



**Emanuel António
Raimundo Moreira**

**Encaminhamento Robusto em Redes GMPLS sobre
SDH**



**Emanuel António
Raimundo Moreira**

**Encaminhamento Robusto em Redes GMPLS sobre
SDH**

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica do Doutor Amaro Fernandes de Sousa, Professor Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

o júri

Presidente

Prof. Doutor Rui Jorge Morais Tomaz Valadas
Professor Associado da Universidade de Aveiro

Prof. Doutor João Luís da Costa Campos Gonçalves Sobrinho
Professor Auxiliar do Instituto Superior Técnico da Universidade Técnica de Lisboa

Prof. Doutor Amaro Fernandes de Sousa (Orientador)
Professor Auxiliar da Universidade de Aveiro

agradecimentos

Ao Prof. Amaro de Sousa por todo o seu apoio, em especial pelas estimulantes reuniões de trabalho e pela compreensão demonstrada.

Aos meus pais pelos carinhosos incentivos que me ajudaram a terminar este trabalho.

À Sandra cuja paciência, compreensão e carinho me serviram sempre de porto de abrigo, principalmente nos momentos mais difíceis. E à Maria Eduarda, a nossa filhota linda, cujo sorriso lindo, me serviu de estímulo na conclusão deste trabalho.

palavras-chave

encaminhamento robusto, algoritmos de custo mínimo, SDH, GMPLS, protecção, simulação.

resumo

Esta dissertação endereça o problema do encaminhamento robusto em redes GMPLS (*Generalised Multi-Protocol Label Switching*) sobre SDH (*Synchronous Digital Hierarchy*). Actualmente, o encaminhamento das redes SDH é feito de forma centralizada e por gestão. As redes SDH têm requisitos de recuperação a falhas muito exigentes pelo que a robustez da rede é tipicamente implementada por mecanismos de protecção. Os mecanismos mais simples e de melhor desempenho em termos de tempo de recuperação a falhas são os que por cada VC (*Virtual Container*) de serviço também estabelecem um VC de protecção cujo percurso na rede não inclui nenhum dos comutadores do percurso de serviço (excepto os comutadores extremo). Estes mecanismos garantem a robustez completa da rede no caso de falha de um único elemento quer seja um comutador ou uma ligação.

A motivação para acrescentar a camada protocolar GMPLS às redes SDH é a de dotar estas redes com a capacidade do estabelecimento de VCs por sinalização e de permitir que o encaminhamento seja implementado o mais possível de uma forma distribuída diminuindo assim a sua dependência de um sistema centralizado de gestão. Os protocolos de encaminhamento GMPLS baseiam-se na atribuição de um custo a cada ligação de rede, fixo ou variável no tempo, e na determinação do encaminhamento pelos percursos cuja soma dos custos das ligações que o compõem é mínima. Nesta dissertação propõe-se a utilização de um algoritmo de pares de percursos disjuntos de custo mínimo no estabelecimento do par VC de serviço, VC de protecção. Quando existem restrições ao encaminhamento, a determinação do percurso de custo mínimo considera apenas as ligações que cumprem com as restrições.

Neste trabalho, propõe-se uma estratégia de atribuição de custos que não só depende da carga da ligação mas também do número e tipo de VCs que a ligação em cada momento suporta. Por simulação, mostra-se que esta estratégia tem melhor desempenho que as estratégias tradicionais de um custo fixo inversamente proporcional à capacidade da ligação ou de um custo que em cada instante é proporcional à carga de cada ligação.

Finalmente, propõe-se um esquema centralizado adicional que, sempre que um VC é libertado, recalcula os percursos de todos os VCs de protecção por forma a diminuir a probabilidade de bloqueio global da rede. O objectivo é obter uma melhoria adicional do desempenho não causando nenhuma interrupção de serviço pois, no estado normal da rede, apenas os VCs de serviço suportam efectivamente o tráfego.

No âmbito desta dissertação, o desempenho dos diferentes algoritmos de encaminhamento é analisado por simulação pelo que foi desenvolvido um simulador de eventos discretos adequado.

keywords

survivable routing, minimum cost routing, SDH, GMPLS, protection, simulation

abstract

This work addresses the problem of survivable routing in SDH (Synchronous Digital Hierarchy) networks with a GMPLS (Generalised Multi-Protocol Label Switching) routing plane. Currently, routing in SDH networks is done in a centralized way by management means. SDH networks have failure recovery exigent requirements so that network survivability is typically implemented with protection mechanisms. The most simple and efficient mechanisms are the ones that for each service VC (*Virtual Container*) also establish one protection VC through a path that does not include any of the nodes of the service VC (besides the origin and destination nodes). These mechanisms garanty the network survivability in case of a single node or link failure.

