36:ad:7e	Learnt	Xg1/2/1
704	00:e0:df:56:08:47	Learnt	Xg1/2/1

5° Passo: Acesse todos os elementos do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos vizinhos foram adicionadas ao Member Port da VLAN, conforme abaixo:

t7300-SW-MGBHE_O1A45# show vlan id 700

Vlan database

Vlan ID : 700
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/3, Gi1/2/4
Untagged Ports : None
Stats Collection State : Enabled
Name : MGMT_DSLAM_VOZ-MGBHE_O1A45
Status : Permanent

6° Passo: Acessar o headend do anel e através do comando “show interface name” verifique pelas descrições das interfaces quais estão conectadas aos armários do anel e ao Switch de Gerência:

t7300-SW-MGBHE_HM01# show interface name
Xg1/2/1 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A42_1/2/2**
Xg1/2/2 Alias Name is LT:CONN_TO_**SW-MGBHE_O1A46_1/2/1**
Gi1/2/6 Alias Name is LT:CONN_TO_**SW-MGMT-BHE01_1/12**

7° Passo: Executar o comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces 10 Gb que estão conectadas aos elementos do anel e a interface que esta conectada ao SW-MGMT foram adicionadas ao Member Port da VLAN, conforme abaixo:

t7300-SW-MGBHE_HM01# show vlan id 700
Vlan database

Vlan ID : 700
Member Ports : Xg1/2/1, Xg1/2/2, Gi1/2/6
Untagged Ports : None
Stats Collection State : Enabled
Name : MGMT_DSLAM
Status : Permanent

8° Passo: Execute o comando “show interface description”, verifique se as interfaces configuradas na VLAN estão com status administrativo e operacional UP:

```
t7300-SW-MGBHE_HM01# show interface description
Interface    Admin    Oper          ALS Admin      Laser
             Status   Status            State        Status
---------    ------   ------        ---------      --------
Xg1/2/1      up       up            disabled       disabled
Xg1/2/2      up       up            disabled       disabled
Gi1/2/6      up       up            disabled       disabled
```

9° Passo: Execute o comando “show mac-address-table dynamic vlan XXX”, verifique se o equipamento esta recebendo os MAC Address vindo dos armários:

```
t7300-SW-MGBHE_HM01# show mac-address-table dynamic vlan 700
show mac-address-table : dynamic unicast
Vlan    Mac Address          Type     Ports
----     -----------          ----     -----
        700    00:e0:df:71:35:73   Learnt   Xg1/2/1
        700    00:e0:df:13:7b:6c   Learnt   Xg1/2/1
        700    00:e0:df:0a:bc:99   Learnt   Xg1/2/1
        700    00:e0:df:08:89:cc   Learnt   Xg1/2/1
        700    00:e0:df:56:df:1a   Learnt   Xg1/2/1
        700    02:04:96:36:ad:7e   Learnt   Xg1/2/1
        700    00:e0:df:70:d4:4d   Learnt   Xg1/2/1
show mac-address-table : dynamic unicast total count 7
```

- Datacom

- Verificando as configurações de serviços de Dados:

1° Passo: Após logar no equipamento execute o comando “show vlan id XXX”, onde XXX é a VLAN de serviços de dados. Devem estar adicionadas ao Member Port a

porta que esta conectada ao DSLAM e as interfaces que estão conectadas aos elementos vizinhos, conforme abaixo:

```
D2NHO01A1001# show vlan id 584
 VLAN:                 584
 Type:                 Static
 Status
        Admin:         Enabled
        Oper:          Up
 Log duplicated IP:    Enabled
 Aging-time:           300 sec.
 Learn-copy:           Disabled
 MAC maximum:          Disabled
 EAPS:                 protected on domain(s) 0
  CFM status:          Disabled
 Link Detection:       Disabled
 Proxy ARP:            Disabled
 Members:              Eth1/1 (static, tagged)
                       Eth1/25 to Eth1/26 (static, tagged)
 Forbidden:            (none)
```

2° Passo: Execute o comando “show interfaces table configuration”, verifique se as interfaces configuradas na VLAN estão com status administrativo e link UP:

```
D2NHO01A1001#show interfaces table configuration

                          Port    Link    Auto       Speed/Duplex       Flow
 Port                     Admin   Status  Neg      CFG       Status      Ctrl    PVID
================================================================================
  1/ 1 LT:CONN_TO_DSL     UP      UP      ON     100/AUTO   100/FULL  NONE    1
  1/25 LT:D2NHO01A030     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
  1/26 LT:D2NHO01SW01     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
================================================================================
              spacebar->toggle screen  ESC->exit
```

3° Passo: Execute o comando “show mac-address-table vlan XXX”, onde XXX é a VLAN de serviços de dados, verifique se o equipamento esta recebendo os MAC Address vindo do DSLAM, cada MAC Address recebido é um modem de cliente que esta conectado ao DSLAM:

```
D2NHO01A1001#show mac-address-table vlan 584
This command may take a while...
Total MAC Addresses for this criterion: 10
Unit    Block  Interface      MAC Address         VLAN VPN   Type
----    -----  ---------      -----------------   ---- ---    -------
  1            Eth  1/ 1      00:0B:23:F8:0E:A6        584   -      Learned
  1            Eth  1/ 1      08:76:FF:91:61:CF        584   -      Learned
  1            Eth  1/ 1      74:31:70:91:6B:7E  584   -      Learned
  1            Eth  1/ 1      4C:09:B4:A0:96:73        584   -      Learned
  1            Eth  1/ 1      84:C9:B2:CC:63:91        584   -      Learned
  1            Eth  1/ 1      A0:F3:C1:4F:EA:B4  584         -      Learned
  1            Eth  1/ 1      6C:2E:85:E9:AA:02        584   -      Learned
  1            Eth  1/26      8C:90:D3:C5:85:2A        584   -      Learned
  1            Eth  1/ 1      00:E9:08:80:5C:58        584   -      Learned
  1            Eth  1/ 1      14:D6:4D:99:CE:78        584   -      Learned
```

4° Passo: Acesse todos os elementos do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces que estão conectadas aos elementos vizinhos foram adicionadas ao Member Port da VLAN, conforme abaixo:

```
D2NHO01A0301# show vlan id 584
 VLAN:                 584
 Type:                 Static
 Status
        Admin:         Enabled
        Oper:          Up
 Log duplicated IP:    Enabled
 Aging-time:           300 sec.
 Learn-copy:           Disabled
 MAC maximum:          Disabled
 EAPS:                 protected on domain(s) 0
  CFM status:          Disabled
 Link Detection:       Disabled
 Proxy ARP:            Disabled
 Members:              Eth1/25 to Eth1/26 (static, tagged)
 Forbidden:            (none)
```

5° Passo: Acessar o headend do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces que estão conectadas aos

elementos do anel e a interface que esta conectada ao BRAS foram adicionadas ao Member Port da VLAN, conforme abaixo:

```
D2NHO01SW01# show vlan id 584
 VLAN:                 584
 Type:                 Static
 Status
        Admin:         Enabled
        Oper:          Up
 Log duplicated IP:    Enabled
 Aging-time:           300 sec.
 Learn-copy:           Disabled
 MAC maximum:          Disabled
 EAPS:                 protected on domain(s) 0
  CFM status:          Disabled
 Link Detection:       Disabled
 Proxy ARP:            Disabled
 Members:              Eth1/28 (static, tagged)
                       Eth1/25 to Eth1/26 (static, tagged)
 Forbidden:            (none)
```

6° Passo: Execute o comando “show interfaces table configuration”, verifique se as interfaces configuradas na VLAN estão com status administrativo e link UP:

```
D2NHO01SW01#show interfaces table configuration
                          Port    Link    Auto       Speed/Duplex       Flow
 Port                     Admin   Status  Neg      CFG       Status      Ctrl    PVID
================================================================================
  1/25 LT:D2NHO01A050     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
  1/26 LT:D2NHO01SW02     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
  1/28 LT:BRAS:SE-NHO01   UP      UP      ON     100/AUTO   100/FULL  NONE    1
================================================================================
          spacebar->toggle screen  ESC->exit
```

7° Passo: Execute o comando “show mac-address-table vlan XXX”, verifique se o equipamento esta recebendo os MAC Address vindo armário:

```
D2NHO01SW01#show mac-address-table vlan 584
This command may take a while...
Total MAC Addresses for this criterion: 10
Unit    Block  Interface       MAC Address        VLAN VPN   Type
```

1		Eth 1/ 26	00:0B:23:F8:0E:A6	584	-	Learned
1		Eth 1/ 26	08:76:FF:91:61:CF	584	-	Learned
1		Eth 1/ 26	74:31:70:91:6B:7E	584	-	Learned
1		Eth 1/ 26	4C:09:B4:A0:96:73	584	-	Learned
1		Eth 1/ 26	84:C9:B2:CC:63:91	584	-	Learned
1		Eth 1/ 26	A0:F3:C1:4F:EA:B4	584	-	Learned
1		Eth 1/ 26	6C:2E:85:E9:AA:02	584	-	Learned
1		Eth 1/ 26	8C:90:D3:C5:85:2A	584	-	Learned
1		Eth 1/ 26	00:E9:08:80:5C:58	584	-	Learned
1		Eth 1/ 26	14:D6:4D:99:CE:78	584	-	Learned

- Verificando as configurações de gerência dos DSLAMs e fontes:

1° Passo: Após logar no equipamento execute o comando “show vlan id XXX”, onde XXX é a VLAN de gerência dos DSLAMs e de fontes. Devem estar adicionadas ao Member Port as portas que estão conectadas aos DSLAMs e as interfaces que estão conectadas aos elementos vizinhos, conforme abaixo:

```
D2NHO01A1001#show vlan id 699
% 11: VLAN does not exist

D2NHO01A1001# show vlan id 700
 VLAN:              700 [MGMT_SHELF_VOZ]
 Type:              Static
 Status
        Admin:      Enabled
        Oper:       Up
 Log duplicated IP: Enabled
 Aging-time:        300 sec.
 Learn-copy:        Disabled
 MAC maximum:       Disabled
 EAPS:              protected on domain(s) 0
  CFM status:       Disabled
 Link Detection:    Disabled
 Proxy ARP:         Disabled
 Members:           Eth1/21 to Eth1/23 (static, untagged)
                    Eth1/25 to Eth1/26 (static, tagged)
 Forbidden:         (none)

D2NHO01A1001# show vlan id 1010
```

```
VLAN:                1010 [MGMT_DSLAM]
Type:                Static
Status
        Admin:       Enabled
        Oper:        Up
Log duplicated IP:   Enabled
Aging-time:          300 sec.
Learn-copy:          Disabled
MAC maximum:         Disabled
EAPS:                protected on domain(s) 0
 CFM status:         Disabled
Link Detection:      Disabled
Proxy ARP:           Disabled
Members:             Eth1/16 to Eth1/18 (static, untagged)
                     Eth1/25 to Eth1/26 (static, tagged)
Forbidden:           (none)

D2NHO01A1001# show vlan id 704
VLAN:                704 [MGMT_FONTE]
Type:                Static
Status
        Admin:       Enabled
        Oper:        Up
Log duplicated IP:   Enabled
Aging-time:          300 sec.
Learn-copy:          Disabled
MAC maximum:         Disabled
EAPS:                protected on domain(s) 0
 CFM status:         Disabled
Link Detection:      Disabled
Proxy ARP:           Disabled
Members:             Eth1/20 (static, untagged)
                     Eth1/25 to Eth1/26 (static, tagged)
Forbidden:           (none)
```

2° Passo: Execute o comando “show interfaces table configuration”, verifique se as interfaces configuradas na VLAN estão com status administrativo e link UP. Neste caso como a configuração da gerência dos DSLAMs é outband a VLAN é atribuída à interface conforme abaixo:

```
D2NHO01A1001#show interfaces table configuration
                          Port    Link    Auto       Speed/Duplex       Flow
 Port                     Admin   Status  Neg      CFG       Status      Ctrl    PVID
================================================================================
  1/16 MGMT_ZHONE_COM     UP      UP      ON     100/AUTO   100/FULL  NONE    1010
  1/17 MGMT_DSLAM_BA1     UP      UP      ON     100/AUTO   100/FULL  NONE    1010
  1/18 MGMT_DSLAN_BIT     UP      UP      ON     100/AUTO   100/FULL  NONE    1010
  1/20 MGMT_FONTE         UP      UP      ON     100/AUTO   100/FULL  NONE    704
  1/21 MGMT_SHELF_VOZ     UP      UP      ON     100/AUTO             NONE    700
  1/22 MGMT_SHELF_VOZ     UP      UP      ON     100/AUTO             NONE    700
  1/23 MGMT_SHELF_VOZ     UP      UP      ON     100/AUTO             NONE    700
  1/25 LT:D2NHO01A030     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
  1/26 LT:D2NHO01SW01     UP      UP      ON     100/AUTO  1000/FULL  NONE    1
================================================================================
          spacebar->toggle screen  ESC->exit
```

3° Passo: Execute o comando “show mac-address-table vlan XXX”, onde XXX é a VLAN de gerência dos DSLAMs, verifique se o equipamento esta recebendo os MAC Address vindo dos DSLAMs, cada MAC Address recebido é um DSLAM que esta conectado ao switch Datacom:

```
D2NHO01A1001#show mac-address-table vlan 700
This command may take a while...
Total MAC Addresses for this criterion: 10
Unit    Block  Interface      MAC Address        VLAN VPN   Type
----    -----  ---------      -----------------  ---- ---   -------
  1            Eth  1/ 21     4C:09:B4:A0:96:73        700   -       Learned
  1            Eth  1/ 22     84:C9:B2:CC:63:91  700         -       Learned
  1            Eth  1/ 23     A0:F3:C1:4F:EA:B4  700         -       Learned
  1            Eth  1/26      5E:70:05:FE:0A:98        700   -       Learned
  1            Eth  1/25      5E:70:09:9D:22:F3        700   -       Learned
  1            Eth  1/25      00:E0:DF:6B:C3:D9  700         -       Learned
  1            Eth  1/25      00:E0:DF:6B:C6:D9        700   -       Learned
  1            Eth  1/25      5E:70:09:9D:26:AB        700   -       Learned
  1            Eth  1/26      4C:32:2D:00:5B:41        700   -       Learned
  1            Eth  1/26      00:25:45:66:D1:09  700   -       Learned
```

4° Passo: Acesse todos os elementos do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces que estão conectadas aos elementos vizinhos foram adicionadas ao Member Port da VLAN, conforme abaixo:

```
D2NHO01A0301# show vlan id 700
VLAN:                 700 [MGMT_SHELF_VOZ]
 Type:                Static
 Status
        Admin:        Enabled
        Oper:         Up
 Log duplicated IP:   Enabled
 Aging-time:          300 sec.
 Learn-copy:          Disabled
 MAC maximum:         Disabled
 EAPS:                protected on domain(s) 0
  CFM status:         Disabled
 Link Detection:      Disabled
 Proxy ARP:           Disabled
 Members:             Eth1/21 to Eth1/23 (static, untagged)
                      Eth1/25 to Eth1/26 (static, tagged)
 Forbidden:           (none)
```

5° Passo: Acessar o headend do anel e através do comando “show vlan id XXX”, verifique se a VLAN esta configurada e se as interfaces que estão conectadas aos elementos do anel e a interface que esta conectada ao SW-MGMT foram adicionadas ao Member Port da VLAN, conforme abaixo:

```
D2NHO01SW01# show vlan id 700
VLAN:                 700 [MGMT_SHELF_VOZ]
 Type:                Static
 Status
        Admin:        Enabled
        Oper:         Up
 Log duplicated IP:   Enabled
 Aging-time:          300 sec.
 Learn-copy:          Disabled
 MAC maximum:         Disabled
 EAPS:                protected on domain(s) 0
  CFM status:         Disabled
 Link Detection:      Disabled
 Proxy ARP:           Disabled
 Members:             Eth1/10 (static, tagged)
                      Eth1/25 to Eth1/26 (static, tagged)
```

Forbidden: (none)

6° Passo: Execute o comando “show interfaces table configuration”, verifique se as interfaces configuradas na VLAN estão com status administrativo e link UP:

```
D2NHO01SW01#show interfaces table configuration
                                Port    Link    Auto       Speed/Duplex       Flow
 Port                           Admin   Status  Neg      CFG       Status      Ctrl    PVID
================================================================================
  1/10 LT:SW-MGMT-NHO01         UP      UP      ON     100/AUTO    100/FULL   NONE    1
  1/25 LT:D2NHO01A100           UP      UP      ON     100/AUTO   1000/FULL   NONE    1
  1/26 LT:D2NHO01SW02           UP      UP      ON     100/AUTO   1000/FULL   NONE    1
================================================================================
                    spacebar->toggle screen  ESC->exit
```

7° Passo: Execute o comando “show mac-address-table vlan XXX”, verifique se o equipamento esta recebendo os MAC Address vindo armário:

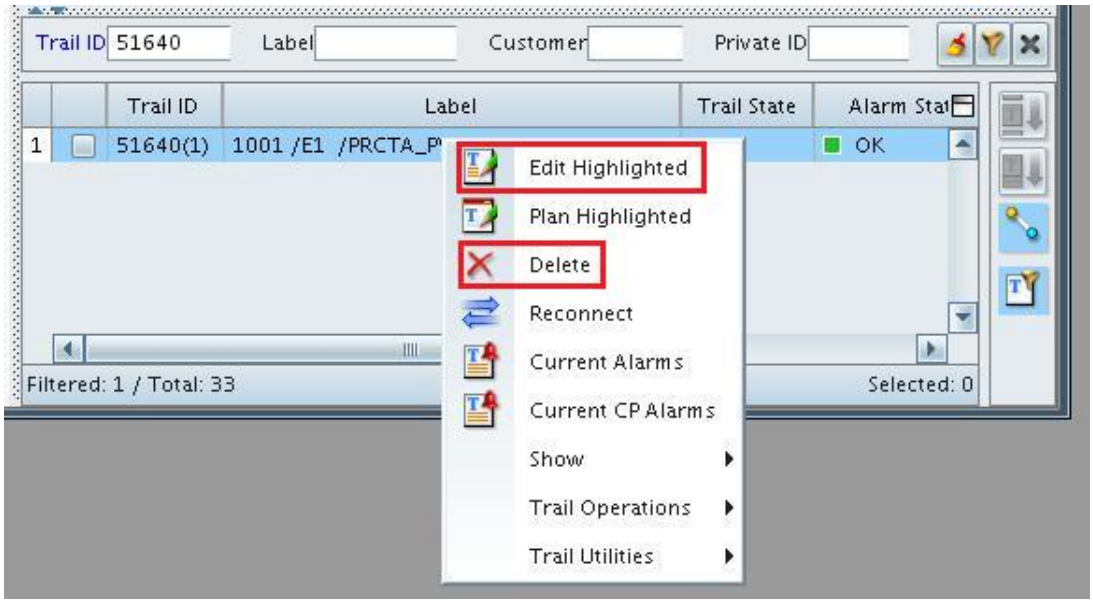
```
D2NHO01SW01#show mac-address-table vlan 700
This command may take a while...
Total MAC Addresses for this criterion: 10
Unit    Block  Interface      MAC Address        VLAN VPN   Type
----    -----  ---------      -----------------  ---- ---    -------
  1            Eth  1/ 26     4C:09:B4:A0:96:73        700   -      Learned
  1            Eth  1/ 26     84:C9:B2:CC:63:91        700   -      Learned
  1            Eth  1/ 26     A0:F3:C1:4F:EA:B4  700         -      Learned
  1            Eth  1/26      5E:70:05:FE:0A:98        700   -      Learned
  1            Eth  1/25      5E:70:09:9D:22:F3        700   -      Learned
  1            Eth  1/25      00:E0:DF:6B:C3:D9  700         -      Learned
  1            Eth  1/25      00:E0:DF:6B:C6:D9        700   -      Learned
  1            Eth  1/25      5E:70:09:9D:26:AB        700   -      Learned
  1            Eth  1/26      4C:32:2D:00:5B:41        700   -      Learned
  1            Eth  1/26      00:25:45:66:D1:09  700   -      Learned
```

