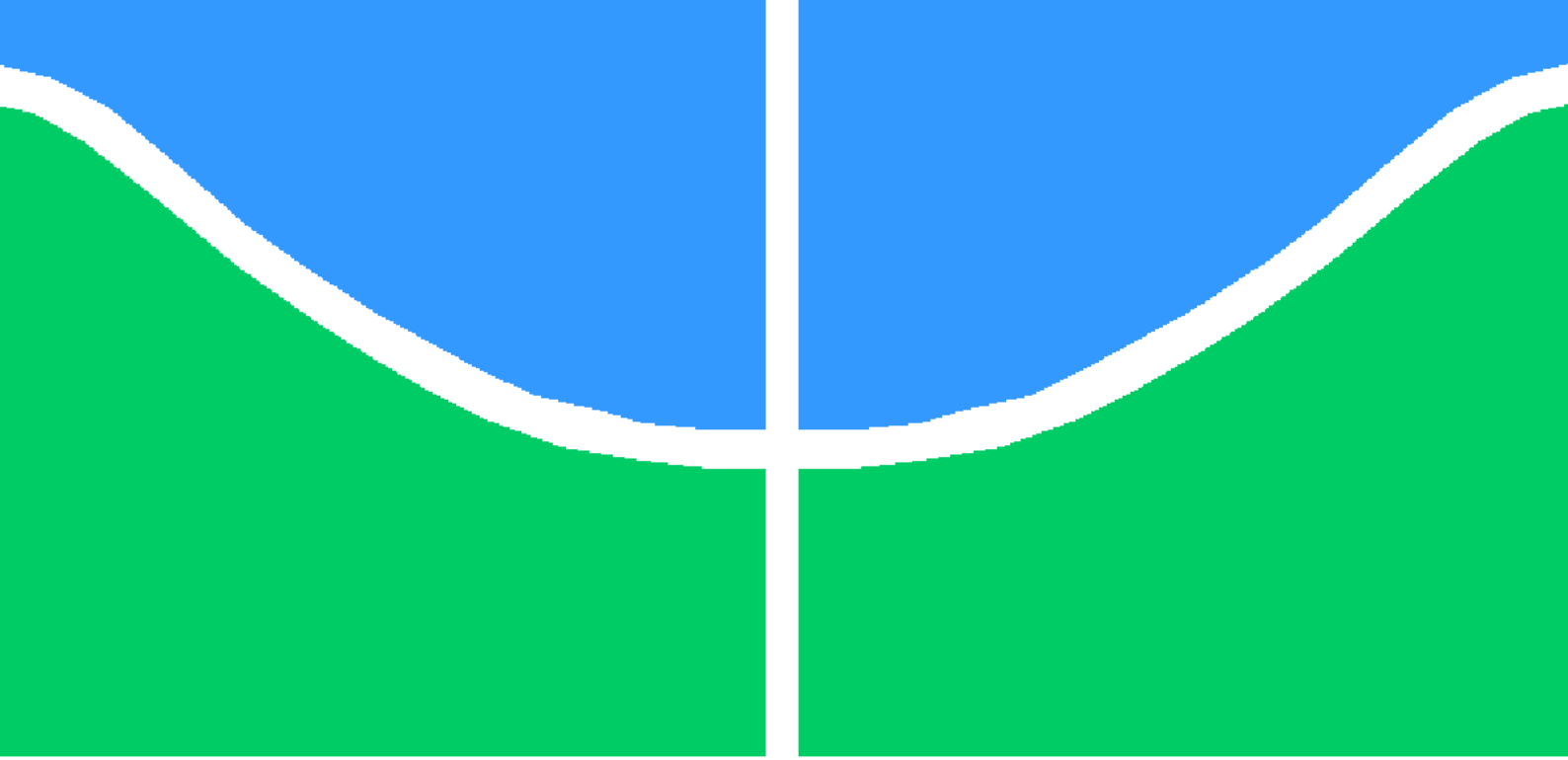


TRABALHO DE GRADUAÇÃO

Elaboração de experimentos de redes SONET/SDH utilizando a infra-estrutura do laboratório Optix.

Leonardo Serra

Brasília, dezembro de 2009

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

Elaboração de experimentos de redes SONET/SDH utilizando a infra-estrutura do laboratório Optix.

Leonardo Serra

Relatório submetido ao Departamento de Engenharia Elétrica
como requisito parcial para obtenção do grau de
Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Dr. William Ferreira Giozza, _____
ENE/UnB
(Orientador)

Prof. Dr. Darli Agusto de Arruda Mello, _____
ENE/UnB
(Membro Interno)

FICHA CATALOGRÁFICA

SERRA, L. Elaboração de experimentos de redes SONET/SDH utilizando a infra-estrutura do laboratório Optix. [Distrito Federal] 2009.
v, 74p. (ENE/FT/UnB, Engenheiro de Redes de Comunicação, 2009)
Monografia de Graduação - Universidade de Brasília. Faculdade de Tecnologia. Departamento de Engenharia Elétrica.
1. Redes Ópticas 2. SONET/SDH
3. Redes de alta velocidade 4. Experimentos
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SERRA, L. (2009). Elaboração de experimentos de redes SONET/SDH utilizando a infra-estrutura do laboratório Optix. Monografia de Graduação, Publicação ENE 01/2010, Departamento de Engenharia
Elétrica, Universidade de Brasília, Brasília, DF, 74p.

CESSÃO DE DIREITOS

NOMES DOS AUTORES: Leonardo Serra

TÍTULO: Elaboração de experimentos de redes SONET/SDH utilizando a infra-estrutura do laboratório Optix.

GRAU / ANO: Engenheiro de Redes de Comunicação / 2009.

_____

Leonardo Serra

Dedicatória

Dedico este trabalho aos meus pais Stefano Maria Serra e Naiza Coelho Serra, aos meus avós Domenico Serra e Silvana Serra e à minha irmã Carolina Coelho Serra que me deram todo o suporte e motivação para concluir com sucesso minha graduação.

Leonardo Serra

Agradecimentos

Agradeço meu professor e orientador William Giozza e todos os meus colegas de Engenharia de Redes de Comunicação.

Leonardo Serra

RESUMO

Graças ao constante avanço das tecnologias de telecomunicações, quantidades maciças de informações percorrem distâncias intercontinentais em frações de segundo, possibilitando o desenvolvimento de aplicações que fazem uso dos recursos oferecidos por essas redes de alta velocidade.

As redes de transporte de alta velocidade exercem um papel fundamental no transporte desse enorme volume de informações geradas globalmente. Desde redes metropolitanas até redes transoceânicas, a tecnologia de transporte de alta velocidade SONET/SDH mostra-se uma escolha segura e eficiente. A rede SONET/SDH foi originalmente desenvolvida para o transporte de tributários PDH (*Plesyochronous Digital Hierarchy)*, mas o desenvolvimento de recentes mecanismos de adaptação ao transporte eficiente de dados (pacotes) consolidou sua presença na maior parte das redes WAN (*Wide Area Networks*) e MAN (*Metropolitan Area Networks*) de operadoras de telecomunicações. As redes SONET/SDH certamente representam uma parcela muito importante das diferentes opções de tecnologias de redes de transporte de alta velocidade disponíveis no mercado.

Este trabalho trata da elaboração e apresentação de três experimentos sobre redes SONET/SDH desenvolvidos para uma futura disciplina que fará uso de um laboratório de redes ópticas para o processo de aprendizado.

O primeiro experimento está relacionado ao sistema de gerência de redes SONET/SDH, que é responsável pelo monitoramento e configuração remota da rede. O segundo experimento trata dos fundamentos básicos das redes SONET/SDH e a aplicação prática do GFP (*Generic Frame Procedure*) no transporte eficiente de quadros Ethernet. O último experimento analisa a capacidade de recuperação automática de falhas em topologias lineares e em anel de redes SONET/SDH.

SUMÁRIO

LISTA DE FIGURAS E TABELAS

Anexo I

Anexo II

Anexo III

Siglas

ADM	*Add/drop multiplexer*
APS	*Automatic protection switching*
ATM	*Asynchronous transfer mode*
AU	*Administrative unit*
AUG	*Administrative unit group*
BER	*Bit error rate*
BIP	*Bit interleaved parity*
BLSR	*Bidirectional line switched ring*
BPSR	*Bidirectional path switched ring*
cHEC	*Core header error correction*
CRC	*Cyclic redundancy check*
DCS	*Digital cross-connects*
ESCON	*Enterprise systems connection*
FCS	*Frame check sequence*
FICON	*Fiber connectivity*
GFP	*Generic frame procedure*
GNE	*Gateway network equipment*
HDLC	*High level data link control*
ICMP	*Internet control message protocol*
IP	*Internet protocol*
ISDN	*Integrated services digital network*
LAN	*Local area network*
LOF	*Loss of frame*
LOS	*Loss of signal*
MAN	*Metropolitan area network*
MPLS	*Multi protocol label switching*
MSP	*Multiplex section protection*
MSOH	*Multiplex section overhead*
NNI	*Network-network interface*
OC	*Optical carrier*
OTN	*Optical transport network*
PDU	*Protocol data unit*
PDH	*Plesiochronous digital hierarchy*
PFI	*Payload FCS indicator*
PLI	*Payload length indicator*
POH	*Path overhead*
PRC	*Primary Reference Clock*
PPP	*Point to point protocol*
PTI	*Payload type identifier*
RSOH	*Regenerator section overhead*
RTT	*Round trip time*
SDH	*Synchronous digital hierarchy*
SONET	*Synchronous optical network*
SPE	*Synchronous payload envelope*
STM	*Synchronous transport module*
STS	*Synchronous transport signal*
TDM	*Time division multiplexing*
TM	*Terminal multiplexer*
TSI	*Time slot Interchanger*
TU	*Tributary unit*
TUG	*Tributary unit group*
TPS	*Tributary protection switching*

TSI	*Time slot interchanger*
UPI	*User payload identifier*
UPSR	*Unidirectional path switched ring*
VT	*Virtual tributary*
VTG	*Virtual tributary groups*
WAN	*Wide area network*
WDM	*Wavelength division multiplexing*
WTR	*Wait-to-Restore*

1 OBJETIVO GERAL

Recentemente, a Universidade de Brasília recebeu a doação de um laboratório de redes ópticas por parte da empresa chinesa de telecomunicações *Huawei*. Dentre os equipamentos fornecidos, estão equipamentos de rede SDH, WDM, sistema de gerência e diversos cordões ópticos e acessórios diversos (detalhes na seção 2.2).

O objetivo deste trabalho, baseado na infra-estrutura oferecida pelo laboratório, é a produção de três experimentos de laboratório que exploram o conceito das redes SONET/SDH e as suas características mais marcantes. A partir de uma fundamentação teórica específica para cada experimento, foi criado um modelo de experimento a ser executado em aulas experimentais de uma futura disciplina de redes ópticas.

Os experimentos estão ordenados de um a três e foram divididos em seis partes (com exceção do experimento nº1 que possui outra estrutura). A primeira parte descreve os objetivos do experimento. Em seguida é feita uma introdução teórica abrangendo os principais conceitos e tópicos envolvidos na execução do experimento. A terceira parte consiste na citação bibliográfica utilizada para a confecção da introdução teórica. A quarta parte descreve um pré-relatório a ser feito previamente à execução do experimento. Após a leitura da introdução teórica e o entendimento dos conceitos tratados no experimento, o aluno deve responder ao questionário presente no pré-relatório e entregá-lo no dia da execução do experimento. Após o pré-relatório, encontra-se a seção dos procedimentos, que descreve a maneira como a parte prática do experimento deve ser apropriadamente conduzida e executada. A lista de materiais utilizados no laboratório e o tempo estimado da duração do experimento também se encontram nesta seção. Por último, o aluno é convidado a fazer o relatório do experimento. O relatório deve conter uma descrição detalhada da execução do experimento, o relato de eventuais falhas ocorridas e deve conter explicações referentes à lista de pontos em destaque.

1.1 OBJETIVO ESPECÍFICO (EXPERIMENTO 1)

O primeiro experimento tem como objetivo a familiarização com o sistema de gerência fornecido pela empresa de telecomunicações *Huawei*. O sistema de gerência iManager T2000 é uma ferramenta responsável por monitorar os equipamentos e garantir o normal funcionamento da rede. Através dessa ferramenta é possível realizar diversas atividades como visualizar a topologia da rede, controlar alarmes em diversos níveis de importância, verificar informações precisas de um determinado equipamento, como a taxa de erro na interface óptica de entrada ou o nível de potência do laser na interface de saída, além de também controlar remotamente diversas funcionalidades dos equipamentos.

1.2 OBJETIVO ESPECÍFICO (EXPERIMENTO 2)

O segundo experimento tem como objetivo a análise do protocolo *Generic Frame Procedure* (GFP) na rede SDH do laboratório e a análise dos funcionamentos básicos da rede. Após a montagem e configuração de uma topologia em anel de três nós, a verificação da conectividade entre duas estações com placas de rede FastEthernet ligadas aos equipamentos SDH é feita com e sem o uso do GFP. O embasamento teórico foi feito de tal forma que cobrisse os princípios fundamentais das redes SONET/SDH como estrutura de quadros SONET/SDH, hierarquia SONET/SDH, tipos de equipamentos de rede encontrados neste tipo de rede e as principais funções e estruturas do GFP.

1.3 OBJETIVO ESPECÍFICO (EXPERIMENTO 3)

O terceiro experimento possui como objetivo a análise das principais formas de proteção e redundância em sistemas de transporte de alta velocidade SONET/SDH e a implementação e o teste prático da proteção em anel unidirecional com duas fibras e três nós. A introdução teórica apresenta os conceitos de falhas em fibras ópticas, comutação automática de proteção (*Automatic Protection Switching*- APS) linear, anéis SONET/SDH, APS em anel, os bytes K1 e K2 do cabeçalho de linha e exemplos de recuperação de falhas. São apresentados três exemplos de APS linear e um caso de APS na topologia em anel bidirecional com quatro fibras. A parte prática consiste na configuração da rede, na configuração da proteção APS e na verificação da recuperação da rede SDH em relação a uma falha provocada manualmente pelo sistema de gerência.

2 METODOLOGIA

2.1 FUNDAMENTAÇÃO TEÓRICA

O embasamento teórico foi elaborado separadamente e especificamente para cada experimento. A fundamentação teórica apresentada a seguir, cobre os pontos principais de interesse para a execução dos procedimentos de cada experimento.

2.1.1 SONET/SDH

Uma rede SONET/ SDH é um conjunto de equipamentos e meios físicos de transmissão que compõem um sistema digital síncrono de transporte de informações. Este sistema tem o objetivo de fornecer uma infra-estrutura básica para redes de dados e voz, e atualmente é utilizado em muitas empresas que prestam serviços de Telecomunicações, públicos e privados, em todo o mundo [1].

A tecnologia SONET/SDH baseia-se no uso da multiplexação TDM (*Time Division Multiplexing*) com altas taxas de bits, tendo a fibra óptica como meio físico preferencial de transmissão. Entretanto, possui ainda interfaces elétricas que permitem o uso de outros meios físicos de transmissão, tais como enlaces de rádios digitais e sistemas ópticos de visada direta, que utilizam feixes de luz infravermelha [1].

A elevada flexibilidade de uma rede SONET/SDH para transportar diferentes tipos de hierarquias digitais permite oferecer interfaces compatíveis com o padrão PDH europeu (nas taxas de 2 Mbps, 8 Mbps, 34 Mbps e 140 Mbps) e americano (nas taxas de 1,5 Mbps, 6 Mbps e 45 Mbps), além do próprio SONET/SDH (nas taxas de 155 Mbps, 622 Mbps, 2,5 Gbps, 10 Gbps e 40 Gbps) [1].

A tecnologia SONET/SDH permite ainda implementar mecanismos variados de proteção nos equipamentos e na própria rede, oferecendo serviços com alta disponibilidade e efetiva segurança no transporte de informações [1].

Hierarquia SONET/SDH

O sinal elétrico em uma rede *synchronous optical network* (SONET) é denominado *synchronous transport signal* (STS) e o sinal óptico é denominado *optical carrier* (OC) [2]. A rede SDH (*synchronous digital hierarchy*) utiliza a notação *synchronous transport module* (STM) para ambos os sinais. A Figura 1 ilustra as diferentes possibilidades atuais de taxas e interfaces da hierarquia SONET/SDH.

Nível Óptico	Nível SONET (elétrico)	Nível SDH (elétrico)	Taxa de dados (Mbps)	Taxa cabeçalho (Mbps)	Taxa *payload* (Mbps)
OC-1	STS-1	-	51,840	1,728	50,112
OC-3	STS-3	STM-1	155,520	5,184	150,336
OC-9	STS-9	STM-3	466,560	15,552	451,008
OC-12	STS-12	STM-4	622,080	20,736	601,344
OC-18	STS-18	STM-6	933,120	31,104	902,016
OC-24	STS-24	STM-8	1244,160	41,472	1202,688
OC-36	STS-36	STM-12	1866,240	62,208	1804,932
OC- 48	STS-48	STM-16	2488,320	82,944	2405,376
OC-96	STS-96	STM-32	4976,640	165,888	4810,752
OC-192	STS-192	STM-64	9953,280	331,776	9621,504
OC-768	STS-768	STM-256	39813,120	1327,104	38486,016
OC-N	STS-N	STM-N/3	N*51,840	N*1,728	N*50,112

Figura 1 – Hierarquia SONET/SDH. Adaptado de [2].

Pode-se dizer que o SONET/SDH é canalizado, uma vez que um STS-3 (STM-1) consiste em três fluxos STS-1 e cada STS-1 consiste em um número de sinais DS-1 (T1) e E1 provenientes da hierarquia PDH. A estrutura básica de um STM-1(SDH) é representada na Figura 2. Ela é representada na forma de uma matriz, mas o quadro é transmitido linha por linha de forma contínua. Cada quadro tem a duração de 125µs e cada célula corresponde a um byte [3]. As nove primeiras colunas são compostas por bytes de *overhead* que é composto por três diferentes estruturas: RSOH (*Regenerator Section Overhead*), MSOH (*Multiplex Section Overhead*) e Ponteiros AU-n (*Administrative Unit*).

As 261 colunas restantes carregam o *payload* STM-1 que consiste em dados do usuário e mais uma coluna de bytes de *overhead* denominado *path overhead* (POH) [4].

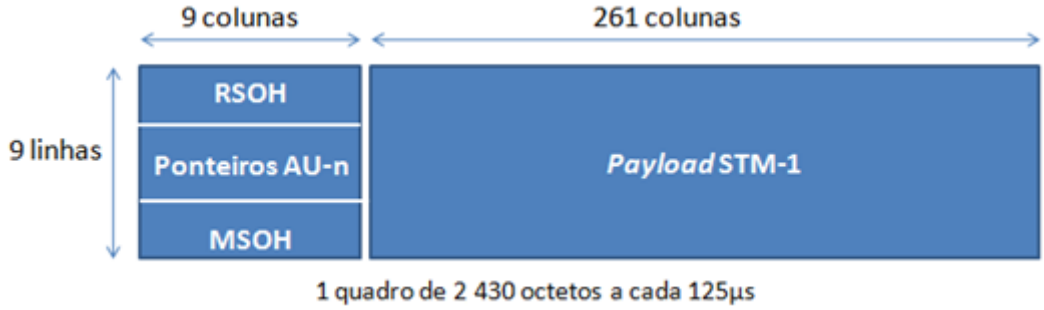


Figura 2 – Quadro STM-1 (SDH). Adaptado de [2].

Para acomodar tributários da hierarquia PDH ou sinais ISDN (*Integrated services digital network*), o SDH utiliza contêineres que podem ser definidos como sinais de várias formas e taxas menores que um STM-1. Vários mapeamentos e multiplexações (Fig. 3) são realizados para transportar um contêiner de baixa velocidade em um sinal SDH de nível STM. Foram definidos seis tipos de contêineres para o SDH: C-11, C-12, C-2, dois C-3 e C-4. Os contêineres de alta ordem são representados pelo C-3 e pelo C-4. Os contêineres de baixa ordem são representados pelo C-2, C-12, e C11 [2]. Cada tipo de tributário percorre um caminho diferente de multiplexação até atingir o nível STM. A Figura 3 ilustra os processos de

mapeamento, alinhamento e multiplexação que cada um desses tributários percorre até a formação do quadro STM na tecnologia SDH.

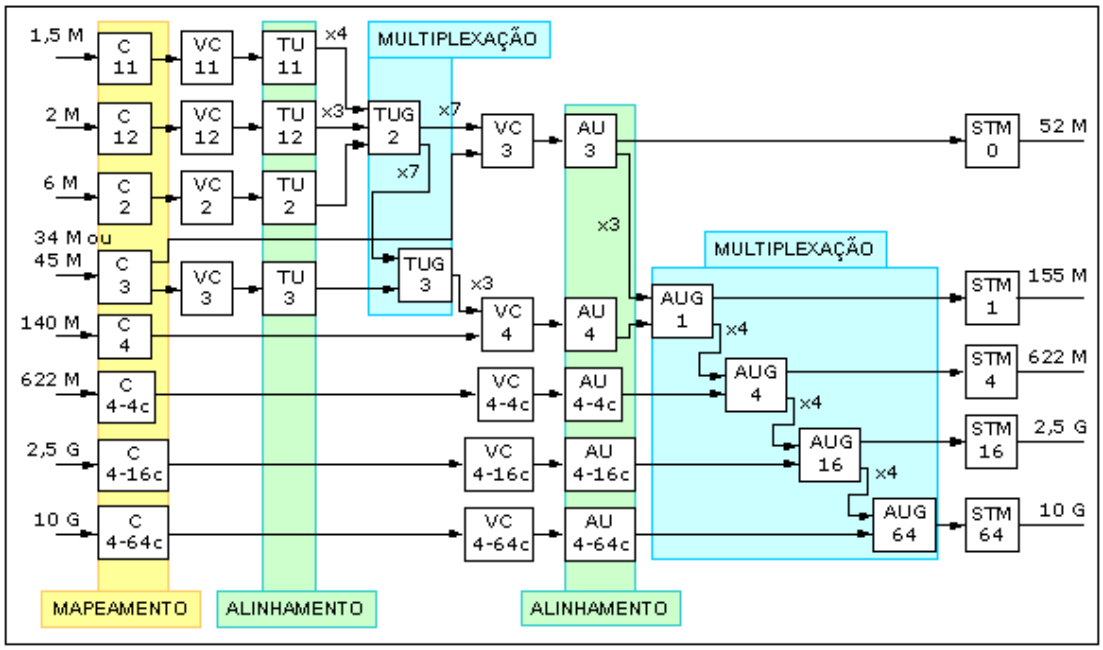


Figura 3 - Multiplexação de tributários no quadro SDH [1]

Sincronismo

O sincronismo certamente é uma das características mais marcantes das redes SONET/SDH. Os relógios do transmissor e do receptor necessitam estar precisamente sincronizados para evitar a detecção errada de bits durante o transporte de informação pela rede. Pequenas variações na sincronização dos relógios dos equipamentos de uma rede podem significar um alto número de bits de informação perdidos e por isso essas variações devem ser minimizadas da melhor maneira possível.

Para garantir o sincronismo da rede SDH, um relógio preciso e confiável como um relógio atômico ou um sinal de GPS é eleito como o relógio de referência primária (*primary reference clock* - PRC) de toda a rede. Equipamentos diretamente conectados ao relógio de referência primária são representados no nível 1. Equipamentos que obtêm a referência a partir de equipamentos do nível 1 são representados no nível 2. Da mesma maneira outros equipamentos obtêm o sincronismo necessário e constituem, dessa forma, uma hierarquia de diversos níveis. Naturalmente, quanto menor o nível, mais preciso é o relógio. Para assegurar uma multiplexação síncrona, as redes SONET/SDH utilizam equipamentos de nível 3 ou menores [2].

Fenômenos como *jitter*, que são variações de freqüência maiores ou iguais a 10 Hz nos instantes significativos de um sinal nas suas posições ideais no tempo e *wander*, que são variações de freqüência menores ou iguais a 10 Hz nos instantes significativos de um sinal digital nas suas posições ideais no tempo provocam pequenos desvios nos relógios do equipamentos e precisam ser compensados com o uso de ponteiros no cabeçalho do quadro SDH [5].

O uso de ponteiros em conjunto com buffers permite acomodar as eventuais diferenças de fase e freqüência dos canais durante o processo de multiplexação. Os ponteiros possuem campos específicos para armazenar os bits ou bytes em excesso ou para indicar a falta destes durante o processo de sincronização (justificação). Os buffers permitem que esse processo ocorra sem a perda de informação armazenando e mantendo o sinal original [1].

Existem quatro modos de sincronismo: síncrono, pseudo-síncrono, plesiócrono e assíncrono. No modo síncrono todos os relógios da rede são referenciados por uma única referência primária de relógio e a rede constitui uma única área de sincronismo. Eventuais ajustes de ponteiro ocorrem de forma aleatória e é o modo de operação normal dentro de uma rede de um único provedor de serviços. No modo pseudo-síncrono nem todos os relógios são referenciados por uma referência primária de relógio e cada PRC forma uma área de sincronismo. Os elementos de rede posicionados nas bordas dessas áreas podem fazer ajustes de ponteiros e esse é o modo de operação normal de provedores de serviço de grande porte (com várias áreas de sincronismo) ou entre redes compostas por vários provedores de serviços. Já o modo plesiócrono, caso o sinal de sincronismo na rede falhe, os equipamentos de rede utilizam suas referências internas e podem ocorrer ajustes de ponteiros de forma persistente em vários pontos da rede enquanto o sinal de sincronismo não for recuperado. No modo assíncrono, falhas do sinal de sincronismo provocam grandes desvios de freqüência entre os relógios dos equipamentos de rede e conseqüentemente alarmes de falhas e interrupção do tráfego da rede podem ocorrer [2].

No caso de uma rede SONET/SDH pequena que não possui comunicação com outras redes, um equipamento de rede pode ser eleito como o mestre e o gerador do PRC. Todos os outros equipamentos podem ser configurados no modo escravo e obter o sincronismo do equipamento de rede eleito como mestre. Esta configuração pode se mostrar muito útil em cenários de laboratório e de teste [6].

Estrutura em Camadas

O padrão SDH foi desenvolvido usando a abordagem cliente/servidor e sua arquitetura de administração e supervisão procurou apoiar-se no modelo de camadas ISO (*Open Systems Interconnection*- OSI), permitindo que a supervisão do transporte de informações seja feita através de camadas hierarquizadas. Foram definidas basicamente duas camadas de transporte SDH: camada de caminho e camada do meio de transmissão [1].

Equipamentos SONET/SDH [3]

Existem basicamente três tipos de equipamentos SONET/SDH: multiplexador terminal (*terminal multiplexer*- TM), multiplexador *add/drop* (*add/drop multiplexer* - ADM) e *digital cross-connect* (DCS).

O TM (Fig. 4) é responsável por multiplexar um número de sinais DS-n ou E1 em um único sinal STM-N. Consiste de um controlador, interfaces de baixa velocidade para os sinais DS-n e E1, uma interface STM-N, e um *time slot interchanger* (TSI). O TM também atua como um demultiplexador.

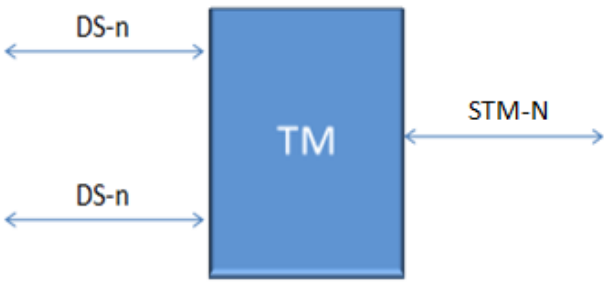


Figura 4 – Multiplexador terminal

O ADM (Fig. 5) é uma versão mais complexa do TM. Ele recebe um sinal STM-N e a partir dele pode demultiplexar e terminar (*drop*) qualquer número de sinais DS-n ou STM-M, onde M < N, ao mesmo tempo que pode adicionar novos sinais DS-n e STM-M no sinal STM-N.

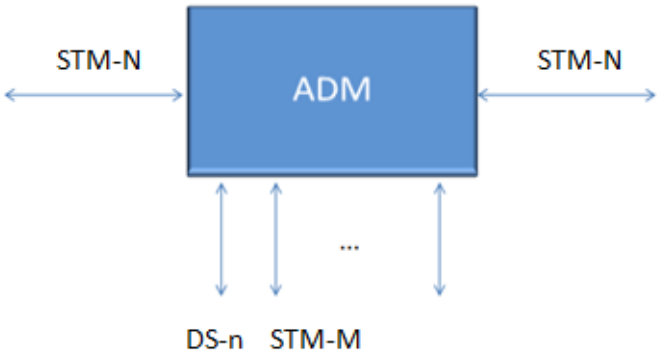


Figura 5 – *Add/drop multiplexer*

Na conexão exemplificada na Fig. 6, temos que o usuário A transmite um sinal DS-1 para o TM1. O TM1 transmite um sinal STM-1 para o ADM1, que por sua vez, adiciona o sinal STM-1 no *payload* de um sinal STM-4 e transmite para o próximo ADM do anel. No ADM3, o sinal DS-1 pertencente a A é retirado do *payload* e transmitido com outros sinais para o TM2. O TM2 finalmente demultiplexa os sinais e transmite o sinal DS-1 para o usuário B.

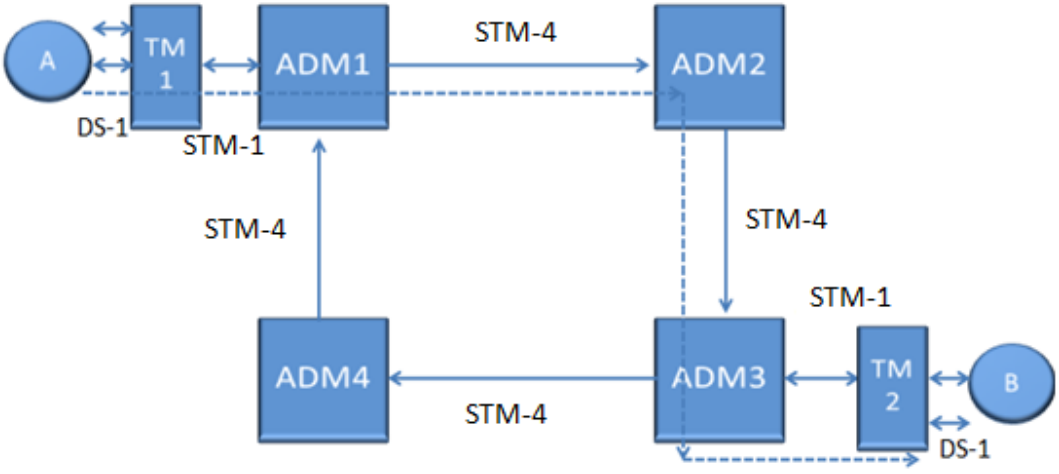


Figura 6 – Exemplo de conexão

O DCS (Fig. 6) é usado para interconectar múltiplos anéis SONET/SDH. É conectado a múltiplas interfaces OC-N (STM-N) de entrada e de saída. Pode retirar ou adicionar qualquer número de sinais DS-n ou OC-M (STM-M) e pode comutar sinais DS-n ou OC-M (STM-M) provenientes de uma interface de entrada para qualquer interface de saída [1].