The motivation to add the GMPLS control plane on SDH networks is to enable these networks to establish VCs by signalling and to allow as far as possible routing in a distributed way reducing the network dependence on centralized management systems. The GMPLS routing protocols are based on minimum cost routing where either a static or variable cost value is assigned to each network link and the routing paths are given by the minimum cost paths. When there are routing constraints, the determination of the minimal cost paths is applied only to links that observe the constraints.

In this work, it is proposed a strategy of cost assignement that depends not only on the link load but also of the number and type of VCs that the link supports at each time. By simulation, it is shown that this strategy has better performance than the traditional strategies of a static cost inversely proportional to link capacity or of a cost that is proportional to link load at each time.

The proposed strategies use a routing algorithm that determines a minimal cost node-disjoint pair of paths in the establishment of the pair service VC and protection VC.

Finally, it is proposed an additional centralized scheme that when one VC is released, all protection VCs are recalculated in order to reduce the network overall blocking probability. This scheme allows an additional performance improvement and does not cause any service disruption because in normal operation the service VC's are the only ones supporting traffic.

The performance of all routing algorithms are determined by simulation with a discret event simulator developed for this purpose.

Índice

Capítulo 1 – Introdução.....	1
1.1. Enquadramento e Motivação.....	1
1.2. Objectivos.....	4
1.3. Estrutura da dissertação.....	6
Capítulo 2 – Tecnologia SDH	7
2.1. Funcionamento da tecnologia SDH	7
2.2. Elementos e Topologias de Rede.....	14
2.2.1. Multiplexador Terminal	14
2.2.2. Multiplexador (Mux/Demux).....	15
2.2.3. Multiplexador <i>Add/Drop</i>	15
2.2.4. Digital Cross-Connect (DXC).....	16
2.2.5. Topologias.....	16
2.3. Protecção SDH.....	18
Capítulo 3 – Redes GMPLS.....	21
3.1. Multiprotocol Label Switching (MPLS)	21
3.1.1. Constraint Routing – Label Distribution Protocol	25
3.1.2. Resource Reservation Protocol – Traffic Engineering	27
3.1.3. Sobrevivencialidade em Redes MPLS	28
3.2. Generalized MPLS.....	29
3.3. Plano de Controlo GMPLS	32
3.4. Extensões chave do GMPLS ao MPLS	35
3.5. Estabelecimento de LSPs em GMPLS	37
3.6. Extensões de Encaminhamento para Suporte de GMPLS	39
3.7. Parâmetros de Tráfego SDH	41
3.8. Sobrevivencialidade em Redes GMPLS.....	43
3.8.1. Estratégias de Recuperação	44
3.8.2. Sinalização de Link Protection	46
Capítulo 4 – Algoritmos de Encaminhamento Propostos.....	49
4.2.1. Algoritmo InvCap	55
4.2.2. Algoritmo InvBand	55
4.2.3. Algoritmo InvCap+PEN.....	57
4.2.4. Algoritmo InvBand+PEN.....	59
4.2.5. Reorganização de VC's de protecção	61
Capítulo 5 – Avaliação de Desempenho dos Algoritmos	65
5.1. Descrição do Simulador.....	65
5.1.1. Parâmetros de Entrada do Simulador	65
5.1.2. Critério de Paragem de Simulação.....	66
5.1.3. Medidas de Desempenho do Simulador.....	69
5.1.4. Funcionamento do Simulador.....	70
5.2. Casos de Estudo	75
5.2.1. Caso de Estudo A.....	75
5.2.2. Caso de Estudo B.....	76
5.2.3. Caso de Estudo C	78
5.3. Apresentação e Discussão de Resultados	79
Capítulo 6 – Considerações Finais	89

6.1. Conclusões.....	89
6.2. Trabalho Futuro.....	92
Referências.....	95
Bibliografia.....	97
Acrónimos.....	99
Anexos.....	103
Anexo A – Algoritmo de Dijkstra [17].....	103
Anexo B – Algoritmo de Suurballe's [17].....	105
Anexo C – Ficheiros de Entrada e Saída do Simulador.....	107
Anexo D – Resultados de Simulação dos Casos de Estudo.....	111

Capítulo 1 – Introdução

1.1. Enquadramento e Motivação

A Internet revolucionou as comunicações à escala mundial e alterou permanentemente os estilos de vida dos seres humanos fornecendo capacidade de comunicação a nível global, tornando-se um meio para a disseminação de informação e um mecanismo para a colaboração e interacção entre indivíduos e os seus computadores, sem olhar à localização geográfica.