Procedimento de alteração, exclusão e criação de serviços (Dados, Voz por V5, Voz por H248 e MGMT)

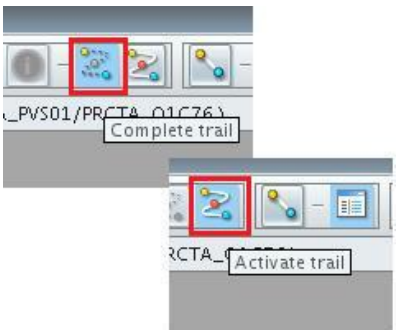
- ECI

- Serviços de Voz por V5:

Para editar ou excluir um serviço clique com o botão direito do mouse no serviço desejado e selecione a opção Edit Highlighted para edita-lo ou Delete para exclui-lo:

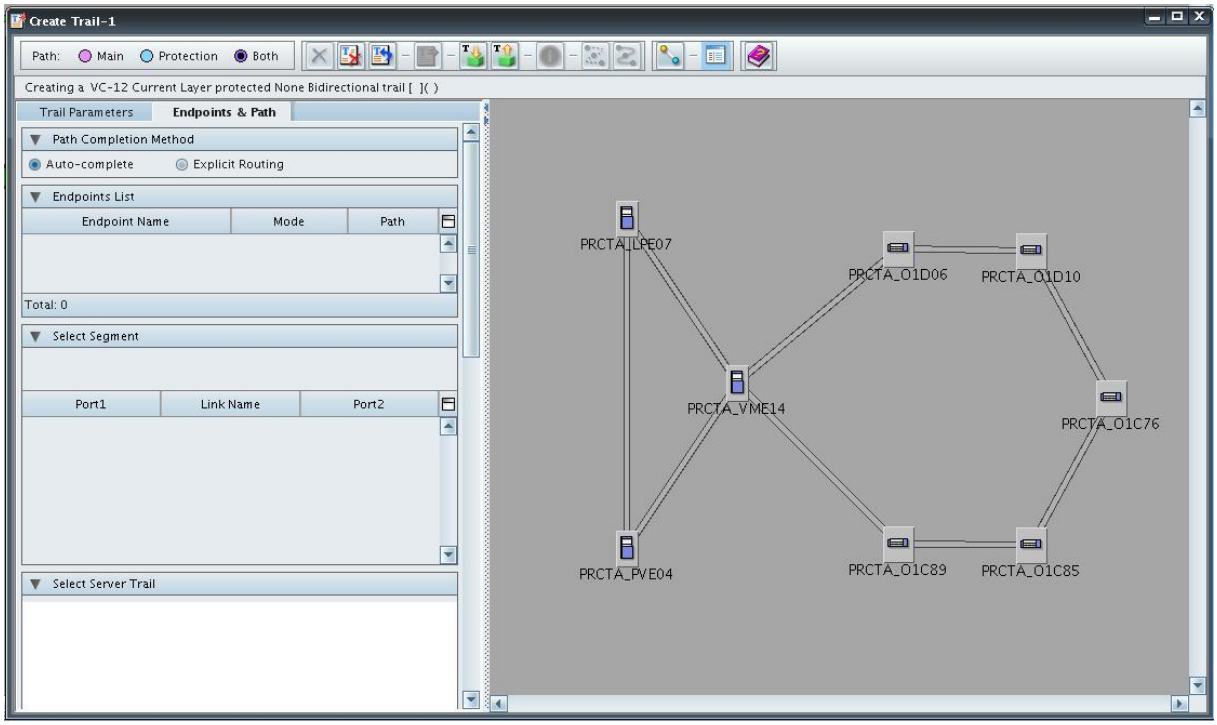


Se editar o serviço depois de finalizado selecione as opções Complete Trail seguido de Activate Trail no canto superior da janela:

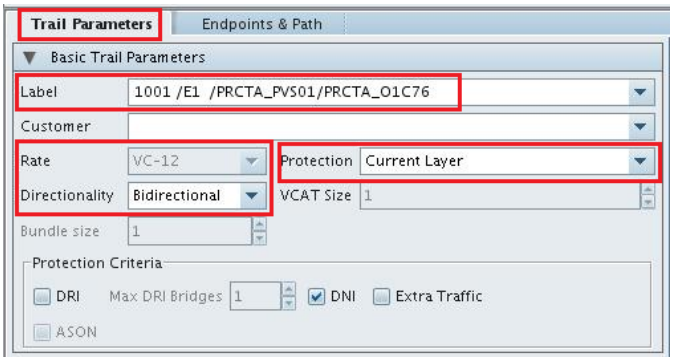


1° Passo: Para criar um novo serviço selecione todos os elementos por onde passará o circuito e selecione a opção Create Trail no canto superior da janela:

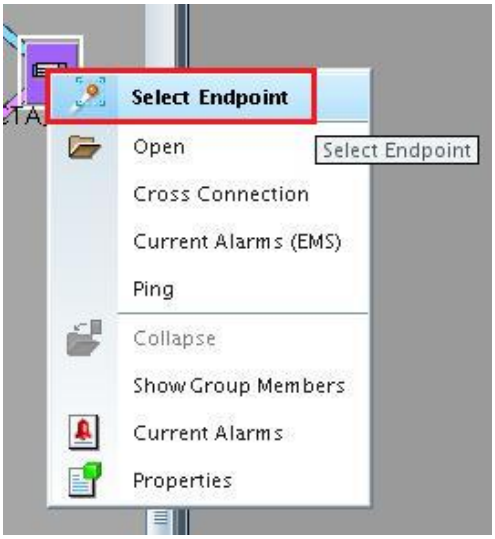
Abrirá uma nova janela com os elementos selecionados:



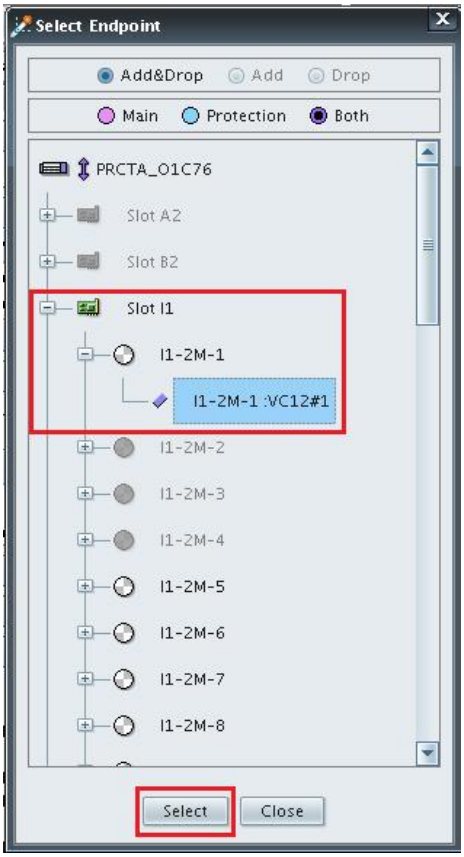
2° Passo: Na aba Trail Parameters adicione a descrição do circuito em Label, selecione a capacidade do circuito em Rate, selecione Bidirectional em Directionality e em Protection selecione Current Layer se desejar que seja protegido ou Unprotected para desprotegido:



3° Passo: Selecione o primeiro elemento onde fechará o circuito, clique com o botão direito do mouse e selecione a opção Select Endpoint:

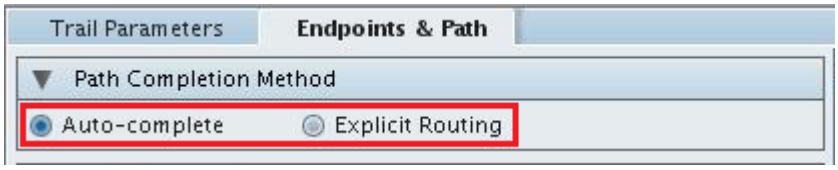


Abrirá uma janela para seleção da interface, após escolhida clique no botão Select:

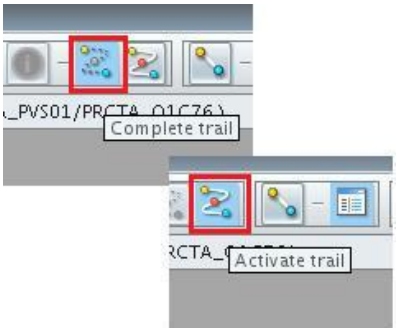


Realize o processo de seleção de interface para o segundo elemento.

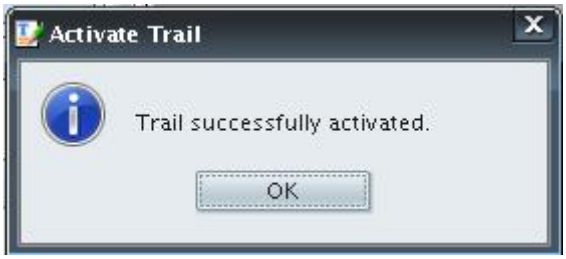
4° Passo: Selecione a aba Endpoints & Path e selecione a opção Auto-complete, neste caso a gerência selecionará os caminhos automaticamente, se for necessário designar o caminho selecione a opção Explicit Routing:



5° Passo: Selecione as opções Complete Trail seguido de Activate Trail no canto superior da janela para finalizar a criação do circuito:

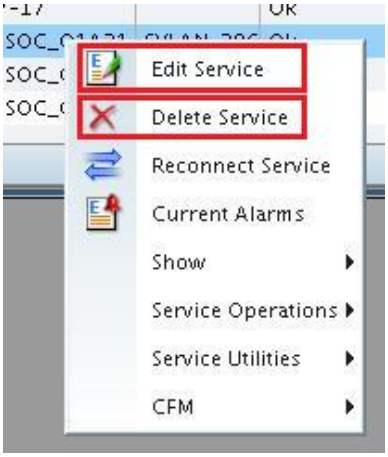


Abrirá uma janela informando que o Trail foi ativado com sucesso:

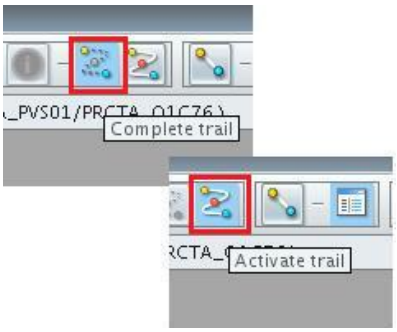


- Serviços de Dados, Voz por H248 e MGMT:

Para editar ou excluir um serviço clique com o botão direito do mouse no serviço desejado e selecione a opção Edit Service para edita-lo ou Delete Service para exclui-lo:

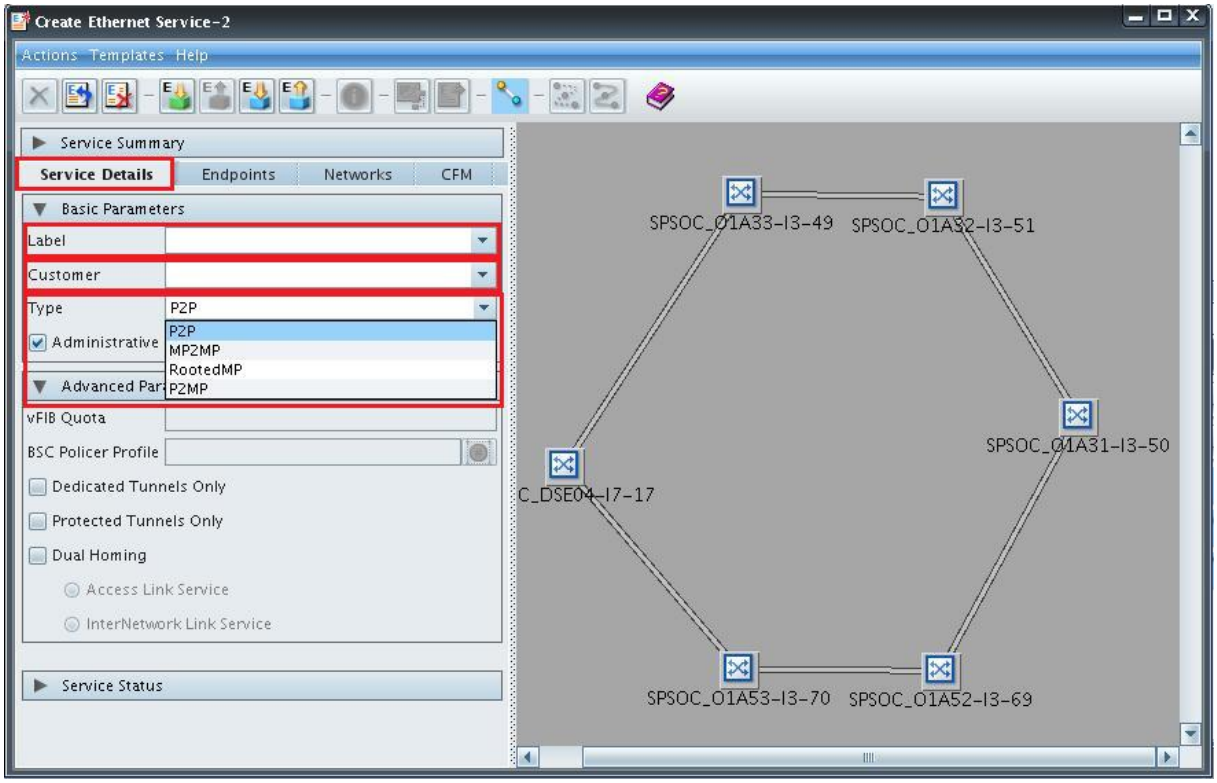


Se editar o serviço depois de finalizado selecione as opções Complete Trail seguido de Activate Trail no canto superior da janela:

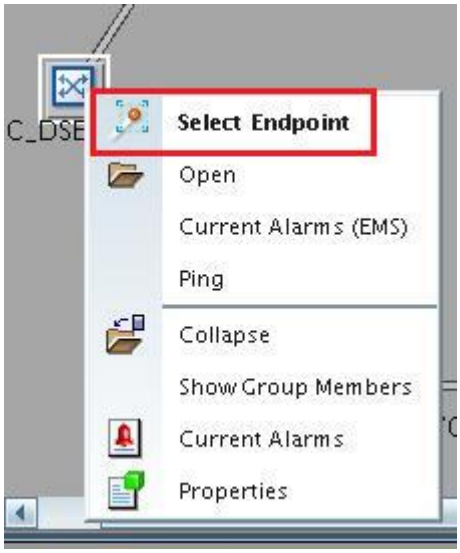


1° Passo: Para criar um novo serviço selecione todos os elementos por onde passará o circuito e selecione a opção Create ETH Service no canto superior da janela:

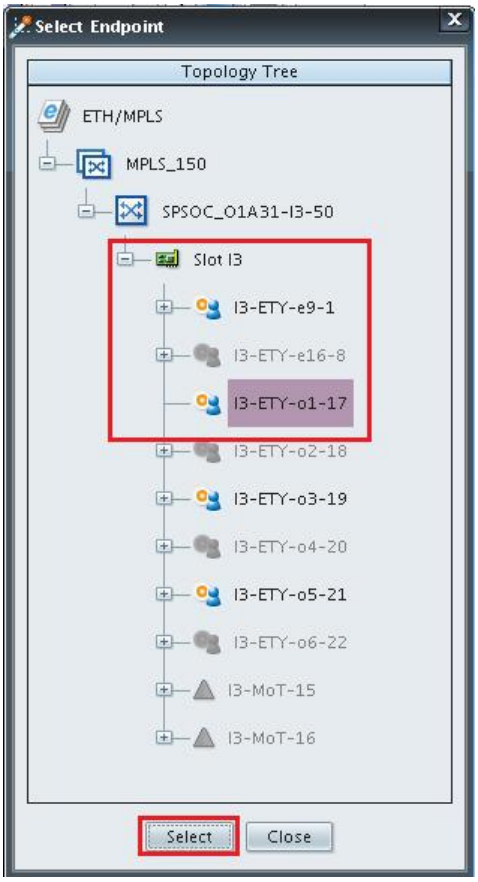
2° Passo: Abrirá uma nova janela com os elementos selecionados. Na aba Service Details adicione a designação do circuito em Label e descrição em Customer, selecione o tipo de serviço que será criado, P2P para serviços de Dados, P2MP para serviços de gerência e MP2MP para serviços de Voz por H248:



3° Passo: Selecione o primeiro elemento onde fechará o serviço, clique com o botão direito do mouse e selecione a opção Select Endpoint:



Abrirá uma janela para seleção da interface, após escolhida clique no botão Select:

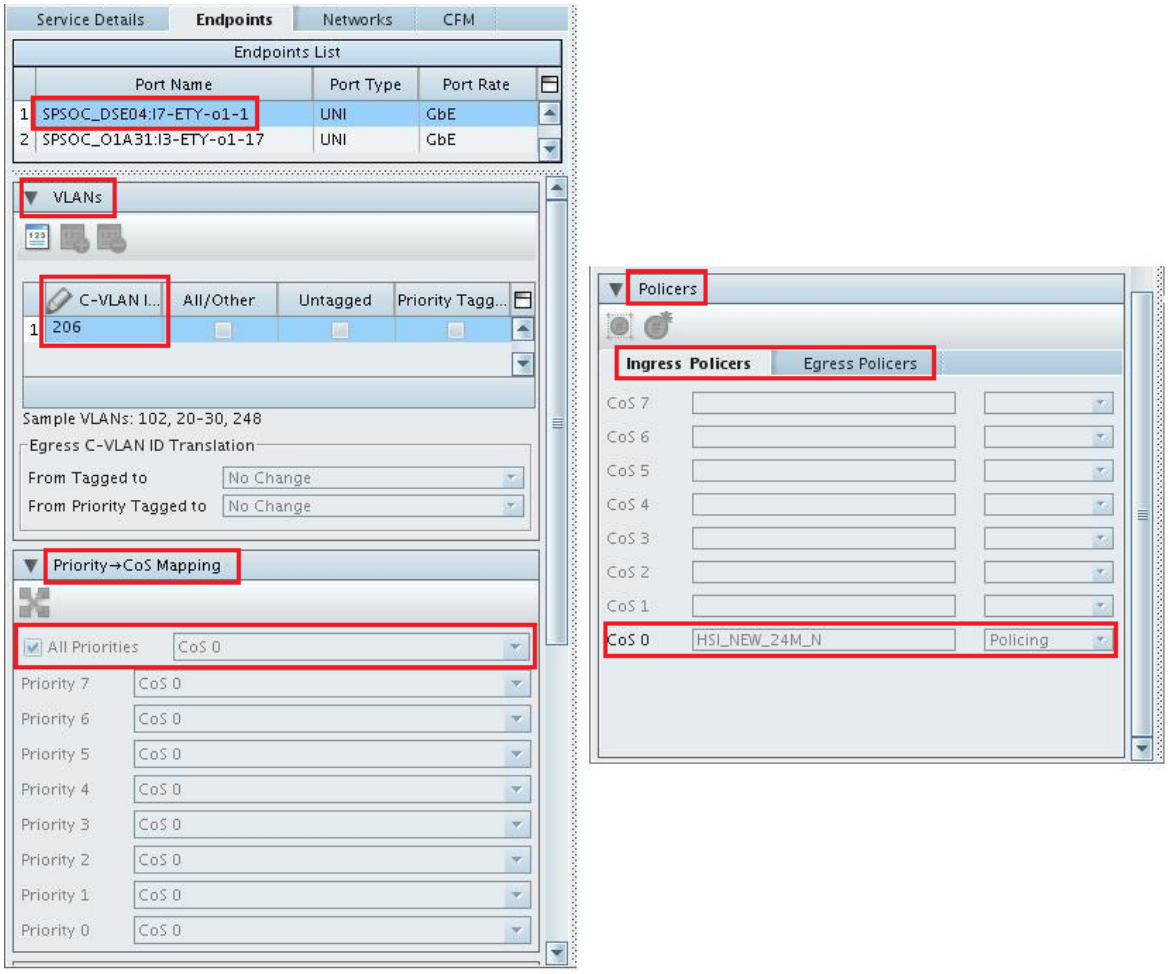


4° Passo: Na aba Endpoints selecione a interface que foi adicionada, e realize as seguintes configurações:

-Adicione a VLAN na aba VLANs: Deve ser o mesmo que foi configurado no DSLAM e BRAS;

- Na aba Priority -> CoS Mapping selecione a opção All Priorities e selecione o CoS conforme o serviço: CoS 0 para os serviços de Dados, CoS 3 ou 4 para os serviços de Gerência e CoS 7 para os serviços de Voz por H248.