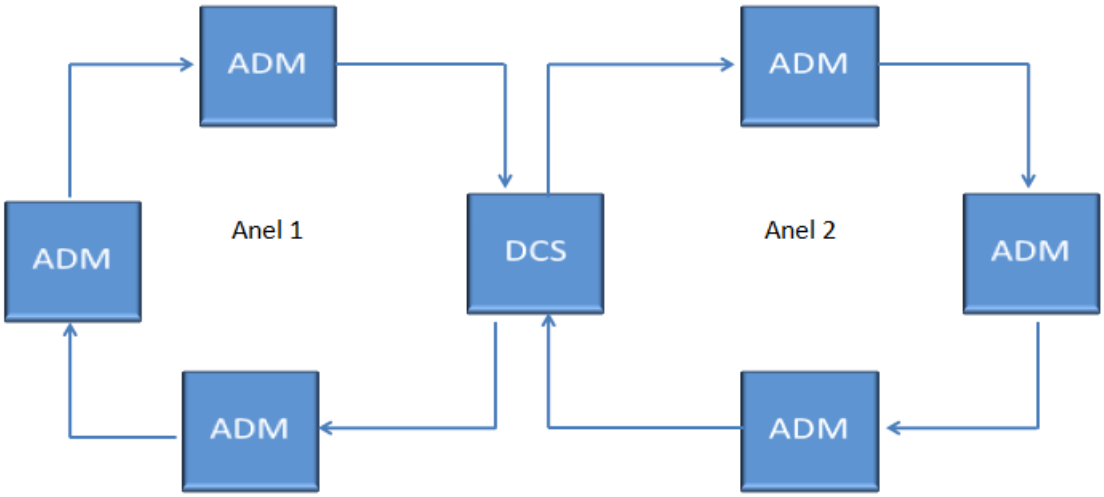


Figura 7 – *Digital cross-connect*

Proteção em redes SONET/SDH

Provavelmente, a característica mais marcante das redes SONET/SDH, quando comparadas ao sistema digital PDH, é a topologia em anel. O conceito de proteção já existia em redes PDH, mas novos padrões de demanda por proteção e confiabilidade foram introduzidos nas redes SONET/SDH [2].

As falhas relacionadas à fibra óptica podem possuir causas diversas, mas em sua grande maioria elas provêm de rompimentos em cabos enterrados provocados por construções ou escavações [2]. Existem basicamente dois tipos de proteção: proteção linear e proteção em anel.

Comutação automática de proteção linear (APS) [2]

A comutação automática de proteção (*Automatic Protection Switching*- APS) é uma técnica que já era utilizada em redes PDH. Existem diferentes tipos de proteção linear. A proteção 1:N que consiste no uso de N enlaces ativos (trabalho) e um enlace de proteção é freqüentemente utilizada em enlaces ponto-a-ponto. Um grave problema associado à proteção 1:N é a situação em que mais de um enlace falhe ao mesmo tempo. Para contornar este problema, áreas de alto-risco adotam a proteção 1:1 (Fig. 8) onde cada enlace ativo possui seu próprio enlace de proteção.

A técnica de proteção 1+1 (Fig.9) refere-se ao fato de que o sinal é transmitido no enlace de trabalho juntamente com uma cópia do sinal transmitido no enlace de proteção. O receptor é incumbido de selecionar o sinal com melhor qualidade. A proteção 1:1 , ao contrário, envia o sinal somente pelo enlace ativo podendo transmitir tráfego de baixa prioridade pelo enlace de proteção. Quando uma falha ocorre, o tráfego do enlace ativo é transferido para o enlace de proteção e o tráfego de baixa prioridade é temporariamente suspenso até que as condições normais sejam restauradas. A técnica 1:1 possui melhor aproveitamento da capacidade dos enlaces, mas exige uma ação de comutação mais elaborada quando uma falha ocorre. Isso afeta diretamente o tempo de resposta de restauração do serviço.

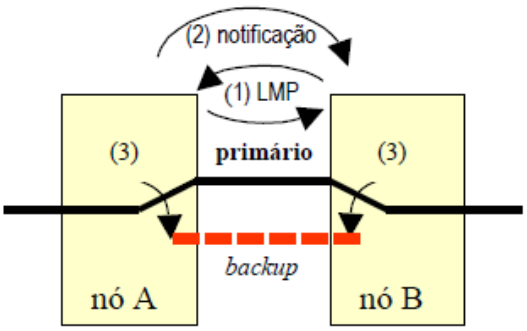


Figura 8 - Proteção 1:1

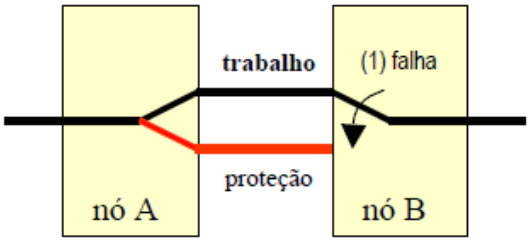


Figura 9 - Proteção 1+1

Anéis SONET/SDH

Um anel SONET/SDH é definido como uma coleção de dois ou mais elementos de rede SONET/SDH que formam um *loop* fechado. Os anéis são comumente conhecidos como *self-healing* pela capacidade automática de restauração após uma falha ou deterioração dos sinais da rede [2].

Existem várias arquiteturas de anéis disponíveis, mas basicamente quatro atributos são responsáveis pelas diferentes composições de arquitetura como ilustrado na Tabela 1 [2].

Atributo	Opções
Número de fibras por enlace	2 ou 4 fibras
Direção do sinal	Unidirecional Bidirecional
Nível de proteção de comutação	Comutação de linha Comutação de caminho
Proteção	Proteção de *span* Proteção de anel

Tabela 1 - Tipos de anéis SONET/SDH

Na prática, com raras exceções, somente os seguintes tipos de anéis são implementados em larga escala:

- 2 fibras, unidirecional, comutação de caminho (*2-fiber Unidirectional Path Switched Ring*, UPSR - SONET) ou proteção de conexão de subrede (*subnetwork connection protection*, SNCP - SDH) [7]

- 2 fibras, bidirecional, comutação de linha (*2-fiber Bidirectional Line Switched Ring*, BLSR-SONET) ou anel de proteção compartilhada da seção de multiplexação com duas fibras (*Multiplex section shared protection ring*, MS-SPRing - SDH) [7]

- 4 fibras, bidirecional, comutação de linha (*4-fiber Bidirectional Line Switched Ring*, BLSR-SONET) ou anel de proteção compartilhada da seção de multiplexação com quatro fibras (MS-SPRing - SDH) [7]

Em um anel unidirecional (Fig. 10), o tráfego é roteado de tal forma que as duas direções de uma conexão entre dois nós viajem em volta do anel pela mesma direção. Dessa forma, cada conexão utiliza toda a capacidade de banda em torno de toda a circunferência do anel. Por convenção, todo o tráfego de trabalho em anéis unidirecionais trafega no sentido horário [2].

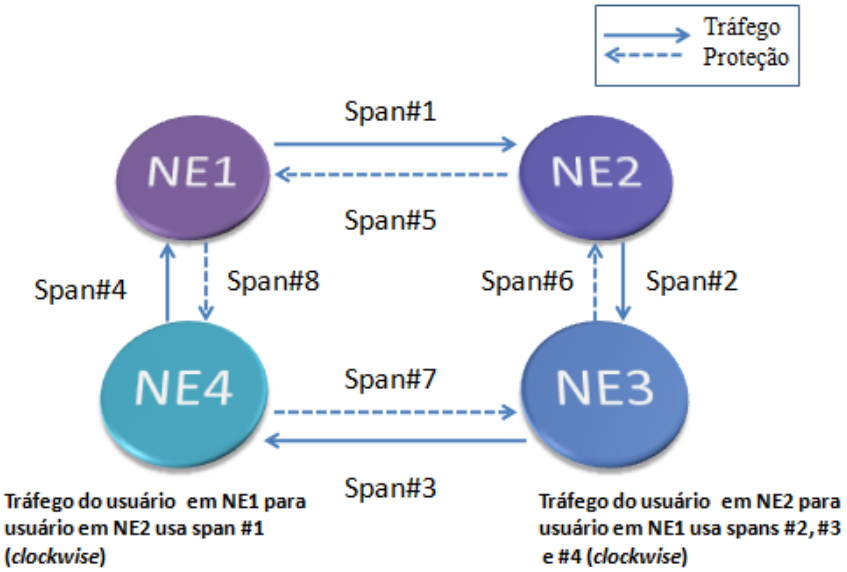


Figura 10 - Anel unidirecional

Já em um anel bidirecional (Fig. 11), o tráfego de trabalho é roteado de tal forma que as duas direções de uma conexão trafeguem os sinais pelo anel pelos mesmos nós, mas em direções opostas [2].

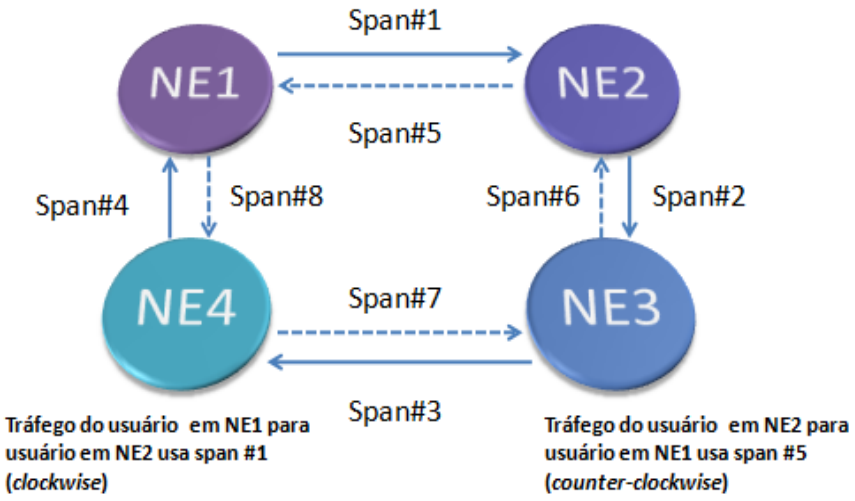


Figura 11 - Anel bidirecional

Os dois tipos de anel podem utilizar duas fibras ou quatro fibras entre cada nó (Fig. 12). Em um anel bidirecional de duas fibras, cada *span* de fibra carrega o canal de tráfego de trabalho e o canal de tráfego de proteção. Já o anel bidirecional de quatro fibras possui, por *span*, duas fibras que carregam os canais de tráfego de trabalho e duas fibras que carregam os canais de proteção [2].

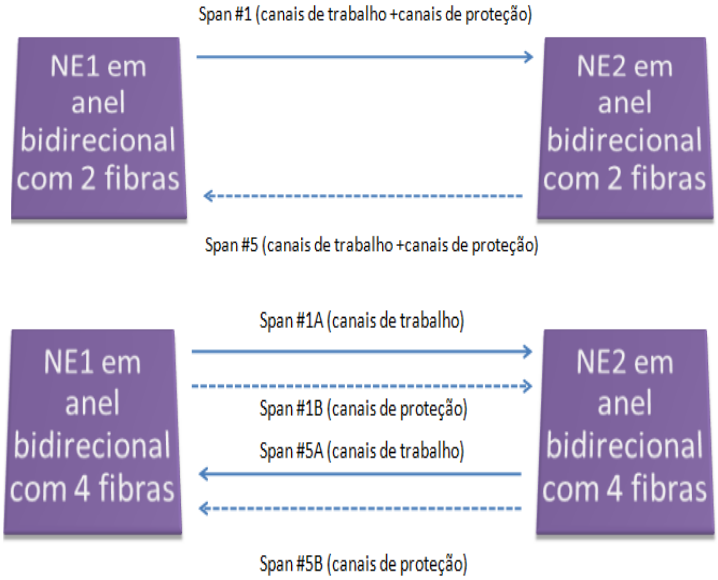


Figura 12 - Proteção bidirecional de duas e quatro fibras

Uma outra característica é o tipo de comutação de proteção empregada. A comutação de linha (Fig.13) restaura todos os canais de tráfego ativo em toda a capacidade STM-n em uma única operação de proteção. A capacidade de proteção não deve ser utilizada enquanto o anel estiver em operação normal. Esse tipo de proteção é caracterizada como compartilhada. [2].

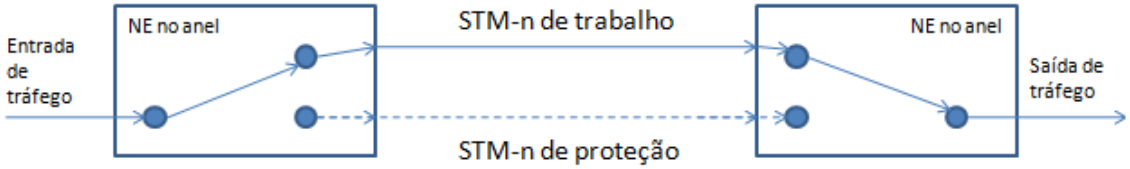


Figura 13 – Comutação de linha

A comutação de caminho (Fig.14) restaura todos os canais a um nível menor do que toda a capacidade STM-n. Os sinais são enviados em ambos os enlaces ativos e de proteção e o receptor monitora ativamente a qualidade dos sinais e escolhe o melhor para a recepção. A comutação de caminho (dedicada) é universalmente feita em anéis unidirecionais de duas fibras. A comutação de linha, por sua vez, é utilizada em anéis bidirecionais de duas ou quatro fibras [2].

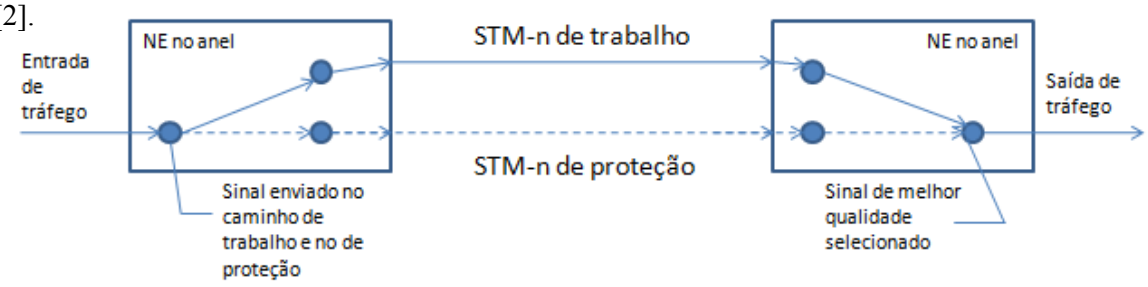


Figura 14 – Comutação de caminho

Anéis que utilizam quatro fibras (Fig. 15) oferecem proteção contra falhas não somente de um par de fibras, mas contra dois pares entre quaisquer dois nós do anel. Durante a operação normal, os sinais são divididos e enviados nas duas direções do anel. Se um par de fibras falhar, o sinal é enviado pelo outro par de fibra na mesma direção (proteção de *span*). Se o outro par de fibras apresentar falha, o sinal será transportado pela outra direção do anel pelo par de proteção (proteção de anel). Dessa maneira, anéis que utilizam quatro fibras podem continuar operando mesmo após múltiplas falhas [2].

Na proteção de *span*, tudo o que é preciso fazer é comutar o tráfego do par ativo para o par de proteção. O fluxo do tráfego não é interrompido. Porém, a comutação de anel provoca a interrupção do fluxo de tráfego entre os dois nós enquanto o sinal viaja ao destino pela outra direção do anel [2]. As duas situações estão ilustradas na Figura 15.

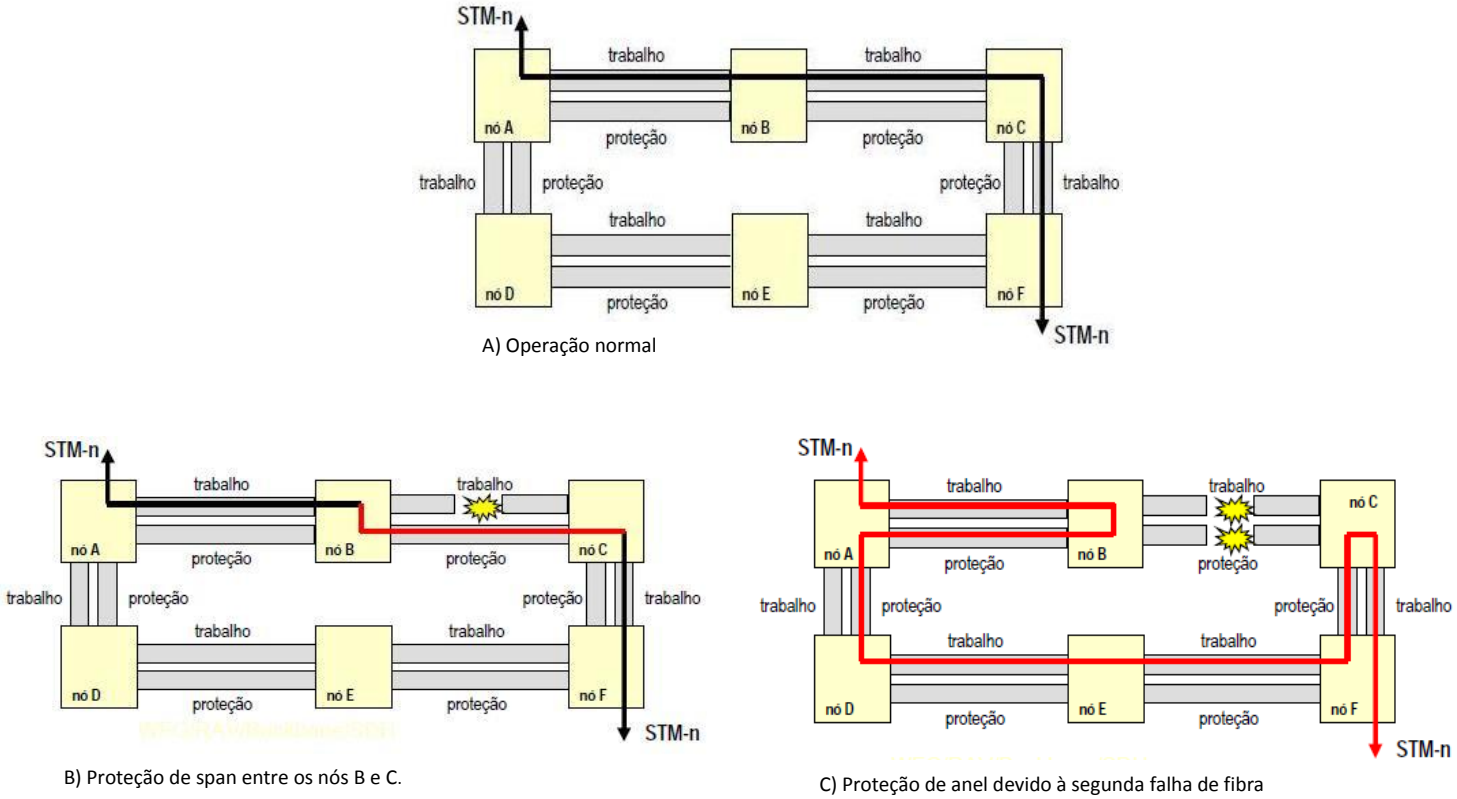


Figura 15 – Proteção de *span* e proteção de anel em um MS-SPring com quatro fibras

Os principais mecanismos de proteção das tecnologias SONET e SDH estão resumidos na Tabela 2.

Tipo de proteção	SONET	SDH
Linear 1+1	Proteção dedicada	Proteção dedicada
Linear 1:N	Proteção compartilhada	Proteção compartilhada
Anel compartilhado	BLSR 2 ou 4 fibras	MS-SPRing 2 ou 4 fibras
Anel dedicado	UPSR	SNCP

Tabela 2 – Mecanismos de proteção SONET/SDH

2.1.2 Generic Frame Procedure (GFP)

A interconexão de escritórios separados por centenas de quilômetros de distância em uma mesma LAN gera um grave problema de compatibilidade de interconexão. Historicamente, muitos protocolos proprietários foram desenvolvidos para prover a interface entre a LAN e a WAN, oferecida pelo provedor de serviços de telecomunicações, uma vez que o protocolo Ethernet não é diretamente suportado pela rede SONET/SDH [8].

O motivo pelo qual o protocolo Ethernet não é carregado diretamente pela rede SONET/SDH é o fato do Ethernet ter sido criado após a tecnologia SONET/SDH. Como resultado, existe uma diferença de taxas entre as tecnologias e uma falta de eficiência dos métodos de encapsulamento até então utilizados. O Ethernet pode operar nas taxas de 10Mbps, 100Mbps, 1Gbps e 10Gbps. Já as taxas do SONET/SDH são otimizadas para o transporte de tráfego de telecomunicações ou de voz e não possui taxas adequadas para o transporte de um fluxo de dados Ethernet (Tabela 3). A diferença entre as taxas provocaria uma grande ineficiência ao transportar uma conexão Ethernet em um canal SONET/SDH.

Ethernet	**SONET**		
Taxa de bit	Taxa SONET	Taxa efetiva *payload*	Eficiência de Banda
10Mbps Ethernet	STS-1	50,112 Mbps	20%
100 Mbps FastEthernet	STS-3	150,336 Mbps	67%
1Gbps Ethernet	STS-48	2045,376 Mbps	49%

Tabela 3 – Taxas típicas Ethernet vs. SONET

Para otimizar o transporte de quadros Ethernet em enlaces SONET/SDH, foi desenvolvido e padronizado o *Generic Frame Procedure* [8].

O GFP é uma tecnologia que oferece uma flexibilização do *framework* de encapsulamento para fluxo de dados codificados em bloco e dados orientados a pacotes. Ele possui o potencial de substituir os protocolos proprietários para transportar dados nas existentes redes SONET/SDH e redes de transporte WDM e OTN (*Optical Transport Network*) emergentes [8].

O GFP suporta todas as funções básicas de quadro como delimitação de quadro, multiplexação de quadro dos clientes e mapeamento de dados do cliente [8].

A estrutura do quadro GFP consiste no *core header* e uma área de *payload* (Fig. 16).

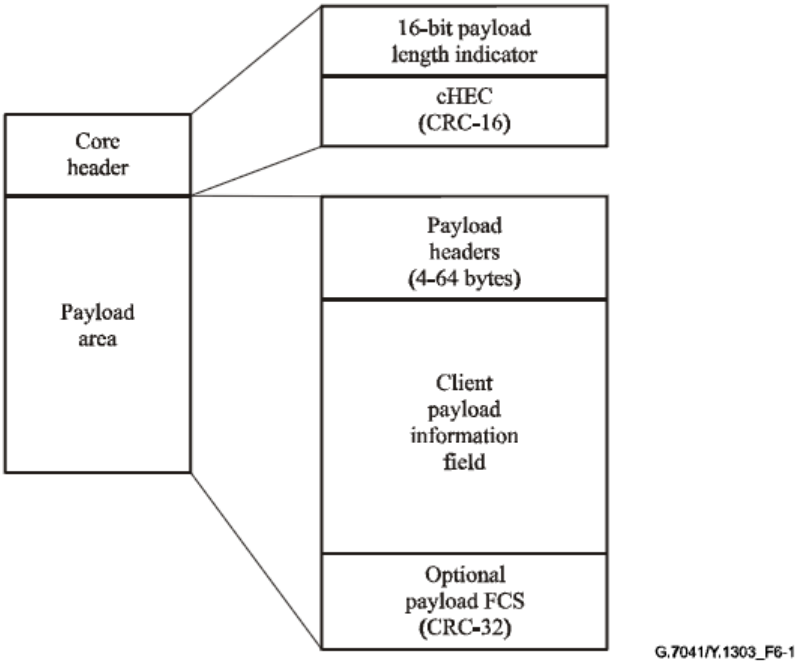


Figura 16 - Estrutura do quadro GFP [9]

Funções do GFP

O campo de informação do *payload* contém os dados do cliente. Existem dois modos de adaptação do sinal cliente definidos para o GFP: *frame-mapped* GFP (GFP-F) aplicável a maioria dos tipos de pacotes e *transparent-mapped* GFP (GFP-T) aplicável a sinais codificados em 8B/10B. Os *payload*s do tipo GFP-F possuem tamanhos variáveis e o quadro do cliente é mapeado inteiramente em um quadro GFP. Exemplos: Ethernet e IP/PPP (*Point-to-point protocol*). No modo GFP-T um número de caracteres de cliente é mapeado em blocos de código eficientes e transportado pelo quadro GFP. [8].

O formato do quadro Ethernet foi definido pelo IEEE 802.3 na seção 3.1. Existe um mapeamento de um para um entre o PDU proveniente de uma camada mais elevada e o PDU GFP. Especificamente, os limites de um PDU GFP são alinhados com os limites dos PDUs de camadas mais altas [9]. Essa relação entre quadros MAC Ethernet e quadros GFP está ilustrada na Figura 17.

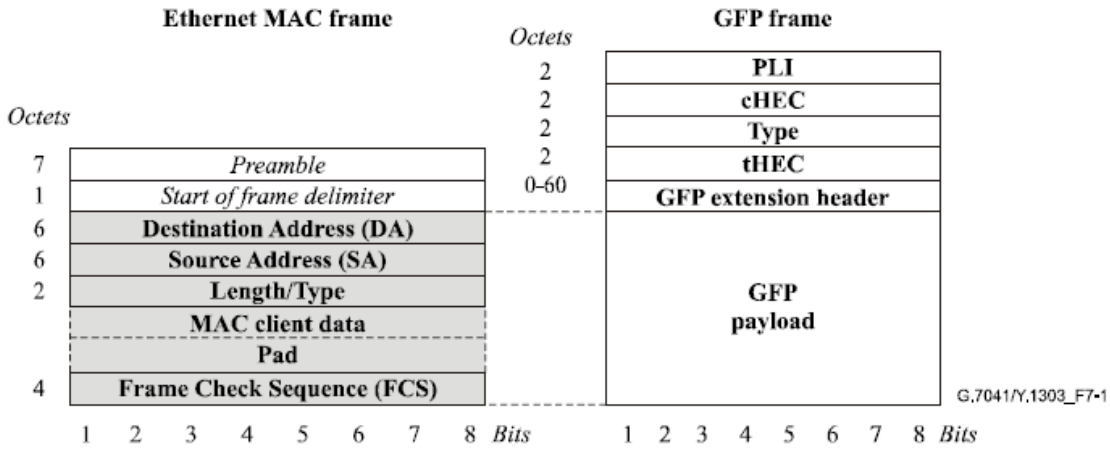


Figura 17- Relação entre o quadro Ethernet e o quadro GFP [9]

Os octetos provenientes do campo de endereço de destino até o *Frame Check Sequence* (FCS) são colocados no campo de informação do *payload* GFP. Os campos de preâmbulo e início do delimitador de quadro não são encapsulados. O tamanho da PDU do cliente é variável e pode ser de até 65 535 octetos. O *payload* Ethernet é mapeado no modo de adaptação GFP-F e os quadros GFP resultantes são transportados pela rede SONET/SDH [9].

2.2 LABORATÓRIO

O laboratório OptiX possui quatro equipamentos SDH, dois equipamentos WDM e um servidor equipado com o sistema de gerência **iManager T2000** (Fig. 18).

Figura 18 – Visão geral do laboratório

SDH OptiX OSN 3500

O equipamento OptiX OSN 3500 (Fig. 19) foi desenvolvido para operar em redes MAN. Ele integra as tecnologias SDH, WDM, Ethernet, ATM, e PDH podendo transportar serviços de voz e dados de maneira eficiente na mesma plataforma [10].
Quantidade: 2

Figura 19 – Visão frontal SDH OptiX OSN 3500

A primeira unidade SDH OptiX OSN 3500 está equipada com as seguintes placas e seus respectivos *slots* no armário (Fig. 20):

D12S (*Slot* 19) - 4 interfaces E1 elétricas (120Ω).
PIUA (*Slots* 27 e 28) (x2) - Suprimento de energia e proteção contra situações anormais de energia.
EFF8 (*Slot* 35) - 8 interfaces 100Base-FX (ópticas).
AUX (*Slot* 37) - Interfaces de gerenciamento e auxiliares.
PQ1 (*Slot* 02) - Interface E1 (*Backplane*).
EFS4 (*Slot* 04) - 4 interfaces 100Base-TX.
BPA (*Slot* 05) - Amplificador do sinal óptico.
SLD4 (*Slot* 06) - 2 interfaces STM-4.
SL64 (*Slots* 08 e 11) (x2) - Interface STM-64.
SXCSA (*Slots* 09 e 10) (x2) - *Cross connect*.
EGS4 (*Slot* 15) - 4 interfaces ópticas Gigabit Ethernet.
GSCC (*Slot* 18) - Provê comunicação do sistema, funções de controle e processa o cabeçalho SDH.

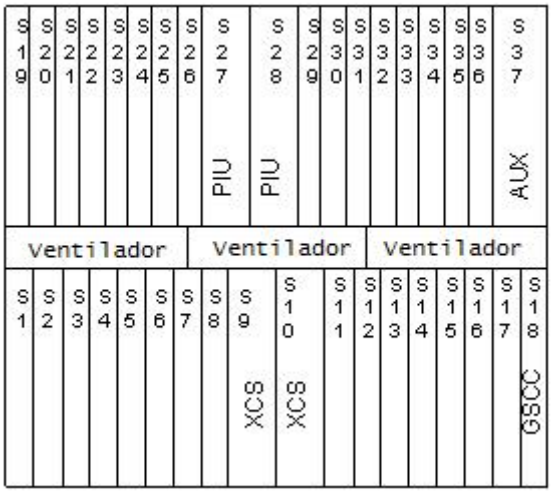


Figura 20 – Disposição dos *slots* SDH Optix OSN 3500

Baseando-se nas placas presentes, esta unidade OSN 3500 pode operar como um *cross-connect* conforme diagrama ilustrado na Figura 21.