A Internet é, nestas circunstâncias, a rede *core*, ou rede de área Alargada (*Wide Area Network - WAN*), que interliga milhares de redes de tamanho mais reduzido: redes de área Metropolitana (*Metropolitan Area Networks – MAN*) e redes de área Local (*Local Area Networks – LAN*). Estas redes de tamanho menor fazem o *upload* ou *download* de fluxos de dados de/ou para a rede *core*.

Conforme o tráfego na Internet cresce, as estratégias de implementação, manutenção e gestão das infra-estruturas tornam-se mais importantes dado que a Internet é constituída por diversos elementos de diferentes tecnologias que apresentam diferenças ao nível do plano de dados, do plano de controlo e do plano de encaminhamento. A acrescentar a isto, o uso das redes por parte dos utilizadores é de difícil previsão, sendo necessária a existência de

um sistema que permita o provisionamento de recursos dinamicamente. Por outro lado, a importância dos dados trocados nas redes e a sua fiabilidade, obriga ao desenvolvimento de soluções de sobrevivência de rede.

De entre as tecnologias que são usadas na Internet, o presente trabalho endereça o SDH (*Synchronous Digital Hierarchy*) [4], uma norma TDM (*Time Division Multiplex*) largamente usada pelos operadores para transportar e multiplexar diferentes circuitos de cliente.

Actualmente, as redes SDH são configuradas de forma estática através de sistemas de gestão centralizados o que levanta múltiplos problemas. Quando um cliente de um operador requer um circuito ponto-a-ponto, o pedido põe em movimento um processo que pode levar algumas semanas. Este processo (composto por uma cadeia de pequenas tarefas administrativas e técnicas) passa pelas fases seguintes: tarefas administrativas, operações manuais, operação de ferramentas de planeamento e provisionamento de circuitos [2].

As tarefas administrativas representam uma parte significativa do tempo de provisionamento. A maioria das tarefas pode ser automatizada, usando aplicações IT, mas o cliente tem de preencher um formulário para requerer o circuito. Este formulário pode ser preenchido através de uma aplicação de *Web* e pode ser automaticamente processado pelo operador.

As operações manuais que envolvem a instalação de equipamento, podem consumir outra parte significativa do tempo. Este tempo é denominado de tempo de primeira ligação (*first-time connection time*).

As tarefas de planeamento para obter o melhor desempenho dos recursos fazem uso de algumas ferramentas existentes que reduzem o tempo destas tarefas.

Depois das três fases anteriores, o operador tem de fornecer os circuitos usando os resultados obtidos no processo de planeamento. O tempo necessário para o provisionamento é muito variável. Pode ser francamente pequeno, na ordem de alguns minutos, se o operador possuir ferramentas que o ajudem no provisionamento sobre redes com equipamento heterogéneo ou o processo pode demorar dias se isso não acontecer. Mas

desenvolver ferramentas de provisionamento para cada novo equipamento e por vendedor é um fardo significativo para o fornecedor de serviços.

Com os recentes avanços da tecnologia WDM, a tecnologia SDH pode parecer ter o futuro comprometido, mas isto não acontecerá num futuro próximo. Com o tráfego IP a tornar-se no tráfego dominante transportado nas redes *core*, num cenário onde é usado o IP sobre WDM e os comprimentos de onda são comutados opticamente, o operador da rede *core* irá vender comprimentos de onda e os clientes constroem os seus próprios *backbones* IP sobre estes comprimentos de onda. Apesar de num futuro próximo o operador poder suportar várias centenas de comprimentos de onda por fibra, nem todos os clientes precisam de 10Gbps ou 40Gbps por circuito e não é provável que os comprimentos de onda se tornem tão baratos que qualquer cliente os possa comprar. Assim, o SDH continuará a ser útil no futuro próximo, dado que permite circuitos com uma menor granularidade em termos de largura de banda. Para além disso, os pacotes IP não podem ser transportados directamente sobre um comprimento de onda; é necessário algum tipo de encapsulamento (*framing*) e o encapsulamento IP sobre SDH é eficiente e bastante usado.