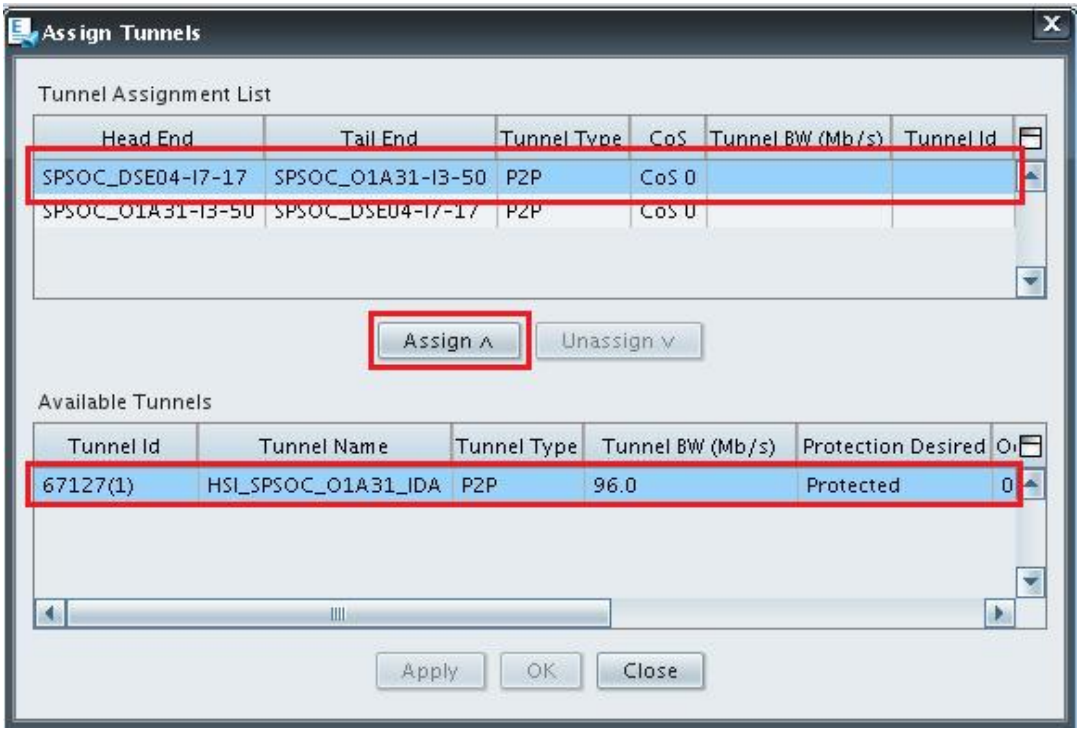
- Na aba Policers selecione o Ingress Policers que foi pré-definido ou deixe em No Rate Limite e Egress Policers setado em No Rate Limite.



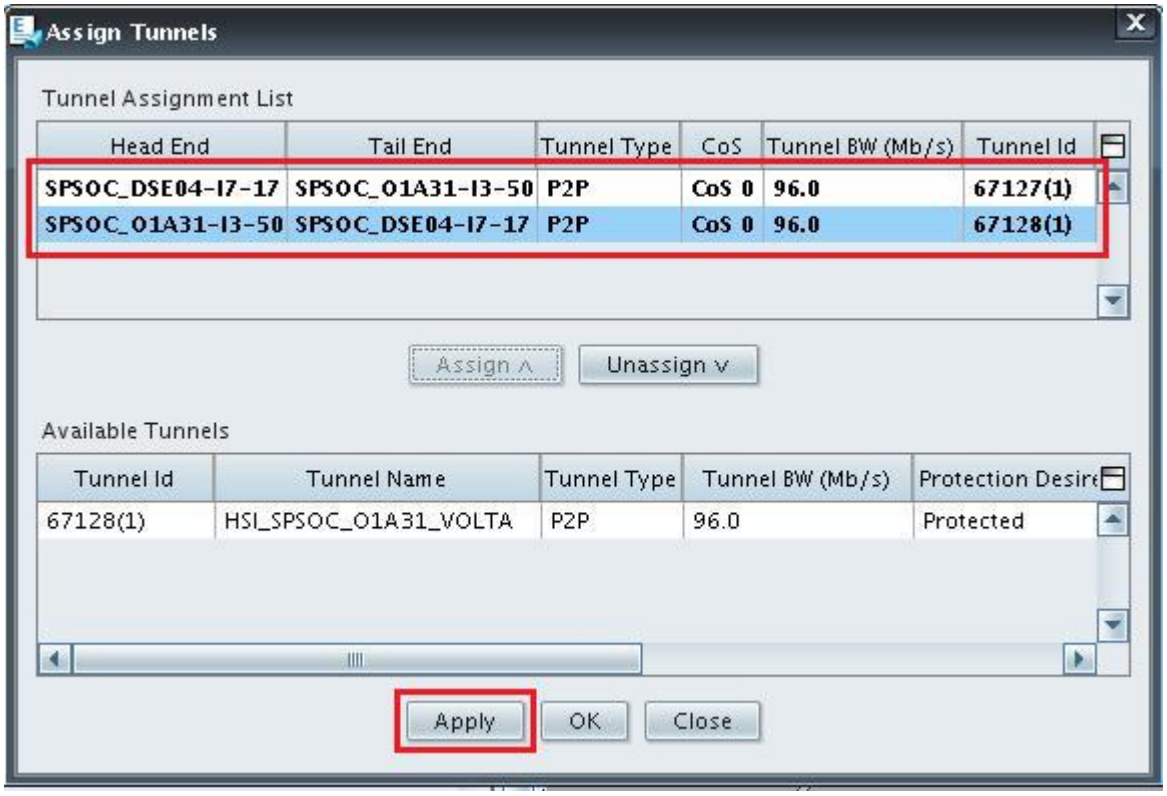
Realize os passos 3 e 4 para seleção de todas as interfaces que forem adicionadas ao serviço.

5° Passo: Selecione a aba Networks e clique no botão Assign Tunnel para adicionar os túneis de passagem da rede MPLS:

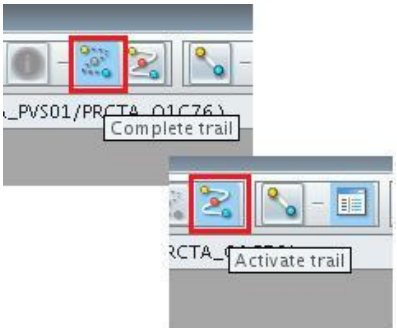
Abrirá uma janela para seleção dos túneis, selecione o caminho em Tunnel Assignment List em seguida selecione o Tunnel em Available Tunnels e clique no botão Assign. Realize este processo até que todos os túneis sejam adicionados aos caminhos:



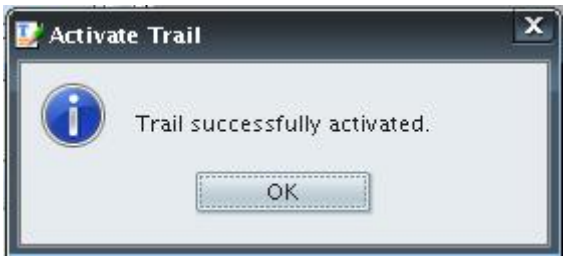
Após adicionar todos os túneis selecione o botão Apply:



6° Passo: Selecione as opções Complete Trail seguido de Activate Trail no canto superior da janela para finalizar a criação do circuito:



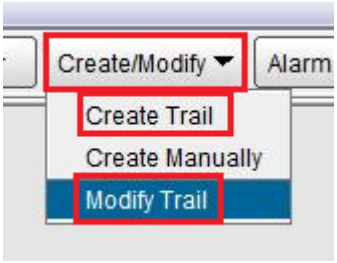
Abrirá uma janela informando que o serviço foi ativado com sucesso:



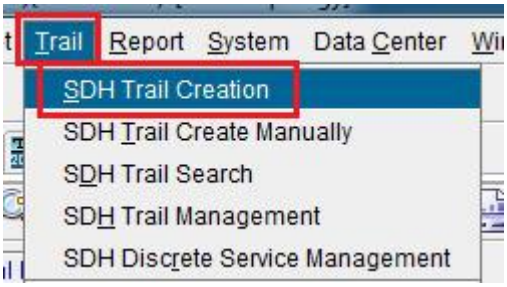
- Huawei

- Serviços de Voz por V5:

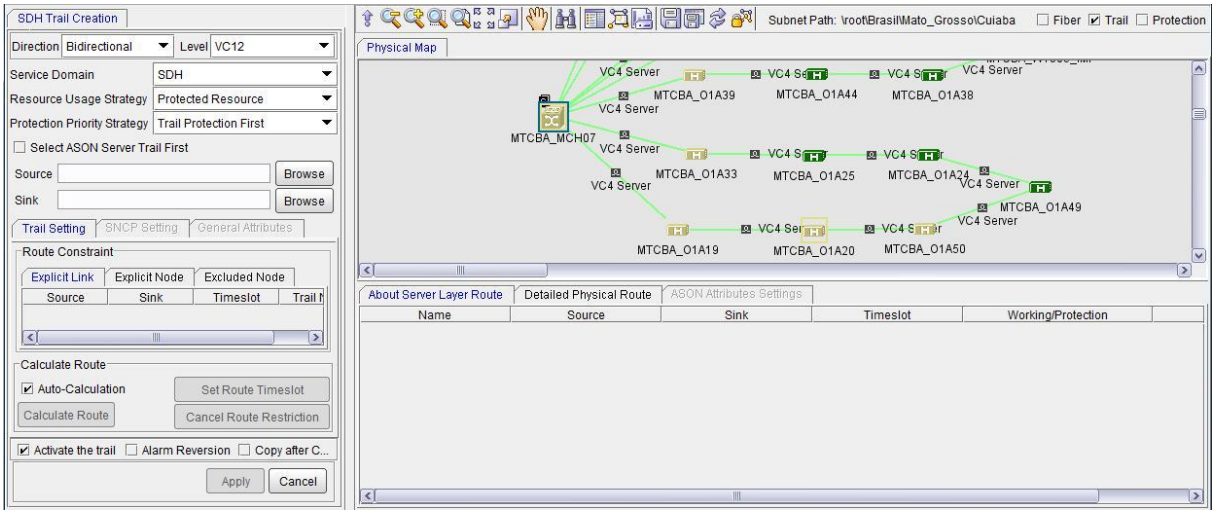
Para editar ou excluir um serviço clique no Create / Modify no serviço desejado e selecione a opção Create Trail para edita-lo ou Modify Trail para exclui-lo:



1° Passo: Para criar um novo serviço selecione a opção Trail seguido de SDH Trail Creation no canto superior da janela:



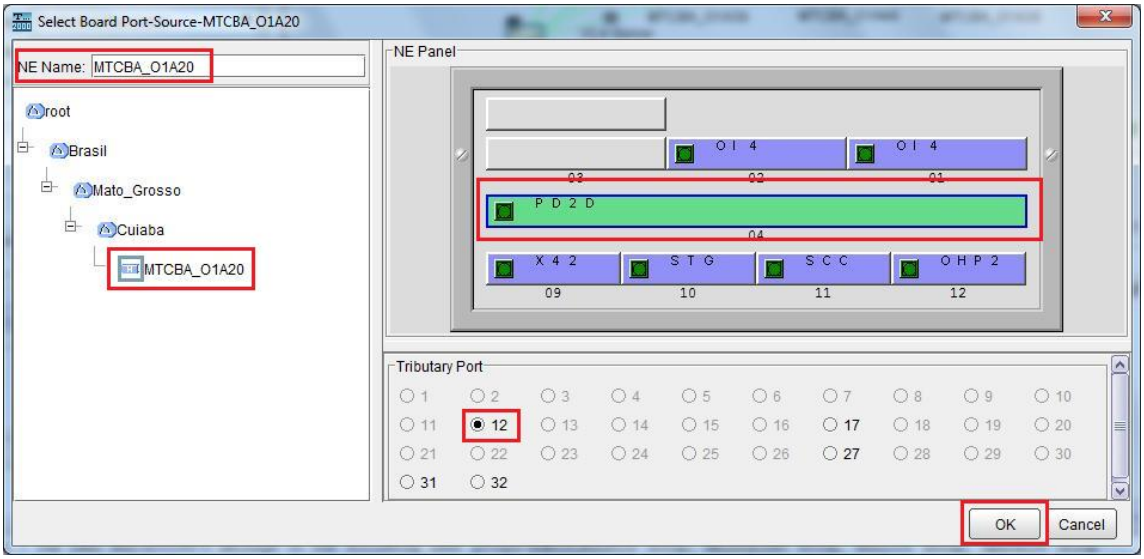
Abrirá uma nova janela para criação do circuito:



2° Passo: Na aba SDH Trail Creation, selecione Bidirectional em Direction e a capacidade do circuito em Level, conforme abaixo:

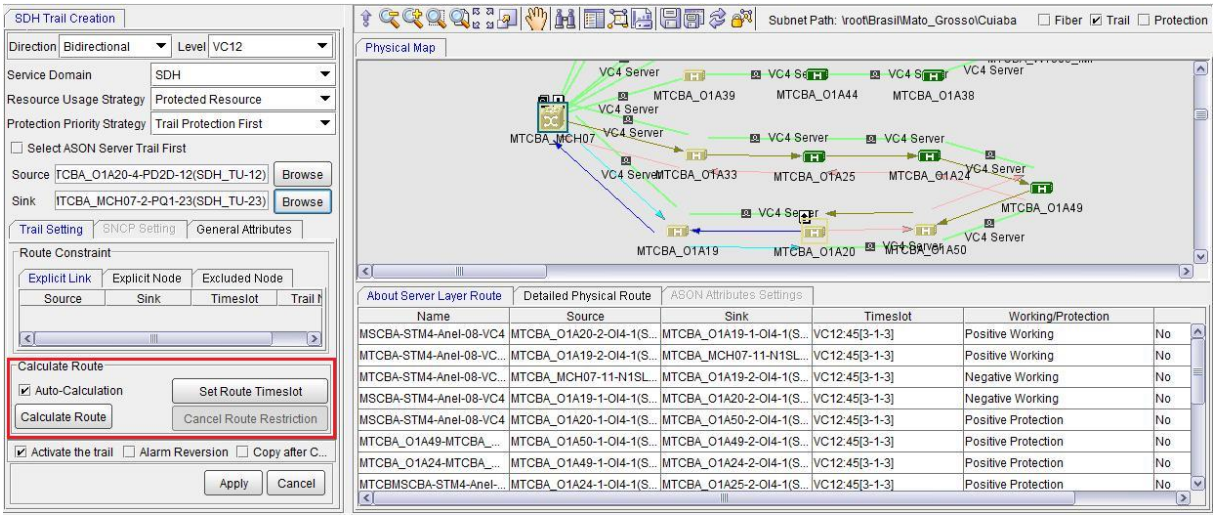
3° Passo: No campo Source selecione o botão Browse para selecionar a interface do primeiro elemento onde fechará o circuito:

Abrirá uma janela para seleção da interface, no campo NE Name insira o nome do SDH da primeira interface, selecione o elemento na coluna de baixo. Em NE Painel selecione a placa e em Tributary port selecione a interface desejada, após escolhida clique no botão OK:

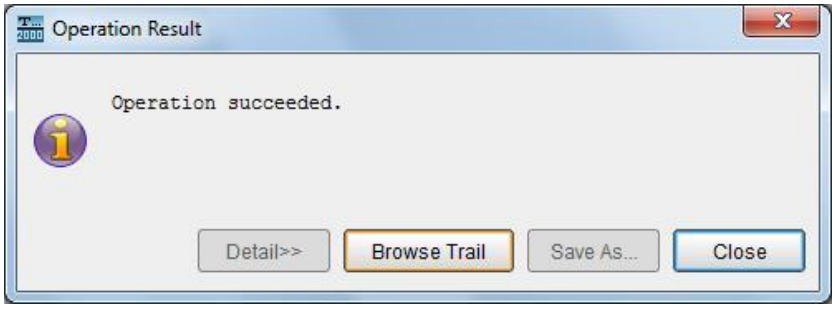


Realize o processo de seleção de interface para o segundo elemento.