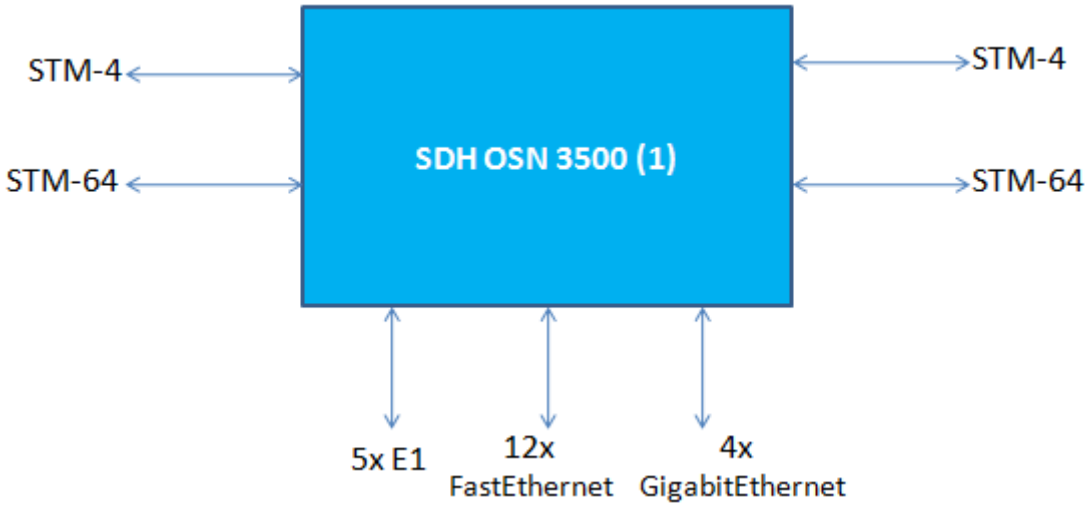


Figura 21 – Diagrama da primeira unidade SDH OSN 3500

A segunda unidade SDH OptiX OSN 3500 está equipada com as seguintes placas:

D12S (*Slot* 19) - 4 interfaces E1 elétricas (120Ω).
PIUA (*Slots* 27 e 28) (x2) - Suprimento de energia e proteção contra situações anormais de energia.
EFF8 (*Slot* 35) - 8 interfaces 100Base-FX (ópticas).
AUX (*Slot* 37) - Interfaces de gerenciamento e auxiliares.
PQ1 (*Slot* 02) - Interface E1 (*Backplane*).
EFS4 (*Slot* 04) - 4 interfaces 100Base-TX.
BPA (*Slot* 05) - Amplificador do sinal óptico.
SLQ4 (*Slot* 06) - 4 interfaces STM-4.
SL64 (*Slots* 08 e 11) (x2) - Interface STM-64.
SXCSB (*Slots* 09 e 10) - *Cross connect*.

EGS4 (*Slot* 15) - 4 interfaces ópticas Gigabit Ethernet.
GSCC (*Slot* 18) - Provê comunicação do sistema, funções de controle e processa o cabeçalho SDH.

Esta unidade OSN 3500 pode operar como um *cross-connect* conforme diagrama ilustrado na Figura 22.

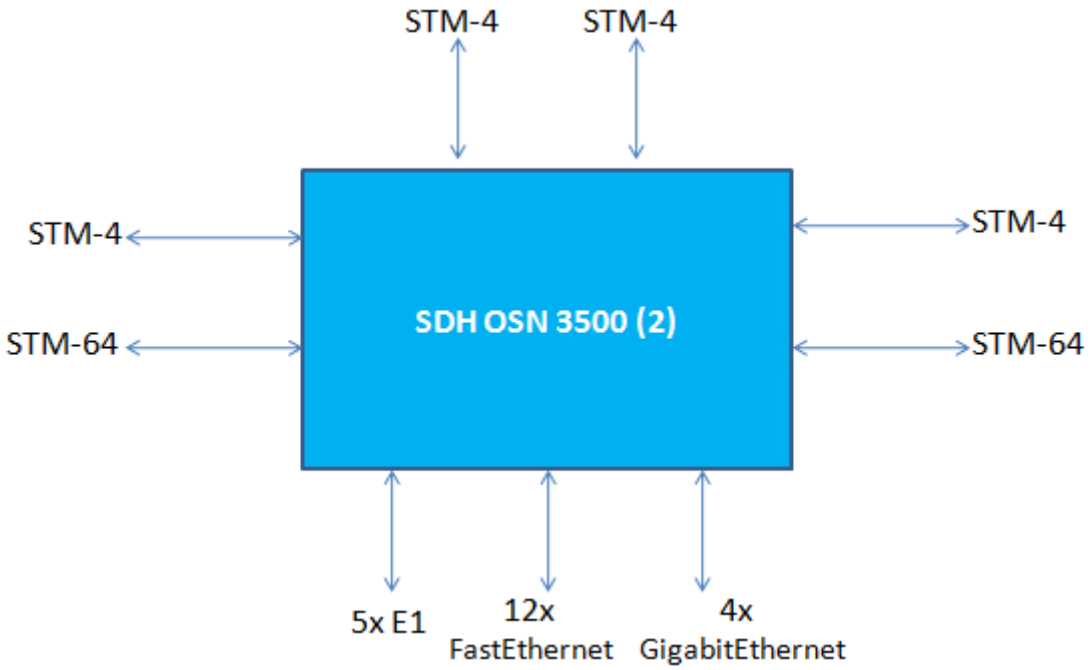


Figura 22 - Diagrama da segunda unidade SDH OSN 3500

SDH OptiX OSN 2500

O equipamento OptiX OSN 2500 (Fig. 23) foi desenvolvido para operar nas camadas de convergência e de acesso nas redes MAN. Ele integra novas tecnologias incluindo SDH, PDH, Ethernet, WDM, ATM, Fibre Channel, ESCON, FICON e DVB-ASI (*Digital Video Broadcast-Asynchronous Serial Interface*) oferecendo a solução para a evolução dos equipamentos SDH existentes para equipamentos de redes ópticas inteligentes [10].
Quantidade:2

Figura 23 - Visão frontal SDH OptiX OSN 2500

A duas unidades SDH OptiX OSN 2500 estão equipadas com as seguintes placas e seus respectivos *slots* no armário (Fig. 24):

PQ1 (*Slot* 06) - Interface E1 (*Backplane*).
CXL1 (*Slots* 09 e 10) (x2) – Interface STM-1 + SCC (Placa controladora) + *Cross Connect*.
SAP (*Slot* 14) - Gerência.
PIU (*Slots* 22 e 23) (x2) - Suprimento de energia e proteção contra situações anormais de energia.

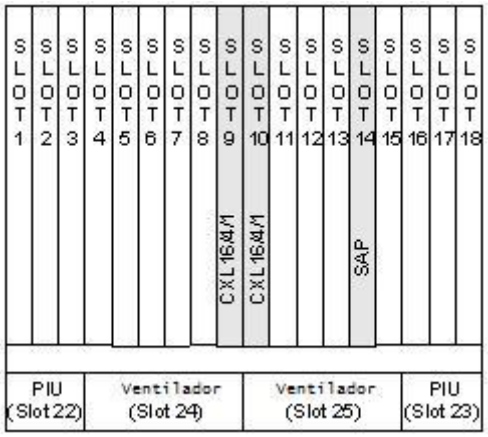


Figura 24 - Disposição dos *slots* SDH OptiX OSN 2500

O OSN 2500 pode operar, nesta configuração, como um multiplexador terminal conforme diagrama ilustrado na Figura 25. Cada unidade possui uma interface E1 e uma interface STM-1.

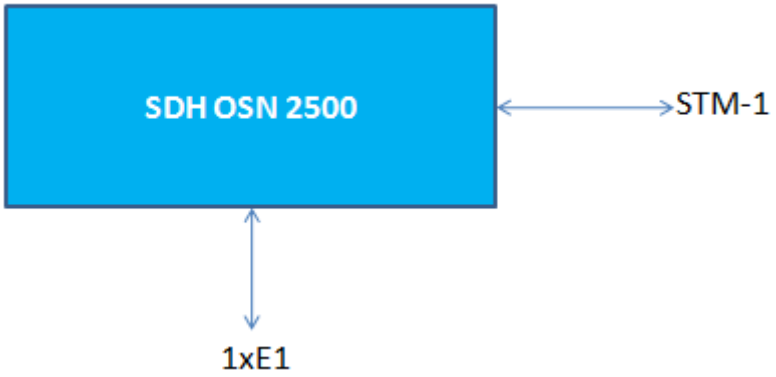


Figura 25 - Diagrama SDH OSN 2500

Sistema de Gerência iManager T2000 [10]

O sistema de gerência é uma ferramenta responsável por monitorar e gerenciar os equipamentos da rede garantindo seu funcionamento normal. Através da ferramenta, é possível visualizar a topologia da rede, o aparecimento de alarmes, o estado da rede e configurar remotamente diversas funcionalidades dos equipamentos. O laboratório está equipado com o *software* de gerência iManager T2000 Huawei.

As funcionalidades básicas do sistema iManager T2000 são apresentadas a seguir.

Inicialização

O T2000 utiliza uma arquitetura cliente-servidor e um modo multiusuário padrão. A senha de usuário do Windows XP é: 123 + (SHIFT+123) + abc. Para inicializar o programa, primeiramente deve-se iniciar o banco de dados SQL. Clique com o botão direito do mouse no ícone na barra do Windows, localizada no canto inferior direito da área de trabalho, e selecione **Start**. Em seguida, o servidor T2000 deve ser iniciado. Duplo clique no ícone **T2000 Server** localizado na área de trabalho. O nome de usuário padrão é **admin** e a senha padrão é **T2000** (Fig. 26). O campo **Server** deve ser preenchido como **Local.** Aguarde alguns instantes até que os serviços **Ems Server**, **Schedulesrv Server**, **Security Server**, **Syslog Agent**, **Topo Server**, **Database Server Process**, e **Toolkit Server** estejam com o status **Running.**

Figura 26 – *Login*

Uma vez que o servidor estiver completamente operacional, clique no ícone **T2000 Client** na área de trabalho para executar a versão cliente do software. O nome de usuário e a senha são por padrão **admin** e **T2000** respectivamente.

Antes de desligar o servidor é necessário sair do cliente. No cliente, clique em **File →Exit** no Menu principal e clique **OK**. No servidor, clique em **System → Shutdown System** para fechar o T2000 Server.

Janelas

O sistema de gerência é composto por vários tipos de janelas de visualização que possibilitam monitorar com precisão um atributo desejado. As principais janelas do sistema iManager T2000 são: **Main Topology**, **NE Explorer**, **Protection View**, **Trail View**, **Clock View**, **SDH NE Panel**, **Browse Alarm and Event** e **Browse Performance**. Elas são apresentadas a seguir:

A interface principal e padrão do cliente T2000 é a janela **Main Topology** (Fig.27). Todas as funções de gerenciamento de topologia podem ser acessadas a partir dessa janela. Essas funções incluem a criação de objetos da topologia, subredes, fibras, cabos e a procura de equipamentos existentes na rede. Para ir para a visualização da janela *Main Topology*, selecione **Window → Main Topology** no Menu principal.

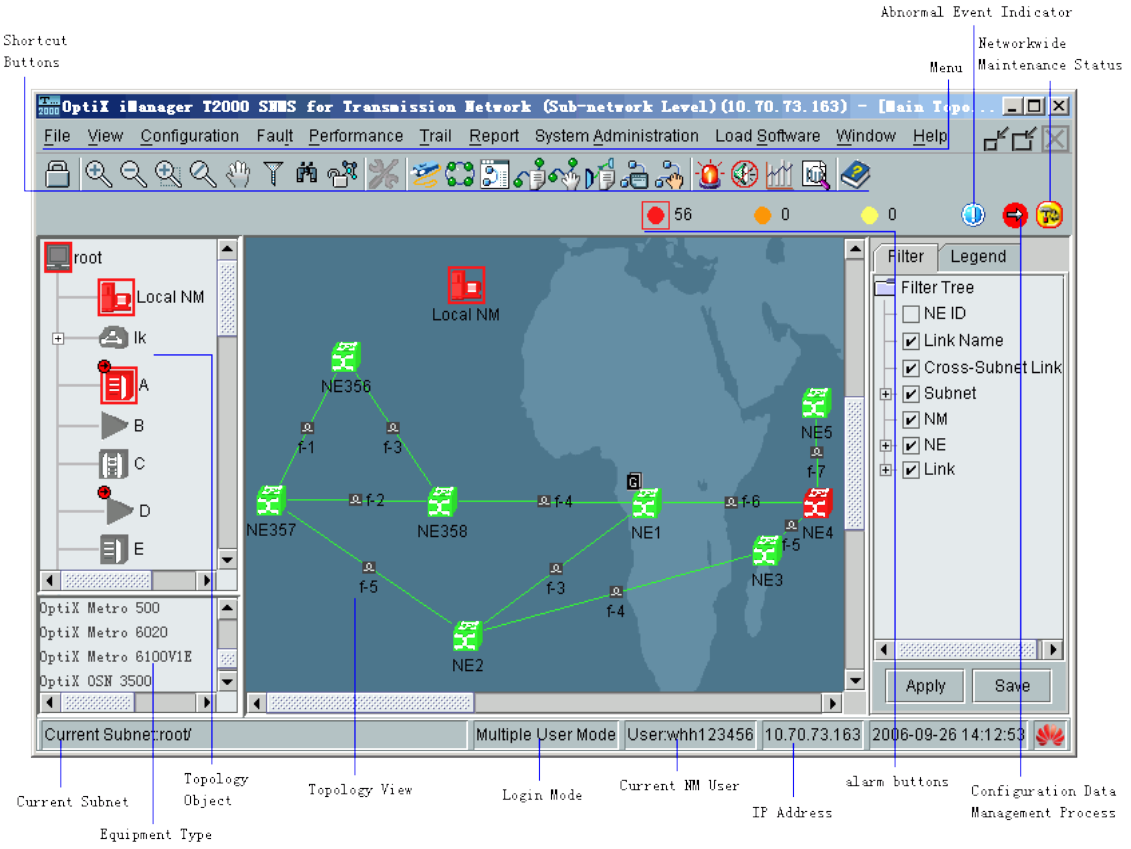


Figura 27 – Interface gráfica *Main Topology*

A janela **NE Explorer** (Fig. 28) é a principal janela utilizada para gerenciar equipamentos OptiX. Nessa janela, o usuário é capaz de configurar, gerenciar e manter individualmente o equipamento de rede. O **NE Explorer** contém uma árvore de funções (*Function Tree*) que facilita bastante as operações. Para visualizar uma janela de configuração de um determinado objeto, o usuário pode selecionar o objeto e selecionar a função desejada na árvore de funções. Para visualizar o **SDH NE Explorer**, clique com o botão direito em um equipamento de rede na *Main Topology* e escolha **NE Explorer** no Menu.

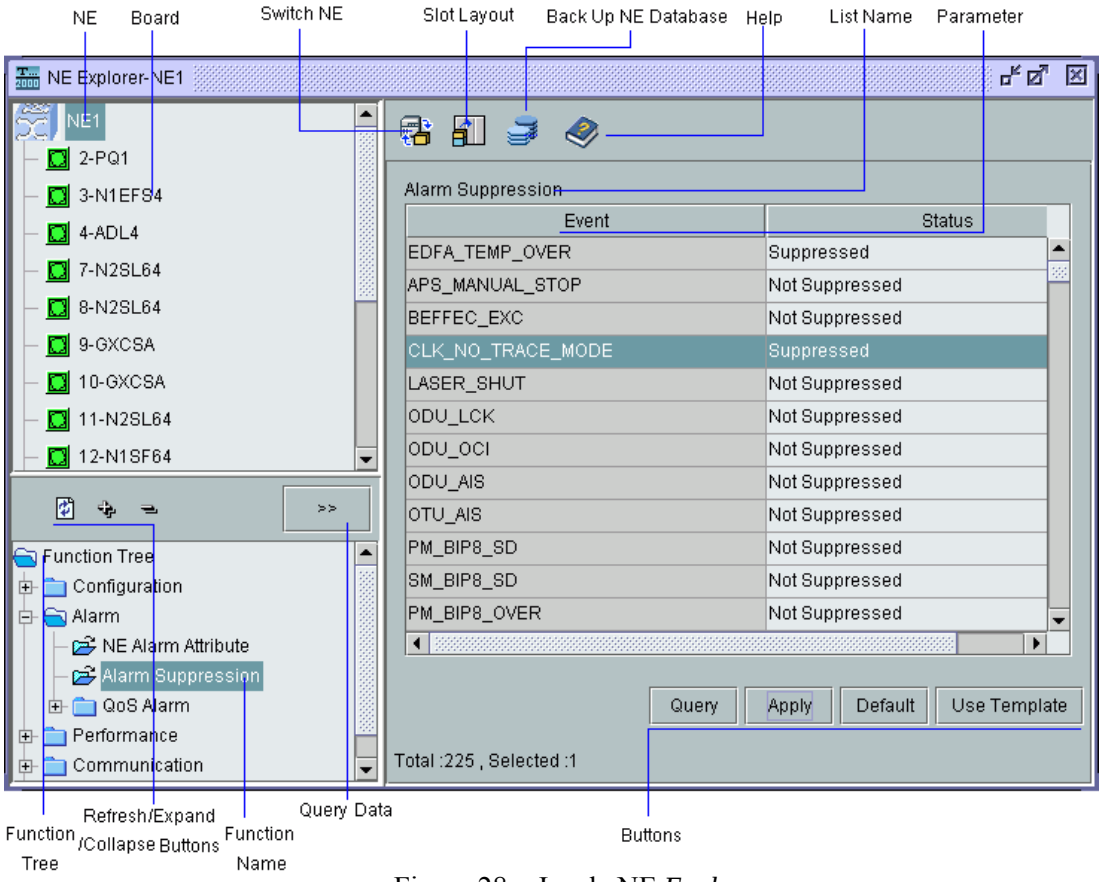


Figura 28 – Janela NE *Explorer*

A janela **Protection View** (Fig. 29) permite a procura, visualização, configuração e o gerenciamento da subrede de proteção assim como o gerenciamento de NNIs dos nós independentes. Para abrir a janela **Protection View** selecione **Configuration → Protection View** no Menu principal.

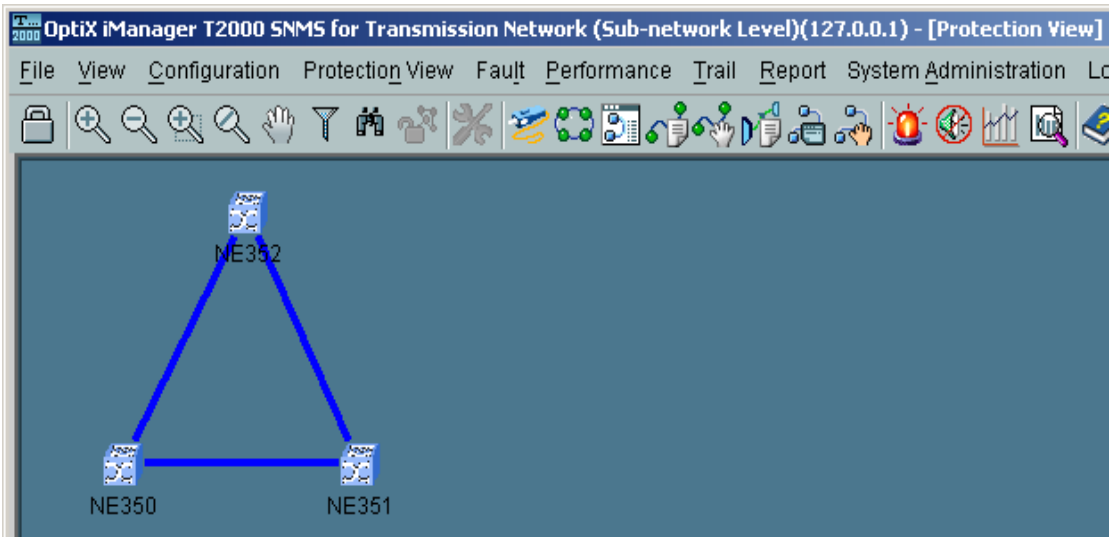


Figura 29 – Janela *Protection View*

A janela **Trail View** (Fig. 30) possibilita a procura, criação, configuração, e gerenciamento das funções de trilhas (*trails*). Para visualizar a **Trail View** selecione **Trail → Trail View** no Menu principal.

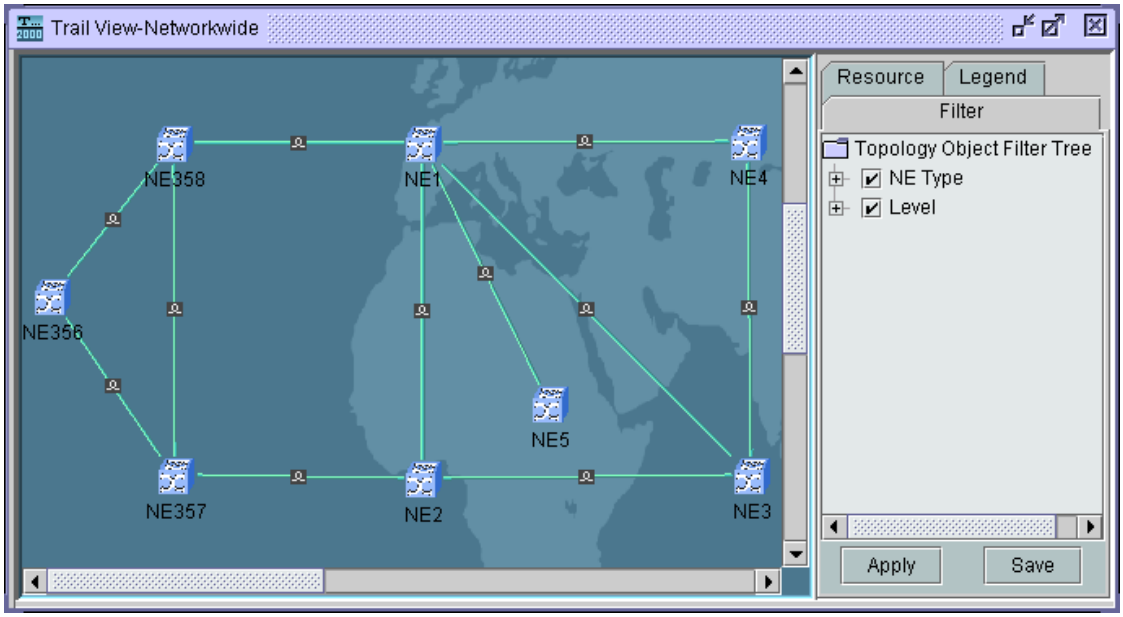


Figura 30 – Janela *Trail View*

Para configurar o relógio dos equipamentos da rede, fazer buscas de status da sincronização do relógio na rede, rastrear os relógios e executar outras funções de busca, a janela **Clock View** é utilizada. Para abrir esta janela selecionar no Menu principal **Configuration → Clock View** (Fig. 31).

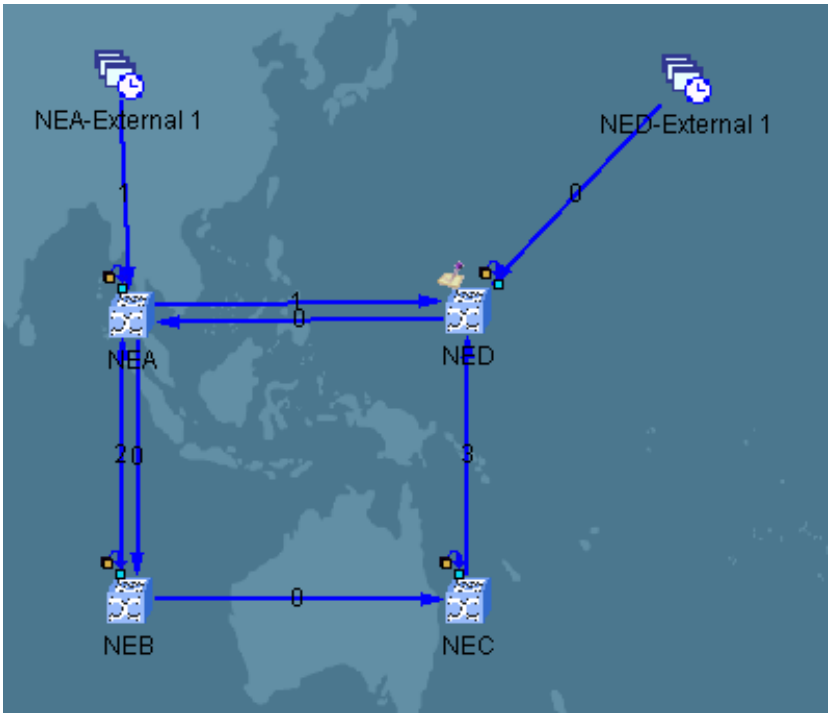


Figura 31 – Janela *Clock View*

A janela **SDH NE Panel** (Figura 32) permite a visualização de placas e portas em diferentes cores que dependem do status atual em que se encontram. No T2000, a maior parte das operações de configuração de equipamento, monitoramento e manutenção são feitas através desta janela. Para abrir a janela NE Panel, dê dois cliques no equipamento de rede desejado. Para adicionar uma placa a um *slot* vazio, basta clicar com o botão direito no *slot* e escolher o tipo de placa.

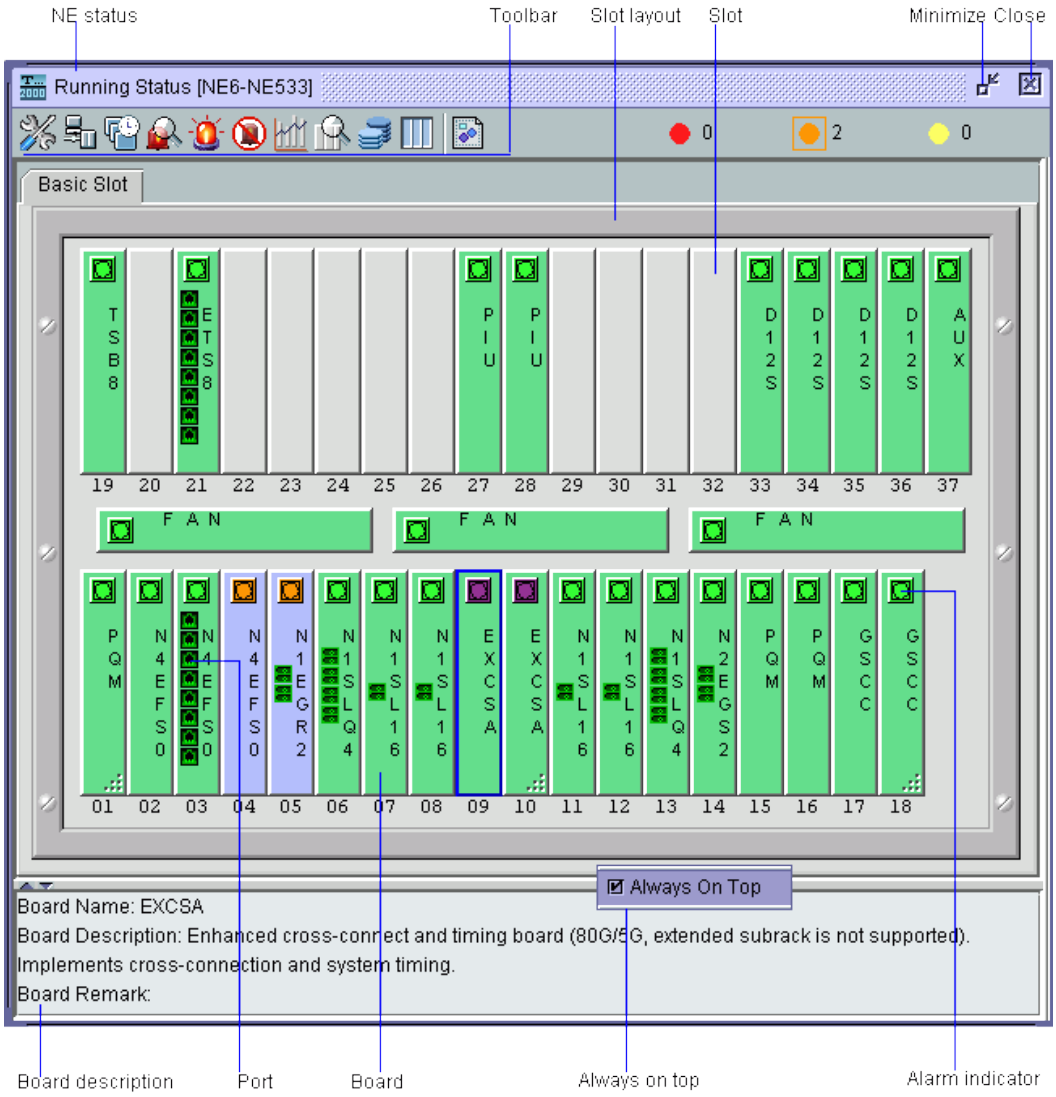


Figura 32 – Janela NE *Panel*

O ultimo ícone  a direita na barra de ferramentas permite visualizar a legenda como na Figura 33.

Legend	Description
	Not Installed
	Installation State
	Running&Uninstalled
	Running&Installed
	Fixed State
	Physical Board
	Critical Alarm
	Major Alarm
	Minor Alarm
	Warning Alarm
	Non-Alarmed
	Bidirectional Optical Port
	Ethernet Port
	Unidirectional Optical Port
	Protection Board Status
	Tributary/Line Loopback
	Resource Division

Figura 33 - Legenda

A visualização de alarmes atuais e a visualização do histórico de alarmes são possíveis através da janela **Browse Alarm and Event Window** (Fig. 34). Eventos anormais, assim como estatísticas de alarmes, também podem ser verificados. Essa janela oferece botões como a analise estática de correlação, filtro, atualização e sincronização que permitem localizar rapidamente a causa do alarme. Para a visualização dos alarmes, clique no Menu principal em **Fault → Browse Current Alarms, Fault → Browse History Alarms, Fault → Browse Abnormal Events** ou em **Fault → Browse Alarms Statistics.**

Para verificar automaticamente os últimos alarmes marque a caixa **Auto Refresh**. Selecione o alarme e seus detalhes aparecerão na tela. Para reconhecer o alarme, selecione os alarmes e clique em **Acknowledge**. Para verificar o histórico de alarmes selecione **Fault → Browse History Alarms** e selecione os equipamentos desejados. Em seguida clique no botão com duas setas (vermelho). O histórico de alarmes de todas as severidades será mostrado. Os resultados podem ser filtrados e para visualizar detalhes do alarme clicar em cima do alarme específico.

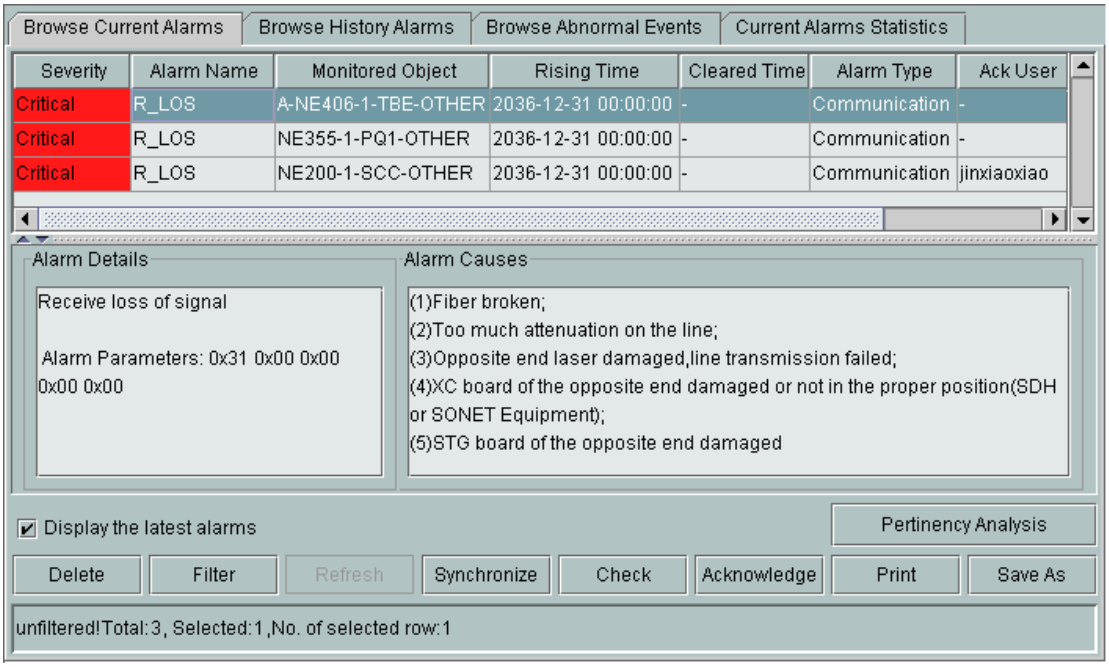


Figura 34 – Janela de alarmes e eventos

A janela **Browse Perfomance** (Fig. 35) permite a visualização de dados da performance atual e histórica, além da visualização de eventos e quedas de performance inferiores aos limites mínimos estipulados. Para abrir a janela selecione no Menu principal **Performance → Browse SDH Perfomance**.

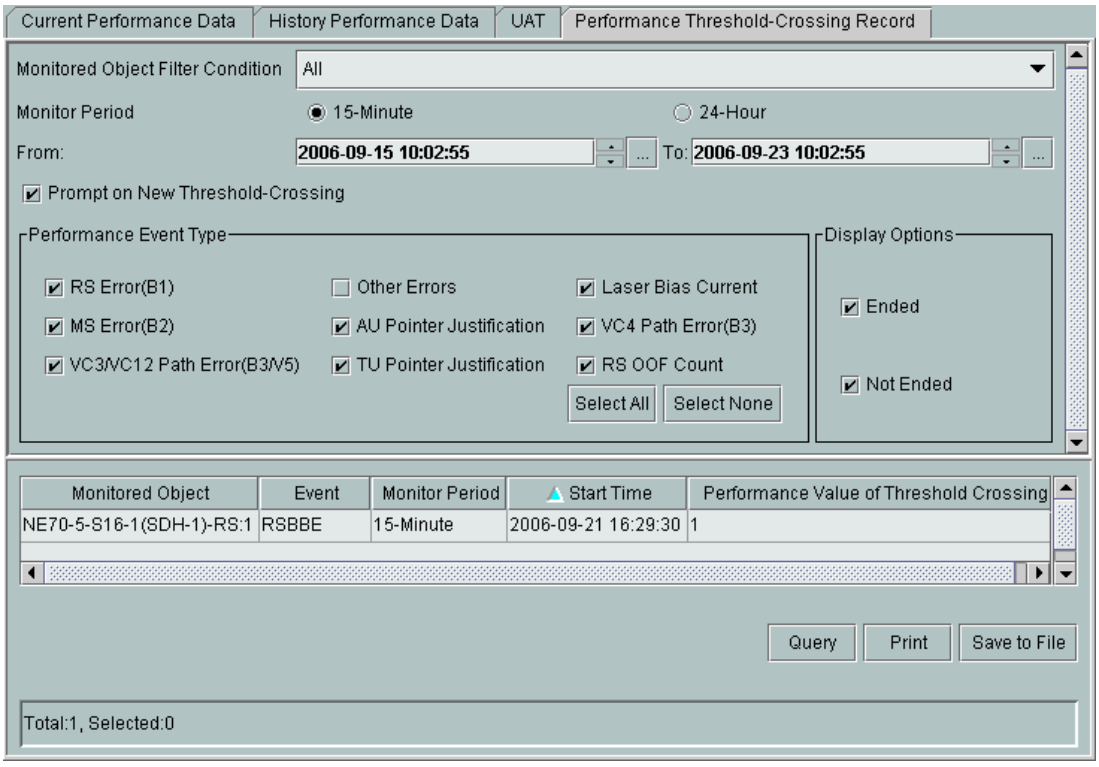


Figura 35 – Janela de monitoramento de performance

Selecione uma ou mais portas no painel à esquerda e clique no botão com duas setas (vermelho). O período de monitoramento pode ser escolhido entre 15 minutos e 24 horas. Em

seguida, selecione um tipo de evento de desempenho. Os tipos de eventos variam com o tipo de placa e de porta. Clique em **Query**.

Criação de topologias

Equipamentos de rede, fibras e cabos só podem ser gerenciados pelo sistema de gerência T2000 após a criação das suas topologias. A topologia se refere a uma operação de objeto correspondente ao equipamento físico. Quando uma topologia é criada, o sistema de gerência configura a comunicação com o equipamento físico da rede. Quando os dados dos equipamentos são descarregados no T2000, a topologia apresenta a mesma informação que o equipamento físico possui. Depois disso, o equipamento e a configuração de placas no T2000 é enviado diretamente aos equipamentos físicos. O software é capaz de gerenciar as seguintes topologias: equipamentos de rede, portas, placas, canais, fibras, subredes, cabos Ethernet, e cabos e portas seriais. Através dessas topologias, o T2000 consegue obter informações ou o estado dos objetos correspondentes na rede física. A subrede, o cabo Ethernet e o cabo serial são conceitos somente lógicos.

Cada equipamento de rede da série OptiX é representado como um equipamento no T2000. Antes de gerenciar o equipamento é necessário criar seu correspondente no sistema de gerência. O equipamento de rede que se comunica diretamente com o sistema de gerência pela rede é chamado de ***gateway network equipment*** (GNE). Todos os outros equipamentos que precisam se comunicar com o sistema de gerência através do gateway são chamados de ***non-gateway* NE**. O GNE se comunica com o T2000 utilizando um protocolo de comunicação. O GNE é a rota de comunicação indispensável para que o T2000 gerencie a rede. Cada T2000 pode se comunicar com o mínimo de um GNE e um máximo de 100 GNEs.

Para criar um equipamento de rede no T2000 clique com o botão direito em um espaço vazio na janela *Main Topology* e selecione **Create → Topology Object**. Uma caixa chamada **Create Topology Object** (Fig. 36) irá aparecer. Escolha o tipo de equipamento na árvore de tipos de objeto. Complete a informação de **ID**, **Extended ID**, **Name** e **Remarks**. Para criar um GNE, escolha **Gateway** em **Gateway Type** e escolha o tipo de protocolo como IP. Já para a criação de um *non-gateway* NE é necessário escolher o equipamento *gateway* ao qual este equipamento está afiliado no campo **Affiliated Gateway.**

Attribute	Value
Type	OptiX OSN 3500
ID	355
Extended ID	9
Name	NE355
Remarks	OSN 3500
Gateway Type	Gateway
Protocol	IP
IP Address	129.9.1.99
Port	1400
NE User	root
Password	******
NE Preconfiguration	☐ Yes

Figura 36– Criando um objeto de topologia

Configuração

Após a criação de um equipamento, ele ainda não se encontra configurado. Para configurá-lo, faça um clique duplo no equipamento não configurado na janela *Main Topology* e

a caixa **NE Configuration Wizard** aparecerá. Escolha a opção **Upload** e clique em **Next**. Uma mensagem informará que o *upload* pode demorar um longo tempo. Clique em OK para iniciar o processo e aguarde o término.

Para criar a comunicação de informações entre o T2000 e os equipamentos, assim como a comunicação entre os equipamentos, os cabos de comunicação devem ser criados permitindo o T2000 gerenciar os equipamentos da rede.

Através da ferramenta de busca de fibra, o usuário pode verificar se uma determinada interface óptica está conectada com uma fibra. Dessa forma, o usuário pode criar rapidamente uma fibra para essa interface no T2000. Para uma rede recentemente criada, após a configuração das placas, todas as interfaces ópticas podem ser achadas e as fibras podem ser criadas. O estado das fibras pode ser verificado em tempo real.

Selecione, no Menu principal, **File → Search for Fiber/Cable**. No painel esquerdo, selecione as portas de um ou mais equipamentos de rede e clique em **Search** para procurar por fibras ou cabos. Uma barra de progresso informará o status da pesquisa e uma caixa aparecerá indicando o sucesso da operação. Clique **Close** e selecione as fibras da lista **Current fiber link** e clique em **Create Fiber/Cable**.

3 DESCRIÇÃO DOS EXPERIMENTOS

3.1 DESCRIÇÃO EXPERIMENTO 1

O documento completo relativo ao experimento nº 1 encontra-se no **ANEXO I.**

O experimento nº 1 se refere ao sistema de gerência e pretende familiarizar o aluno com a operação do *software* de gerência e realização de configurações básicas na rede SDH. Normalmente cada fabricante de equipamentos de rede produz seu próprio software de gerência baseado na enorme capacidade de monitoramento e gerenciamento que as redes SONET/SDH oferecem em sua arquitetura. O laboratório dispõe do *software* de gerência iManager T2000 Huawei compatível com os equipamentos SDH presentes.

As principais funcionalidades do sistema de gerência são descritas em um modelo passo-a-passo e um exemplo real é apresentado no final do experimento. O experimento, porém, não possui a intenção de cobrir todos os pontos e todas as operações disponíveis no sistema. Após a conclusão do experimento, o aluno deve ser capaz de buscar informações sobre status de interfaces, interpretar e liberar alarmes, estabelecer enlaces, configurar esquemas de proteção e configurar serviços SDH/PDH. O tempo de execução estimado do experimento é de 03h00min devido à sua extensão e devido ao primeiro contato que o usuário terá com o sistema de gerência. Como mencionado anteriormente, este experimento difere dos outros dois experimentos por ter um caráter puramente explanatório. Ele consiste somente de um guia de operações do sistema de gerência seguido de um exemplo prático.

Uma sugestão de uso do laboratório é a utilização de quatro estações equipadas com a versão cliente do sistema de gerência e a divisão dos alunos em quatro grupos de três integrantes, cada um trabalhando paralelamente em cada nó SDH.

3.2 DESCRIÇÃO EXPERIMENTO 2

O documento completo relativo ao experimento nº 2 encontra-se no **ANEXO II.**

O experimento nº2 trata do uso do GFP em redes SONET/SDH. Após a execução do experimento nº1 o aluno estará habilitado a realizar a configuração no sistema de gerência da topologia em anel utilizada no experimento nº2 e realizar todas as configurações necessárias. Durante a execução do experimento nº2 a configuração do uso do GFP para o transporte de quadros Ethernet pelo anel SDH é explorada. Apesar do laboratório não dispor de uma ferramenta geradora de tráfego Ethernet e de equipamentos GFP, o experimento foca no funcionamento do GFP e na verificação de conectividade entre as estações com placas de rede FastEthernet através da rede SDH. Dada a limitação imposta pela falta de um gerador de tráfego Ethernet, o protocolo ICMP (*Internet Control Message Protocol*) será responsável por verificar a conectividade entre as estações. A principal vantagem do GFP, que é a eficiência no transporte de sinais Ethernet em quadros SDH, não pode ser verificada devido às limitações mencionadas. O volume de dados gerado pelo comando *ping* é muito pequeno para verificar realmente a grande capacidade de multiplexação de quadros cliente Ethernet na rede SONET/SDH que utiliza o GFP.

Uma sugestão de uso do laboratório para este experimento é a utilização de três estações equipadas com a versão cliente do sistema de gerência e a divisão dos alunos em três grupos de três integrantes, cada um trabalhando paralelamente em cada nó SDH.

A parte prática do experimento se inicia com cinco perguntas da seção IV do pré-relatório:

Questões:

1. Explique a finalidade dos contêineres e de que forma eles são utilizados em uma rede SONET/SDH.

2. Esquematize a estrutura do quadro de um sinal STS-48 (STM-16).

3. Explique a função de cada equipamento SONET/SDH e exemplifique o uso de ADMs, TMs, e DCSs em redes metropolitanas.

4. De que maneira o tráfego Ethernet é transportado em uma rede SONET/SDH que utiliza GFP? E como seria transportado sem o uso do GFP?

5. Explique detalhadamente os dois modos de mapeamento de *payload* do GFP. Exemplifique.

As perguntas do pré-relatório têm como função consolidar a fundamentação teórica apresentada na seção II do documento. Elas estão relacionadas aos principais tópicos da introdução teórica e são essenciais para o entendimento do uso do GFP na rede SDH e para o entendimento da maneira na qual os dados de um cliente são transportados pela rede de alta velocidade.

Após o pré-relatório, o procedimento localizado na seção V deve ser executado. O tempo de execução estimado do experimento é de 02h00min e os seguintes materiais e ferramentas são utilizados:

- Três nós SDH.
- Seis interfaces STM-64.
- Duas interfaces de tributário FastEthernet com GFP.
- Atenuadores variáveis.
- Cordões ópticos e cabos UTP Cat5e.
- Sistema de gerência iManager T2000.
- Dois computadores com interfaces de rede FastEthernet.

Primeiramente, a topologia em anel unidirecional com duas fibras deve ser criada e configurada. Isso inclui a conexão física das fibras às interfaces STM-64 e a configuração dos nós e enlaces no sistema de gerência. O nível de potência na saída da interface STM-64 é bastante elevado e deve ser atenuado por meio de um atenuador variável. A potência do sinal recebida pode ser verificada pelo sistema de gerência e alarmes serão gerados se a potência de entrada for muito alta. A fibra que transporta o tráfego no sentido horário deve ser definida como a fibra de trabalho e a fibra restante como a fibra de proteção do sistema.

Em seguida, conectar a primeira estação munida de uma placa de rede FastEthernet à interface FastEthernet do nó SDH 1. O mesmo procedimento deve ser feito para a segunda estação e o nó SDH 2 conforme Figura 37. Verificar que a rede está operando normalmente e os quadros estão sendo transportados sem nenhum *payload* GFP (O GFP ainda não foi configurado) nas fibras de trabalho. Verificar também que não há tráfego nas fibras de proteção. Isso pode ser verificado na seção de alarmes do sistema de gerência como um aviso de baixa importância indicando que os quadros estão sendo recebidos e transportados vazios.

Após assegurar-se que a rede SDH está funcionando corretamente, definir o endereço IP da estação A como 192.168.1.1 e a máscara de sub-rede como 255.255.255.0. Definir o endereço IP da estação B como 192.168.1.2 e a máscara de sub-rede como 255.255.255.0. Dessa maneira, ambas as estações estarão na mesma sub-rede. Em seguida, abrir o *prompt* de comando da estação A e executar o seguinte comando: ping 192.168.1.2. O protocolo disparará

três pacotes *echo request* de controle para a estação B e esperará por três pacotes *echo reply*. Se o transporte de ida e volta pela rede SDH for bem sucedida, o resultado do comando *ping* deve obter sucesso e mostrar detalhes do tempo total de ida e volta dos três pacotes (*Round Trip Time*- RTT). Anotar estes valores e repetir o processo para a estação B. Como a rede SONET/SDH é baseada em circuitos e não há atrasos de filas, os tempos RTT devem ser constantes neste cenário.

Por último deve-se ativar e configurar o GFP nas interfaces FastEthernet dos equipamentos SDH através do sistema de gerência e repetir o teste de conectividade. Antes de executar o comando *ping* assegurar-se que a rede está operando normalmente.

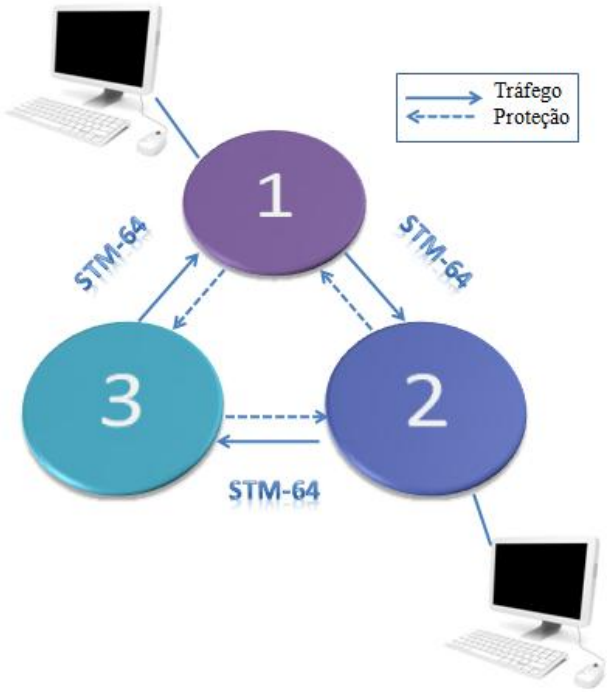


Figura 37 – Topologia SDH em anel unidirecional com duas fibras e três nós

Após a execução de todos os passos descritos, o aluno deve construir um relatório descrevendo detalhadamente quais foram os resultados obtidos nos procedimentos. Eventuais falhas ocorridas devem ser relatadas e os seguintes pontos devem estar bem citados e explicados no relatório:

- Captura da tela da topologia operante no sistema de gerência.
- Captura da tela com os resultados do comando *ping* sem o GFP ativo e com o GFP ativo.
- Explicação da maneira na qual o quadro Ethernet contendo o protocolo ICMP foi encapsulado e transportado no caso em que usou o GFP e no caso em que o GFP não foi utilizado.
- Devido a algumas limitações de equipamentos, o cenário elaborado no laboratório não permitiu explorar a verdadeira vantagem do GFP. Para tal, muitos usuários FastEthernet deveriam ser conectados à rede SDH e terem seus dados mapeados em quadros GFP. Explique qual seria a diferença, neste caso, se não fosse utilizado o GFP.

3.3 DESCRIÇÃO EXPERIMENTO 3

O documento completo relativo ao experimento nº 3 encontra-se no **ANEXO III.**

O experimento nº 3 explora a importante robustez de redes SONET/SDH em relação a falhas e habilitará o aluno a configurar e verificar a resposta automática da rede SDH diante de uma falha provocada manualmente em uma interface óptica. Assim como o experimento nº2, uma topologia de três nós deve ser estabelecida e devidamente configurada como um anel unidirecional com duas fibras. Os parâmetros de APS também devem ser configurados. Durante o experimento, deseja-se que seja verificado pelo sistema de gerência, o envio de quadros SDH sem nenhum *payload* uma vez que o laboratório não dispõe de equipamentos que geram tráfegos tributários. A aparição de alarmes (originados pelo cabeçalho SDH) de baixa importância alertando sobre recepção de quadros vazios e o alarme de alta importância de perda de sinal (LOS) também deve ser verificada. Após o restabelecimento do laser da interface desligada, a verificação do retorno ao modo de operação normal da rede SDH deve ser constatada devido ao acionamento automático da comutação automática de proteção (APS) previamente configurada.

Uma sugestão de uso do laboratório para este experimento é a utilização de três estações equipadas com a versão cliente do sistema de gerência e a divisão dos alunos em três grupos de três integrantes, cada um trabalhando paralelamente em cada nó SDH.

A parte prática do experimento se inicia com as cinco perguntas a seguir extraídas da seção IV do pré-relatório:

Questões:

1. Cite e explique os diferentes tipos de comutação automática de proteção (APS) linear existentes.
2. Qual tipo de proteção em anel utiliza melhor a largura de banda disponível? Por quê?
3. Explique a diferença entre proteção de *span* e proteção de anel.
4. Explique sucintamente as vantagens e as desvantagens das diversas topologias de proteção em anel.
5. Seguindo o modelo das Figuras 16 e 17, desenhe o diagrama temporal e ilustre os estados dos bytes K1 e K2 para o caso de uma corte na fibra de proteção de um anel bidirecional de quatro fibras com quatro nós (N1, N2, N3 e N4). Assuma que a falha tenha ocorrido entre o nó 1 e o nó 2.

As perguntas do pré-relatório têm como função consolidar a fundamentação teórica apresentada na seção II do documento. As questões exploram a parte de APS linear, APS em anel, uso da largura de banda em anéis e o estado dos bytes K1 e K2 localizados no cabeçalho de linha que são responsáveis pela troca de informações APS.

Após o pré-relatório, o procedimento localizado na seção V deve ser executado. O tempo de execução estimado do experimento é de 02h00min e os seguintes materiais e ferramentas são utilizados:

- Três nós SDH.
- Seis interfaces STM-64.
- Atenuadores variáveis.
- Cordões ópticos.
- Sistema de gerência iManager T2000.

Primeiramente, a topologia em anel unidirecional com duas fibras (Fig. 38) deve ser criada e configurada. Isso inclui a conexão física das fibras às interfaces STM-64 e a configuração dos nós e enlaces no sistema de gerência. O nível de potência na saída da interface STM-64 é bastante elevado e deve ser atenuado por meio de um atenuador variável. A potência do sinal recebida pode ser verificada pelo sistema de gerência e alarmes serão gerados se a potência de entrada no equipamento for muito alta. A fibra que transporta o tráfego no sentido horário deve ser definida como a fibra de trabalho e a fibra restante como a fibra de proteção do sistema.

O APS deve ser configurado em todos os nós da rede como uma topologia unidirecional com duas fibras. O APS deve ser configurado, também, para comutar o tráfego da fibra de proteção para a fibra de trabalho assim que o estado de perda de sinal for removido e o parâmetro de *Wait-To-Restore* (WTR) deve ser reduzido do seu padrão de cinco minutos para um minuto.

Verificar pelo sistema de gerência que a rede está operando normalmente e os quadros estão sendo transportados sem nenhum *payload* e que não há tráfego no enlace de proteção. Isso pode ser verificado na seção de alarmes do sistema de gerência como um aviso de baixa importância indicando que os quadros estão sendo recebidos e transportados vazios.

Criar um ponto de falha, pelo sistema de gerência, desativando-se o laser da interface STM-64 ativa da fibra de trabalho do nó 1. Para tal, clique em **Window** selecione **NE Information List**. Clique com o botão direito no NE e selecione **NE Explorer**. Em seguida, selecione uma placa e clique em **Configuration→ SDH Interface** na árvore de funções. No botão tipo rádio, selecione a opção **By Board/Port(Channel)**. Escolha **Port** na lista dê um clique duplo no campo **Laser Switch**, e clique em **Close**. Selecione **Apply** e uma mensagem de aviso de interrupção de serviços aparecerá. Clique em **OK**.

Confirmar pela aparição de alarmes no sistema de gerência que foi detectada a perda de sinal (LOS) na fibra de trabalho entre nó 1 e nó 2 e observar se ocorre a comutação automática de proteção da fibra de trabalho para a fibra de proteção como previamente configurado. Os quadros transportados anteriormente pelo STM-64 (nó 1→nó 2) devem utilizar o caminho de proteção 1-3-2 para sair do nó 1 e chegar ao nó 2.

Novamente através do sistema de gerência, reativar o laser da interface STM-64 e verificar se ocorre a comutação do tráfego da fibra de proteção para a fibra de trabalho devido à expiração do tempo WTR previamente configurado como um minuto. Esse tempo deve ser medido para ser comparado posteriormente no relatório ao tempo configurado.

Verificar o restabelecimento da operação normal da rede pelo sistema de gerência e verificar se a fibra de trabalho que interliga a interface STM-64 do nó 1 à interface STM-64 do nó 2 está transportando novamente os quadros sem *payload* e se não há nenhum tipo de tráfego na fibra de proteção.

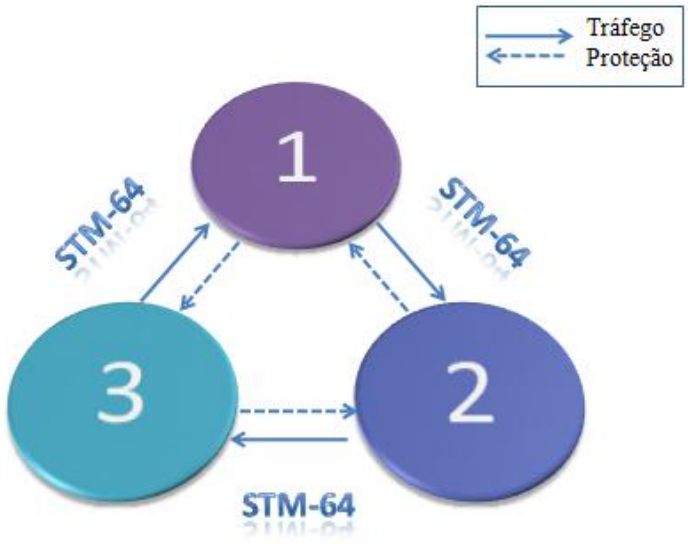


Figura 38 – Topologia SDH de anel unidirecional
com duas fibras e três nós

Após a execução de todos os passos descritos acima, o aluno deve construir um relatório descrevendo detalhadamente quais foram os resultados obtidos durante a execução do experimento. Eventuais falhas ocorridas devem ser relatadas e os seguintes pontos devem estar bem citados e explicados no relatório:

- Captura da tela da topologia operante no sistema de gerência.
- Descrição detalhada dos alarmes gerados e seus respectivos significados no sistema de gerência.
- Explicação da maneira no qual se comportaram os bytes K1 e K2 durante o experimento para todos os nós da rede SDH.
- Verificação do tempo medido com o tempo configurado do WTR.

4 CONCLUSÃO

O conhecimento das redes SONET/SDH e seus mecanismos de adaptação ao transporte de dados na forma de pacotes é de fundamental importância no campo das redes de transporte de alta velocidade. Este trabalho permitiu o contato teórico e prático com o sistema de proteção nativo das redes SONET/SDH e a tecnologia GFP, padronizada pelo ITU-T G.7041, para possibilitar o melhor aproveitamento dos canais SONET/SDH no transporte de dados do usuário na forma de pacotes. Além disso, o monitoramento e gerenciamento, que é uma característica que torna as redes SONET/SDH uma escolha atraente em redes WAN, foi demonstrado.

O trabalho teve como proposta inicial a de colocar em funcionamento e em completa operação o laboratório de redes ópticas. Entretanto, algumas interfaces dos equipamentos SONET/SDH e WDM ainda não estão disponíveis na quantidade necessária para a execução correta dos experimentos e no caso do experimento nº2, o módulo GFP precisa ser incorporado nas interfaces FastEthernet. Considerando que estes fatores influenciam diretamente a execução das práticas laboratoriais, os experimentos foram elaborados de maneira a assumir que todos estes componentes estejam disponíveis e em perfeito funcionamento.

REFERÊNCIAS

[1] FILHO, Huber B. *Tutorial redes SDH* (2009). Disponível em: < http://www.teleco.com.br/tutoriais/tutorialrsdh/default.asp> Acesso em: 12 de dezembro de 2009.

[2] GORALSKI, Walter J. *SONET/SDH*, Third edition (2002).

[3]PERROS, Harry. *Connection-Oriented Networks* (2005). Disponível em: <http://www4.ncsu.edu/~hp/Chapter2.pdf> Acesso em: 15 de novembro de 2009.

[4] Recomendação ITU-T G.707/Y.1322 (2007) *Network node interface for the synchronous digital hierarchy (SDH).*

[5] Recomendação ITU-T G.810 (1996) *Definitions and terminology for synchronization networks*

[6] Recomendação ITU-T G.803 (2000) *Architecture of transport networks based on the synchronous digital hierarchy (SDH).*

[7] Recomendação ITU-T G.841 (1998) *Types and characteristics of SDH network protection architectures.*

[8] BERNSTEIN, Greg; RAJAGOPALAN Bala; SAHA Debanjan, *Optical Network Control Architecture Protocols and Standards* (2003).

[9] Recomendação ITU-T G.7041/Y.1303 (2005) *Generic Frame Procedure (GFP).*

[10] *Huawei Selected Collections of Maintenance Documentation for Huawei Optical Network Products*, Manual de operação e manutenção de equipamentos ópticos Huawei.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Experimento nº1

Sistema de gerência iManager T2000 Huawei

Anexo I

I. OBJETIVO

Familiarização com o sistema de gerência iManager T2000 Huawei e operações básicas de configuração e monitoramento de uma rede SDH.

II. INTRODUÇÃO

O sistema de gerência é uma ferramenta responsável por monitorar e gerenciar os equipamentos da rede garantindo seu funcionamento normal. Através da ferramenta, é possível visualizar a topologia da rede, os alarmes, os estados e configurar remotamente diversas funcionalidades dos equipamentos. O laboratório está equipado com o software de gerência iManager T2000 Huawei.

III. PROCEDIMENTOS [1]

Inicialização

O T2000 utiliza uma arquitetura cliente-servidor e um modo multiusuário padrão. A senha de usuário do Windows XP é: 123 + (SHIFT+123) + abc. Para inicializar o programa, primeiramente deve-se iniciar o banco de dados SQL. Clique com o botão direito do mouse no ícone na barra do Windows, localizada no canto inferior direito da área de trabalho, e selecione **Start**. Em seguida, o servidor T2000 deve ser iniciado. Duplo clique no ícone **T2000 Server** localizado na área de trabalho. O nome de usuário padrão é **admin** e a senha padrão é **T2000** (Fig. 1). O campo **Server** deve ser preenchido como **Local.** Aguarde alguns instantes até que os serviços **Ems Server**, **Schedulesrv Server**, **Security Server**, **Syslog Agent**, **Topo Server**, **Database Server Process**, e **Toolkit Server** estejam com o status **Running.**

Figura 1 – Login

Uma vez que o servidor estiver completamente operacional, clique no ícone **T2000 Client** na área de trabalho para executar a versão cliente do software. O nome de usuário e a senha são por padrão **admin** e **T2000** respectivamente.

Antes de desligar o servidor é necessário sair do cliente. No cliente, clique em **File →Exit** no Menu principal e clique **OK**. No servidor, clique em **System → Shutdown System** para fechar o T2000 Server.