4° Passo: Selecione a opção Auto-Calculation e clique no botão Calcule Route, a gerência selecionará os caminhos automaticamente, se for necessário designar o caminho selecione a opção Set Route Timeslot:



5° Passo: Selecione a opção Apply no canto inferior da janela para finalizar a criação do circuito, Abrirá uma janela informando que o Trail foi ativado com sucesso:



- Tellabs 7345 Switch Agregação Ethernet

- Serviços de Dados, Voz por H248 e MGMT:

Para excluir um serviço do elemento Tellabs 7345 basta deletar a VLAN que foi configurada para o serviço conforme exemplo abaixo:

```
t7300-SW-MGBHE_O1A44# configure terminal
t7300-SW-MGBHE_O1A44(config)# no vlan 123
t7300-SW-MGBHE_O1A44(config)# end
```

Para criar um novo serviço no elemento Tellabs 7345 deve-se executar os comandos na mesma ordem do exemplo abaixo adicionando a porta do DSLAM e as interfaces 10 Gb que estão conectadas aos elementos vizinhos. Nos outros elementos do anel adicionar somente as portas 10 Gb:

```
t7300-SW-MGBHE_O1A44# configure terminal
t7300-SW-MGBHE_O1A44(config)# vlan 123
t7300-SW-MGBHE_O1A44(config-vlan)# ports add gi 1/2/5
t7300-SW-MGBHE_O1A44(config-vlan)# ports add xg 1/2/1
t7300-SW-MGBHE_O1A44(config-vlan)# ports add xg 1/2/2
t7300-SW-MGBHE_O1A44(config-vlan)# end
```

Confirmar as configurações realizadas através do comando “show vlan id XXX”:

```
t7300-SW-MGBHE_O1A44# show vlan id 123
Vlan database
---------------------------------------------------
Vlan ID                 : 123
Member Ports            : Xg1/2/1, Xg1/2/2, Gi1/2/5
Untagged Ports          : None
Stats Collection State  : Disabled
Name                    : 123
```

Status : Permanent

Após confirmar as configurações executar o comando “write startup-config” para que as alterações sejam salvas na memória do equipamento:

t7300-SW-MGBHE_O1A44# write startup-config
Write operation [Complete]

- Datacom

- Serviços de Dados e MGMT:

Para excluir um serviço do elemento Datacom basta deletar a VLAN que foi configurada para o serviço conforme exemplo abaixo:

D2NHO01A1001#configure
D2NHO01A1001(config)#no interface vlan 123
D2NHO01A1001#exit

Para criar um novo serviço no elemento Datacom deve-se executar os comandos na mesma ordem do exemplo abaixo adicionando a porta do DSLAM e as interfaces que estão conectadas aos elementos vizinhos. Nos outros elementos do anel adicionar somente as portas do anel:

D2NHO01A1001#configure
D2NHO01A1001(config)#interface vlan 123
D2NHO01A1001(config-if-vlan-123)#set-member tagged ethernet 1/2
D2NHO01A1001(config-if-vlan-123)#set-member tagged ethernet range 1/25 1/26

Confirmar as configurações realizadas através do comando “show vlan id XXX”:

D2NHO01A1001#show vlan id 123
VLAN: **123**
Type: Static
Status
Admin: Enabled
Oper: Up
Log duplicated IP: Enabled

Aging-time:	300 sec.
Learn-copy:	Disabled
MAC maximum:	Disabled
EAPS:	protected on domain(s) 0
CFM status:	Disabled
Link Detection:	Disabled
Proxy ARP:	Disabled
Members:	**Eth1/2 (static, tagged)**
	Eth1/25 to Eth1/26 (static, tagged)
Forbidden:	(none)

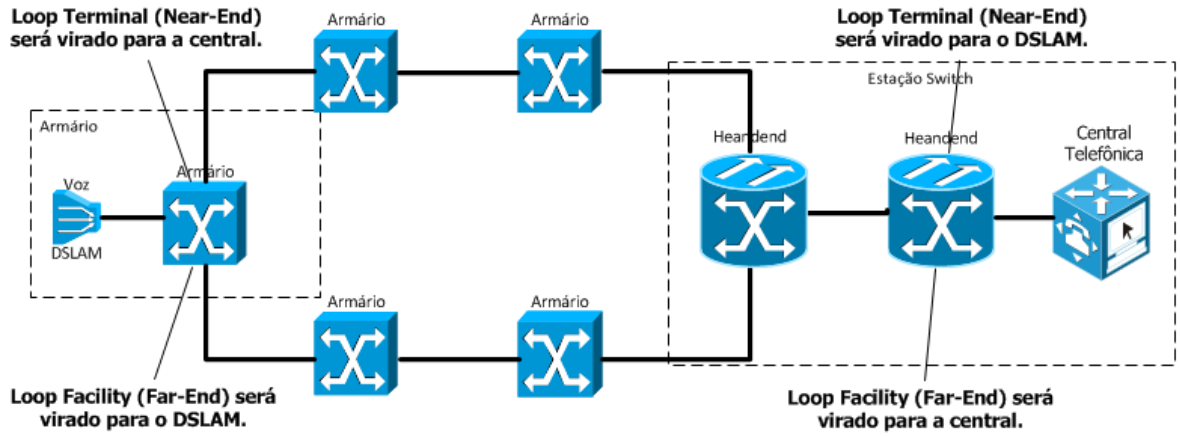
Após confirmar as configurações executar o comando “copy running-config startup-config” para que as alterações sejam salvas na memória do equipamento:

```
D2NHO01A1001#copy running-config startup-config
Saving configuration in flash 1...
Done.
```

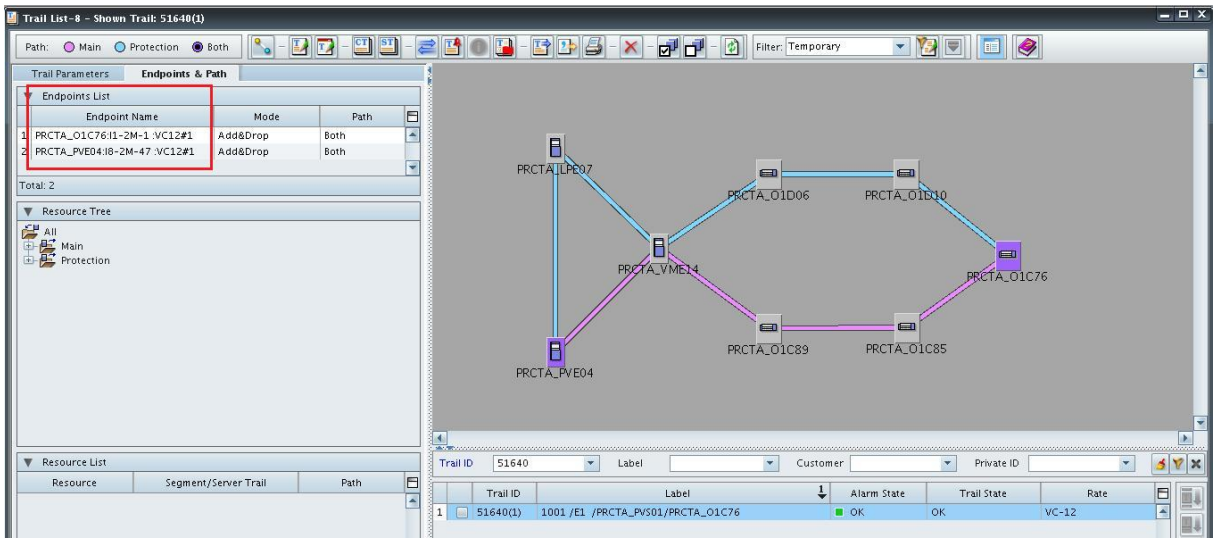
Procedimento de testes de circuitos com loopback

- ECI

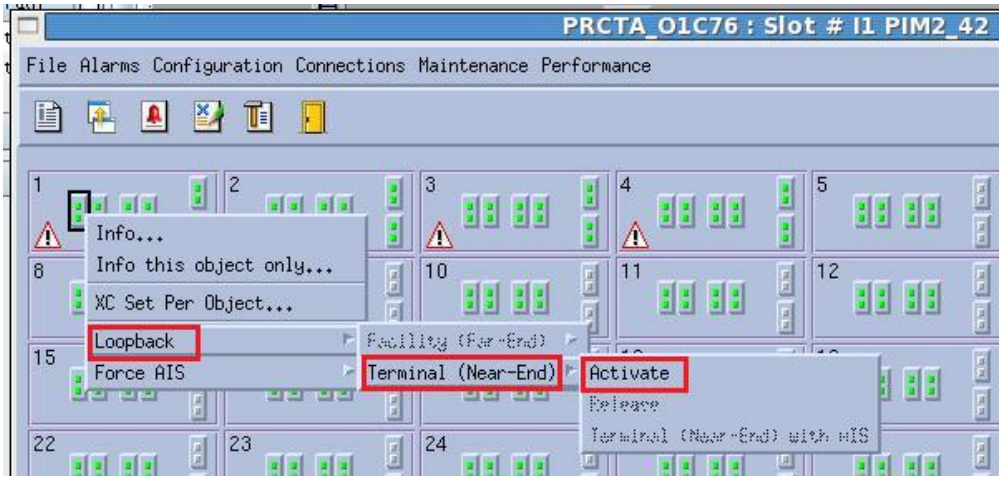
Nas interfaces do tipo tributário dos equipamentos SDH podemos realizar testes dos circuitos com loopback lógico, este loop é realizado pela matriz do SDH. Nos equipamentos ECI o loopback Terminal (Near-End) é fechado para o agregado, ou seja, é apontado para o outro SDH do circuito sendo assim para a extremidade mais distante do circuito em relação a interface onde esta sendo realizado o loop. O loopback Facility (Far-End) é apontando para fora do SDH, portanto para fora do tributário, onde esta conectado o equipamento cliente que neste caso é o DSLAM ou a Central de Comutação. Abaixo temos um exemplo para facilitar o entendimento:



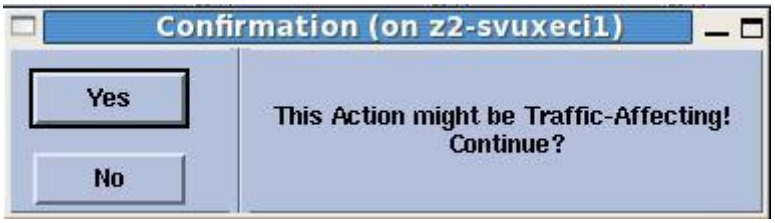
1° Passo: Após identificar o circuito a ser testado (verificar o procedimento de verificação de configurações) verificar quais são as interfaces onde fecha o circuito:



2° Passo: Selecionar no equipamento a interface que será testada, selecionar o primeiro botão da interface, clicar com o botão direito do mouse, selecionar a opção Loopback seguida de Terminal (Near-End) e Activate:

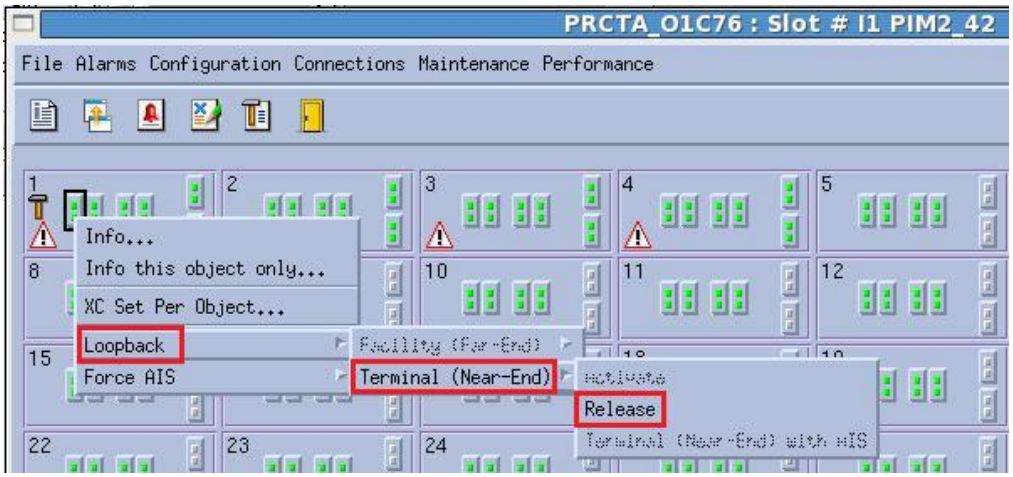


Abrirá uma janela para confirmação da ação, clique em Yes:

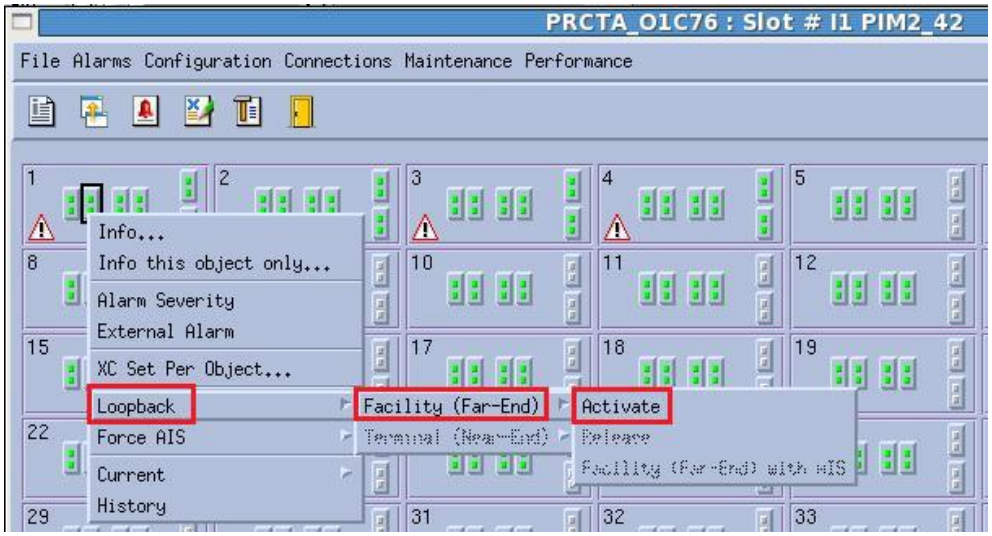


Quando estiver com loop ativo a interface ficará com um ícone indicando manutenção, conforme abaixo:

3° Passo: Para retirar o loop clique novamente com o botão direito do mouse no primeiro botão da interface, selecione a opção Loopback seguida de Terminal (Near-End) e Realease:



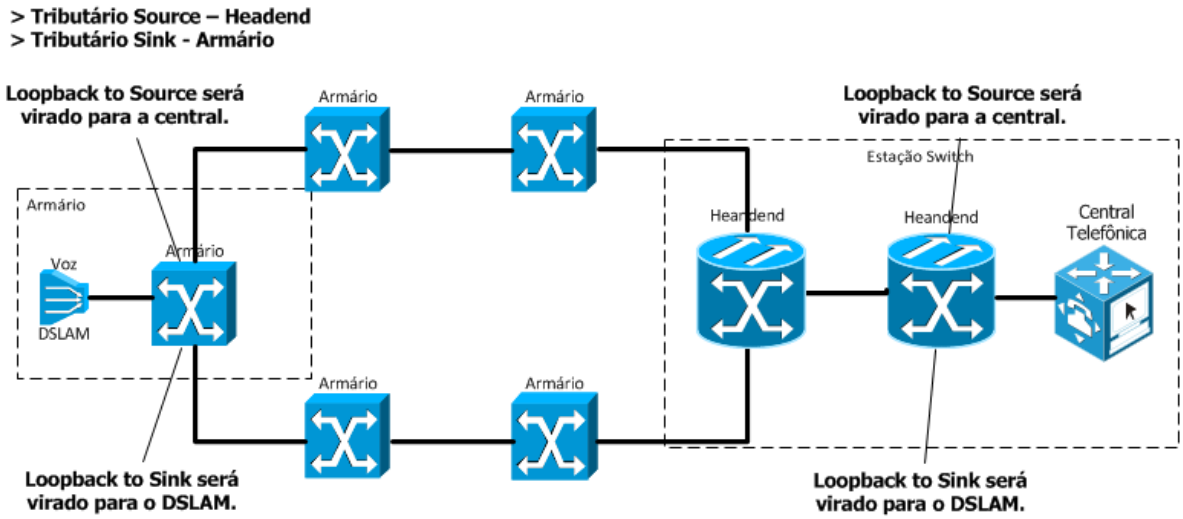
4° Passo: Para fechar loop Facility (Far-End), selecionar o segundo botão da interface, clique com o botão direito do mouse, selecionar a opção Loopback seguida de Facility (Far-End) e Activate:



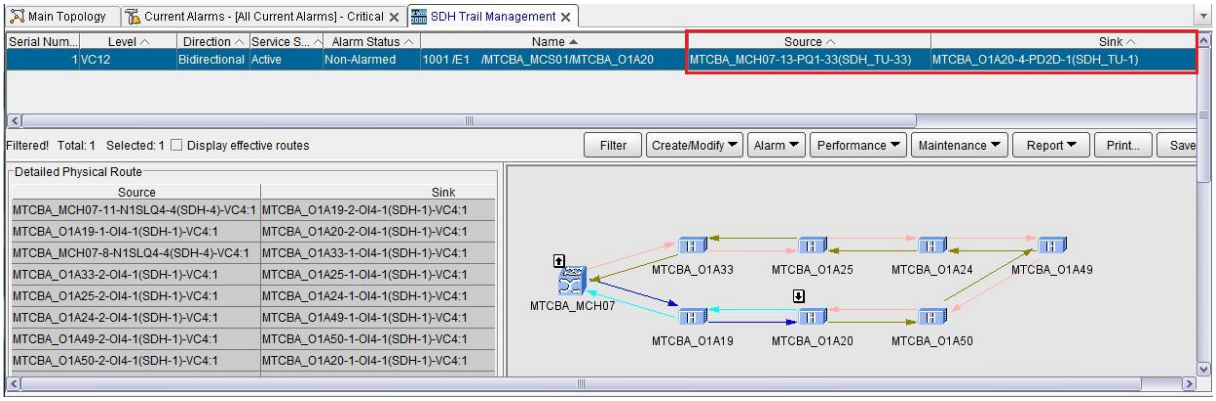
5° Passo: Para retirar o loop clique novamente com o botão direito do mouse no segundo botão, selecionar a opção Loopback seguida de Facility (Far-End) e Realease.

- Huawei

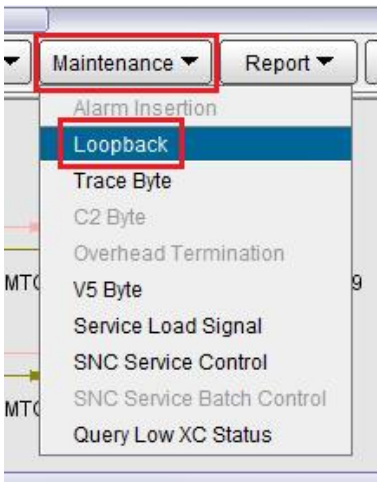
Nos equipamentos Huawei deve ser identificado qual é a interface Source e qual é a interface Sink, pois o loop é virado para cada interface, no exemplo abaixo a interface tributária do headend é o Source e a interface tributária do armário é o Sink, portanto se for fechado o Loopback to Source em ambos os elementos será virado para a central de comutação e se for fechado o loopback to Sink será virado para o DSLAM:



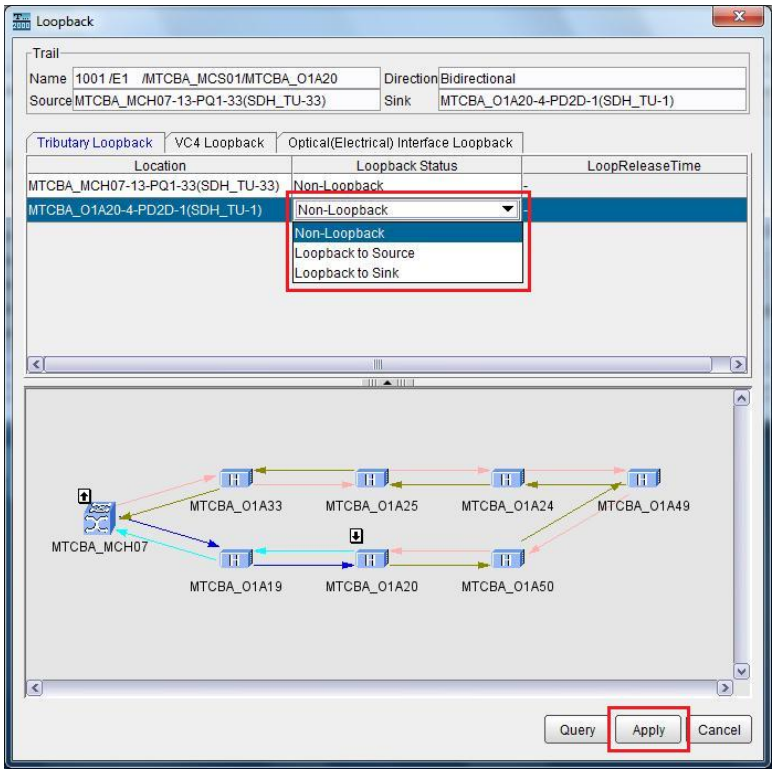
1° Passo: Após identificar o circuito a ser testado (verificar o procedimento de verificação de configurações) verificar qual é a interface Source e qual é a interface Sink onde fecha o circuito:



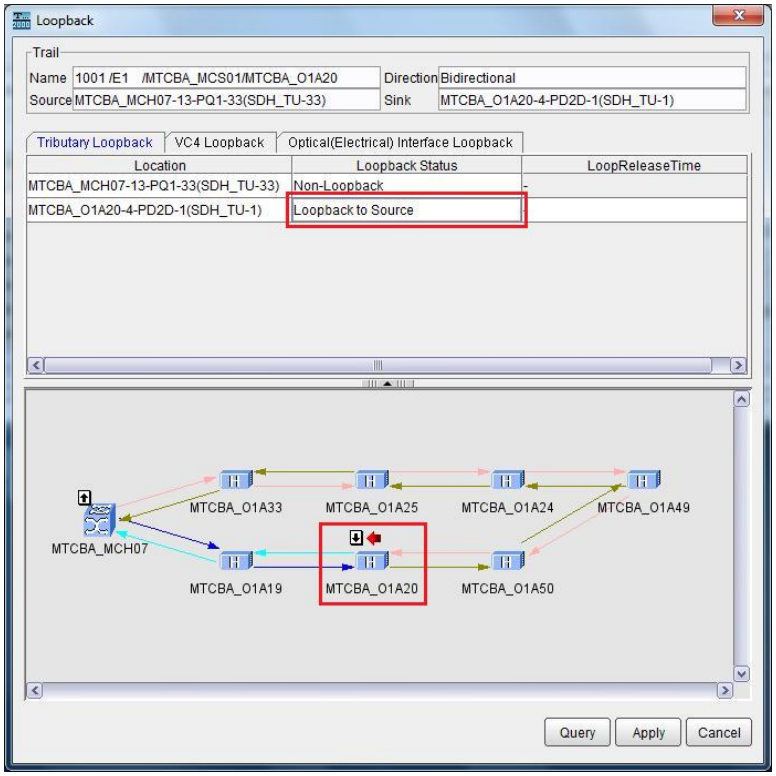
2° Passo: Clicar no botão Maintenance e selecionar a opção Loopback:



3° Passo: Abrirá uma janela para execução dos testes, clique na opção Loopback Status e selecione o loop que deseja realizar, neste exemplo o Loopback to Source será virado para a central de comutação e o loopback to Sink será virado para o DSLAM. Após selecionar a opção clique no botão Apply:



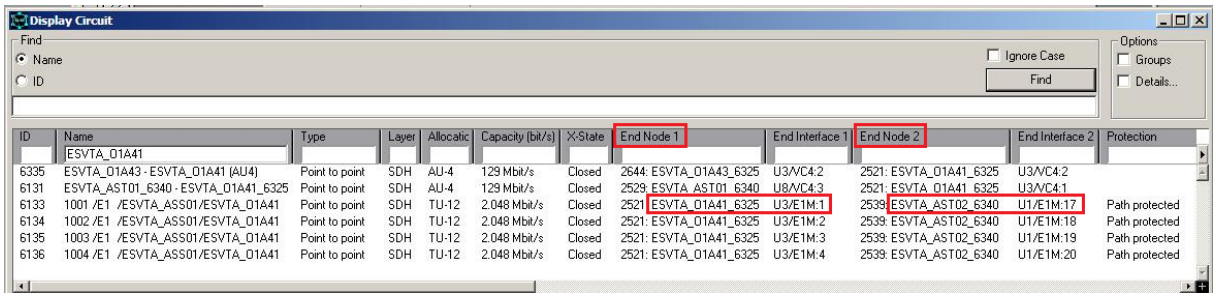
Quando estiver com loop ativo a interface ficará com um ícone indicando o sentido do loop, conforme abaixo:

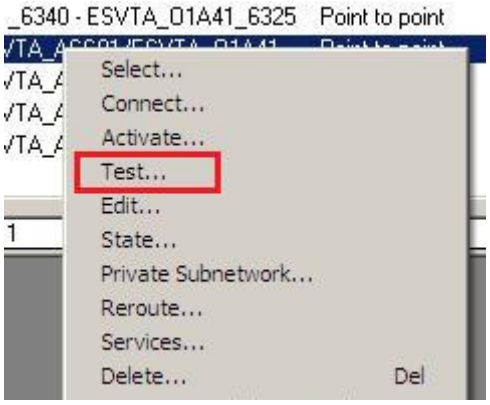


4° Passo: Para retirar o loop clique na opção Loopback Status e selecione a opção Non-Loopback, em seguida clique na opção Apply.

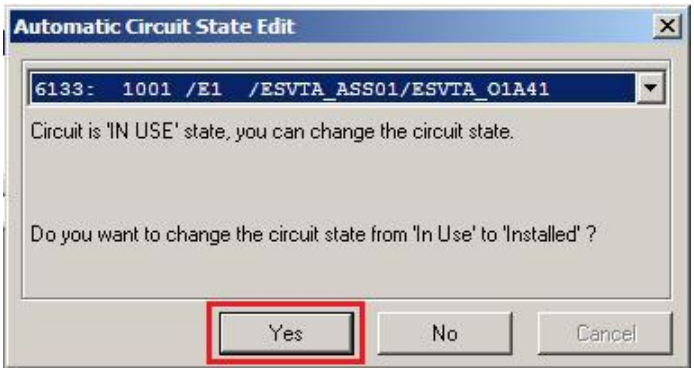
- Tellabs 6325 Edge Node

1° Passo: Após identificar o circuito a ser testado (verificar o procedimento de verificação de configurações) verifique qual é o End Node 1 e End Node 2, em seguida clique com o botão direito do mouse no serviço e selecione a opção Test:

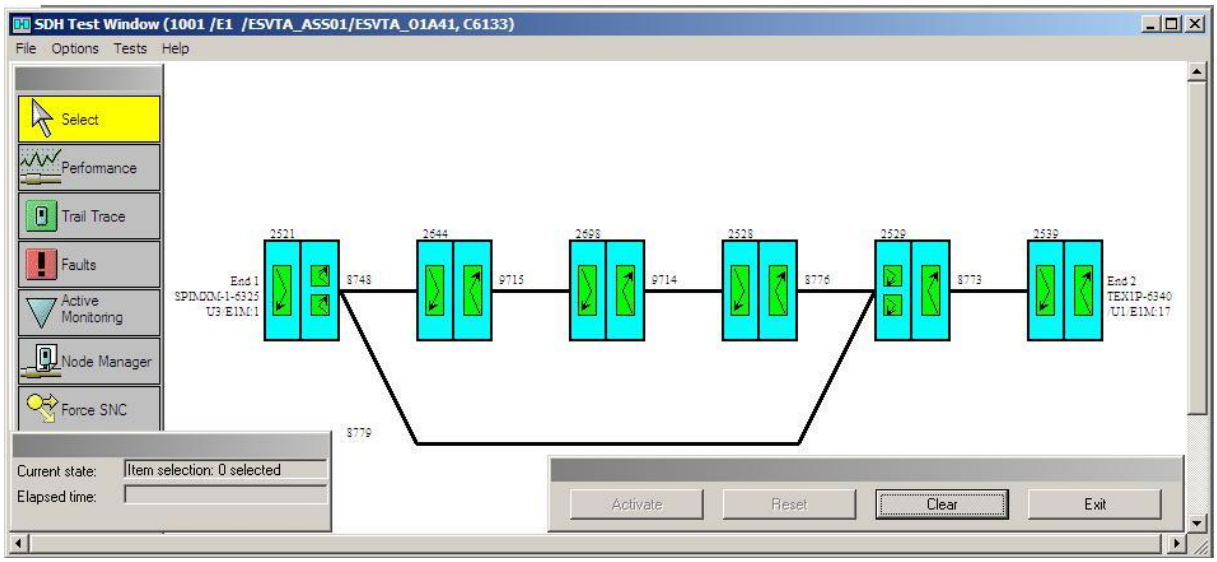


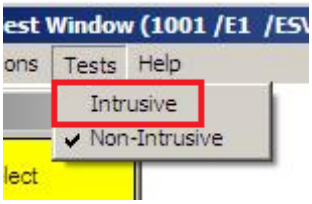


2° Passo: Abrirá uma janela informando que o status do circuito será alterado de In Use para Installed, confirme clicando no botão Yes:

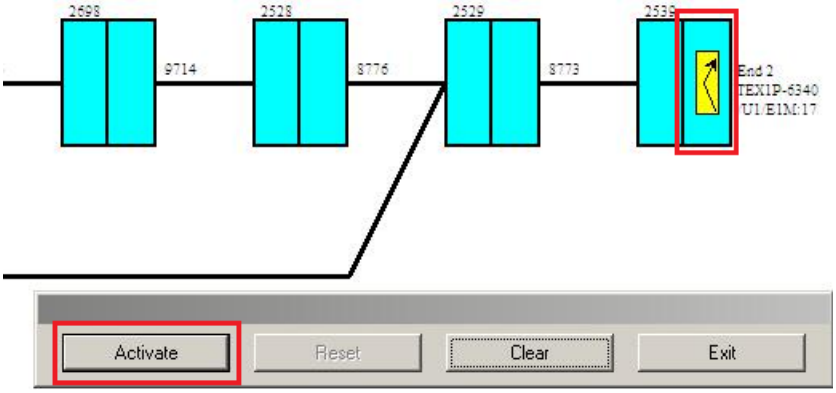


3° Passo: Após abrir a janela de testes selecione no canto superior da janela no botão Tests a opção Intrusive:

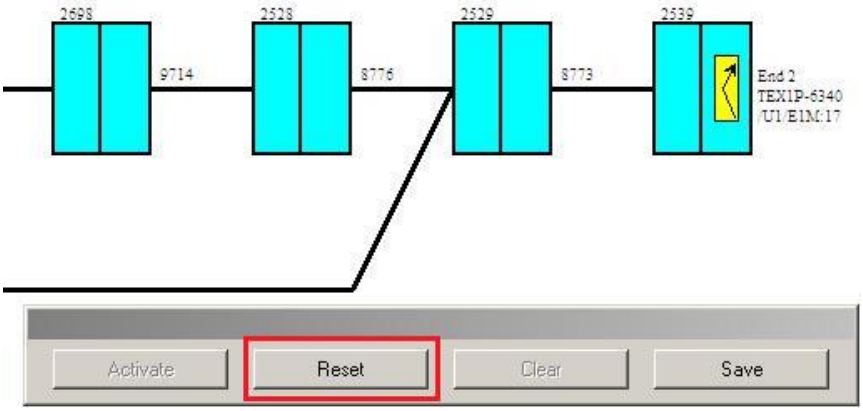




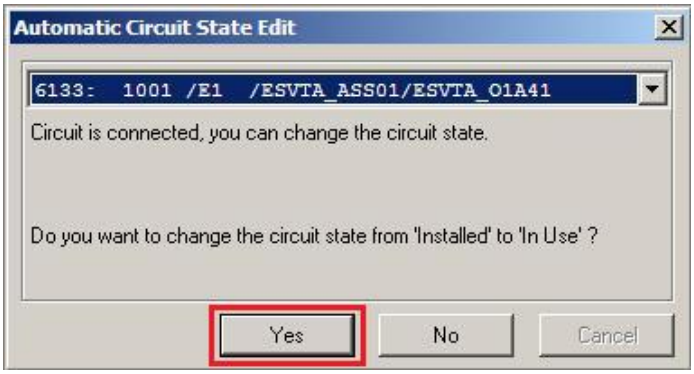
4° Passo: Para fechar o loop selecione o botão do elemento onde será realizado o loop e clique no botão Active:



5° Passo: Para retirar o loop clique no botão Reset:



6° Passo: Após finalizar os testes feche a janela de testes, abrirá uma janela informando que o status do circuito será alterado de Installed para In Use, confirme clicando no botão Yes:



TRATAMENTO DE FALHAS DE TRANSMISSÃO

LOS (Loss of Signal) – Rede Ótica

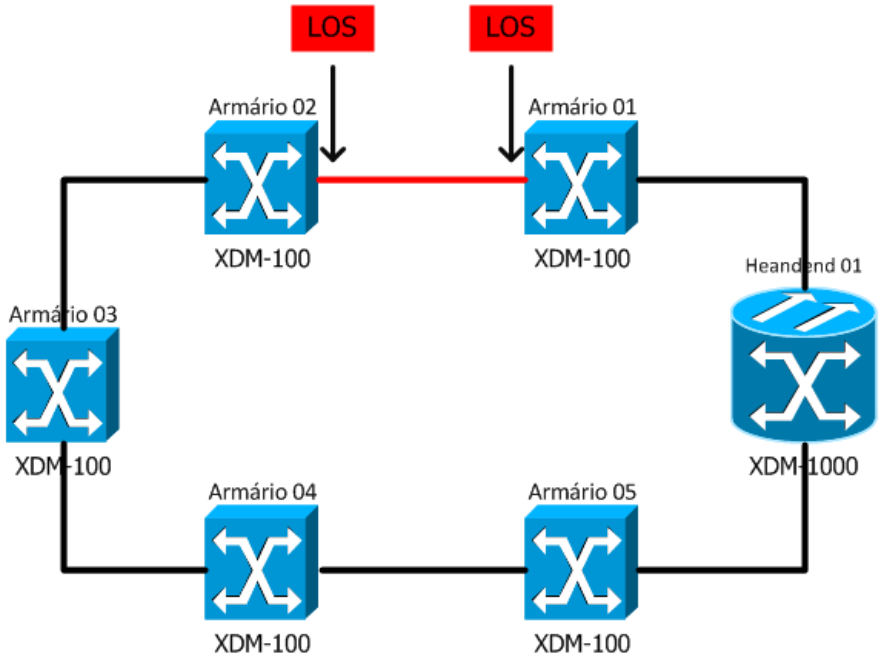
Como já sabemos um alarme de LOS sinaliza ausência de potência ótica na RX da interface. Sempre que encontrado este alarme alguns detalhes devem ser analisados, pois mesmo que seja o mesmo alarme as causas podem ser diferentes. Abaixo alguns exemplos:

- Alarme de LOS entre vários elementos, todos ao mesmo tempo, indica rompimento de cabo ótico, por exemplo, um cabo de 32 pares de fibras, se todas as fibras estiverem sendo utilizadas haverá falha em 32 links entre elementos.
- Alarmes de LOS em um elemento e SIA no outro pode indicar uma falha de conexão, cordão quebrado ou falha de placa.
- Alarme de LOS entre dois elementos pode indicar rompimento de fibra, falha de conexão, cordão quebrado ou falha de placa.
- Alarme de LOS entre vários elementos.

Nos casos de LOS entre vários elementos ao mesmo tempo deve ser acionado o supervisor de rede externa informando todos os links que estão alarmados, ele possui acesso aos projetos de rede externa, ele realizará a análise de qual o cabo utilizado estão os links alarmados e na sequência o supervisor de rede acionará a equipe de manutenção de rede externa, para medição de fibra a fim de localizar o ponto exato da falha. Neste procedimento a equipe utiliza um instrumental chamado OTDR (Optical Time Domain Reflectometer), que indica a distância exata em metros até onde o sinal de teste esta chegando, indicando o ponto exato da falha. Este instrumento também indica valores de atenuações de fibra e suas respectivas distâncias. Após as medições e identificado no projeto o local aproximado da falha, a

equipe se desloca até o local, caso não seja identificado a falha visualmente é aberto a caixa de emendas mais próxima e realizado novas medições a partir deste ponto até que seja localizado o local exato da falha. As causas mais comuns de rompimento de cabo ótico são veículos com carga alta, poda e queda de árvores, queda de postes, acidentes de veículos, linhas de pipas, entre outros. Nos casos de rompimentos por linhas de pipas a falha é de difícil identificação, pois o cabo é cortado parcialmente sem que haja uma falha visível, dificultando a localização pela equipe de campo.

- Alarme de LOS entre dois elementos.
- Alarmes de LOS em um elemento e SIA no outro.

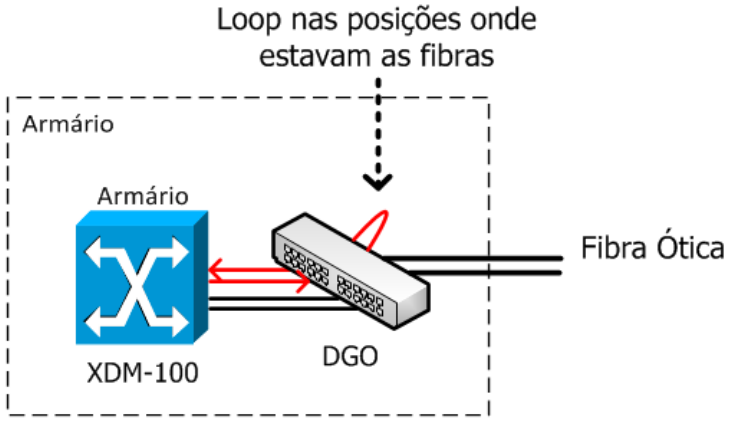


Exemplo de alarme de LOS entre dois armários.

Nos casos de LOS entre dois elementos ou LOS em um elemento e SIA no outro deve ser verificado se há algum alarme de falha de hardware, se há potência de TX nos dois lados e desligar a função ALS quando houver, pois neste caso pode mascarar uma falha de TX ou em apenas um dos lados. Se não houver potência de TX verificar de o laser esta ligado, se mesmo ligado não transmitir possivelmente haverá uma falha de SFP, sendo necessária a sua substituição.

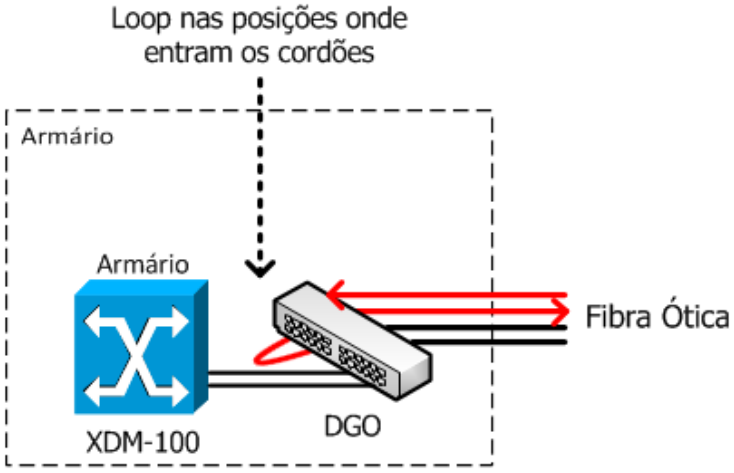
Se após a análise não for identificado o problema deve ser acionado um técnico de campo para a realização de testes nos armários 01 e 02, deverá levar um

instrumental Power Meter Ótico que realiza a leitura de potência ótica em sua RX, levar também cordões novos, atenuadores e SFPs do modelo utilizado nos armários.
1° Passo: Com o técnico no armário 01, no primeiro passo realizar testes de loop no DGO, com um cordão deve ser fechado loop nas duas posições onde entram as fibras, conforme a imagem abaixo, com isso a potência de TX do armário 01 deve voltar para a sua RX, se após o loop o alarme de LOS limpar no SDH indica que as conexões internas do armário estão OK.
Sempre que reconectar cordões ou fibras deve se realizado a limpeza das conexões com álcool isopropílico, escova e flanela próprias para fibras e cordões óticos.



Teste de loop das conexões internas.

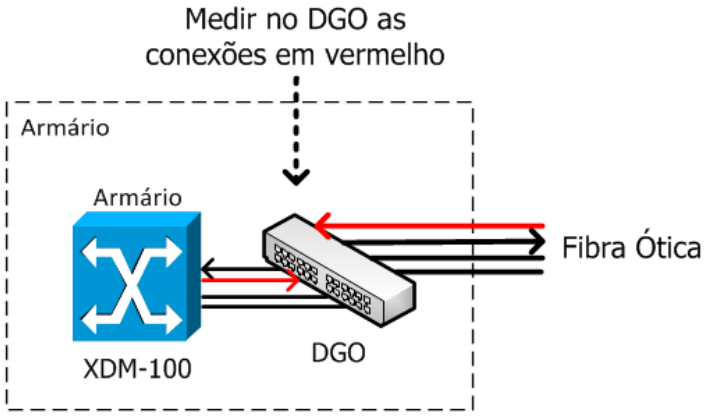
Fechar loop nas duas posições onde entram os cordões, conforme a imagem abaixo, com isso a potência de TX do armário 02 deve voltar para a sua RX, se após o loop o alarme de LOS limpar no SDH indica que as fibras e as conexões internas do armário 02 e estão OK.



Teste de loop das fibras e conexões do outro armário.

Durante os testes de loop se o alarme de LOS limpar será gerado um alarme de TIM, pois o SDH receberá o próprio label identificador.