Janelas

A interface principal e padrão do cliente T2000 é a janela **Main Topology** (Fig.2). Todas as funções de gerenciamento de topologia podem ser acessadas a partir dessa janela. Essas funções incluem a criação de objetos da topologia, subredes, fibras, cabos e a procura de equipamentos existentes na rede. Para ir para a visualização da janela *Main topology*, selecione **Window → Main Topology** no Menu principal.

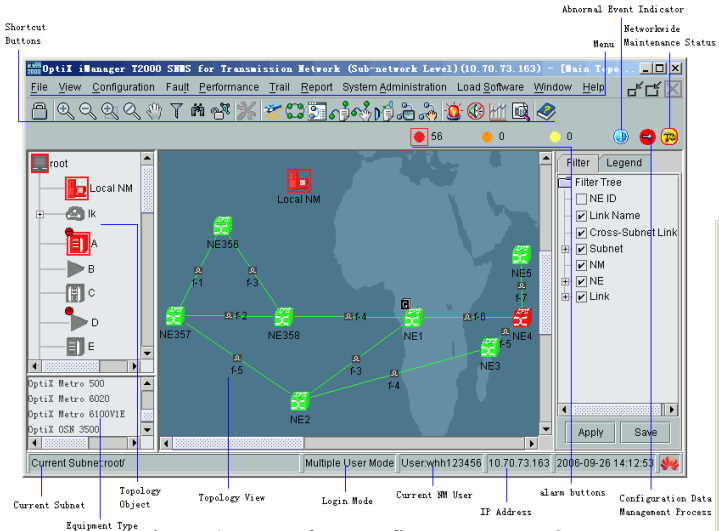


Figura 2 – Interface gráfica *Main Topology*

A janela **NE Explorer** (Fig. 3) é a principal janela utilizada para gerenciar equipamentos OptiX. Nessa janela, o usuário é capaz de configurar, gerenciar e manter individualmente o equipamento de rede. O NE Explorer contém uma árvore de funções (*Function Tree*) que facilita bastante as operações. Para visualizar uma janela de configuração de um determinado objeto, o usuário pode selecionar o objeto e selecionar a função desejada na árvore de funções. Para visualizar o SDH NE Explorer, clique com o botão direito em um equipamento de rede na *Main topology* e escolha NE Explorer no Menu.

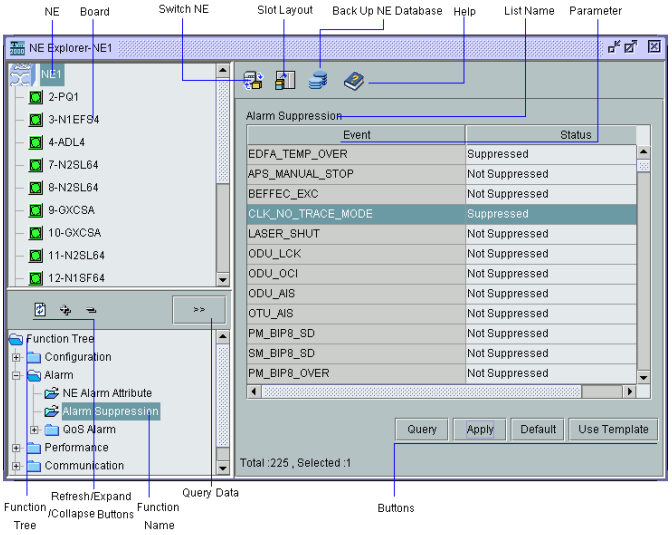


Figura 3 - Janela NE *Explorer*

A janela **Protection View** (Fig. 4) permite a procura, visualização, configuração e o gerenciamento da subrede de proteção assim como o gerenciamento de NNIs dos nós independentes. Para abrir a janela **Protection View** selecione **ConFig.tion → Protection View** no Menu principal.

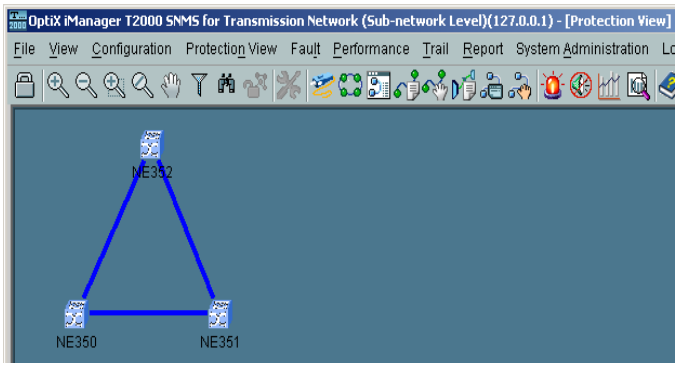


Figura 4 – Janela *Protection View*

A janela **Trail View** (Fig. 5) possibilita a procura, criação, configuração, e gerenciamento das funções de trilhas (*trails*). Para visualizar a Trail View selecione **Trail → Trail View** no Menu principal.

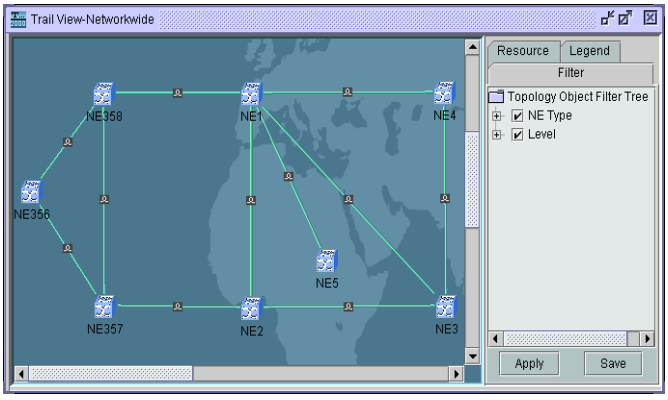


Figura 5 – Janela *Trail View*

Para configurar o relógio dos equipamentos da rede, fazer buscas de status da sincronização do relógio na rede, rastrear os relógios e executar outras funções de busca, a janela **Clock View** é utilizada. Para abrir esta janela selecionar no Menu principal **Configuration → Clock View** (Fig. 6).

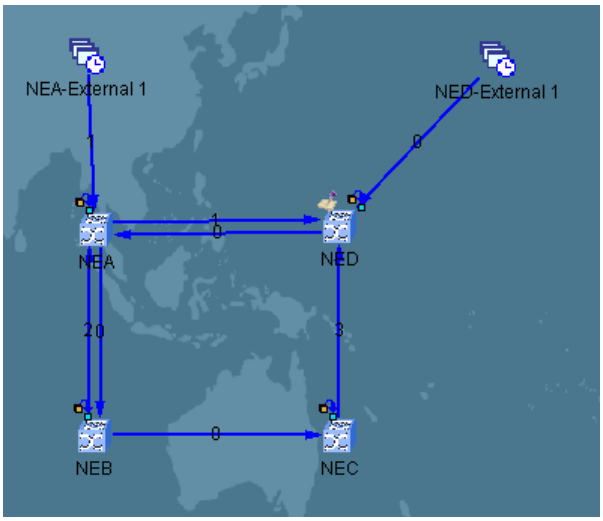


Figura 6 – Janela *Clock View*

A janela **SDH NE Panel** (Fig. 7) permite a visualização de placas e portas em diferentes cores que dependem do status atual em que se encontram. No T2000, a maior parte das operações de configuração de equipamento, monitoramento e manutenção são feitas através desta janela. Para abrir a janela *NE Panel*, dê dois cliques no equipamento de rede desejado. Para adicionar uma placa a um *slot* vazio, basta clicar com o botão direito no *slot* e escolher o tipo de placa.

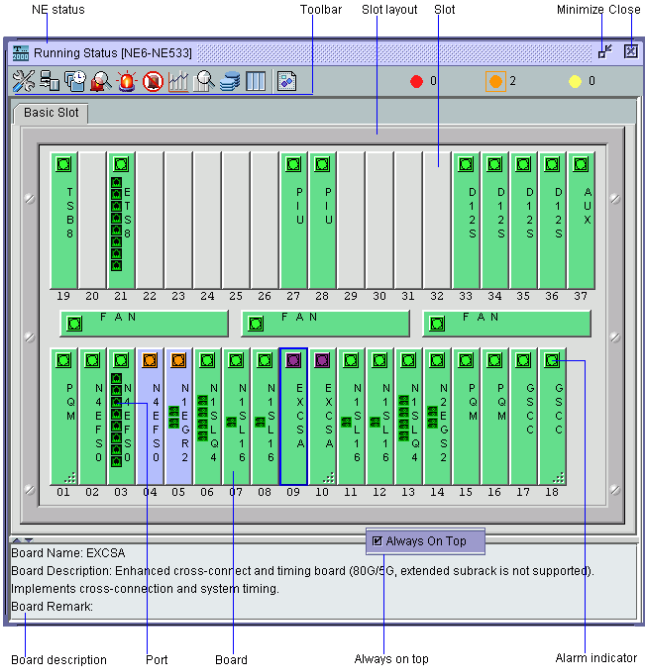


Figura 7 – Janela NE *Panel*

O ultimo ícone  a direita na barra de ferramentas permite visualizar a legenda como na Figura 8.

Legend	Description
	Not Installed
	Installation State
	Running&Uninstalled
	Running&Installed
	Fixed State
	Physical Board
	Critical Alarm
	Major Alarm
	Minor Alarm
	Warning Alarm
	Non-Alarmed
	Bidirectional Optical Port
	Ethernet Port
	Unidirectional Optical Port
	Protection Board Status
	Tributary/Line Loopback
	Resource Division

Figura 8 - Legenda

A visualização de alarmes atuais e a visualização do histórico de alarmes são possíveis através da janela **Browse Alarm and Event Window** (Fig. 9). Eventos anormais ,assim como estatísticas de alarmes, também podem ser verificados. Essa janela oferece botões como a analise estática de correlação, filtro, atualização e sincronização que permitem localizar rapidamente a causa do alarme. Para a visualização dos alarmes, clique no Menu principal em **Fault → Browse Current Alarms, Fault → Browse History Alarms, Fault → Browse Abnormal Events** ou em **Fault → Browse Alarms Statistics.**

Para verificar automaticamente os últimos alarmes marque a caixa **Auto Refresh**. Selecione o alarme e seus detalhes aparecerão na tela. Para reconhecer o alarme, selecione os alarmes e clique em **Acknowledge**. Para verificar o histórico de alarmes selecione **Fault → Browse History Alarms** e selecione os equipamentos desejados. Em seguida clique no botão com duas setas

(vermelho). O histórico de alarmes de todas as severidades será mostrado. Os resultados podem ser filtrados e para visualizar detalhes do alarme clicar em cima do alarme específico.

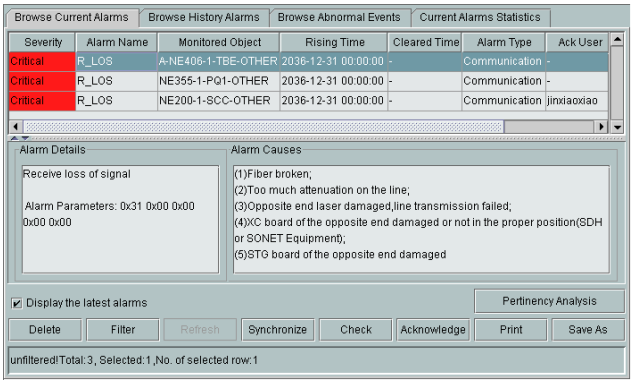


Figura 9 – Janela de alarmes e eventos

A janela **Browse Performance** (Fig. 10) permite a visualização de dados da performance atual e histórica, além da visualização de eventos e quedas de performance inferiores aos limites mínimos estipulados. Para abrir a janela selecione no Menu principal **Performance → Browse SDH Perfomance**.

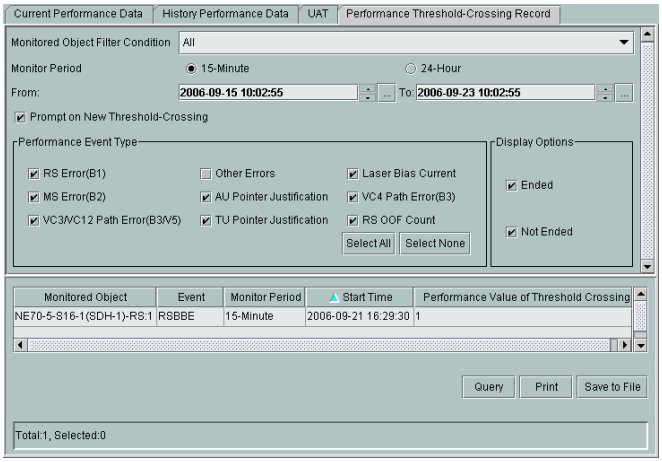


Figura 10 – Janela de monitoramento de performance

Selecione uma ou mais portas no painel à esquerda e clique no botão com duas setas (vermelho). O período de monitoramento pode ser escolhido entre 15 minutos e 24 horas. Em seguida, selecione um tipo de evento de desempenho. Os tipos de eventos variam com o tipo de placa e de porta. Clique em **Query**.

Criando topologias

Equipamentos de rede, fibras e cabos só podem ser gerenciados pelo sistema de gerência T2000 após a criação das suas topologias. A topologia se refere a uma operação de objeto correspondente ao equipamento físico. Quando uma topologia é criada, o sistema de gerência configura a comunicação com o equipamento físico da rede. Quando os dados dos equipamentos são descarregados no T2000, a topologia apresenta a mesma informação que o equipamento físico possui. Depois disso, o equipamento e a configuração de placas no T2000 é enviado diretamente aos equipamentos físicos. O software é capaz de gerenciar as seguintes topologias: equipamentos de rede, portas, placas, canais, fibras, subredes, cabos Ethernet, e cabos e portas seriais. Através dessas topologias, o T2000 consegue obter informações ou o estado dos objetos correspondentes na rede física. A subrede, o cabo Ethernet e o cabo serial são conceitos somente lógicos.

Cada equipamento de rede da série OptiX é representado como um equipamento no T2000. Antes de gerenciar o equipamento é necessário criar seu correspondente no sistema de gerência. O equipamento de rede que se comunica diretamente com o sistema de gerência pela rede é chamado de ***gateway network equipment*** (GNE). Todos os outros equipamentos que precisam se comunicar com o sistema de gerência através do gateway são chamados de ***non-gateway*** **NE**. O GNE se comunica com o T2000 utilizando um protocolo de comunicação. O GNE é a rota de comunicação indispensável para que o T2000 gerencie a rede. Cada T2000 pode se comunicar com o mínimo de um GNE e um máximo de 100GNEs.

Para criar um equipamento de rede no T2000 clique com o botão direito em um espaço vazio na janela *Main topology* e selecione **Create → Topology Object**. Uma caixa chamada **Create Topology Object** (Fig. 11) irá aparecer. Escolha o tipo de equipamento na árvore de tipos de objeto. Complete a informação de **ID**, **Extended ID**, **Name** e **Remarks**. Para criar um GNE, escolha **Gateway** em **Gateway Type** e escolha o tipo de protocolo como IP. Já para a criação de um *non-gateway* NE é necessário escolher o equipamento *gateway* ao qual este equipamento está afiliado no campo **Affiliated Gateway.**

Attribute	Value
Type	OptiX OSN 3500
ID	355
Extended ID	9
Name	NE355
Remarks	OSN 3500
Gateway Type	Gateway
Protocol	IP
IP Address	129.9.1.99
Port	1400
NE User	root
Password	******
NE Preconfiguration	☐ Yes

Figura 11 – Criando um objeto de topologia

Configuração

Após a criação de um equipamento, ele ainda não se encontra configurado. Para configurá-lo, faça um clique duplo no equipamento não configurado na janela *Main topology* e a caixa **NE Configuration Wizard** aparecerá. Escolha a opção **Upload** e clique em **Next**. Uma mensagem informará que o *upload* pode demorar um longo tempo. Clique em OK para iniciar o processo e aguarde o término.

Para criar a comunicação de informações entre o T2000 e os equipamentos, assim como a comunicação entre os equipamentos, os cabos de comunicação devem ser criados permitindo o T2000 gerenciar os equipamentos da rede.

Através da ferramenta de busca de fibra, o usuário pode verificar se uma determinada interface óptica está conectada com uma fibra. Dessa forma, o usuário pode criar rapidamente uma fibra para essa interface no T2000. Para uma rede recentemente criada, após a configuração das placas, todas as interfaces ópticas podem ser achadas e as fibras podem ser criadas. O estado das fibras pode ser verificado em tempo real.

Selecione, no Menu principal, **File → Search for Fiber/Cable**. No painel esquerdo, selecione as portas de um ou mais equipamentos de rede e clique em **Search** para procurar por fibras ou cabos. Uma barra de progresso informará o status da pesquisa e uma caixa aparecerá indicando o sucesso da operação. Clique **Close** e selecione as fibras da lista **Current fiber link** e clique em **Create Fiber/Cable**.

Exemplo

Este exemplo descreve como configurar serviços SDH/PDH para o equipamento OptiX 2500 no sistema de gerência OptiX iManager T2000 no cenário descrito a seguir.

Uma cidade necessita que uma rede de comunicações seja construída entre A, B, C, D e E. A Tabela 1 lista os serviços requisitados.

NE	Descrição do serviço	Proteção	Distância
A	**32x E1 com B** **31x E1 com C** **32x E1 com D**	**Proteção no nível de rede**	**25 km de B** **40 km de D**
B	**32x E1 com A**	**Proteção no nível de rede**	**25 km de A** **25 km de C**
C	**31x E1 com A** **32x E1 com E**	**Proteção no nível de rede**	**35 km de B** **30 km de D**
D	**32x E1 com A** **31x E1 e 3x E3 com E**	**Proteção no nível de rede**	**40 km de A** **30 km de C** **80 km de E**
E	**32x E1 com C** **31x E1 e 3x E3 com D**	**Proteção no nível de rede não requerida**	**80 km de D**

Tabela 1- Exemplo de serviços requeridos

A Figura 12 ilustra cinco equipamentos OptiX 2500 formando um anel bidirecional de proteção da seção de multiplexação (*multiplex section protection* - MSP) com duas fibras e utilizando interfaces STM-16. Um segmento sem proteção utilizando interfaces STM-4 também está presente na rede. Os equipamentos NE1, NE2, NE3, NE4 estão no anel. O NE5 está no segmento linear e o NE1 é o GNE.

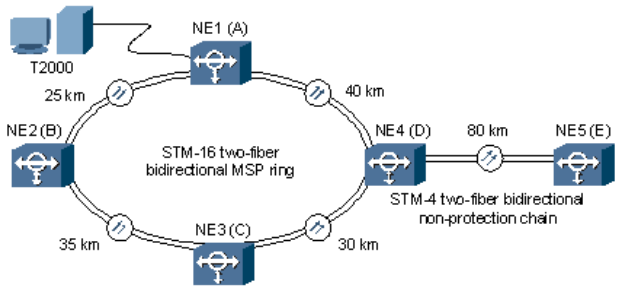


Figura 12- Topologia de rede

Um esquema de alocação de endereços IP é definido na Figura 13:

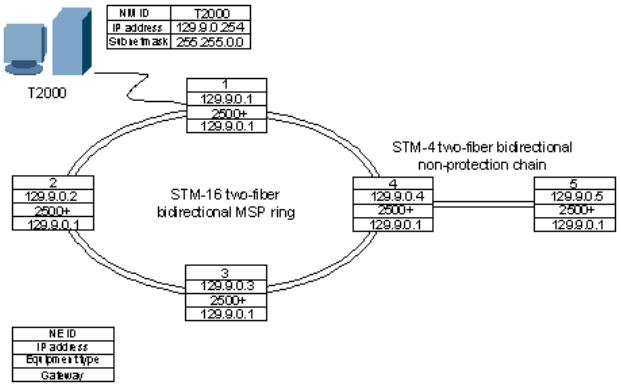


Figura 13 – Alocação de endereços

A primeira linha se refere à identificação, a segunda linha ao endereço IP, terceira linha ao tipo de equipamento e a última linha ao endereço IP do *gateway*.

Após fazer o *login* no T2000, criar o NE1 como GNE na *Main topology* com os seguintes parâmetros:

Passo	Ação
1	Na janela *Main topology*, clique com o botão direito e selecione **Create** > **Topology Object**. Selecione na árvore de objetos o equipamento OptiX 2500+ em **MSTP Series**.
2	Configure os seguintes parâmetros: ID: 1 Extended ID: 9 Name: NE1 Gateway Type: Gateway Protocol: IP IP Address: 129.9.0.1 Port: 1400 NE User: root Password: password Não selecione **NE Preconfiguration**. O T2000 gera automaticamente um endereco IP de acordo com o NE ID e o extended ID.
3	Clique em Ok
4	Clique na janela *Main topology* e o símbolo do NE1 irá aparecer. Dois símbolos também vão aparecer: e no NE1, indicando que o NE1 é o GNE e não está configurado.

Para os NEs (*Non-gateways*) 1 a 5 siga as seguintes configurações:

Passo	Ação
1	Na *Main topology*, clique com o botão direito e selecione **Create** > **Topology Object**. Selecione na árvore de objetos o equipamento OptiX 2500+ em **MSTP Series**.
2	Configure os seguintes parâmetros: ID: 2 Extended ID: 9 Name: NE2 Gateway Type: Non-Gateway Affiliated Gateway: NE1 NE User: root Password: password Não selecione **NE Preconfiguration**.
3	Clique em **OK**.
4	Clique na janela *Main topology* e o símbolo do NE2 irá aparecer.

	O símbolo no NE2 indica que o NE2 não está configurado.
5	Repita os passos de 1 a 4 para criar o NE3, NE4 e NE5.

O método de *upload* é usado para configurar as placas da seguinte maneira.

Passo	Ação
1	Na janela *Main topology* dê um clique duplo no NE1 para mostrar a janela NE Configuration Wizard.
2	Selecione **Upload** e clique **Next**.
3	Uma mensagem de sucesso aparecerá. Clique em **Close**.
4	Repita os passos de 1 a 3 para criar as placas dos NE2,N3,NE4 e NE5.

Em seguida, baseado na Tabela 2 e na janela mostrada na Figura 14, configurar as fibras e as conexões como descrito a seguir:

Local end				Remote end			
NE name	Slot	Board name	Port No.	NE name	Slot	Board name	Port No.
NE1	5	S16	1IN	NE4	6	S16	1OUT
NE1	5	S16	1OUT	NE4	6	S16	1IN
NE2	5	S16	1IN	NE1	6	S16	1OUT
NE2	5	S16	1OUT	NE1	6	S16	1IN
NE3	5	S16	1IN	NE2	6	S16	1OUT
NE3	5	S16	1OUT	NE2	6	S16	1IN
NE4	5	S16	1IN	NE3	6	S16	1OUT
NE4	5	S16	1OUT	NE3	6	S16	1IN
NE5	9	SL4	1IN	NE4	9	SL4	1OUT
NE5	9	SL4	1OUT	NE4	9	SL4	1IN

Tabela 2 – Conexão de fibras e cabos

Passo	Ação
1	Na janela *Main topology*, selecione para alterar o ponteiro do mouse para "+".
2	Ainda na *Main topology*, selecione NE1 como a fonte NE, 6-S16 como a placa fonte, e 1 como a porta fonte. Clique **OK**.
3	Selecione NE2 como NE de destino, 5-S16 como a placa de destino, e 1 como a porta de destino. Clique **OK**.
4	Na caixa **Create Fiber** selecione **fiber attributes**. Clique **OK**.
5	Repita os passos 1 a 4 para criar as conexões de fibras e cabos entre os NEs para formar a topologia da Figura 12.

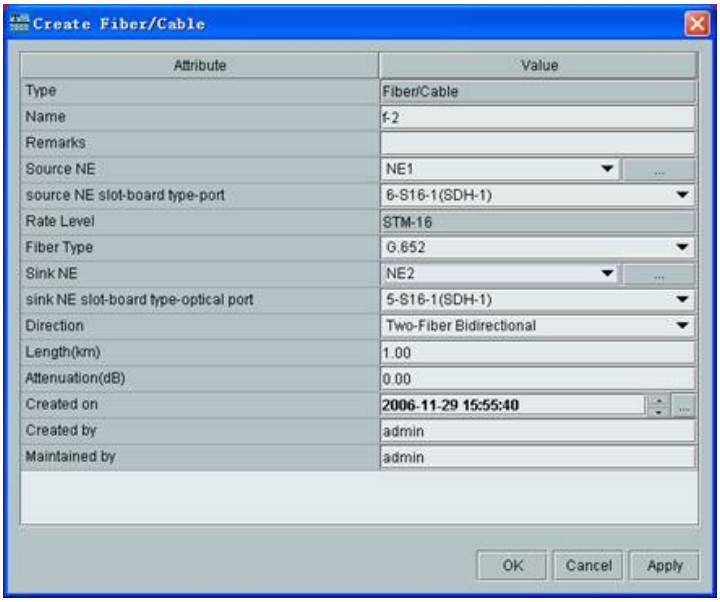


Figura 14 – Janela **Create Fiber/Cable**

Antes de prosseguir para a configuração de serviços, o usuário deve criar a subrede de proteção (Fig. 15). Nesse exemplo de cenário, um anel bidirecional MSP de duas fibras é usado juntamente com um segmento linear sem proteção.

Para a configuração do anel contendo NE1, NE2, NE3 e NE4 siga os seguintes passos:

Passo	Ação
1	Na janela *Main topology*, selecione **Configuration** > **Protection View**.
2	Na janela Protection View, selecione **Protection View** > **Create SDH Protection Subnet** > **2f_MSP SPRing**, para visualizar o **Wizard for Creating Two-Fiber Bidirectional MS Shared Protection Ring**.
3	No **Wizard for Creating Two-Fiber Bidirectional MS Shared Protection Ring**, configure os seguintes parâmetros: Name: 2f_MS_SPRing_1 Rate: STM-16 Não selecione **Resource Sharing** ou **Assigned by VC4**
4	Na topologia a direita, dê um clique duplo em cada ícone do NE1 ao NE4 para adicionar eles ao anel bidirecional MSP de duas fibras. O **Node Attributes** é **MSP Node** por padrão. Clique em **Next**.
5	Verifique a informação de link e clique **Finish**. Uma mensagem aparecerá indicando o sucesso da operação.

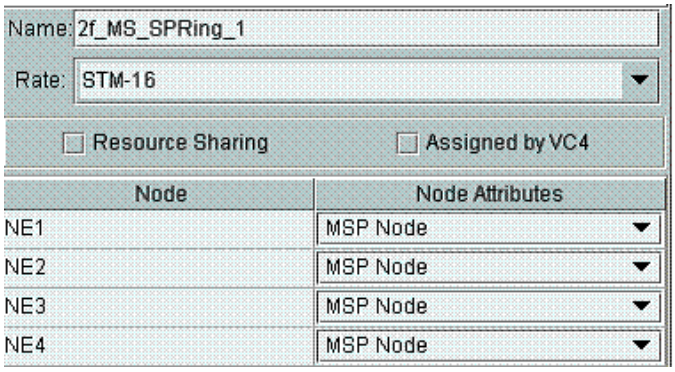


Figura 15 – Criando uma subrede de proteção (anel)

Para criar o segmento linear, entre na **janela Protection View**. Selecione **Protection View** > **Create SDH Protection Subnet** > **NP_Chain** para abrir o **Wizard for Creating Chain without Protection**. Complete as informações com os seguintes parâmetros: Name- NP_Chain_1, Rate- STM-4 e não selecione **Resource Sharing** ou **Assigned** por **VC4** (Fig. 16). Na topologia à direita, dê um duplo clique nos ícones NE4 e NE5 para adicioná-los à subrede de proteção. Clique **Next**. Verifique a informação de link e clique **Finish**. Uma mensagem aparecerá indicando o sucesso da operação.

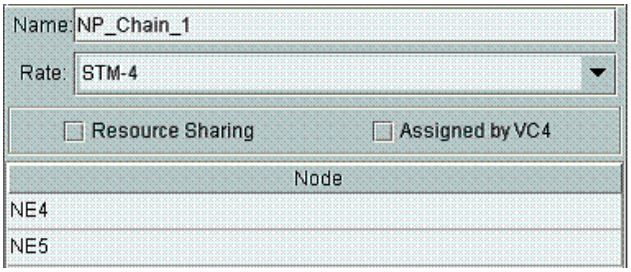


Figura 16 - Criando uma subrede de proteção (linear)

Criação de serviços *Add/Drop* para o NE1

1. Na *Main topology*, selecione o NE1 e selecione **Configuration** > **NE Explorer**.

2. Na árvore de funções, selecione **Configuration** > **SDH Service Configuration**. Clique  .

3. Crie serviços E1 de NE1 a NE2.
Clique em **Create**. Na caixa **Create SDH Service** (Fig.17), configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 2-PQ1
Source Time Slot Range: 1¨C32
Sink Slot: 6-S16-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 1¨C32
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

4. Crie serviços E1 de NE1 a NE3.
Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional

Source Slot: 2-PQ1
Source Time Slot Range: 33¨C63
Sink Slot: 6-S16-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 33¨C63
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

5. Crie serviços E1 de NE1 a NE4. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 3-PQ1
Source Time Slot Range: 1¨C32
Sink Slot: 5-S16-1(SDH-1)
Sink VC4: VC4-2
Sink Time Slot Range: 1¨C32
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

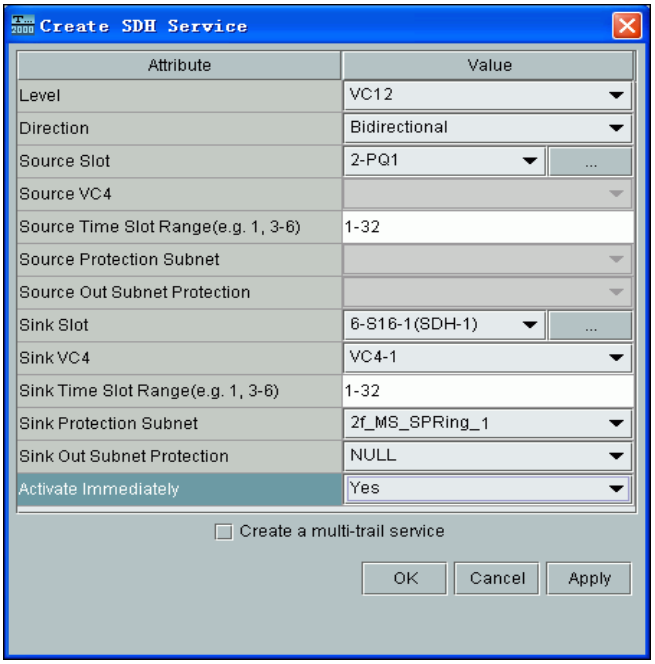


Figura 17 – Criando serviços SDH

Criação de serviços *Pass-Through* para o NE2

1. Na *Main topology*, selecione o NE2 e selecione **Configuration** > **NE Explorer**.

2. Na árvore de funções, selecione **Configuration** > **SDH Service Configuration**. Clique  .

3. Configure os serviços de NE1 a NE3 para passar diretamente por NE2.
Clique **Create**. Na caixa **Create SDH Service** , configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 5-S16-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 33¨C63
Source Protection Subnet: 2f_MS_SPRing_1
Source Out Subnet Protection: NULL
Sink Slot: 6-S16-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 33¨C63
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

Criação de serviços *Add/Drop* para o NE2

1. Crie serviços E1 de NE1 a NE2. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 5-S16-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 1¨C32
Source Protection Subnet: 2f_MS_SPRing_1
Source Out Subnet Protection: NULL
Sink Slot: 2-PQ1
Sink Time Slot Range: 1¨C32
Activate Immediately: Yes
Clique **OK**.