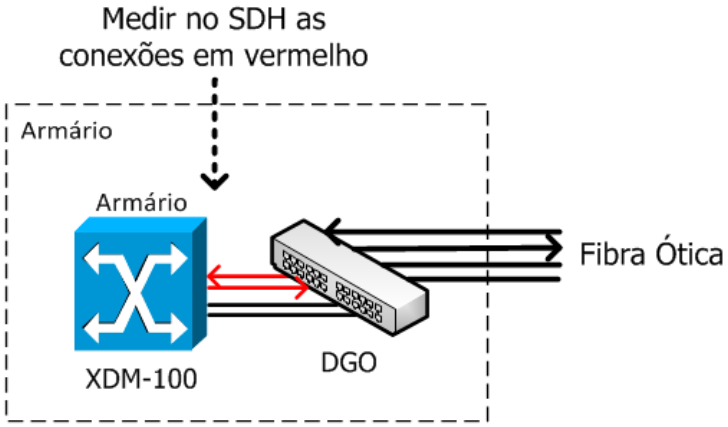
2° Passo: Deverão sem medidos as duas posições no DGO, a RX das fibras vindo do armário 02, e a RX do cordão que transmite para o armário 02 conforme a imagem abaixo:



Medições no DGO

3° Passo: Se não houver potência de RX no cordão que transmite para o armário 02 deverá ser medido direto na interface do SDH, se não houver potência de TX na saída da interface, a SFP deve ser substituída, se a potência de TX estiver normal deve ser substituído o cordão.

4° Passo: Se houver potência de RX vindo das fibras do armário 02 deverá ser medida a ponta do cordão que entra na interface do SDH, se a potência de RX estiver normal deve ser substituído a SFP, caso contrário deve ser substituído o cordão.



Medições no SDH

Se todas as conexões internas do armário estiverem OK, todos os passos realizados anteriormente devem ser realizados no armário 02. Se após todos os testes realizados não for encontrada falha nas conexões internas dos armários deve ser acionado o supervisor de rede externa para verificação das fibras.

LOS (Loss of Signal) – Cabos elétricos

Os alarmes de LOS em cabos elétricos são reportados em conexões do tipo tributários E1, E3, STM-1, entre outros. Neste tipo de conexão a distância entre os elementos é curta, normalmente é utilizada para conexão entre elementos dentro do mesmo ambiente.

Abaixo alguns exemplos deste tipo de falha:

- Alarmes de LOS em um elemento e SIA no outro.
- Alarme de LOS entre dois elementos.

Podem indicar falha de conexão, cabo danificado, falha na interface ou falha de placa.

Deve ser verificado se há algum alarme de falha de hardware e verificar se a interface esta habilitada. Se o outro equipamento não for de transmissão, por exemplo, uma central telefônica, o analista da equipe do CGR-Comutação deve ser envolvido nos testes.

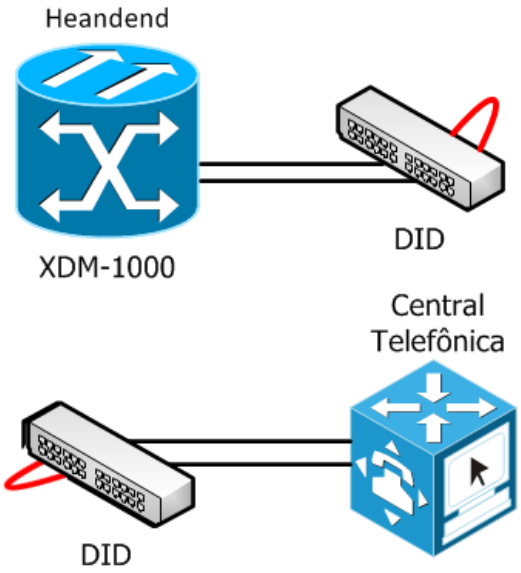
Se após a análise não for identificado o problema deve ser acionado um técnico de campo para a realização de testes no local, deverá levar cabos novos e as placas do modelo utilizado.

1° Passo: Com o técnico no local solicitar que o mesmo verifique a conexão no primeiro elemento, se não houver problema fechar loop físico direto na interface do elemento, se o alarme limpar indica que a interface esta OK. Se o alarme permanecer após o loop deverá ser reconfigurado o circuito mudando para outra interface vaga.

Realizar o mesmo procedimento para o segundo elemento.

2° Passo: Deve-se realizar testes de loop no DID, com um cabo de teste deve ser fechado loop nas duas posições onde entram os cabos vindo do primeiro elemento, conforme a imagem abaixo, com isso o alarme de LOS deve limpar indicando que as conexões do elemento até o DID estão OK. Caso o alarme permaneça os cabos entre o DID e o elemento deve sem substituídos.

Realizar o mesmo procedimento para o segundo elemento.



Teste de loop das conexões entre os elementos.

High Tx Power / Low Tx Power

Para os alarmes de potência de TX possivelmente a falha será na interface, pois os valores transmitidos por ela não podem ser alterados, portanto o transceiver (SFP ou XFP) deve ser substituído. Se após a substituição o alarme permanecer a placa onde o transceiver é conectado deve ser substituída.

High Rx Power

Para o alarme de potência alta de RX deve-se adequar o nível de potência da interface alarmada, para isto basta inserir um atenuador na sua RX respeitando os limiares de RX aceitáveis pela interface de acordo com o modelo utilizado.

Low Rx Power / Signal Degraded / Out of Frame

Os alarmes de potência baixa de RX ou sinal degradado indica que o valor de RX esta abaixo do limiar aceitável pela interface de acordo com o modelo utilizado.

As principais causas destes alarmes são:

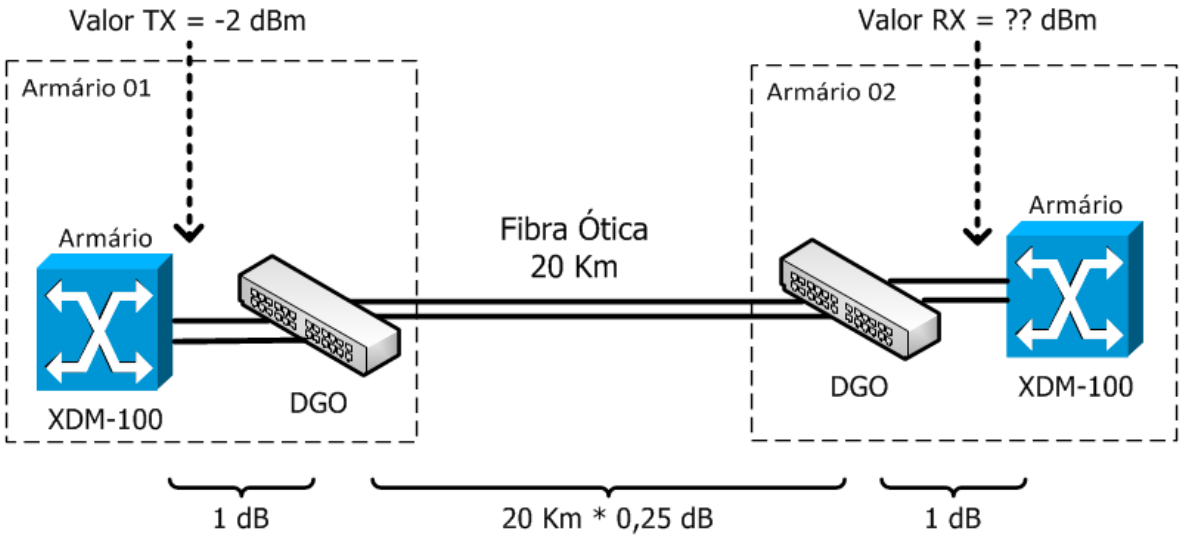
- Falha de hardware no receptor ou no transmissor.
- Falha de conexão, cordão ou fibra danificados.

Primeiro deve-se verificar os valores de RX da interface alarmada e de TX do elemento vizinho seguindo o procedimento de verificação de potência ótica nos equipamentos. Após anotar os valores verificados podemos fazer um cálculo simples para verificar qual o valor total de atenuação do enlace.

Utilizamos valores aproximados de atenuação de fibra e um valor pré-determinado para as atenuações geradas por conexões entre os equipamentos, cordões, DGOs e fibra ótica. Para fibra o valor de atenuação padrão é de 0,25 dB por km, e para todas as conexões do enlace o valor é de 2 dB (1 dB por extremidade). Portanto subtraindo o valor transmitido pelo equipamento do valor total de atenuações do enlace teremos o valor de RX do elemento vizinho, abaixo esta a fórmula utilizada:

Valor RX = Valor TX - [(Distância total do enlace * 0,25) + 2]

Para o exemplo abaixo temos um enlace de 20 Km entre os elementos:



Valor RX = (-2) - [(20 * 0,25) + 2]

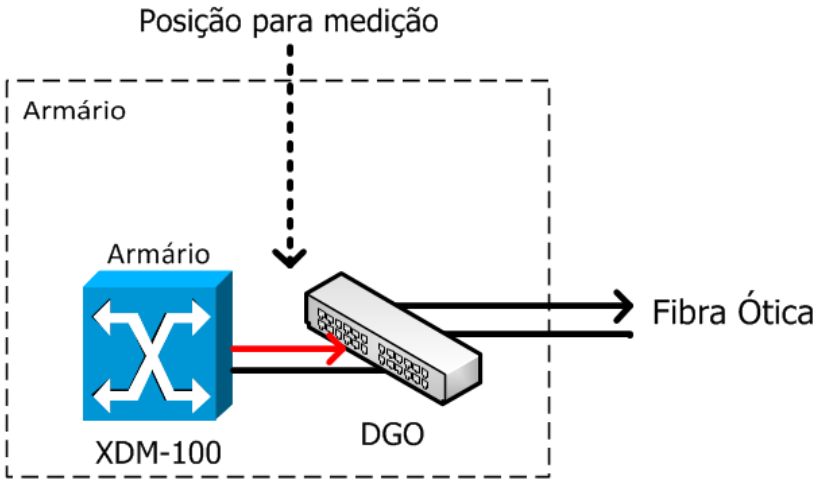
Valor RX = (-2) - [5 + 2]

Valor RX = -9 dBm.

Portanto o valor de RX do elemento será em torno de -9 dBm.

Após calcular o valor aproximado de RX do elemento deve ser acionado um técnico de campo para a realização de testes nos armários, deverá levar um instrumental Power Meter Ótico, cordões novos, atenuadores e SFPs do modelo utilizado nos armários.

1° Passo: Com o técnico no primeiro armário deverá ser medido a RX do cordão que entra no DGO transmitindo para o segundo armário, conforme a imagem abaixo:



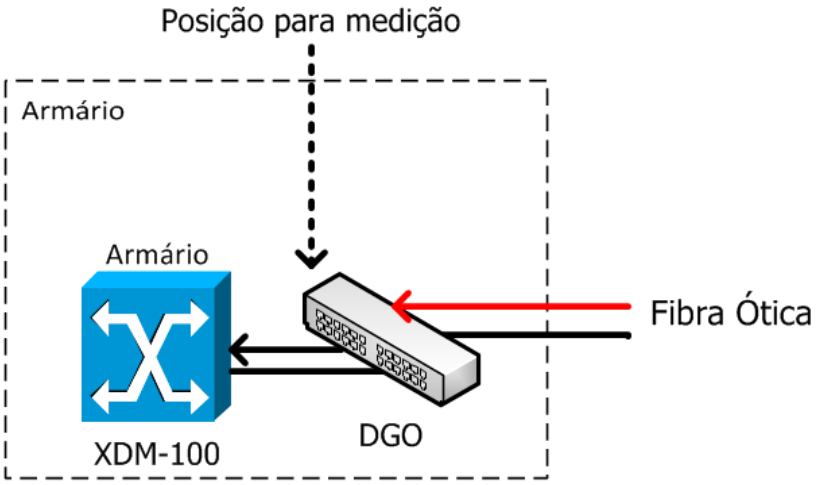
Medições no DGO

Se o valor medido estiver com mais de 2 dB de diferença do valor transmitido, ir para o 2° passo, caso contrário ir direto para o 3° passo.

2° Passo: Deverá ser medido direto na interface do SDH, se o valor medido estiver com mais de 2 dB de diferença do valor transmitido a SFP deve ser substituída, se a potência de TX estiver normal deve ser substituído o cordão. Se após este processo o alarme continuar o técnico deve ir para o segundo armário para o próximo passo.

3° Passo: Com o técnico no segundo armário, verificar se há atenuadores na RX da interface do SDH, se houver o seu valor de atenuação deve ser adicionado ao valor de RX calculado. Medir no cordão que entra direto na interface do SDH, se o valor medido estiver com menos de 2 dB de diferença do valor de RX calculado a SFP deve ser substituída. Caso contrário ir para o próximo passo.

4° Passo: Medir a RX na posição do DGO onde entra a fibra vinda do primeiro armário, conforme a imagem abaixo:



Medições no DGO

Se o valor medido estiver com menos de 2 dB de diferença do valor de RX calculado deve ser substituído o cordão, caso contrário deve ser acionado o supervisor de rede externa para verificação das fibras.

Link Down

O alarme de Link Down é reportado em conexões do tipo Ethernet de conexões ótica ou elétrica. Este tipo de falha pode ser resultado de falha no processo de auto negociação, perda de sinal sobre a ligação resultante a partir de fibras ou cabos desconectados, ou uma falha de hardware. Para as conexões com cabos elétricos são utilizado cabos Ethernet, portanto não é realizada passagem por DIDs, portanto a conexão é direta.

Deve ser verificado se há algum alarme de falha de hardware e verificar se a interface esta habilitada. Verificar também se as configurações das interfaces dos dois elementos estão iguais, principalmente a auto negociação. Se o outro equipamento não for de transmissão, por exemplo, um switch, o analista da equipe do CGR-Dados deve ser envolvido.

Se após a análise não for identificado o problema deve ser acionado um técnico de campo para a realização de testes no local, deverá levar cabos e cordões novos, SFPs quando utilizar, pois em alguns equipamentos a interface é direto na placa, e levar as placas do modelo utilizado.

Para conexões elétricas solicitar ao técnico que verifique as conexões nas interfaces dos equipamentos, se não houver problema substituir o cabo entre os elementos, caso o alarme permaneça deverá substituir a SFP no primeiro elemento, se o alarme

persistir substituir a SFP no segundo elemento. Se as interfaces forem fixas será necessário reconfigurar o circuito mudando para outra interface vaga.

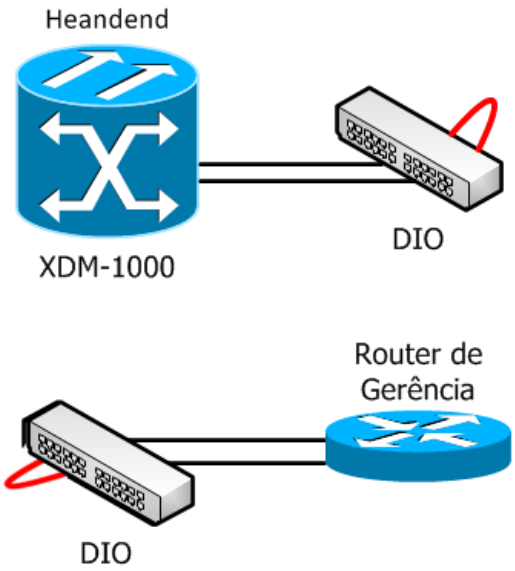
Para conexões óticas seguir os passos abaixo:

1° Passo: Com o técnico no local solicitar que o mesmo verifique a conexão no primeiro elemento, se não houver problema fechar loop físico direto na interface do elemento, se o alarme limpar indica que a interface esta OK. Se o alarme permanecer após o loop deverá ser substituída a SFP.

Realizar o mesmo procedimento para o segundo elemento.

2° Passo: Deve-se realizar testes de loop no DIO, com um cordão de teste deve ser fechado loop nas duas posições onde entram os cordões vindo do primeiro elemento, conforme a imagem abaixo, com isso o alarme de LOS deve limpar indicando que as conexões do elemento até o DIO estão OK. Caso o alarme permaneça os cordões entre o DIO e o elemento devem ser substituídos.

Realizar o mesmo procedimento para o segundo elemento.



Teste de loop das conexões entre os elementos.

DEG (Degraded) / EXC (Excessive Errors)

Os alarmes de DEG e EXC indicam taxa de erro no link.

As principais causas destes alarmes são:

- Falha de hardware no receptor ou no transmissor.
- Falha de conexão, cordão ou fibra danificado.
- Potência de RX baixa ou alta.

Esta falha pode ocorrer entre:

- Elementos de um anel.
- Elementos dentro de um armário.
- Elementos dentro da Estação Switch.

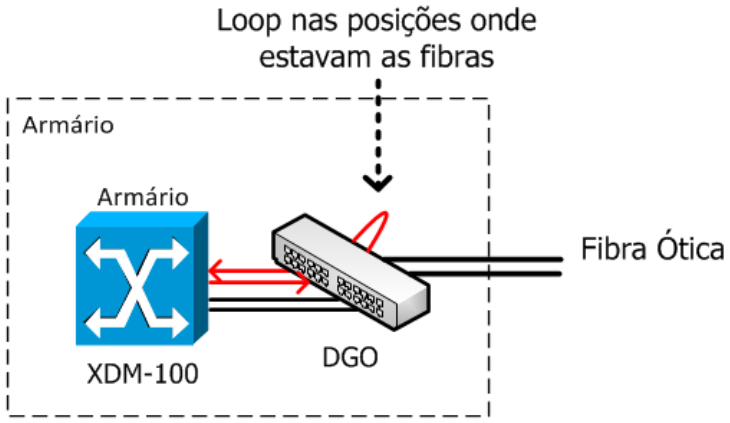
Caso o outro equipamento não seja de transmissão o analista da outra tecnologia deve ser envolvido.

Deve ser analisado se há alarmes de falha de hardware ou algum outro alarme no link que indique a causa da taxa de erro, verificar como estão as potências de RX das interfaces, se os níveis de RX estiverem muito alto ou muito baixo devem ser corrigidos.

Se após a análise não for identificado o problema deve ser acionado um técnico de campo para a realização de testes no local, deverá levar cordões novos e as placas do modelo utilizado.

- Para falha entre elementos de um anel:

1° Passo: Com o técnico no primeiro elemento realizar testes de loop no DGO, com um cordão deve ser fechado loop nas duas posições onde entram as fibras, conforme a imagem abaixo:

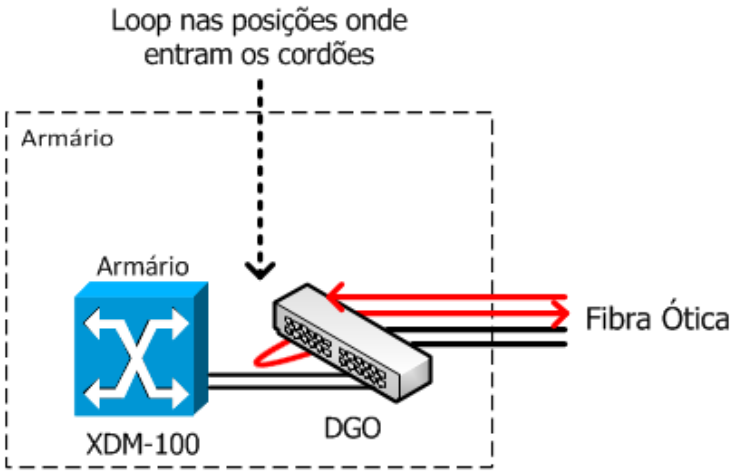


Teste de loop.

Verificar se os contadores não incrementaram erro, caso não ocorra indica que não a falha para o trecho testado, ir para o 2° passo.

Se a taxa de erro continuar deverá ser fechado loop direto na interface do SDH, se continuar taxando erro deverá ser substituído a SFP, caso não haja taxa de erro devem ser substituídos os cordões.

2° Passo: Fechar loop nas duas posições onde entram os cordões conforme a imagem abaixo, testando assim as conexões do outro elemento e as fibras, verificar os contadores da interface do segundo elemento.



Teste de loop.