Criação de serviços *Add/Drop* para o NE3

1. Crie serviços E1 de NE1 a NE3. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC12
Direction: Bidirectional
Source Slot: 5-S16-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 33¨C63
Source Protection Subnet: 2f_MS_SPRing_1
Source Out Subnet Protection: NULL
Sink Slot: 2-PQ1
Sink Time Slot Range: 33¨C63
Activate Immediately: Yes
Clique **OK**.

2. Crie serviços E1 de NE3 a NE5. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC12
Direction: Bidirectional
Source Slot:2-PQ1
Source Time Slot Range: 1¨C32
Sink Slot: 6-S16-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 1¨C32
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

Criação de serviços *Pass-Through* para o NE4

1. Configure os serviços de NE3 a NE5 para passar diretamente por NE4.
Clique **Create**. Na caixa **Create SDH Service** , configure os seguintes parâmetros:

Level: VC12
Direction: Bidirectional
Source Slot: 5-S16-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 1¨C32
Source Protection Subnet: 2f_MS_SPRing_1
Source Out Subnet Protection: NULL
Sink Slot: 9-SL4-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 1¨C32
Sink Protection Subnet: Non-Protection Chain_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes

Criação de serviços *Add/Drop* para o NE4

1. Crie serviços E1 de NE4 a NE5. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 2-PQ1
Source Time Slot Range: 33¨C63
Sink Slot: 9-SL4-1(SDH-1)
Sink VC4: VC4-1
Sink Time Slot Range: 33¨C63
Sink Protection Subnet: Non-Protection Chain_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

2. Crie serviços E1 de NE4 a NE1. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC12
Direction: Bidirectional
Source Slot: 2-PQ1
Source Time Slot Range: 1¨C32
Sink Slot: 6-S16-1(SDH-1)
Sink VC4: VC4-2
Sink Time Slot Range: 1¨C32
Sink Protection Subnet: 2f_MS_SPRing_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

3. Crie serviços E3 de NE4 a NE5. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC3
Direction: Bidirectional
Source Slot: 12-PL3
Source Time Slot Range: 1¨C3
Sink Slot: 9-SL4-1(SDH-1)
Sink VC4: VC4-3
Sink Time Slot Range: 1¨C3
Sink Protection Subnet: Non-Protection Chain_1
Sink Out Subnet Protection: NULL
Activate Immediately: Yes
Clique **OK**.

Criação de serviços *Add/Drop* para o NE4

1. Crie serviços E1 de NE4 a NE1. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:
Level: VC12
Direction: Bidirectional
Source Slot: 9-SL4-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 1¨C32
Source Protection Subnet: Non-Protection Chain_1
Source Out Subnet Protection: NULL
Sink Slot: 2-PQ1
Sink Time Slot Range: 1¨C32
Activate Immediately: Yes
Clique **OK**.

2. Crie serviços E1 de NE4 a NE5. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC12
Direction: Bidirectional
Source Slot: 9-SL4-1(SDH-1)
Source VC4: VC4-1
Source Time Slot Range: 33¨C63
Source Protection Subnet: Non-Protection Chain_1
Source Out Subnet Protection: NULL
Sink Slot: 2-PQ1
Sink Time Slot Range: 33¨C63
Activate Immediately: Yes
Clique **OK**.

3. Crie serviços E3 de NE4 a NE5. Clique em **Create**. Na caixa **Create SDH Service**, configure os seguintes parâmetros:

Level: VC3
Direction: Bidirectional
Source Slot: 9-SL4-1(SDH-1)
Source VC4: VC4-3
Source Time Slot Range: 1¨C3
Source Protection Subnet: Non-Protection Chain_1
Source Out Subnet Protection: NULL
Sink Slot: 12-PL3
Sink Time Slot Range: 1¨C3
Activate Immediately: Yes
Clique **OK**.

Para configurar a comutação de proteção de tributários (*Tributary Protection Switching* - TPS) os passos a seguir devem ser seguidos:

Passo	Ação
1	Na janela *Main topology*, clique com o botão direito o NE1 e selecione **NE Explorer**.
2	Na árvore de funções, selecione **Configuration** > **TPS Protection**. Clique  .
3	Clique em **Create**. Na caixa **Create SDH TPS Protection Group** configure os seguintes parâmetros: Protection Board: 16-PQ1 Working board: 2-PQ1, 3-PQ1 Marque a caixa **Enable Protection Switching**. WTR Time (s): 600 Switching Priority: Priority-1 for 2-PQ1, Priority-2 for 3-PQ1
4	Clique **OK**.

Para configurar a proteção 1+1 das placas os seguintes passos devem ser seguidos:

Passo	Ação
1	Na janela *Main topology*, clique com o botão direito o NE1 e selecione **NE Explorer**.
2	Na árvore de funções, selecione **Configuration**> **TPS Protection**. Clique  .
3	Clique em **Create**.
4	Configure os seguintes parâmetros: 1+1 Protection Type: Cross-connect Protection Pair Primary Board: 7-XCS Secondary Board: 8-XCS
5	Clique em **Apply**.
6	Repita os passos 2 a 5 para configurar a proteção 1+1 para o NE4 e o NE5.

Uma vez que todas essas configurações foram feitas com sucesso, os parâmetros de configuração para o monitoramento de performance da rede devem ser configurados.

Passo	Ação
1	Na janela *Main topology*, selecione **Configuration** > **NE Time Synchronization**.
2	Selecione o NE1 até o NE5 e clique  .
3	Selecione o NE1 até o NE5. Clique com o botão direito na coluna embaixo da aba **Synchronous Mode** e selecione **NM** ou clique com o botão direito embaixo de outra aba e selecione **Synchronize with NM Time**. Escolha **Yes** na mensagem de confirmação.
4	Uma mensagem de sucesso da operação aparecerá. Clique em **Close**.
5	Na janela *Main topology*, selecione **Performance** > **NE Performance Monitor Time**.
6	Selecione o NE1 e clique  .
7	Configure os seguintes parâmetros: 15min-monitoring: Open 24h-monitoring: Open Start time: necessita ser mais tarde que o NM e o NE Clique em **Apply**.
8	Repita os passos 6 e 7 para configurar os parâmetros de performance para o NE2 ao NE5.

Por último, os parâmetros de alarme (Fig. 18) devem ser configurados:

Passo	Ação
1	Na janela *Main topology*, selecione **System Administration** > **Database Management** > **Dump**.
2	Selecione a aba **Dump Condition** e selecione um evento de performance. Para o registro que precisa de dump periodic, configure o seguinte parâmetro: Dump Periodically or Not: Yes **Dump Interval (Day)** and **Time Limit (Days Before)** e outros parâmetros adotam os valores padrão.
3	Clique em OK.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

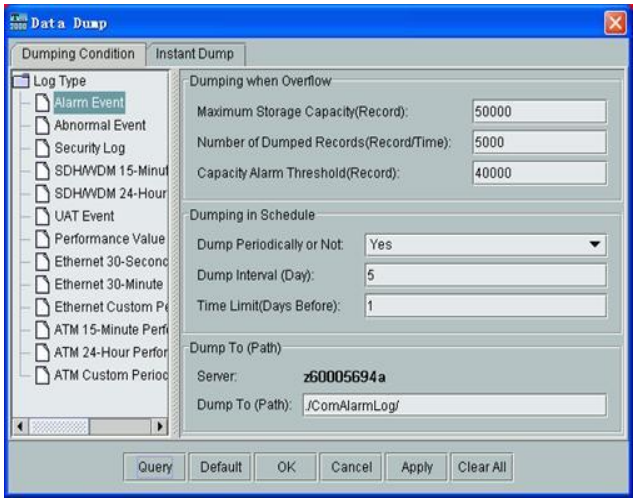


Figura 18 – Configuração dos parâmetros de alarme

IV. Referências Bibliográficas

[1] *Huawei Selected Collections of Maintenance Documentation for Huawei Optical Network Products*, Manual de operação e manutenção equipamentos ópticos Huawei.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Experimento nº2

Generic Frame Procedure SONET/SDH

Anexo II

I. OBJETIVO

Análise e verificação do funcionamento básico da rede SDH e do protocolo *Generic Framing Procedure* (GFP). Além disso, verificação da conectividade entre duas estações FastEthernet conectadas a dois nós da rede através do uso da ferramenta do sistema de gerência e do uso do protocolo ICMP (*ping*).

II. INTRODUÇÃO

O atual cenário de telecomunicações é ainda dominado basicamente por duas tecnologias: Ethernet nas redes locais (LAN) e SONET/SDH na parte do provedor de serviços (WAN). Apesar da crescente substituição de redes metropolitanas SONET/SDH por soluções metro Ethernet, as redes SONET/SDH ainda representam uma sólida e atuante tecnologia de transporte de alta velocidade [1].

A interconexão de escritórios separados por centenas de quilômetros de distância em uma mesma LAN gera um grave problema de compatibilidade de interconexão. Historicamente, muitos protocolos proprietários foram desenvolvidos para prover a interface entre a LAN e a WAN, oferecida pelo provedor de serviços de telecomunicações, uma vez que o protocolo Ethernet não é diretamente suportado pela rede SONET/SDH [2].

Os motivos pelos quais o protocolo Ethernet não é carregado diretamente pela rede SONET/SDH são: a diferença de taxas entre as tecnologias e a falta de eficiência dos métodos de encapsulamento até então utilizados. O Ethernet pode operar nas taxas de 10Mbps, 100Mbps, 1Gbps e 10Gbps. Já as taxas do SONET/SDH são otimizadas para o transporte de tráfego de telecomunicações ou de voz e não possui taxas adequadas para o transporte de um fluxo de dados Ethernet (Tabela 1). A diferença entre as taxas provocaria uma grande ineficiência ao transportar uma conexão Ethernet em um canal SONET/SDH

Ethernet	**SONET**		
Taxa de bit	Taxa SONET	Taxa efetiva *payload*	Eficiência de Banda
10Mbps Ethernet	STS-1	50,112 Mbps	20%
100 Mbps FastEthernet	STS-3	150,336 Mbps	67%
1Gbps Ethernet	STS-48	2045,376 Mbps	49%

Tabela 1 – Taxas típicas Ethernet vs. SONET

Para otimizar o transporte de quadros Ethernet em enlaces SONET/SDH, foi desenvolvido e padronizado o *Generic Frame Procedure* [2].

Hierarquia SONET/SDH

O sinal elétrico em uma rede *synchronous optical network* (SONET) é denominado *synchronous transport signal* (STS) e o sinal óptico é denominado *optical carrier* (OC) [3]. A rede *synchronous digital hierarchy* (SDH) utiliza a notação *synchronous transport module* (STM) para ambos os sinais. Uma regra básica para conversão de STM-n para OC-m é fazer m=3*n. A Figura 1 ilustra as diferentes possibilidades atuais de taxas e interfaces da hierarquia SONET/SDH.

Nível Óptico	Nível SONET (elétrico)	Nível SDH (elétrico)	Taxa de dados (Mbps)	Taxa cabeçalho (Mbps)	Taxa *payload* (Mbps)
OC-1	STS-1	-	51,840	1,728	50,112
OC-3	STS-3	STM-1	155,520	5,184	150,336
OC-9	STS-9	STM-3	466,560	15,552	451,008
OC-12	STS-12	STM-4	622,080	20,736	601,344
OC-18	STS-18	STM-6	933,120	31,104	902,016
OC-24	STS-24	STM-8	1244,160	41,472	1202,688
OC-36	STS-36	STM-12	1866,240	62,208	1804,932
OC- 48	STS-48	STM-16	2488,320	82,944	2405,376
OC-96	STS-96	STM-32	4976,640	165,888	4810,752
OC-192	STS-192	STM-64	9953,280	331,776	9621,504
OC-768	STS-768	STM-256	39813,120	1327,104	38486,016
OC-N	STS-N	STM-N/3	N*51,840	N*1,728	N*50,112

Figura 1 – Hierarquia SONET/SDH. Adaptado de [3]

Pode-se dizer que o SONET/SDH é canalizado uma vez que um STS-3 (STM-1) consiste em três fluxos STS-1 e cada STS-1 consiste em um número de sinais DS-1 (T1) e E1 provenientes da hierarquia PDH. Um STS-12 (STM-4) consiste em 12 fluxos STS-1. A estrutura básica de um STM-1 é representada na Figura 2. Ela é representada na forma de uma matriz, mas o quadro é transmitido linha por linha de forma contínua. Cada quadro tem a duração de 125µs e cada célula corresponde a um byte [1]. As nove primeiras colunas são compostas por bytes de *overhead* que é composto por três diferentes estruturas:

- RSOH (*Regenerator Section Overhead*), processado em cada equipamento da rede, contém informações de alinhamento de quadro, identificação de quadro, monitoração de erro de regeneração, alarmes físicos externos ao equipamento, e supervisão de sistema. Contém também um canal de voz, para comunicação de técnicos entre equipamentos [4].
- MSOH (*Multiplex Section Overhead*), processado apenas em equipamentos onde existe inserção ou retirada de canais multiplexados, contém informações de monitoração e indicação de erros de multiplexação, controle de chaveamento de mecanismos de proteção, monitoração de sincronismo e gerência de sistema [4].
- Ponteiros AU-n (*Administrative Unit*), processado em cada equipamento, possui os ponteiros que indicam onde se localiza o primeiro byte dos contêineres virtuais dentro da área de informação útil (*payload*) do quadro, e eventuais bytes provenientes de justificação desses contêineres virtuais [4].

As 261 colunas restantes carregam o *payload* STM-1 que consiste em dados do usuário e mais uma coluna de bytes de *overhead* denominado *path overhead* (POH).

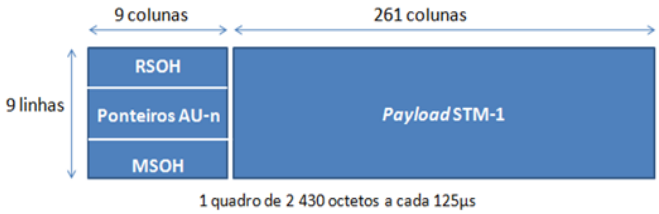


Figura 2 – Quadro STM-1 (SDH). Adaptado de [3].

Para acomodar tributários da hierarquia PDH ou sinais ISDN (*Integrated services digital network*), o SDH utiliza contêineres que podem ser definidos como sinais de várias formas e taxas menores que um STM-1. Vários mapeamentos e multiplexações são realizados para transportar um contêiner de baixa velocidade em um sinal SDH de nível STM. Foram definidos seis tipos de contêineres: C-11, C-12, C-2, dois C-3 e C-4. Os contêineres de alta ordem são representados pelo C-3 e pelo C-4. Os contêineres de baixa ordem são representados pelo C-2, C-12, e C11 [3].

Um sinal DS-1 de 1,544 Mbps ou um sinal ISDN H11 pode ser colocado em um C-11(contêiner nível 1, tipo 1). Um sinal E-1 de 2,048 Mbps ou um sinal ISDN H12 pode ser colocados em um C-12. Um sinal DS-2 de 6,312 Mbps é mapeado em um C-2 enquanto um sinal DS-3 de 44,736 Mbps ou um ISDN H32 é carregado em um C-3 que também pode carregar um E-3 de 34,368 Mbps ou um sinal ISDN H31. A mais alta taxa de um sinal ITU-T PDH de 139,264 Mbps (E-4) ou um sinal ISDN H4 pode ser transportado em um C-4 [3].

Após o mapeamento inicial, o contêiner percorre um caminho até formar um quadro STM-1 (Fig.3). Por exemplo, um C-4 ocupa 9 linhas e 260 colunas em um quadro com intervalo de 125 µs. Dessa maneira, ele possui uma taxa de 149,76 Mbps (9x260x64 kbps). Adicionando uma coluna com cabeçalho VC-4 (contêiner virtual nível 4) POH, o resultado é um VC-4. É um quadro com 9 linhas e 261 colunas. Em seguida, 9 octetos dos ponteiros AU-4 são adicionados ao VC-4 para formar um AU-4. Finalmente, 27 octetos de cabeçalho RSOH e 54 octetos de cabeçalho MSOH são adicionados ao AU-4, que tem o mesmo significado que um AUG (*Administrative Unit Group*), para formar o sinal SDH STM-1 [3].

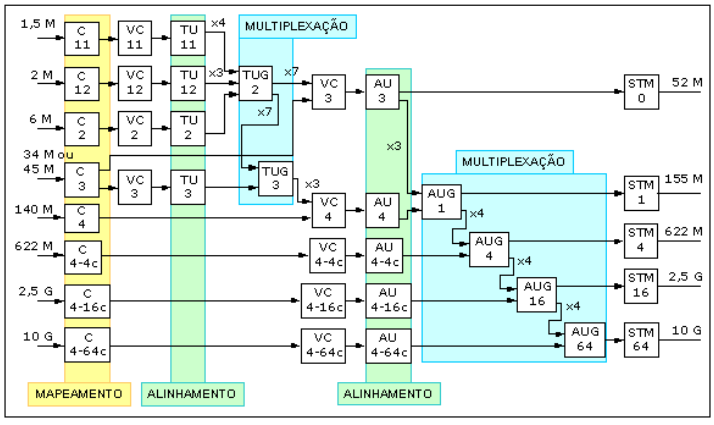


Figura 3 – Multiplexação de tributários no quadro SDH [4]

O contêiner C-3 ocupa 9 linhas e 84 colunas e pode seguir dois caminhos de acordo com a Figura 3. No caminho da direita sua taxa é de 48,384 Mbps e após a inserção de nove octetos de cabeçalho VC-3 POH ele se torna um VC-3. Ele possui uma estrutura de 9 linhas e 85 colunas e uma taxa de 48,96 Mbps. Para formar o próximo sinal, TU-3 (*Tributary Unit*), 3 octetos do ponteiro TU-3 são inseridos na coluna 86. Dessa forma, o TUG-3 (*Tributary Unit Group*) está formado. Bits de preenchimento podem ser necessários. Três sinais TUG-3 são então multiplexados e mapeados em um VC-4 para formar um sinal AUG. Em seguida 27 octetos de cabeçalho RSOH e 54 octetos de cabeçalho MSOH são adicionados para formar o sinal SDH STM-1. Todos os outros contêineres seguem os diferentes caminhos da estrutura da Figura 3 para a formação do sinal STM-1 [3].

A terminologia utilizada pelas redes SONET possui termos diferentes para a estrutura de multiplexação em um quadro STS-N. C-11, C-12, C-2, C-3 e C-4 equivalem a VT-1.5 (*Virtual Tributaries*), VT-2, VT-6,STS-*1 payload capacity* e STS-3 *payload capacity* respectivamente [3].

O *payload* STS-1 é dividido em sete *virtual tributary groups* (VTG). Cada VTG consiste em 108 bytes (12 colunas) e cada VTG pode carregar um número de tributários virtuais. Os seguintes tributários virtuais foram definidos para o SONET [1]:

- VT-1.5: Esse tributário virtual carrega um sinal DS-1 e está contido em três colunas que correspondem a 27 bytes. Quatro VT-1.5 podem ser transportados em um único VTG [1].

- VT-2: Esse tributário virtual carrega um sinal E1 de 2,048 Mbps. Está contido em quatro colunas que correspondem a 36 bytes. Três VT-2 podem ser transportados em um único VTG [1].

- VT-3: Transporta um sinal DS-1 não canalizado. Está contido em 6 colunas e corresponde a 54 bytes. Isso significa que um VTG pode carregar dois VT-3 [1].

- VT-6: Esse tributário transporta um sinal DS-2 que transporta 96 canais de voz. Está contido em 12 colunas e corresponde a 108 bytes. Um VTG transporta exatamente um VT-2 [1].

Sincronismo

O sincronismo certamente é uma das características mais marcantes das redes SONET/SDH. Os relógios do transmissor e do receptor necessitam estar precisamente sincronizados para evitar a detecção errada de bits durante o transporte de informação pela rede. Pequenas variações na sincronização dos relógios dos equipamentos de uma rede podem significar um alto número de bits de informação perdidos e por isso essas variações devem ser minimizadas da melhor maneira possível.

Para garantir o sincronismo da rede SDH, um relógio preciso e confiável como um relógio atômico ou um sinal de GPS é eleito como o relógio de referência primária (*primary reference clock* - PRC) de toda a rede. Equipamentos diretamente conectados ao relógio de referência primária são representados no nível 1. Equipamentos que obtêm a referência a partir de equipamentos do nível 1 são representados no nível 2. Da mesma maneira outros equipamentos obtêm o sincronismo necessário e constituem, dessa forma, uma hierarquia de diversos níveis. Naturalmente, quanto menor o nível, mais preciso é o relógio. Para assegurar uma multiplexação síncrona, as redes SONET/SDH utilizam equipamentos de nível 3 ou menores [3].

Fenômenos como *jitter,* que são variações de freqüência maiores ou iguais a 10 Hz nos instantes significativos de um sinal nas suas posições ideais no tempo e *wander* , que são variações de freqüência menores ou iguais a 10 Hz nos instantes significativos de um sinal digital nas suas posições ideais no tempo provocam pequenos desvios nos relógios do equipamentos e precisam ser compensados com o uso de ponteiros no cabeçalho do quadro SDH [5].

O uso de ponteiros em conjunto com buffers permite acomodar as eventuais diferenças de fase e freqüência dos canais durante o processo de multiplexação. Os ponteiros possuem campos específicos para armazenar os bits ou bytes em excesso ou para indicar a falta destes durante o processo de sincronização (justificação). Os buffers permitem que esse processo ocorra sem a perda de informação armazenando e mantendo o sinal original [1].

Existem quatro modos de sincronismo: síncrono, pseudo-síncrono, plesiócrono e assíncrono. No modo síncrono todos os relógios da rede são referenciados por uma única referência primária de relógio e a rede constitui uma única área de sincronismo. Eventuais ajustes de ponteiro ocorrem de forma aleatória e é o modo de operação normal dentro de uma rede de um único provedor de serviços. No modo pseudo-síncrono nem todos os relógios são referenciados por uma referência primária de relógio e cada PRC forma uma área de sincronismo. Os elementos de rede posicionados nas

bordas dessas áreas podem fazer ajustes de ponteiros e esse é o modo de operação normal de provedores de serviço de grande porte (com várias áreas de sincronismo) ou entre redes compostas por vários provedores de serviços. Já o modo plesiócrono, caso o sinal de sincronismo na rede falhe, os equipamentos de rede utilizam suas referências internas e podem ocorrer ajustes de ponteiros de forma persistente em vários pontos da rede enquanto o sinal de sincronismo não for recuperado. No modo assíncrono, falhas do sinal de sincronismo provocam grandes desvios de freqüência entre os relógios dos equipamentos de rede e conseqüentemente alarmes de falhas e interrupção do tráfego da rede podem ocorrer [3].

No caso de uma rede SONET/SDH pequena que não possui comunicação com outras redes, um equipamento de rede pode ser eleito como o mestre e o gerador do PRC. Todos os outros equipamentos podem ser configurados no modo escravo e obter o sincronismo do equipamento de rede eleito como mestre. Esta configuração pode se mostrar muito útil em cenários de laboratório e de teste [6].

Estrutura em Camadas [4]

O padrão SDH foi desenvolvido usando a abordagem cliente/servidor e sua arquitetura de administração e supervisão procurou apoiar-se no modelo de camadas ISO (*Open Systems Interconnection*- OSI), permitindo que a supervisão do transporte de informações seja feita através de camadas hierarquizadas. Foram definidas basicamente duas camadas de transporte SDH: camada de caminho e camada do meio de transmissão.

Entende-se por caminho o percurso percorrido pelo sinal entre a origem e o destino. Nesse caminho o sinal é acondicionado no quadro SDH que faz o seu transporte através de todos os equipamentos da rede nessa rota. Em cada equipamento, de acordo com a sua função, o quadro é processado pelas camadas adequadas para ser restaurado ou para extrair ou inserir novos serviços. Em cada etapa desse processo, informações de administração e supervisão do SDH são geradas e inseridas no quadro.

A camada do meio de transmissão é dependente do meio utilizado, e por isso foi dividida em duas camadas distintas: meio físico e seção. A camada do meio físico realiza o condicionamento do sinal de acordo com esse meio, seja ele óptico ou elétrico.

A camada de seção também está dividida em duas novas camadas. A camada de seção de regeneração, que é responsável pelo processamento dos quadros em todos os equipamentos da rede, sejam eles de passagem, de extração ou inserção de tributários, ou de terminação de caminho, e a camada de seção de multiplexação que é responsável pelo processamento fim-a-fim dos quadros nos equipamentos de extração ou inserção de tributários, ou de terminação de caminho.

A camada de caminho está divida em alta ordem e baixa ordem. Nessa camada cada contêiner virtual é uma estrutura com a informação útil (contêiner) e um cabeçalho que o caracteriza (POH). No caminho de baixa ordem, cada contêiner virtual contém um único contêiner e seu cabeçalho (VC-11, VC-12, VC-2 ou VC-3). No caminho de alta ordem, um contêiner virtual pode conter um único contêiner e seu cabeçalho (VC-3 ou VC-4), ou um conjunto de contêineres de menor ordem e o respectivo cabeçalho.

A camada de circuito realiza o condicionamento da informação útil retirada do contêiner para a interface elétrica ou óptica definida para cada serviço a ser fornecido pelo equipamento.

Equipamentos SONET/SDH [1]

Existem basicamente três tipos de equipamentos SONET/SDH: multiplexador terminal (*terminal multiplexer* - TM), multiplexador *add/drop* (*add/drop multiplexer* - ADM) e *digital cross-connect* (DCS).

O TM (Fig. 4) é responsável por multiplexar um número de sinais DS-n ou E1 em um único sinal STM-N. Consiste de um controlador, interfaces de baixa velocidade para os sinais DS-n e E1, uma interface STM-N, e um *time slot interchanger* (TSI). O TM também atua como um demultiplexador.

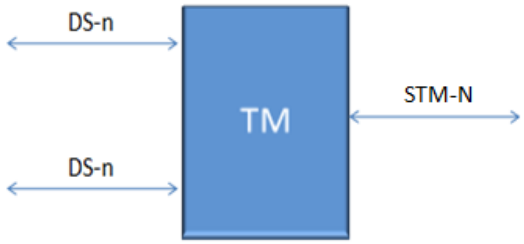


Figura 4 – Multiplexador terminal

O ADM (Fig. 5) é uma versão mais complexa do TM. Ele recebe um sinal STM-N e a partir dele pode demultiplexar e terminar (*drop*) qualquer número de sinais DS-n ou STM-M, onde M<N, ao mesmo tempo que pode adicionar novos sinais DS-n e STM-M no sinal STM-N.

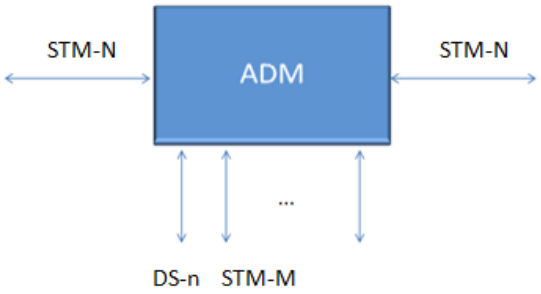


Figura 5 – *Add/drop multiplexer*

Na conexão exemplificada na Figura 6, temos que o usuário A transmite um sinal DS-1 para o TM1. O TM1 transmite um sinal STM-1 para o ADM1, que por sua vez, adiciona o sinal STM-1 no *payload* de um sinal STM-4 e transmite para o próximo ADM do anel. No ADM3, o sinal DS-1 pertencente a A é retirado do *payload* e transmitido com outros sinais para o TM2. O TM2 finalmente demultiplexa os sinais e transmite o sinal DS-1 para o usuário B.

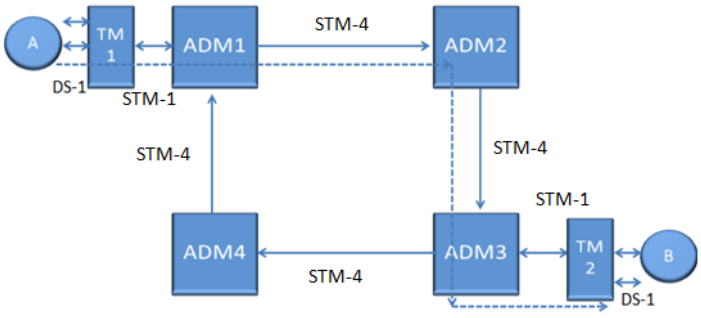


Figura 6 – Exemplo de conexão

O DCS (Fig. 7) é usado para interconectar múltiplos anéis SONET/SDH. É conectado a múltiplas interfaces OC-N (STM-N) de entrada e de saída. Pode retirar ou adicionar qualquer número de sinais DS-n ou OC-M (STM-M) e pode comutar sinais DS-n ou OC-M (STM-M) provenientes de uma interface de entrada para qualquer interface de saída.

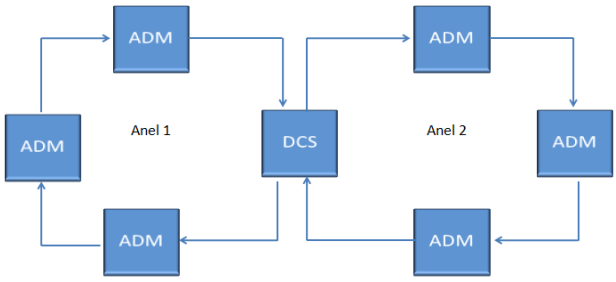


Figura 7 – *Digital cross-connect*

Generic Frame Procedure (GFP)

O GFP é uma tecnologia que oferece uma flexibilização do *framework* de encapsulamento para fluxo de dados codificados em bloco e dados orientados a pacotes. Ele possui o potencial de substituir os protocolos proprietários para transportar dados nas existentes redes SONET/SDH e redes de transporte WDM/OTN emergentes [2].

O GFP suporta todas as funções básicas de quadro como delimitação de quadro, multiplexação de quadro dos clientes e mapeamento de dados do cliente [2].

A técnica utiliza um mecanismo de delimitação similar ao do ATM *(Asynchronous Transfer Mode)*, mas generalizado para pacotes de tamanho fixo ou variável. Como resultado, não é necessário procurar por caracteres especiais de controle no fluxo de dados do cliente como requerido pela codificação 8B/10B ou pelos delimitadores de quadro do protocolo HDLC (*High Level Data Link Control)*. O GFP permite a multiplexação flexível onde os dados originados de múltiplos clientes ou múltiplas sessões clientes podem ser enviados no mesmo enlace em uma configuração ponto a ponto ou anel. O transporte de dados orientados a pacote como o Ethernet e o IP e de dados orientados a caracteres como o Fiber Channel são suportados pelo GFP. Considerando que também suporta o encapsulamento e o transporte de PDUs (*Protocol Data Units*) de tamanho variável, o GFP não necessita de funções complexas de segmentação e remontagem ou de enchimento de bits para preencher espaços vazios no *payload* [2].

A estrutura do quadro GFP consiste no *core header* e uma área de *payload* (Fig. 8). O *core header* possui o tamanho de 4 bytes e tem a função de suportar algumas funções específicas de gerenciamento GFP da camada de enlace e de tornar a delimitação do quadro independente do conteúdo do *payload*. Ele é subdividido

em dois campos: indicador de tamanho do *payload* (*payload length indicator*- PLI) e campo de correção de erros do *core header* (*core header error correction* (cHEC) *field*) [7].

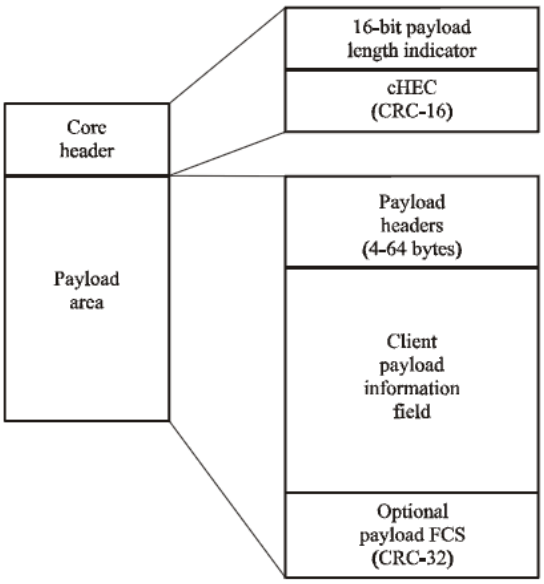


Figura 8 - Estrutura do frame GFP

O primeiro campo contém dois bytes que indicam o tamanho do *payload* GFP em bytes. O segundo campo também possui dois octetos que contém a seqüência de *cyclic redundancy check* (CRC) que protege a integridade do *core header* [7].

O tamanho do *payload* é variável (0 - 65535 octetos) e transporta dados do cliente como PDUs ou, informação de gerenciamento do cliente. A área de *payload* consiste no *payload header*, o campo de informação do *payload* (*payload information field*) e um campo opcional de *Frame Check Sequence* (FCS) que é utilizado para detectar a existência de dados corrompidos no *payload* [7].

O *payload header* consiste em um campo de tipo de *payload* (*payload type field)* e um campo de correção de erros do *header* (*Header Error Correction* (tHEC) *field*) que protege a integridade do campo de tipo de *payload*. Opcionalmente, o *payload header* pode incluir uma extensão do *header* [2]. O campo de tipo de *payload* consiste nos seguintes subcampos:

- Identificador de tipo de *payload* (*Payload Type Identifier*- PTI) que identifica o tipo de quadro. Os dois tipos são quadros de dados do usuário ou quadros de gerenciamento do cliente [2].

- Indicador FCS do *payload* (*Payload FCS Indicator* - PFI). Esse subcampo determina a presença ou ausência do campo *payload* FCS [2].

- Identificador da extensão do *header*. Identifica o tipo de extensão de *header* no quadro GFP. Ele facilita a adoção do GFP para diferentes protocolos e redes. Três tipos estão definidos: nulo, extensão linear para redes ponto a ponto e extensão de anel para redes em anel [2].

- Identificador do *payload* do usuário (*User Payload Identifier* - UPI). Ele é definido conforme o tipo de sinal cliente transportado. Os valores definidos atualmente são: Ethernet, PPP (incluindo IP e *Multi Protocol Label Switching* -MPLS), Fibre Channel, FICON (*Fiber Connectivity*), ESCON (*Enterprise Systems Connection*) e Gigabit Ethernet [2].

O campo de informação do *payload* contém os dados do cliente. Existem dois modos de adaptação do sinal cliente definidos para o GFP: *frame-mapped* GFP (GFP-F) aplicável a maioria dos tipos de pacotes e *transparent-mapped* GFP (GFP-T) aplicável a sinais codificados em 8B/10B. Os *payloads* do tipo GFP-F possuem tamanhos variáveis e o quadro do cliente é mapeado inteiramente em um quadro GFP. Exemplos: Ethernet e IP/PPP. No modo GFP-T um número de caracteres de cliente é mapeado em blocos de código eficientes e transportado pelo quadro GFP [2].

Funções do GFP

O transmissor e o receptor GFP operam em modo assíncrono. O transmissor insere quadros GFP no enlace físico de acordo com o alinhamento de bits da interface SONET/SDH. O receptor é responsável por identificar o limite correto do quadro GFP na inicialização do enlace e após eventuais falhas ou perdas de quadros (*Loss Of Frame* - LOF). O receptor monitora o início de um quadro GFP utilizando os últimos 4 octetos de dados recebidos. Primeiramente ele computa o valor do cHEC baseado nesses octetos e se esse valor for igual ao do campo cHEC, ele assume que identificou o limite do quadro. Caso contrário, ele desloca para frente em 1 bit e tenta novamente. Em seguida, ele aguarda pelo próximo quadro GFP candidato baseado no campo PLI. Se um número de quadros validos consecutivos é detectado, o receptor entra

no estado de operação normal. Neste estado, o receptor examina o campo PLI, valida o campo cHEC e extrai o PDU do quadro. Esse processo é chamado de delimitação de quadro [2].

O GFP suporta a multiplexação de quadro e de cliente. Quadros de diversos processos GFP como quadros vazios, quadro de dados do cliente e quadros de gerenciamento do cliente podem ser multiplexados no mesmo enlace. Quadros de dados do cliente possuem prioridade em relação aos outros dois, quadros vazios só são inseridos quando não há quadros de gerenciamento e quadros de dados do cliente para transmissão. O GFP suporta capacidades de multiplexação de cliente por meio dos cabeçalhos de extensão linear e de anel. Por exemplo, o *header* de extensão linear, contém um identificador de canal (CID) de 8 bits que é usado para multiplexar dados de até 256 sessões de clientes em um enlace ponto a ponto [2].

No GFP, o *core header* e a área de *payload* são embaralhados. Dessa forma garante-se que um número adequado de transições 0-1 ocorra e o transmissor permaneça sincronizado com o receptor [2].

Como já mencionado, o mapeamento de *payload* no GFP é feito em dois modos: GFP-F e GFP-T. O mapeamento de quadro de *payloads* nativos de clientes no GFP tem o objetivo de facilitar a manipulação de PDUs entrantes. O transmissor encapsula um quadro de dados inteiro de um cliente em um quadro GFP. Multiplexação de quadros é suportada pelo GFP-F. O GFP-F utiliza a estrutura básica de um quadro GFP cliente incluindo o *payload header*. O GFP-T tem como objetivo facilitar o transporte de sinais clientes codificados em bloco 8B/10B com baixa latência de transmissão. Ao invés de armazenar em buffer todo o quadro do cliente e depois encapsular em um quadro GFP, os caracteres individuais do fluxo de dados do cliente são extraídos e um número fixo deles é mapeado em quadros GFP de tamanho fixo e periódicos. O mapeamento acontece indiferentemente se o tipo de caractere é de controle ou dados. A multiplexação de quadros é possível com o GFP-T que utiliza a mesma estrutura do GFP-F incluindo o requerido *payload header* [7].

O formato do quadro Ethernet foi definido pelo IEEE 802.3 na seção 3.1. Existe um mapeamento de um para um entre o PDU proveniente de uma camada mais elevada e o PDU GFP. Especificamente, os limites de um PDU GFP são alinhados com os limites dos PDUs de camadas mais altas. Essa relação entre quadros MAC Ethernet e quadros GFP está ilustrada na Figura 9 [7].

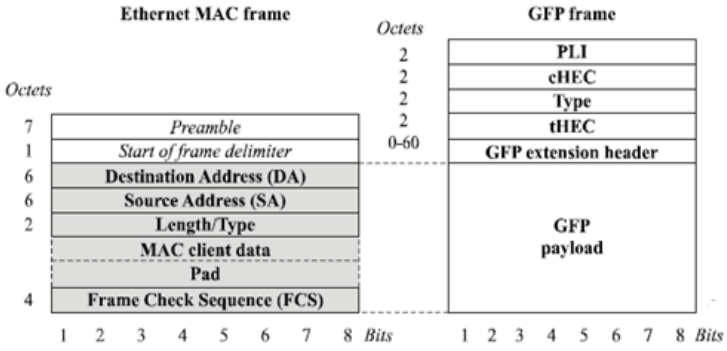


Figura 9- Relação entre o quadro Ethernet e o quadro GFP [7]

Os octetos provenientes do campo de endereço de destino até o *Frame Check Sequence* (FCS) são colocados no campo de informação do *payload* GFP. Os campos de preâmbulo e início do delimitador de quadro não são encapsulados. O tamanho da PDU do cliente é variável e pode ser de até 65 535 octetos. O *payload* Ethernet é mapeado no modo de adaptação GFP-F e os quadros GFP resultantes são transportados pela rede SONET/SDH [7].

III. Referências Bibliográficas

[1]PERROS, Harry. *Connection-Oriented Networks* (2005). Disponível em: <http://www4.ncsu.edu/~hp/Chapter2.pdf> Acesso em: 15 de novembro de 2009.

[2] BERNSTEIN, Greg; RAJAGOPALAN Bala; SAHA Debanjan, *Optical Network Control Architecture Protocols and Standards* (2003).

[3] GORALSKI, Walter J. *SONET*, Second edition (2000).

[4] FILHO, Huber B. *Tutorial redes SDH* (2009). Disponível em: < http://www.teleco.com.br/tutoriais/tutorialrsdh/default.asp> Acesso em: 12 de dezembro de 2009.

[5] Recomendação ITU-T G.810 (1996) *Definitions and terminology for synchronization networks*.

[6] Recomendação ITU-T G.803 (2000) *Architecture of transport networks based on the synchronous digital hierarchy (SDH).*

[7] Recomendação ITU-T G.7041/Y.1303 (2005) *Generic Frame Procedure (GFP)*.

IV. Pré-relatório

Após a leitura da introdução teórica, responder os itens abaixo:

1. Explique a finalidade dos tributários virtuais e de que forma eles são utilizados em uma rede SONET/SDH.

2. Esquematize a estrutura do quadro de um sinal STS-48 (STM-16).

3. Explique a função de cada equipamento SONET/SDH e exemplifique o uso de ADMs, TMs, e DCSs em redes metropolitanas.

4. De que maneira o tráfego Ethernet é transportado em uma rede SONET/SDH que utiliza GFP? E como seria transportado sem o uso do GFP?

5. Explique detalhadamente os dois modos de mapeamento de *payload* do GFP. Exemplifique.

V. Procedimentos

Lista de equipamentos e ferramentas utilizados:
- Três nós SDH OptiX OSN 3500 .
- Seis interfaces STM-64.
- Duas interfaces de tributário FastEthernet com GFP.
- Atenuadores variáveis.
- Cordões ópticos e cabos UTP Cat5e.
- Sistema de gerência T2000 Huawei.
- Duas estações com interfaces FastEthernet.

O experimento possui duração de 02h00min e deve ser executado no laboratório Optix.

1. Criar os três nós do anel unidirecional SDH no sistema de gerência e ligar fisicamente as interfaces STM-64 conforme topologia da Figura 10. Atenção para os níveis de potência utilizados. Para reduzir o nível de potência na entrada das interfaces STM-64, inserir atenuadores variáveis que também simulam as perdas inerentes de transmissões de longa distância.

2. Estabelecer e configurar os enlaces com duas fibras entre quaisquer dois nós adjacentes. Configurar a fibra que percorre o sentido horário como fibra de trabalho e a outra como fibra de proteção.

3. Conectar uma estação com placa de rede FastEthernet (100Mbps) à interface FastEthernet do equipamento do nó 1 e uma segunda estação à interface FastEthernet do equipamento do nó 2. Verificar que a rede está operando normalmente e os quadros estão sendo transportados sem nenhum *payload* GFP nas fibras de trabalho. Verificar também se não há tráfego nas fibras de proteção. Isso pode ser verificado na seção de alarmes do sistema de gerência como um aviso de baixa importância indicando que os quadros estão sendo recebidos e transportados vazios

4. Após configuração da rede, definir o endereço IP da estação A como 192.168.1.1 e a máscara de sub-rede como 255.255.255.0. Definir o endereço IP da estação B como 192.168.1.2 e a máscara de sub-rede como 255.255.255.0. Dessa maneira, ambas as estações estarão na mesma sub-rede. Em seguida, abrir o *prompt* de comando da estação A e executar o seguinte comando: ping 192.168.1.2. O protocolo disparará três pacotes *echo request* de controle para a estação B e esperará por três pacotes *echo reply*. Se o transporte pela rede SDH for bem sucedida, o resultado do comando *ping* deve obter sucesso e mostrar detalhes do tempo de ida e volta dos três pacotes (*Round Trip Time*- RTT). Anotar estes valores e repetir o processo para a estação B. Como a rede SONET/SDH é baseada em circuitos e não há atrasos de filas, os tempos RTT devem ser constantes neste cenário.

5. Ativar e configurar o GFP no sistema de gerência e verificar que a rede está operando normalmente e os quadros estão sendo transportados sem nenhum *payload* GFP nas fibras de trabalho. Verificar também se não há tráfego nas fibras de proteção.

6. Repetir item 4.

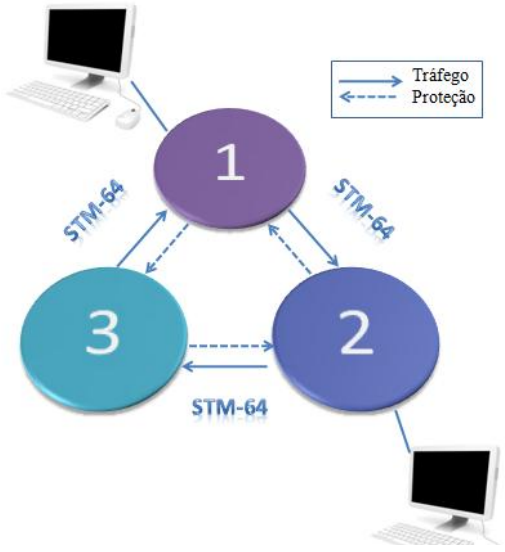


Figura 10 – Topologia SDH em anel unidirecional com duas fibras e três nós

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

VI. Relatório

Após a execução do experimento, descrever eventuais problemas ocorridos e incluir os seguintes pontos no relatório (formato IEEE).

- Captura da tela da topologia operante no sistema de gerência.
- Captura da tela com os resultados do comando *ping* sem o GFP ativo e com o GFP ativo.
- Explicação da maneira que o quadro Ethernet contendo o protocolo ICMP foi encapsulado e transportado no caso em que usou o GFP e no caso em que o GFP não foi utilizado.
- Devido a algumas limitações de equipamentos, o cenário elaborado no laboratório não permitiu explorar a verdadeira vantagem do GFP. Para tal, muitos usuários FastEthernet deveriam ser conectados à rede SDH e terem seus dados mapeados em quadros GFP. Explique qual seria a diferença, neste caso, se não fosse utilizado o GFP.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Experimento nº3

Proteção em sistemas SONET/SDH

Anexo III

I. Objetivo

Análise das principais formas de proteção e redundância em sistemas de transporte de alta velocidade SONET/SDH e implementação da proteção em anel unidirecional com duas fibras e três nós.

II. Introdução

Provavelmente, a característica mais marcante das redes SONET/SDH, quando comparadas com o sistema digital PDH, é a topologia em anel. O conceito de proteção já existia em redes PDH, mas novos padrões de demanda por proteção e confiabilidade foram introduzidos nas redes SONET/SDH [1].

As falhas relacionadas à fibra óptica podem possuir causas diversas, mas em sua grande maioria elas provêm de rompimentos em cabos enterrados provocados por construções ou escavações conforme mostrado na Tabela 1 [1].

Causa da falha	Porcentagem
Rompimento em cabos enterrados	51%
Rompimentos em cabos aéreos	24%
Outras causas e equipamentos	15%
Cross-connects digitais	7%
Sincronismo	2%
Componentes internos de energia	1%

Tabela 1 - Causas de falhas de sistemas de fibra óptica. Adaptado de [1].

Comutação automática de proteção linear (APS) [1]

A comutação automática de proteção (*Automatic Protection Switching*- APS) é uma técnica que já era utilizada em redes PDH. Existem diferentes tipos de proteção linear. A proteção 1:N que consiste no uso de N enlaces ativos (trabalho) e um enlace de proteção é freqüentemente utilizada em enlaces ponto-a-ponto. Assim que o sistema detecta uma falha em qualquer um dos enlaces ativos, automaticamente é feita a comutação do tráfego daquele enlace especifico para o enlace de proteção. Normalmente, o processo inverso de retornar o tráfego para o enlace original é feito manualmente. A detecção de uma falha do enlace pode ser ativada não somente por uma falha total do enlace, mas por uma alta quantidade de erros ou baixa qualidade de sinal. Para o usuário final, em uma conversação telefônica, os efeitos dessa troca de enlace são percebidos como uma breve interrupção da conversação ou como um rápido congelamento da imagem em um cenário de *broadcast* de televisão. O tempo médio da comutação é geralmente menor que 50 milissegundos.

Um grave problema associado à proteção 1:N é a situação em que mais de um enlace falhe ao mesmo tempo. Para contornar este problema, áreas de alto-risco adotam a proteção 1:1 (Fig. 1) onde cada enlace ativo possui seu próprio enlace de proteção.

A técnica de proteção 1+1 (Fig. 2) refere-se ao fato de que o sinal é transmitido no enlace de trabalho juntamente com uma cópia do sinal transmitido no enlace de proteção. O receptor é incumbido de selecionar o sinal com melhor qualidade. A proteção 1:1, ao contrário, envia o sinal somente pelo enlace ativo podendo transmitir tráfego de baixa prioridade pelo enlace de proteção. Quando uma falha ocorre, o tráfego do enlace ativo é transferido para o enlace de proteção e o tráfego de baixa prioridade é temporariamente suspenso até que as condições normais sejam restauradas. A técnica 1:1 possui melhor aproveitamento da capacidade dos enlaces, mas exige uma ação de comutação mais elaborada quando uma falha ocorre. Isso afeta diretamente o tempo de resposta de restauração do serviço.

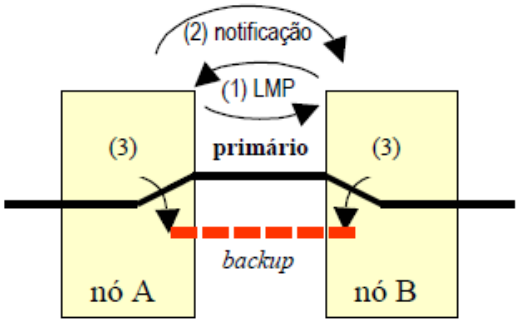


Figura 1 - Proteção 1:1

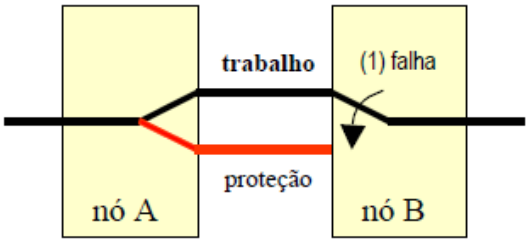


Figura 2 - Proteção 1+1

Um importante fator quando se trata de proteção é o posicionamento e caminho dos enlaces. Conforme apresentado na Figura 3, as diferentes rotas e caminhos tomados pelas fibras em um sistema são fatores determinantes na capacidade de sobrevivência de sistemas com proteção. Fibras que se localizam no mesmo duto e no mesmo *feeder* possuem uma altíssima probabilidade de se romperem ao mesmo tempo. Já fibras que passam por *feeders* diferentes e por rotas diferentes apresentam uma baixa probabilidade de falharem ao mesmo tempo. O melhor arranjo possível para a rede de acesso apresentada na Figura 3 seria o uso de duas centrais ligadas entre si com *feeders* diferentes e rotas diferentes. Porém, essa é uma solução que apresenta um alto custo de implementação e nem sempre é uma opção viável.

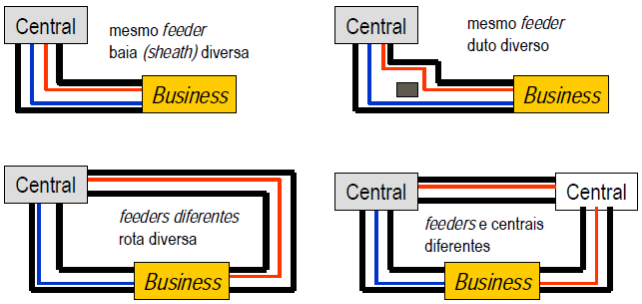


Figura 3 - Diversidade e proteção da rede de acesso

Anéis SONET/SDH [1]

Um anel SONET/SDH é definido como uma coleção de dois ou mais elementos de rede SONET/SDH que formam um *loop* fechado. Os anéis são comumente conhecidos como *self-healing* pela capacidade automática de restauração após uma falha ou deterioração dos sinais da rede.

Existem várias arquiteturas de anéis disponíveis, mas basicamente três atributos são responsáveis pelas diferentes composições de arquitetura como ilustrado na Tabela 2.

Atributo	Opções
Número de fibras por enlace	2 ou 4 fibras
Direção do sinal	Unidirecional Bidirecional
Nível de proteção de comutação	Comutação de linha Comutação de caminho
Proteção	Proteção de *span* Proteção de anel

Tabela 2 - Tipos de anéis SONET/SDH

Na prática, com raras exceções, somente os seguintes tipos de anéis são implementados em larga escala:

- 2 fibras, unidirecional, comutação de caminho (*2-fiber Unidirectional Path Switched Ring*, UPSR - SONET) ou proteção de conexão de subrede (*subnetwork connection protection*, SNCP - SDH)

- 2 fibras, bidirecional, comutação de linha (*2-fiber Bidirectional Line Switched Ring,* BLSR- SONET) ou anel de proteção compartilhada da seção de multiplexação com duas fibras (*Multiplex section shared protection ring,* MS-SPRing - SDH)

- 4 fibras, bidirecional, comutação de linha (*4-fiber Bidirectional Line Switched Ring*, BLSR- SONET) ou anel de proteção compartilhada da seção de multiplexação com quatro fibras (MS-SPRing - SDH)

Em um anel unidirecional (Fig. 4), o tráfego é roteado de tal forma que as duas direções de uma conexão entre dois nós viajem em volta do anel pela mesma direção. Dessa forma, cada conexão utiliza toda a capacidade de banda em torno de toda a circunferência do anel. Por convenção, todo o tráfego de trabalho em anéis unidirecionais trafega no sentido horário.

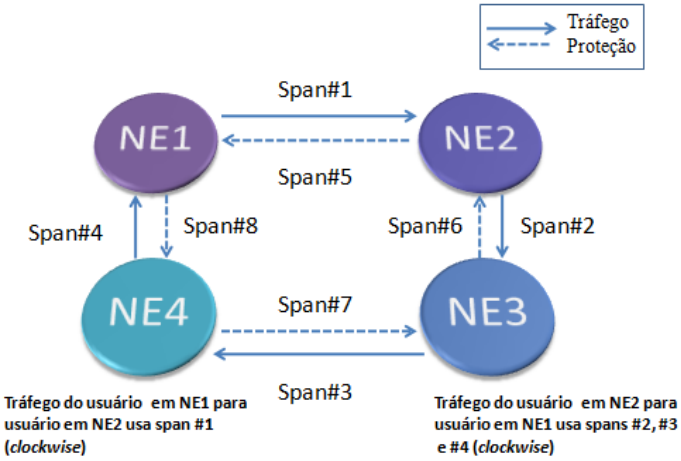


Figura 4 - Anel unidirecional

Já em um anel bidirecional (Fig. 5), o tráfego de trabalho é roteado de tal forma que as duas direções de uma conexão trafeguem os sinais pelo anel pelos mesmos nós, mas em direções opostas.

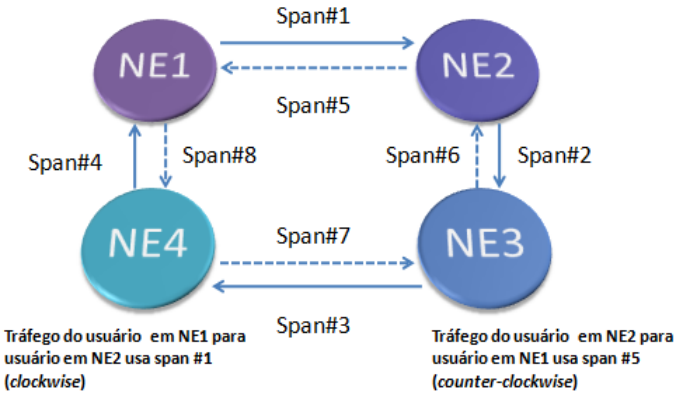


Figura 5 - Anel bidirecional

Os dois tipos de anel podem utilizar duas fibras ou quatro fibras entre cada nó conforme ilustrado na Figura 6. Em um anel bidirecional de duas fibras, cada *span* de fibra carrega o canal de tráfego de trabalho e o canal de tráfego de proteção. Já o anel bidirecional de quatro fibras possui, por *span*, duas fibras que carregam os canais de tráfego de trabalho e duas fibras que carregam os canais de proteção.

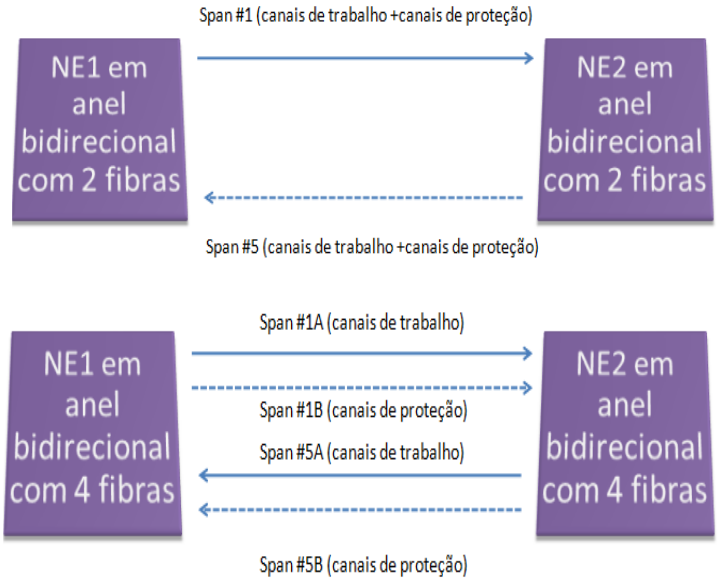


Figura 6 - Proteção bidirecional de duas e quatro fibras

Uma outra característica é o tipo de comutação de proteção empregada. A comutação de linha (Fig. 7) restaura todos os canais de tráfego ativo em toda a capacidade OC-n em uma única operação de proteção. A capacidade de proteção não deve ser utilizada enquanto o anel estiver em operação normal. Esse tipo de proteção é caracterizada como compartilhada.

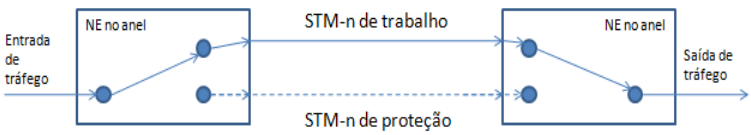


Figura 7 - Comutação de linha

A comutação de caminho (Fig. 8) restaura todos os canais a um nível menor do que toda a capacidade OC-n (STM-n). Os sinais são enviados em ambos os enlaces ativos e de proteção e o receptor monitora ativamente a qualidade dos sinais e escolhe o melhor para a recepção. A comutação de caminho (dedicada) é universalmente feita em anéis unidirecionais de duas fibras. A comutação de linha, por sua vez, é utilizada em anéis bidirecionais de duas ou quatro fibras.

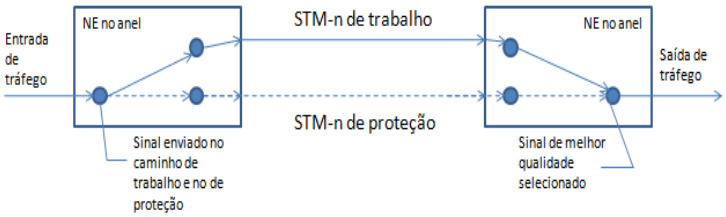
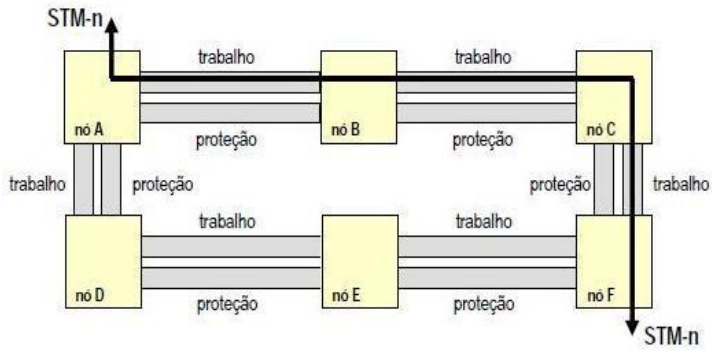


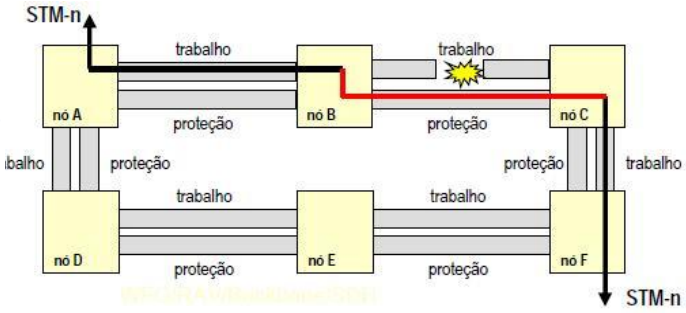
Figura 8 - Comutação de caminho

Anéis que utilizam quatro fibras oferecem proteção contra falhas não somente de um par de fibras, mas contra dois pares entre quaisquer dois nós do anel. Durante a operação normal, os sinais são divididos e enviados nas duas direções do anel. Se um par de fibras falhar, o sinal é enviado pelo outro par de fibra na mesma direção (proteção de *span*). Se o outro par de fibras apresentar falha, o sinal será transportado pela outra direção do anel pelo par de proteção (proteção de anel). Dessa maneira, anéis que utilizam quatro fibras podem continuar operando mesmo após múltiplas falhas.