Se a taxa de erro persistir o técnico deverá ir até o local do segundo elemento e realizar o mesmo teste. Com o loop fechado no DGO sentido para o primeiro elemento, verificar os contadores da interface do primeiro elemento, se houver incremento de taxa de erro deve ser acionado o supervisor de rede externa para verificação das fibras. Caso não incremente taxa de erro no primeiro elemento devem ser realizados os testes do 1° passo para o segundo elemento.

- Para falha entre elementos dentro de um armário ou Estação Switch.

Para conexões elétricas solicitar ao técnico que verifique as conexões nas interfaces dos equipamentos, se não houver problema substituir o cabo entre os elementos, verificar os contadores das interfaces dos elementos, se houver incremento de taxa de erro deverá substituir a SFP no primeiro elemento, verificar novamente os contadores das interfaces dos elementos, se a taxa de erro persistir substituir a SFP no segundo elemento. Se as interfaces forem fixas será necessário reconfigurar o circuito mudando para outra interface vaga.

Para conexões óticas seguir os passos abaixo:

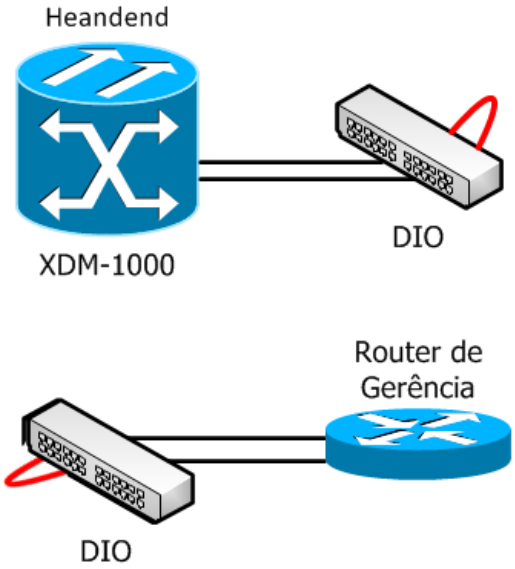
1° Passo: Solicitar ao técnico que verifique a conexão no primeiro elemento, se não houver problema fechar loop físico direto na interface do elemento, verificar os contadores da interface, se não houver taxa de erro indica que a interface esta OK. Se a taxa de erro permanecer após o loop deverá ser substituída a SFP.

Realizar o mesmo procedimento para o segundo elemento.

Para conexões dentro de armário, se as interfaces dos elementos estiverem OK devem ser substituídos os cordões entre os elementos, caso o link seja entre elementos dentro da estação switch realizar os testes do 2° passo.

2° Passo: Deve-se realizar testes de loop no DIO, com um cordão de teste deve ser fechado loop nas duas posições onde entram os cordões vindo do segundo elemento testando assim as conexões do primeiro elemento, conforme a imagem abaixo, verificar os contadores da interface do elemento, se incrementar erro deve ser substituído os cordões entre o DIO e o elemento.

Se após o loop não taxar erro indica que as conexões do elemento até o DIO estão OK, portanto deve realizar o mesmo teste para o segundo elemento.



Teste de loop das conexões entre os elementos.

LOF (Loss of Frame) / LOA (Loss of Alignment) / LOD (Loss of Data) / LOM (Loss of Multiframe) / LOP (Loss of Pointer) / PLM (Payload Label Mismatch) / SSF (Server Signal Fail) / Loss of Synchronization / Signal Failure

Todos estes alarmes indicam falha no sinal recebido, portanto há potência de RX na interface, porém o receptor não consegue reconhecer parte ou toda a informação recebida.

As principais causas deste alarme são:

- Falha de hardware no receptor ou no transmissor.
- Falha de conexão, cordão ou fibra danificados.

- Potência de RX baixa ou alta.
- Taxa de erro.

Esta falha pode ocorrer entre:

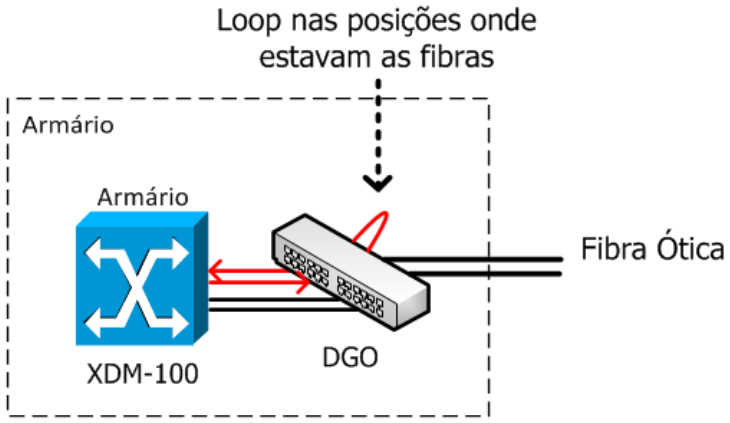
- Elementos de um anel.
- Elementos dentro da Estação Switch.

Deve ser analisado se há alarmes de falha de hardware ou algum outro alarme no enlace que indique a causa do alarme, verificar como estão as potências de RX das interfaces, se os níveis de RX estiverem muito alto ou muito baixo devem ser corrigidos e por último se for constatado que há degradação ou taxas de erro nas interfaces deve ser eliminada.

Se após a análise não for identificado o problema deve ser acionado um técnico de campo para a realização de testes no local, deverá levar cordões novos e as placas do modelo utilizado.

- Para falha entre elementos de um anel:

1° Passo: Com o técnico no primeiro elemento realizar testes de loop no DGO, com um cordão deve ser fechado loop nas duas posições onde entram as fibras, conforme a imagem abaixo:

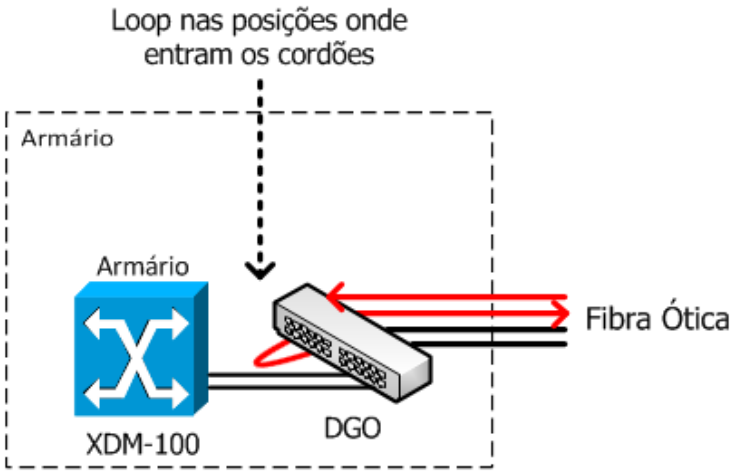


Teste de loop.

Se o alarme normalizar, indica que não a falha para o trecho testado, ir para o 2° passo.

Se o alarme continuar deverá ser fechado loop direto na interface do SDH, se após o loop o alarme continuar deverá ser substituído a SFP, caso não haja alarme após o loop devem ser substituídos os cordões.

2° Passo: Fechar loop nas duas posições onde entram os cordões conforme a imagem abaixo, testando assim as conexões do outro elemento e as fibras, verificar a interface do segundo elemento.



Teste de loop.

Se o alarme persistir o técnico deverá ir até o local do segundo elemento e realizar o mesmo teste. Com o loop fechado no DGO sentido para o primeiro elemento, se o alarme permanecer deve ser acionado o supervisor de rede externa para verificação das fibras. Caso não incremente taxa de erro no primeiro elemento devem ser realizados os testes do 1° passo para o segundo elemento.

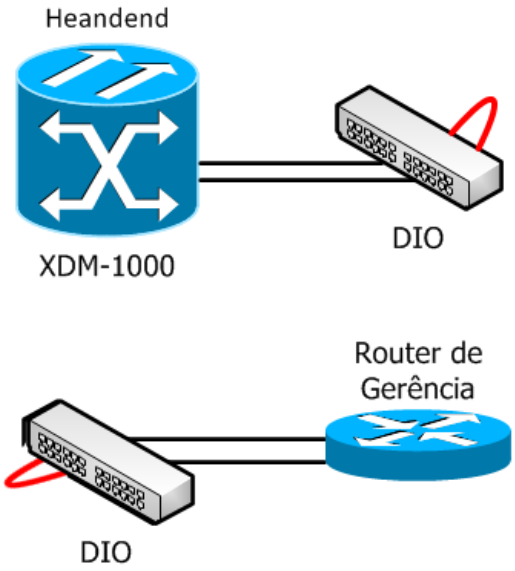
- Para falha entre elementos dentro da Estação Switch.

1° Passo: Solicitar ao técnico que verifique a conexão no primeiro elemento, se não houver problema fechar loop físico direto na interface do elemento, se o alarme normalizar indica que a interface esta OK. Caso o alarme permaneça após o loop deverá ser substituída a SFP.

Realizar o mesmo procedimento para o segundo elemento.

2° Passo: Deve-se realizar testes de loop no DIO, com um cordão de teste deve ser fechado loop nas duas posições onde entram os cordões vindo do segundo elemento testando assim as conexões do primeiro elemento, conforme a imagem abaixo, verificar a interface do elemento, se continuar alarmado deve ser substituído os cordões entre o DIO e o elemento.

Se após o loop o alarme normalizar indica que as conexões do elemento até o DIO estão OK, portanto deve realizar o mesmo teste para o segundo elemento.



Teste de loop das conexões entre os elementos.

RAI (Remote Alarm Indication) / RDI (Remote Defect Indication)

Estes alarmes indicam falha na ponta remota, sempre que estes alarmes ocorrerem haverá outro alarme na ponta oposta como, por exemplo, LOS, LOF, DEG, entre outros. Portanto se a falha da ponta remota for corrigida automaticamente o alarme de RAI ou RDI será normalizado.

TIM (Trace Identifier Mismatch)

Este alarme indica que o label identificador recebido é diferente do esperado, portanto deve-se verificar se os labels estão configurados corretamente conforme o procedimento para verificação de configurações de interfaces. Normalmente o label identificador contêm o nome do equipamento, slot e interface emissora, por exemplo, o label Armário01 I01-1. Se após a verificação das configurações for identificado que o label transmitido esta descrito de forma incorreta deve ser corrido, da mesma forma o label esperado deve estar exatamente igual ao label enviado pela ponta remota.

Este alarme pode indicar uma inversão de conexões entre equipamentos, desta forma deve ser verificado se o label enviado pelo equipamento esta chegando ao equipamento correto. Se for identificado que o label recebido é de outro equipamento devem ser verificadas as conexões entre estes equipamentos e corrigidas.

TRATAMENTO DE FALHAS DE EQUIPAMENTOS

Card Failure / Unit Problem / Card Out / Unit missing / Unit Problem / Replacement Unit Missing / Transceiver Response Fail

Estes alarmes indicam falha na placa ou ausência da mesma no slot alarmado. Primeiro deve-se verificar se não há outros alarmes que indiquem falha de hardware do equipamento, que pode indicar uma possível falha de energia ou de temperatura, neste caso solicitar verificação pela equipe CGR-Infra que verificará o estado da fonte e temperatura do ambiente. Caso não seja identificada nenhuma anormalidade no equipamento realizar os passos a seguir:

1° Passo: Realizar reset lógico* da placa alarmada, aguardar por alguns minutos, se o estado da placa permanecer o mesmo deverá ser acionado um técnico de campo para a realização de testes no local levando uma placa do modelo utilizado no equipamento.

*Observação: Há dois tipos de reset lógico, o *warm reset* e o *cold reset*. O warm reset apenas reiniciar os processos da placa sem desliga-la, o cold reset força a reinicialização do hardware desligando a sua alimentação e religando após alguns segundos, portanto o cold reset é mais eficaz.

2°Passo: Com o técnico no local certificar-se de que o mesmo esteja utilizando as devidas precauções para evitar danos ao hardware como pulseira anti-estática devidamente aterrada ao shelf do equipamento. Solicitar que seja realizado reset físico da placa, retirando-a do seu slot e recolocando após cerca de 1 minuto, após a inserção da placa, aguardar por alguns minutos. Caso o alarme permaneça seguir o próximo passo.

3° Passo: Realizar a substituição da placa. Aguardar por alguns minutos até que o processo de inserção do novo hardware seja finalizado. Alguns equipamentos podem levar até 30 minutos para finalizar o processo de inserção de um novo hardware, neste caso consultar o manual do fabricante. Caso o alarme permaneça, substituir novamente a unidade por outra nova para certificar-se de que a nova placa não esteja com defeito. Se mesmo assim o alarme permanecer pode haver uma falha no shelf do equipamento, portanto realizar o próximo passo.

4° Passo: Realizar a substituição do shelf do equipamento. Se mesmo após todos os procedimentos o alarme permanecer deverá ser acionado o Suporte Especializado.

Type Mismatch / Mismatch Equipment

Este alarme indica incompatibilidade da placa inserida no slot com o modelo configurado no equipamento, ou o equipamento não esta conseguindo reconhecer a unidade.

Primeiro deve-se verificar se o modelo da placa inserida no slot é diferente do que está configurado no equipamento, caso seja diferente a placa deve ser substituída pelo modelo padrão.

Caso o equipamento não esteja identificando o modelo da placa deverá ser verificado se não há outros alarmes que indiquem falha de hardware do equipamento, que pode indicar uma possível falha de energia ou de temperatura, neste caso solicitar verificação pela equipe CGR-Infra. Caso não seja identificada nenhuma anormalidade no equipamento realizar os passos a seguir:

1° Passo: Realizar reset lógico da placa alarmada, aguardar por alguns minutos, se o estado da placa permanecer o mesmo deverá ser acionado um técnico de campo para a realização de testes no local levando uma placa do modelo utilizado no equipamento.

2°Passo: Com o técnico no local certificar-se de que o mesmo esteja utilizando as devidas precauções para evitar danos ao hardware como pulseira anti-estática devidamente aterrada ao shelf do equipamento. Solicitar que seja realizado reset físico da placa, retirando-a do seu slot e recolocando após cerca de 1 minuto, após a inserção da placa, aguardar por alguns minutos. Caso o alarme permaneça seguir o próximo passo.

3° Passo: Realizar a substituição da placa. Aguardar por alguns minutos até que o processo de inserção do novo hardware seja finalizado. Caso o alarme permaneça, substituir novamente a unidade por outra nova para certificar-se de que a nova placa não esteja com defeito. Se mesmo assim o alarme permanecer pode haver uma falha no shelf do equipamento, portanto realizar o próximo passo.

4° Passo: Realizar a substituição do shelf do equipamento. Se mesmo após todos os procedimentos o alarme permanecer deverá ser acionado o Suporte Especializado.

Program Fail

Este alarme indica que ou o software ou sistema não está funcionando corretamente na placa controladora. Primeiro deve-se verificar se não há outros alarmes que indiquem falha de hardware do equipamento, que pode indicar uma possível falha de

energia ou de temperatura, neste caso solicitar verificação pela equipe CGR-Infra que verificará o estado da fonte e temperatura do ambiente. Caso não seja identificada nenhuma anormalidade no equipamento realizar os passos a seguir:

1°Passo: Verificar se a placa alarmada esta como controladora principal do equipamento, caso esteja deverá ser comutado o controle do equipamento para a placa controladora backup. A comutação demora alguns minutos, se após finalizar o processo o alarme permanecer, seguir para o próximo passo.

2° Passo: Realizar reset lógico da placa alarmada, aguardar por alguns minutos, se o estado da placa permanecer o mesmo deverá ser acionado um técnico de campo para a realização de testes no local levando uma placa do modelo utilizado no equipamento e notebook para formatação do cartão de memória.

3°Passo: Com o técnico no local certificar-se de que o mesmo esteja utilizando as devidas precauções para evitar danos ao hardware como pulseira anti-estática devidamente aterrada ao shelf do equipamento. Solicitar que seja realizado reset físico da placa, retirando-a do seu slot e recolocando após cerca de 1 minuto, após a inserção da placa, aguardar por alguns minutos. Caso o alarme permaneça seguir para o próximo passo.

4°Passo: Retirar o cartão de memória e realizar a formatação do mesmo conforme o procedimento, depois de formatada colocar novamente na placa alarmada e aguardar o fim do processo. Se o alarme permanecer realizar o próximo passo.

5° Passo: Realizar novamente a formatação do cartão de memória e inserir uma nova placa controladora com o cartão de memória formatado. Aguardar por alguns minutos até que o processo de inserção do novo hardware seja finalizado. Caso o alarme permaneça, substituir novamente a unidade por outra nova para certificar-se de que a nova placa não esteja com defeito. Se mesmo após todos os procedimentos o alarme permanecer deverá ser acionado o Suporte Especializado.

BIT Degraded / BIT Failed

Os alarmes citados indica uma falha de equipamento que pode afetar a sua funcionalidade. Primeiramente deve-se anotar o BIT code apresentado pela placa alarmada para que seja enviado junto com a placa ao fabricante no caso de ela ser substituída.

Para placas controladoras deverão ser executado os mesmos passos citados no alarme de Program Fail, para o restante das placas executar os passos citados no alarme de Card Failure.

High Temperature / Low Temperature

Primeiro deve-se verificar se não há outros alarmes que indiquem falha de hardware do equipamento, que pode indicar uma possível falha de energia ou de temperatura, neste caso solicitar verificação pela equipe CGR-Infra que verificará o estado da fonte e temperatura do ambiente. Caso não seja identificada nenhuma anormalidade no equipamento deverá ser acionado um técnico de campo para verificação no local.

1° Passo: Com o técnico no local solicitar que verifique a temperatura do ambiente, caso seja constatado que a temperatura esta muito elevada envolver a equipe do CGR-Infra para tomar as devidas providencias. Caso a temperatura do ambiente esteja normal seguir para o próximo passo.

2°: Solicitar verificação do funcionamento das FANs do equipamento, caso seja identificada qualquer anormalidade em seu funcionamento as FANs devem ser substituídas, caso não haja problema seguir para o passo seguinte.

3° Passo: Retirar a placa alarmada, deixando-a fora do equipamento por alguns minutos. Recoloca-la novamente e monitorar o equipamento por alguns minutos. Caso permaneça alarmado executar o próximo passo.

4°Passo: Realizar a substituição da placa. Se o alarme permanecer deverá ser acionado o suporte especializado.

TRATAMENTO DE FALHA DE GERÊNCIA

NE Disconnected / NE Unavailable / NE Fault / NE Communication Fault / Gateway NE Communication Fault

Este alarme indica perda de comunicação do elemento de rede com o servidor de gerência.

Possíveis causas desta falha:

- Falha de comunicação do elemento com a rede de gerência, podendo ser causado por falha na rede de gerência, falha de configuração, falha de transmissão ou falha no equipamento.

- Queda do elemento de rede, podendo ser causado por falha de energia, falha de transmissão, falha de configuração ou falha no equipamento.

Primeiro deve-se verificar se o elemento esta apenas sem gerência ou se houve queda do elemento de rede. Verificar com a equipe CGR-Acesso se os serviços de dados e voz do armário estão funcionando, se estiverem funcionando normalmente indica que o elemento esta apenas com falha de gerência, caso os serviços de dados e voz do armário estejam totalmente sem funcionar indica que o equipamento “caiu”, ou seja, não esta operando corretamente e desta forma esta afetando os serviços dos clientes.

- Falha de comunicação do elemento com a rede de gerência

1° Passo: Verificar se os elementos do mesmo anel estão gerenciáveis, se estiverem ir para o próximo passo. Se os elementos do anel também não estiverem gerenciáveis deve verificar o elemento gateway destes elementos, o gateway realiza a interface entre os equipamentos e a rede de gerência, sendo assim ele está diretamente conectado a um switch ou router de gerência. Se o gateway não estiver gerenciável solicitar verificação pela equipe CGR-Dados do equipamento que está conectado ao gateway e da rede de gerência. Caso não seja identificada falha de Infraestrutura seguir para o próximo passo.

2° Passo: Verificar os alarmes do elemento afetado, mesmo com o elemento sem gerência os últimos alarmes antes da queda ficam presente no sistema de gerência até que seja restabelecida a comunicação do elemento para sincronização dos alarmes. Verificar se há alarmes que justifiquem falha de transmissão nos elementos vizinhos e no restante do anel. Se for constatado qualquer alarme de transmissão no anel que justifique a falha de transmissão do elemento deverá ser corrigido.

3° Passo: Acionar um técnico de campo para a verificação no local, o mesmo deverá levar notebook com os softwares necessários instalados para acesso local ao equipamento, levar cordões novos e placas controladora e de comunicação ótica dos modelos utilizados no elemento.

4° Passo: Com o técnico no local solicitar que acesse o equipamento, se conseguir acessa-lo deve verificar quais os alarmes ativos, corrigir todos os alarmes que justifiquem a falha de transmissão. Verificar as configurações de gerência do equipamento, se constatado qualquer divergência nas configurações devem ser corrigidas. Se não conseguir acessa-lo deve verificar se o notebook e o cabo

utilizado estão funcionando corretamente, se ambos estiverem OK pode ser um indício de que o equipamento esta travado, porém sem serviços afetados.

5° Passo: Verificar se as interfaces óticas utilizadas para comunicação com os elementos vizinhos estão alarmadas fisicamente e medir a RX de cada uma. Realizar os testes utilizados nos alarmes de LOS.

6° Passo: Verificar se as placas controladora e de comunicação ótica estão com o LED de FAIL acesso, se houver alguma placa alarmada deve ser substituída. Se mesmo assim o equipamento continuar sem gerência e sem acesso local seguir para o próximo passo.

7° Passo: Realizar reset físico do equipamento em janela de manutenção (durante a madrugada), pois neste caso haverá afetação dos serviços dos clientes. Após o reset aguardar por alguns minutos e verificar se o equipamento volta à gerência. Caso o equipamento continue sem gerência o técnico deve tentar acessa-lo novamente. Se não conseguir acessa-lo deverá ser acionado o suporte especializado.

Após o restabelecimento da gerência do elemento todas as configurações de gerência do equipamento devem ser revisadas.

- Queda do elemento de rede

1° Passo: Verificar com a equipe CGR-Infra se há alguma falha de energia ou de temperatura para o elemento. Se houver falha de energia o equipamento estará desligado, portanto haverá alarmes de LOS nos equipamentos vizinhos. Caso não seja identificada falha de Infraestrutura seguir para o próximo passo.

2° Passo: Verificar os alarmes do elemento afetado. Verificar se há alarmes que justifiquem falha de transmissão nos elementos vizinhos e no restante do anel. Verificar com a equipe CGR-Acesso se os serviços de dados e voz de todos os elementos do anel estão OK. Se for constatado qualquer alarme de transmissão no anel que justifique a falha de transmissão do elemento deverá ser corrigido.

3° Passo: Acionar um técnico de campo para a verificação no local, o mesmo deverá levar notebook com os softwares necessários instalados para acesso local ao equipamento, levar cordões novos e placas controladora e de comunicação ótica dos modelos utilizados no elemento.

4° Passo: Com o técnico no local solicitar que acesse o equipamento, se conseguir acessa-lo deve verificar quais os alarmes ativos, corrigir todos os alarmes que

justifiquem a falha de transmissão. Verificar as configurações de gerência do equipamento, se constatado qualquer divergência nas configurações devem ser corrigidas. Se não conseguir acessa-lo deve verificar se o notebook e o cabo utilizado estão funcionando corretamente, se ambos estiverem OK pode ser um indício de que o equipamento esta travado.

5° Passo: Verificar se as interfaces óticas utilizadas para comunicação com os elementos vizinhos estão alarmadas fisicamente e medir a RX de cada uma. Realizar os testes utilizados nos alarmes de LOS.

6° Passo: Verificar se as placas controladora e de comunicação ótica estão com o LED de FAIL acesso, se houver alguma placa alarmada deve ser substituída. Se mesmo assim o equipamento continuar sem gerência e sem acesso local seguir para o próximo passo.

7° Passo: Realizar reset físico do equipamento. Após o reset aguardar por alguns minutos e verificar se o equipamento volta à gerência. Caso o equipamento continue sem gerência o técnico deve tentar acessa-lo novamente. Se não conseguir acessa-lo deverá ser acionado o suporte especializado.

Após o restabelecimento da gerência do elemento todas as configurações de gerência do equipamento devem ser revisadas.

TRATAMENTO DE FALHAS DE TEMPORIZAÇÃO E SINCRONISMO

Primary Timing Source Not Active / Loss of Time Input / Timing Generator Holdover / Holdover Synchronization

Estes alarmes indicam falha na fonte de sincronismo do equipamento. Normalmente o sincronismo é gerado por um GPS, neste caso o GPS esta conectado diretamente a um equipamento de transmissão, e este equipamento fornecera o sincronismo para toda a rede. Se houver alarme neste equipamento deve ser verificada a conexão com o GPS e o funcionamento do mesmo. Quando a fonte de sincronismo é vem da rede na grande maioria das vezes a causa da falha de sincronismo é devido a uma falha na transmissão, portanto a falha na transmissão deve ser corrigida.

TRATAMENTO DE FALHAS DE SERVIÇOS

UNEQ (Unequipped)

Este alarme indica que o circuito esta desconfigurada, pode ser causado por uma desconexão.

Primeiro deve-se verificar as configurações do circuito, se for encontrada alguma anormalidade deve ser corrigida, caso não encontre nenhuma falha o circuito deve ser deletado e recriado.

Service Degraded

Este alarme indica degradação no sinal do circuito em tráfego. Na maioria dos casos, esta falha ocorre devido a degradação no meio de transmissão, portanto deve ser verificado se não há alarme de transmissão, principalmente DEG e EXC. Qualquer alarme encontrado deve ser corrigido.

Service Failed

Este alarme indica que ambos os caminhos principal e proteção não estão transmitindo o tráfego do circuito. Na maioria dos casos, esta falha ocorre devido a falha dupla afetando tanto o caminho principal quanto a proteção. Primeiro deve-se verificar se o circuito possui outros alarmes como de falhas de transmissão e equipamento, se houver alarmes devem ser corrigidos. Se não houver alarmes o circuito deve ser deletado e recriado.

Indisponibilidade de serviços

- Indisponibilidade de serviços para um DSLAM
- Todos os serviços (Voz, Dados e gerência do DSLAM)

Primeiro deve-se verificar se todos os serviços dos outros DSLAMs do armário também estão sendo impactados, se confirmado que somente um dos DSLAMs esteja com todos os serviços indisponíveis solicitar verificação do DSLAM pela equipe de Acesso, se a equipe de Acesso não identificar nenhuma falha devem ser realizados os passos a seguir:

1° Passo: Identificar as interfaces utilizadas pelo DSLAM com o auxilio da equipe de Acesso, verificar se possuem alarmes e se há comunicação entre o equipamento de transmissão e o DSLAM verificando os contadores das interfaces, se houver alarmes nas interfaces devem ser corrigidos. Na maioria dos casos em que apenas um DSLAM apresenta indisponibilidade a principal causa é de falha de comunicação

com o equipamento de transmissão, se não houver falha no DSLAM. Se não houver alarmes ir para o próximo passo.
2° Passo: Listar os serviços do DSLAM e verificar se possuem alarmes que justifiquem a falha dos serviços. Se não houver alarmes ir para o próximo passo.
3° Passo: Verificar se as configurações dos serviços listados. Utilizar o procedimento de verificação de configurações de serviços, se constatado qualquer anormalidade deve ser corrigido.
4° Passo: Se após todas as verificações não for identificado falha nas interfaces e nos serviços de transmissão solicitar para que a equipe de Acesso verifique junto ao seu suporte especializado.

- Somente serviço de Voz por V5

Primeiro deve-se verificar se todos os serviços dos outros DSLAMs do armário também estão sendo impactados, se confirmado que somente um dos DSLAMs esteja com serviço de Voz por V5 indisponível solicitar verificação do DSLAM pela equipe de Acesso, se a equipe de Acesso não identificar nenhuma falha devem ser realizados os passos a seguir:
1° Passo: Identificar os tributários utilizados pelo DSLAM com o auxilio da equipe de Acesso.
2° Passo: Listar os serviços do DSLAM e verificar se possuem alarmes nos tributários. Se houver alarmes nos tributários informar à equipe de Acesso para que seja corrigido. Se não houver alarmes nas portas ir para o próximo passo.
3° Passo: Verificar se há alarmes nos serviços, se for identificado qualquer alarme que justifique a falha deve se corrigido.
4° Passo: Verificar as configurações dos serviços listados. Utilizar o procedimento de verificação de configurações de serviços, se constatado qualquer anormalidade deve ser corrigido.
5° Passo: Realizar testes de loop utilizando o procedimento de testes de circuitos com loopback. Primeiro fechar loop do SDH do armário para o DSLAM, se alinhar no DSLAM não há falha no mesmo, caso contrário a falha deve ser verificada pela equipe de Acesso. Segundo fechar loop do headend para a central de comutação, se alinhar na central não há falha na estação switch, caso contrário a falha deve ser verificada pela equipe de Acesso em conjunto com a equipe de Comutação. Terceiro realizar loop do headend para o DSLAM e do armário para a central de comutação,

se alinhar não haverá falha de transmissão, caso contrário o meio de transmissão deve ser verificado.
5° Passo: Se após os testes de loop for constatado que a falha é na transmissão, porém não tenha sido identificados alarmes para os serviços deve-se anotar todos os dados dos circuitos utilizados e então deletar e recriar os circuitos.
6° Passo: Se após todas as verificações e após deletar e recriar os circuitos a falha permanecer o suporte especializado deve ser acionado.

- Serviço de Voz por H248 ou Dados ou Gerência do DSLAM

Primeiro deve-se verificar se todos os serviços dos outros DSLAMs do armário também estão sendo impactados, se confirmado que somente um dos DSLAMs esteja com o serviço indisponível solicitar verificação do DSLAM pela equipe de Acesso, se a equipe de Acesso não identificar nenhuma falha devem ser realizados os passos a seguir:
1° Passo: Identificar as interfaces utilizadas pelo DSLAM com o auxilio da equipe de Acesso, verificar se possuem alarmes e se há comunicação entre o equipamento de transmissão e o DSLAM verificando os contadores das interfaces, se houver alarmes nas interfaces devem ser corrigidos. Na maioria dos casos em que apenas um DSLAM apresenta indisponibilidade a principal causa é de falha de comunicação com o equipamento de transmissão, se não houver falha no DSLAM. Se não houver alarmes ir para o próximo passo.
2° Passo: Listar o serviço do DSLAM e verificar se possuem alarmes que justifiquem a falha dos serviços. Se não houver alarmes ir para o próximo passo.
3° Passo: Verificar se as configurações do serviço listado. Utilizar o procedimento de verificação de configurações de serviços, se constatado qualquer anormalidade deve ser corrigido.
4° Passo: Se após todas as verificações não for identificado falha nas interfaces e nos serviços de transmissão solicitar para que a equipe de Acesso verifique junto ao seu suporte especializado.

- Indisponibilidade de serviços para todos os DSLAMs de um armário
  - Todos os serviços (Voz, Dados e gerência dos DSLAMs)

Primeiro deve-se verificar se todos os serviços dos outros armários do mesmo anel estão sendo impactados, se for confirmado que somente os serviços de um armário

estejam indisponíveis solicitar verificação pela equipe CGR-Infra sobre uma possível falha de energia ou de temperatura, nos casos de falha de energia o equipamento de transmissão é o ultimo a cair, pois é alimentado pelo banco de baterias. Caso não seja identificada nenhuma anormalidade realizar os passos a seguir:

1° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o armário, pois são as a principais causas de indisponibilidade, se não houver falha de energia. Se houver qualquer alarme que justifique a falha deve ser corrigido.

2° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para todos os elementos do anel até chegar ao headend. Caso não haja falha ir para o próximo passo.

3° Passo: Listar todos os serviços do armário e verificar se possuem algum alarme, sem possuir devem ser corrigido.

4° Passo: Verificar as interfaces do armário que estão conectadas aos DSLAMs e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e os DSLAMs verificando os contadores das interfaces, se houver alarmes nas interfaces devem ser corrigidos. Se não for identificado problema ir para o próximo passo.

5° Passo: Identificar as interfaces do headend onde fecham serviços do armário e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e os equipamentos de Dados e de Comutação (se o armário possuir V5), se houver alarmes nas interfaces devem ser corrigidos, neste caso verificar em conjunto com a equipe de Dados e Comutação.

6° Passo: Se não for constatado falha deve-se acionar um técnico para verificação no armário. Verificar alimentação dos equipamentos e temperatura ambiente. Se estiver normal solicitar que realize testes de chamada e de navegação no armário.

7° Passo: Se após os todas as verificações não for identificado a causa raiz o suporte especializado deve ser acionado.

- Somente serviço de Voz por V5

Primeiro deve-se verificar se todos os serviços dos outros armários do mesmo anel estão sendo impactados, se for confirmado que somente os serviços de Voz por V5 de um armário estejam indisponíveis, realizar os passos a seguir:

1° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o armário, pois são as a principais causas de indisponibilidade, se não houver falha de energia. Se houver qualquer alarme que justifique a falha deve ser corrigido.
2° Passo: Listar os serviços armário e verificar se possuem alarmes. Se houver alarmes nos tributários informar à equipe de Acesso para que seja corrigido. Se não houver alarmes nas portas ir para o próximo passo.
3° Passo: Verificar se há alarmes nos serviços, se for identificado qualquer alarme que justifique a falha deve se corrigido.
4° Passo: Verificar as configurações dos serviços listados. Utilizar o procedimento de verificação de configurações de serviços, se constatado qualquer anormalidade deve ser corrigido.
5° Passo: Realizar reset da placa de Voz do armário, se a falha persistir ir para o próximo passo.
6° Passo: Realizar testes de loop utilizando o procedimento de testes de circuitos com loopback. Primeiro fechar loop do SDH do armário para o DSLAM, se alinhar no DSLAM não há falha no mesmo, caso contrário a falha deve ser verificada pela equipe de Acesso. Segundo fechar loop do headend para a central de comutação, se alinhar na central não há falha na estação switch, caso contrário a falha deve ser verificada pela equipe de Acesso em conjunto com a equipe de Comutação. Terceiro realizar loop do headend para o DSLAM e do armário para a central de comutação, se alinhar não haverá falha de transmissão, caso contrário o meio de transmissão deve ser verificado.
7° Passo: Se após os testes de loop for constatado que a falha é na transmissão, porém não tenha sido identificados alarmes para os serviços deve-se anotar todos os dados dos circuitos utilizados e então deletar e recriar os circuitos.
8° Passo: Se após todas as verificações e após deletar e recriar os circuitos a falha permanecer o suporte especializado deve ser acionado.

- Serviço de Voz por H248 ou Dados ou Gerência do DSLAM

Primeiro deve-se verificar se todos os serviços dos outros armários do mesmo anel estão sendo impactados, se for confirmado que somente os serviços de um armário estejam indisponíveis, realizar os passos a seguir:

1° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o armário, pois são as a principais causas de indisponibilidade, se não houver falha de energia. Se houver qualquer alarme que justifique a falha deve ser corrigido.
2° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para todos os elementos do anel até chegar ao headend. Caso não haja falha ir para o próximo passo.
3° Passo: Listar todos os serviços do armário e verificar se possuem algum alarme, sem possuir devem ser corrigido.
4° Passo: Verificar as interfaces do armário que estão conectadas aos DSLAMs e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e os DSLAMs verificando os contadores das interfaces, se houver alarmes nas interfaces devem ser corrigidos. Se não for identificado problema ir para o próximo passo.
5° Passo: Identificar as interfaces do headend onde fecham serviços do armário e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e o equipamento de Dados, se houver alarmes nas interfaces devem ser corrigidos, neste caso verificar em conjunto com a equipe de Dados.
6° Passo: Se não for constatado falha deve-se acionar um técnico para verificação no armário. Verificar alimentação dos equipamentos e temperatura ambiente. Se estiver normal solicitar que realize testes de chamada e de navegação no armário.
7° Passo: Se após os todas as verificações não for identificado a causa raiz o suporte especializado deve ser acionado.

- Indisponibilidade de serviços para mais de um armário
- Todos os serviços (Voz, Dados e gerência dos DSLAMs)

Primeiro deve-se verificar a relação entre os armários afetados, se são do mesmo anel e se o seus serviços fecham nas mesmas interfaces do headend. As principais causas de falhas de serviços para vários armários são falha de energia para uma grande região, falha no headend ou nos equipamentos de Dados ou Comutação ou se for um anel possivelmente poderá ser falha dupla de equipamento e ou de transmissão. Solicitar verificação pela equipe CGR-Infra sobre uma possível falha de energia para os armários afetados. Caso não seja identificada nenhuma anormalidade realizar os passos a seguir:

1° Passo: Solicitar verificação pelas equipes de Dados e Comutação.
2° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para os armários afetados. Se houver qualquer alarme que justifique a falha deve ser corrigido. Se não houver siga para o próximo passo.
3° Passo: Verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o headend. Caso não haja falha ir para o próximo passo.
4° Passo: Identificar as interfaces do headend onde fecham serviços do armário e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e os equipamentos de Dados e de Comutação (se o armário possuir V5), se houver alarmes nas interfaces devem ser corrigidos, neste caso verificar em conjunto com a equipe de Dados e Comutação.
5° Passo: Se após os todas as verificações não for identificado a causa raiz o suporte especializado deve ser acionado.

- Somente serviço de Voz por V5

Primeiro deve-se verificar a relação entre os armários afetados, se são do mesmo anel e se o seus serviços fecham nas mesmas interfaces do headend. Solicitar verificação pela equipe CGR-Infra sobre uma possível falha de energia para os armários afetados. Caso não seja identificada nenhuma anormalidade realizar os passos a seguir:
1° Passo: Solicitar verificação pela equipe de Comutação.
2° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para os armários afetados. Se houver qualquer alarme que justifique a falha deve ser corrigido. Se não houver siga para o próximo passo.
3° Passo: Verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o headend. Caso não haja falha ir para o próximo passo.
4° Passo: Identificar as interfaces do headend onde fecham serviços do armário e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e o equipamento de Comutação, se houver alarmes nas interfaces devem ser corrigidos, neste caso verificar em conjunto com a equipe de Comutação.
5° Passo: Se após os todas as verificações não for identificado a causa raiz o suporte especializado deve ser acionado.

- Serviço de Voz por H248 ou Dados ou Gerência do DSLAM

Primeiro deve-se verificar a relação entre os armários afetados, se são do mesmo anel e se o seus serviços fecham nas mesmas interfaces do headend. As principais causas de falhas de serviços para vários armários são falha de energia para uma grande região, falha no headend ou nos equipamentos de Dados ou se for um anel possivelmente poderá ser falha dupla de equipamento e ou de transmissão. Solicitar verificação pela equipe CGR-Infra sobre uma possível falha de energia para os armários afetados. Caso não seja identificada nenhuma anormalidade realizar os passos a seguir:

1° Passo: Solicitar verificação pela equipe de Dados.

2° Passo: Deve-se verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para os armários afetados. Se houver qualquer alarme que justifique a falha deve ser corrigido. Se não houver siga para o próximo passo.

3° Passo: Verificar se não há alarmes que indiquem falha de equipamento ou de transmissão para o headend. Caso não haja falha ir para o próximo passo.

4° Passo: Identificar as interfaces do headend onde fecham serviços do armário e verificar se possuem algum alarme e se há comunicação entre o equipamento de transmissão e o equipamento de Dados, se houver alarmes nas interfaces devem ser corrigidos, neste caso verificar em conjunto com a equipe de Dados.

5° Passo: Se após os todas as verificações não for identificado a causa raiz o suporte especializado deve ser acionado.