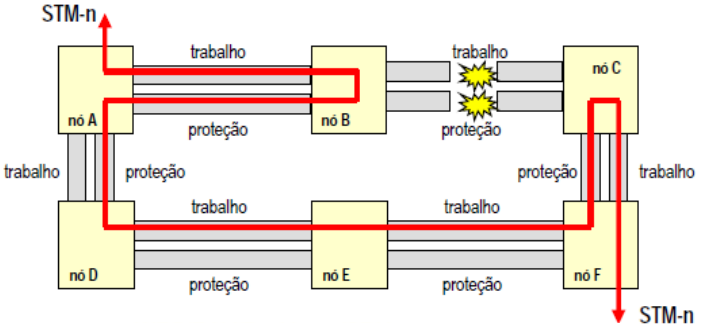
Na proteção de *span*, tudo o que é preciso fazer é comutar o tráfego do par ativo para o par de proteção. O fluxo do tráfego não é interrompido. Porém, a comutação de anel provoca a interrupção do fluxo de tráfego entre os dois nós enquanto o sinal viaja ao destino pela outra direção do anel. As duas situações estão ilustradas na Figura 9.



A) Operação normal



B) Proteção de *span* entre os nós B e C.



C) Proteção de anel devido à segunda falha de fibra

Figura 9 – Proteção de *span* e proteção de anel em um MS-SPring com quatro fibras

Os principais mecanismos de proteção das tecnologias SONET e SDH estão resumidos na Tabela 3.

Tipo de proteção	SONET	SDH
Linear 1+1	Proteção dedicada	Proteção dedicada
Linear 1:N	Proteção compartilhada	Proteção compartilhada
Anel compartilhado	BLSR 2 ou 4 fibras	MS-SPRing 2 ou 4 fibras
Anel dedicado	UPSR	SNCP

Tabela 3 – Mecanismos de proteção SONET/SDH

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

Comutação automática de proteção de anel (APS)

Dois bytes provenientes do RSOH (SDH) que são conferidos por todos os equipamentos da rede SONET/SDH com exceção dos regeneradores, exercem um papel fundamental na comutação automática de proteção. Os bytes K1 e K2 comunicam mensagens APS e são usados especificamente para a recuperação de enlaces após a ocorrência de uma falha [2].

A comutação automática de proteção ocorre no nível de seção de multiplexação e a detecção da perda de sinal (*Loss of signal- LOS*) é um alarme de nível STM. Todos os STM-n devem ser capazes de decidir se e onde o APS deve ocorrer [2]. Quando utilizado em uma topologia em anel SDH, os bytes K1 e K2 possuem a estrutura e as mensagens descritas na Figuras 10 e 11 respectivamente.

Byte K1 para APS em anel

Switch Request (b1-4)	Destination Node (b5-8)

0000 - No Request (NR)
1111 - Lockout of Protection (span) (LP-S)
1110 - Forced Switched (span) (FS-S)
1101 - Forced Switched (ring) (FS-R)
1100 - Signal Fail (span) (SF-S)
1011 - Signal Fail (ring) (SF-R)
1010 - Signal Degrade (protection) (SD-P)
1001 - Signal Degrade (span) (SD-S)
1000 - Signal Degrade (ring) (SD-R)
0111 - Manual Switch Request (span) (MS-S)
0110 - Manual Switch Request (ring) (MS-R)
0101 - Wait to Restore (WTR)
0100 - Exerciser (span) (EXER-S)
0011 - Exerciser (ring) (EXER-R)
0010 - Reverse Request (span) (RR-S)
0001 - Reverse Request (ring) (RR-R)

Figura 10 – Codificação byte K1 para APS em anel (SDH). Adaptado de [1]

Byte K2 para APS em anel

Source Node (b1-4)	L/S	Status (b6-8)

000 - Idle (normal)
111 - MS-AIS
110 - MS-RDI
101 - Reserved for future use
100 - Reserved for future use
011 - Extra Traffic on protection channels
010 - Bridged and Switched (Br&Sw)
001 - Bridged (Br)

Figura 11 – Codificação byte K2 para APS em anel (SDH). Adaptado de [1].

Os primeiros quatro bits do byte K1 são os bits de *Switch Request*. Dezesseis mensagens são possíveis e estão listadas na Figura 10. Em operação normal, nenhuma requisição de APS é feita e os bits são '0000'. Essas requisições podem ser de anel ou de *span* e podem ser iniciadas externamente (ex: MS-R) ou sinalizadas automaticamente (ex: SF-R) pelos nós do anel. Por exemplo, falhas de sinal (SF-S, SF-R) são ativadas pela perda de frame (*Loss of frame* - LOF) ou a perda de sinal (LOS) no nó. Já a degradação de sinal (SD-P, SD-S, SD-R) é causada por taxas elevadas de erros indicados pelo byte B1 *Bit Interleaved Parity* (BIP) do MSOH [1].

Os últimos quatro bits do byte K1 referenciam o identificador do nó de destino. São possíveis 16 nós de destinos. O nó de destino é sempre o nó final do anel para onde a mensagem K1 é destinada [1].

De acordo com a Figura 11, temos que os quatro primeiros bits do byte K2 referenciam o nó de origem do anel (0-15). O quinto bit é o bit *Long/Short bit.* Quando seu valor está em '0', significa caminho curto e quando seu valor está em '1' significa caminho longo. Mensagens 'S' interpretam *Switch Requests* (*span*) como requisições. Mensagens 'L' interpretam *Switch Requests* (*span*) como relatórios de status. Para o SONET, existe uma pequena diferença na codificação do byte K2 em relação ao SDH. O MS-AIS é substituído por *Alarm Indication Signal* e o MS-RDI é substituído por *Remote Defect Indicator* [1].

Os últimos três bits do byte K2 indicam oito possíveis mensagens de status. A operação normal do anel é indicada com '000' (*idle*).

As Figuras 12 e 13 indicam como seria a operação normal de um anel SDH e quais valores os bytes K1 e K2 assumiriam para cada STM.

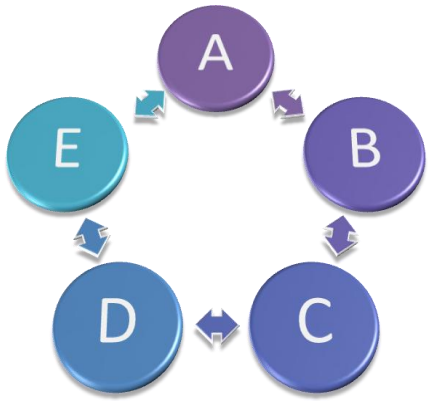


Figura 12 - Anel SDH com cinco nós

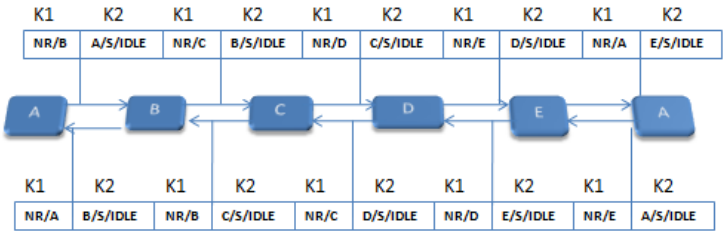


Figura 13 - Bytes K1/K2 em operação normal no anel

Todos os quatros primeiros e últimos bits dos bytes K1/K2 são zeros. Isto indica que não há requisição de APS, o caminho curto está sendo utilizado, e que APS está inoperante. Os oito bits centrais formam os identificadores de nós de origem e destino.

Exemplos

APS linear 1:N unidirecional [2]

Considerando o cenário da Figura 14, um corte é feito na fibra de trabalho 1 e imediatamente o APS linear entra em funcionamento para se recuperar da falha. Por convenção, o equipamento de rede A (transmissor) é chamado de *head end* e o equipamento de rede B (receptor) é chamado de *tail end*. É dever do *tail end* requisitar uma comutação APS baseado na detecção de perda de sinal (LOS), perda de qualidade do sinal, ou por comando externo. A perda de sinal é detectada pelo receptor quando não é detectada nenhuma transição do sinal, antes do embaralhamento, por T segundos, onde 2,3 µs $\leq$ T $\leq$100 µs. O estado de LOS é removido quando são percebidas transições no sinal por 125 µs. A degradação da qualidade do sinal é percebida pelo byte B1 *Byte Interleaved Parity* 8 (BIP-8). O receptor é capaz de contar quantos erros foram detectados no total de bytes recebidos e fazer uma estimativa da taxa de erro (BER).

Assim que a perda de sinal é detectada, o código '1100' é enviado nos bits de 1-4 do byte K1 pelo receptor ao transmissor (Fig. 10). O código do canal que está requerendo proteção também é enviado nos bits 5-8 do byte K1. Quando o transmissor recebe a requisição do receptor, ele primeiramente comuta o tráfego da fibra de trabalho com problemas para a fibra de proteção. Em seguida, o número do canal da fibra de trabalho é enviado nos bits 1-4 do byte K2 na fibra de proteção. O receptor, então, seleciona a fibra de proteção como substituta da fibra de trabalho defeituosa.

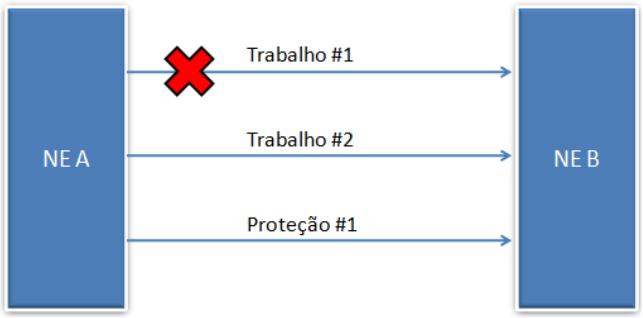


Figura 14 – APS linear 1:N unidirecional

APS linear 1:N bidirecional [2]

No cenário bidirecional da Figura 15, a fibra de trabalho 1 sofre um corte na direção do equipamento de rede A para o equipamento de rede B.

No caso bidirecional, o transmissor é responsável por iniciar a segunda metade da comutação bidirecional. Ele insere o código '0010' (*Reverse Request Code*) nos bits 1-4 do byte K1 e o número do canal da fibra de trabalho a ser comutada nos bits 5-8 do byte K1. O receptor processa a requisição de comutação e coloca o tráfego da fibra de trabalho defeituosa na fibra de

proteção. O número do canal também é inserido nos bits 1-4 do byte K2 enviado na fibra de proteção. Dessa maneira, o APS linear bidirecional está completo.

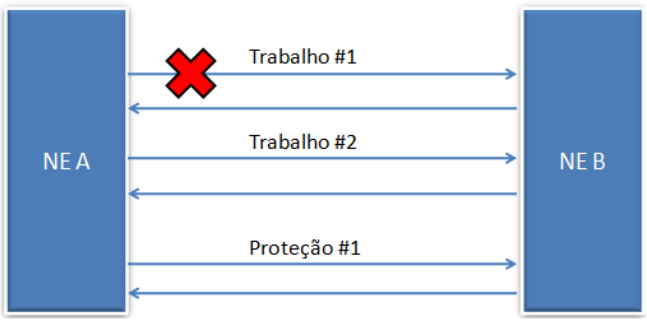


Figura 15 – APS linear 1:N bidirecional

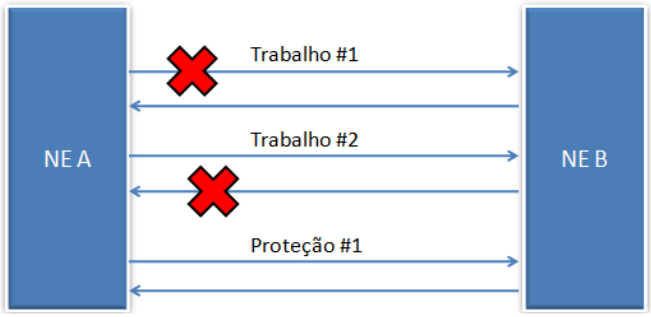


Figura 16 – APS linear 1:N bidirecional com múltiplas falhas

APS linear 1:N bidirecional com múltiplas falhas [2]

O cenário da Figura 16 explora o caso de múltiplas falhas e a questão de prioridade das requisições de comutação.

A falha na fibra de trabalho 1 foi causada por corte da fibra e ocorre no tempo T_2. A falha na fibra de trabalho 2 ocorre devido à degradação do sinal e ocorre no tempo T_1 ($T_2 > T_1$).

Como a fibra de trabalho 2 entra no estado de degradação da qualidade do sinal antes da fibra de trabalho 1, uma comutação bidirecional é executada prontamente. O equipamento A detecta esta condição e envia ao equipamento B o código '1001' de degradação de sinal nos bits 1-4 do byte K1. 'B' comuta o tráfego para fibra de proteção e envia o byte K2 com o número do canal. 'A' seleciona a fibra de proteção como substituta da fibra de trabalho 2. Em seguida, 'B' envia o *reverse request* para a fibra de trabalho 2 no byte K1 e após ter recebido o byte K2 também muda para a fibra de proteção. No tempo T_2, 'B' detecta a perda de sinal na fibra de trabalho 1 e envia o código '1100' (SF-S) para 'A' no byte K1. Como a prioridade da perda de sinal é maior que a perda da qualidade do sinal, 'A' comuta o tráfego da fibra de trabalho para a fibra de proteção e envia o byte K2 para 'B'. Por sua vez, 'B' seleciona a fibra de proteção no lugar da fibra de trabalho 1. Por último, 'A' envia o *reverse request* da fibra de trabalho 1 no byte K1 e aguarda o byte K2. 'B' comuta o tráfego da fibra de trabalho 1 para a fibra de proteção e envia o byte K2 para 'A'. 'A' finalmente seleciona a fibra de proteção no lugar da fibra de trabalho 1.

APS em um anel bidirecional com 4 fibras [3]

Considerando a topologia em anel com sete nós da Figura 17, temos uma falha na fibra de trabalho (*span*) que vai do nó E ao nó F e foi causada por um corte na fibra. Neste exemplo, uma comutação de *span* é executada e a condição de perda de sinal nos canais de trabalho do anel de quatro fibras bidirecional é removida. O estado inicial do anel é o estado *idle*. A ação de *bridge* ilustrada na Figura 11 nos códigos '010' e '001' se refere ao fato de se transmitir sinais idênticos nos canais da fibra de trabalho e na fibra de proteção enquanto a ação de *switch,* ilustrada nas Figuras 10 e 11, se refere à seleção do tráfego normal proveniente da fibra de proteção em detrimento da fibra de trabalho.

No tempo T_1, o nó F detecta a condição de perda de sinal (LOS) na fibra de trabalho. Ele se torna um nó de comutação e envia requisições de comutação em ambas as direções do anel. O nó G e todos os nós intermediários do caminho longo entram no modo *pass-through K-byte*. Neste estado, os nós simplesmente retransmitem a informação recebida na mesma direção da transmissão. Ao receber a requisição de comutação do nó F no caminho curto, o nó E executa uma comutação de *span* e transmite uma requisição de comutação de *span* no caminho longo e uma *reverse request* no caminho curto. O nó F, ao receber os reconhecimentos de comutação do nó E no caminho curto, executa um *span bridge and switch* (Br&Sw) e atualiza seu byte K. O nó E ao receber os reconhecimentos

do Br&Sw do nó F no caminho curto, completa a comutação. A sinalização atinge, então, um estado estável.

No tempo T_2, a condição de perda de sinal é removida, o nó F entra no estado *Wait-To-Restore* (WTR) e sinaliza seu estado para ambas as direções do anel. O nó E ao receber a requisição de comutação WTR do nó F no caminho curto envia um *reverse request* no caminho curto e um WTR no caminho longo. Quando o tempo T_3 é atingido, o intervalo do WTR expira. O nó F retira a comutação de *span* e envia o código '0000'(*No Request*) no byte K1. O nó E ao receber o código '0000' do nó F no caminho curto, retira seu Br&Sw e envia o código *idle* no byte K2. O nó F ao receber o código *idle* no caminho curto, retira seu estado *bridge* e envia também o código *idle* no byte K2. Em seguida, todos os nós restantes cascateiam de volta ao estado *idle*. As Figuras 18 e 19 ilustram a troca de informações dos bytes K1 e K2 e os diversos estados dos nós.

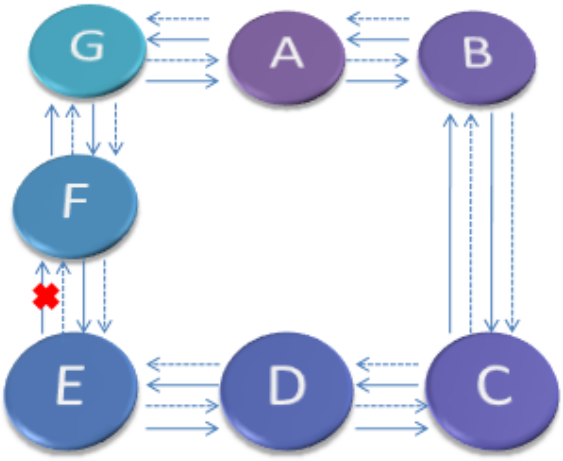


Figura 17 – Anel bidirecional 4 fibras

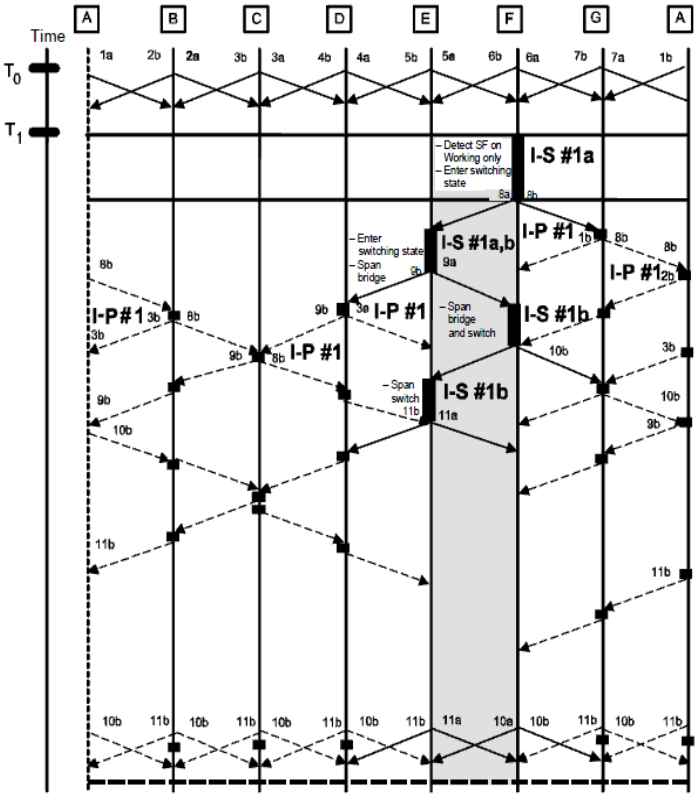


Figura 18 – Diagrama temporal [3]

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

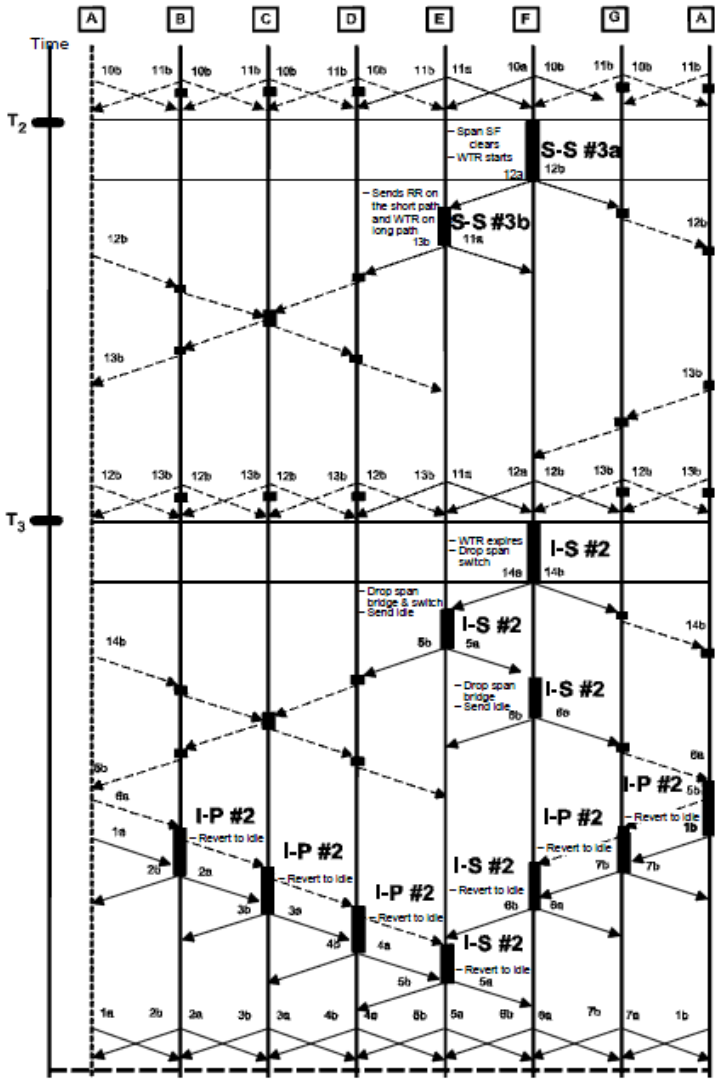


Figura 18 – Diagrama temporal (cont.) [3]

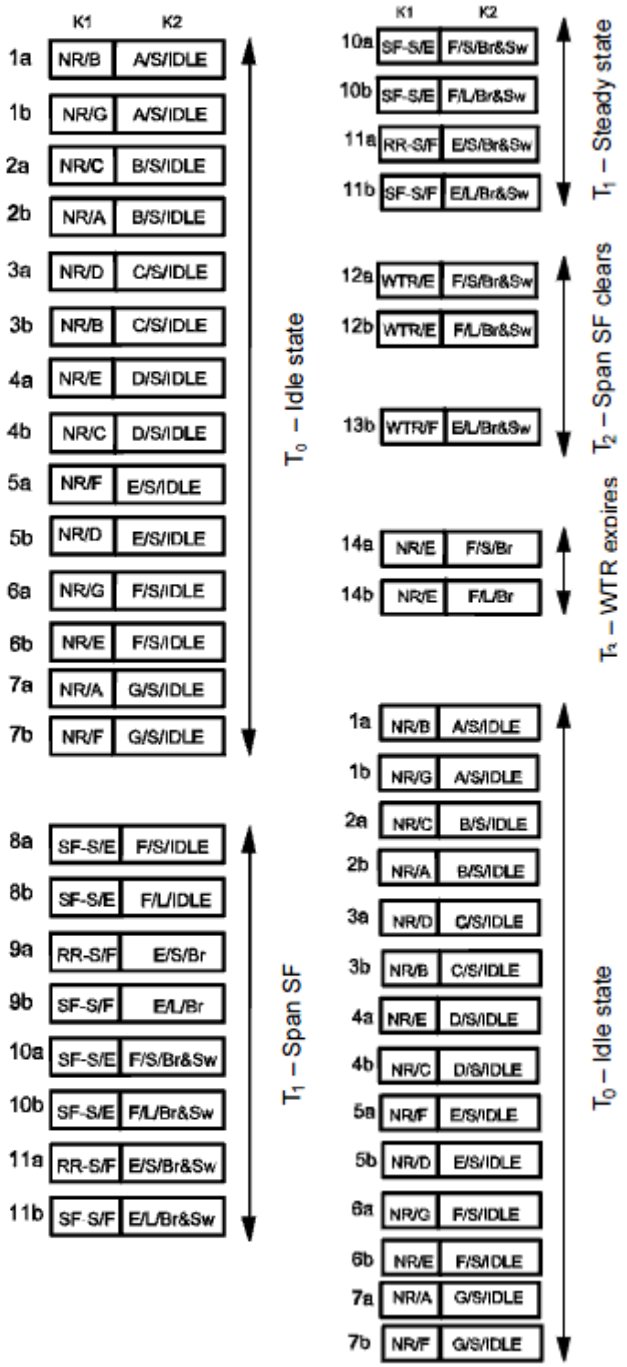


Figura 19 – Estados dos bytes K1 e K2 [3]

III. Referências Bibliográficas

[1] GORALSKI, Walter J. *SONET/SDH*, Third edition (2002).
[2] BERNSTEIN, Greg; RAJAGOPALAN Bala; SAHA Debanjan, *Optical Network Control Architecture Protocols and Standards* (2003).
[3] Recomendação ITU-T G.841 (1998) *Types and characteristics of SDH network protection architectures.*

IV. Pré-relatório

Após a leitura da introdução teórica, responder os itens abaixo:

1. Cite e explique os diferentes tipos de comutação automática de proteção (APS) linear existentes.
2. Qual tipo de proteção em anel utiliza melhor a largura de banda disponível? Por quê?
3. Explique a diferença entre proteção de *span* e proteção de anel.
4. Explique sucintamente as vantagens e as desvantagens das diversas topologias de proteção em anel.
5. Seguindo o modelo das Figuras 18 e 19, desenhe o diagrama temporal e ilustre os estados dos bytes K1 e K2 para o caso de uma corte na fibra de proteção de um anel bidirecional de quatro fibras com quatro nós (n1, n2, n3 e n4). Assuma que a falha tenha ocorrido entre o nó 1 e o nó 2.

V. Procedimentos

Lista de equipamentos e ferramentas utilizados:
- Três nós SDH OptiX OSN 3500.
- Seis interfaces STM-64.
- Atenuadores variáveis.
- Cordões ópticos.
- Sistema de gerência T2000 Huawei.

O experimento possui duração de 02h00min e deve ser executado no laboratório Optix.

1. Criar os três nós do anel unidirecional SDH no sistema de gerência e ligar fisicamente as interfaces STM-64 conforme topologia da Figura 20. Atenção para os níveis de potência utilizados. Para reduzir o nível de potência na entrada das interfaces STM-64, inserir atenuadores variáveis que também simulam as perdas inerentes de transmissões de longa distância.
2. Estabelecer e configurar os enlaces com duas fibras entre quaisquer dois nós adjacentes. Configurar a fibra que percorre o sentido horário como fibra de trabalho e a outra como fibra de proteção.
3. Configurar o APS em todos os nós da rede para que seja restabelecido o tráfego na fibra de trabalho assim que for removido o estado de perda de sinal. Alterar o valor padrão do tempo de *Wait-To-Restore* de 5 minutos para 1 minuto.
4. Verificar pelo sistema de gerência que a rede está operando normalmente e os quadros estão sendo transportados sem nenhum *payload* e que não há tráfego no enlace de proteção. Isso pode ser verificado na seção de alarmes do sistema de gerência como um aviso de baixa importância indicando que os quadros estão sendo recebidos e transportados vazios.
5. Criar um ponto de falha, pelo sistema de gerência, desativando-se o laser da interface STM-64 ativa da fibra de trabalho do nó 1. Para tal, clique em **Window** selecione **NE Information List**. Clique com o botão direito no **NE** e selecione **NE Explorer**. Em seguida, selecione uma placa e clique em **Configuration→ SDH Interface** na árvore de funcões. No botão rádio, selecione a opção **By Board/Port(Channel)**. Escolha **Port** na lista, dê um clique duplo no campo **Laser Switch**, e clique em **Close**. Selecione **Apply** e uma mensagem de aviso de interrupção de serviços aparecerá. Clique em **OK**.
6. Confirmar pela aparição de alarmes no sistema de gerência que foi detectada a perda de sinal (LOS) na fibra de trabalho entre nó 1 e nó 2 e observar se ocorre a comutação automática de proteção da fibra de trabalho para a fibra de proteção como previamente configurado. Os quadros transportados anteriormente pelo STM-64 (nó 1→nó 2) devem utilizar o caminho de proteção 1-3-2 para sair do nó 1 e chegar ao nó 2.
7. Novamente através do sistema de gerência, reativar o laser da interface STM-64 e verificar se ocorre a comutação do tráfego da fibra de proteção para a fibra de trabalho devido à expiração do tempo WTR previamente configurado como um minuto. Medir o tempo. O processo de ativação do laser é o mesmo da desativação exceto pela escolha de **Open** no campo **Laser Switch**.
8. Verificar o restabelecimento da operação normal da rede pelo sistema de gerência e verificar se a fibra de trabalho que interliga a interface STM-64 do nó 1 à interface STM-64 do nó 2 está transportando novamente os quadros sem *payload* e se não há nenhum tipo de tráfego na fibra de proteção.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br

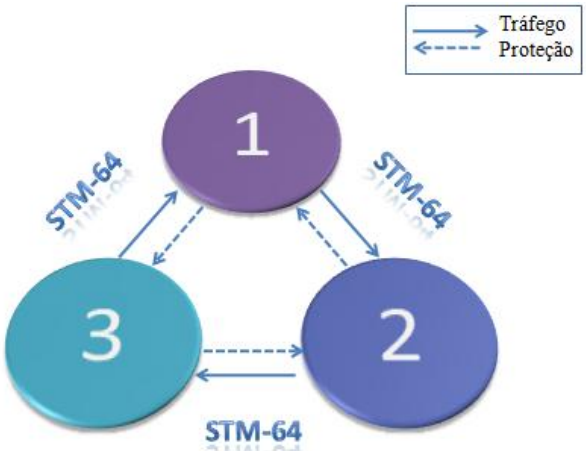


Figura 20 – Topologia SDH de anel unidirecional com duas fibras e três nós.

VI. Relatório

Após a execução do experimento, descrever eventuais problemas ocorridos e incluir os seguintes pontos no relatório (formato IEEE).

- Captura da tela da topologia operante no sistema de gerência (passo 4).
- Descrição detalhada dos alarmes gerados e seus respectivos significados no sistema de gerência.
- Explicação da maneira no qual se comportaram os bytes K1 e K2 durante o experimento para todos os nós da rede SDH.
- Verificação do tempo medido com o tempo configurado do *Wait-to-Restore*.

Faculdade de Tecnologia, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Gleba A, Avenida L3 Norte, CEP 70.910-900, Brasília - DF
Caixa postal 4386, fone +55 61 3307 2300, fone/fax +55 61 3273 8893, ftd@unb.br, www.ft.unb.br