Um problema das redes actuais prende-se com a sobrevivencialidade dos dados que a atravessam. Uma rede é considerada com capacidade de sobrevivência se tiver capacidade de continuar a suportar o tráfego quando ocorre uma falha numa ligação ou num equipamento de comutação.

As redes SDH actuais são baseadas em topologia de anel que permitem mecanismos de protecção muito eficientes em termos de tempo de recuperação a falhas mas com uma utilização de recursos muito ineficiente. Por esta razão, os operadores começam a interessar-se por topologias em malha que permitam uma utilização mais eficiente dos recursos da rede desde que a eficiência do processo de recuperação a falhas não seja substancialmente degradada. Os mecanismos mais simples e de melhor desempenho em termos de tempo de recuperação a falhas são os que por cada VC (*Virtual Container*) de serviço também estabelecem um VC de protecção cujo percurso na rede não inclui nenhum dos comutadores do percurso de serviço (excepto os comutadores extremo). Estes mecanismos

garantem a robustez completa da rede no caso de falha de um único elemento quer seja um comutador ou uma ligação. Em redes em malha, o SDH permite o uso de mecanismos de protecção tipo 1+1 e 1:N.

As soluções existentes para a gestão de redes SDH são centralizadas o que implica problemas de falta de escalabilidade e de flexibilidade. Uma das soluções actualmente mais promissoras para contrapor aos sistemas centralizados e que permite a gestão de diferentes tecnologias, é o GMPLS (*Generalized Multi-Protocol Label Switching*) [1]. O GMPLS é uma extensão ao MPLS (*Multi-Protocol Label Switching*) [3] que suporta novos tipos de comutação tais como, comutação TDM e comutação de lambda, mantendo no geral a estrutura de funcionamento do MPLS. Ao usar a mesma estrutura de sinalização e protocolos de reserva de recursos semelhantes para fazer o controlo dos diferentes níveis inferiores, o GMPLS pretende reduzir a complexidade das tarefas de operação e manutenção das redes. Os *Label Switching Routers* (LSRs), em GMPLS, suportam diferentes tipos de interfaces: pacotes, tramas/células, *slots* temporais, comprimentos de onda ou portos físicos (fibra óptica).

A motivação para o uso da arquitectura GMPLS como plano de controlo de uma rede SDH é de, através do funcionamento distribuído do GMPLS, permitir que o encaminhamento seja implementado o mais possível de forma distribuída diminuindo assim a sua dependência de um sistema centralizado de gestão e de dotar estas redes com a capacidade de estabelecimento e terminação de VCs por sinalização.

1.2. Objectivos

Para poder dar garantias da qualidade de serviço e da gestão optimizada da largura de banda de uma rede, um sistema de gestão de redes de um operador tem de contemplar a sobrevivência e robustez da rede. Por sobrevivência da rede entende-se os mecanismos que a rede possui de modo a garantir que na falha de um elemento de rede o canal de comunicação seja retomado no mais breve espaço de tempo. O conceito de robustez define a forma eficiente, do ponto de vista de gestão de recursos,

como os mecanismos de sobrevivência actuam. Para garantir a sobrevivência da rede a tecnologia SDH cria, tipicamente, um circuito de serviço e um circuito de protecção. Um sistema de gestão baseado em GMPLS terá de fazer uso desses mecanismos para obter uma rede robusta.

A arquitectura GMPLS faz uso dos seus protocolos para determinar percursos entre os nós extremo. Neste trabalho, explora-se as particularidades da multiplexagem SDH para tornar mais eficiente a forma como são determinados esses percursos. Por outro lado, como se pretende obter uma rede com sobrevivência/robustez e, assumindo que se usam mecanismos de protecção, é necessário que o sistema de gestão determine dois percursos disjuntos em nós entre a origem e o destino.

A presente dissertação endereça o problema do encaminhamento robusto em redes GMPLS sobre SDH, efectuando o desenvolvimento e avaliação de desempenho de algoritmos de encaminhamento robusto de custo mínimo. Neste trabalho são investigados algoritmos de encaminhamento robusto de custo mínimo, para redes em malha, que se baseiam no estado das ligações para determinar os circuitos de serviço e de protecção. Estes circuitos serão determinados e estabelecidos por sinalização e de forma distribuída, recorrendo a uma camada protocolar GMPLS sobre SDH.

Estes algoritmos pretendem otimizar o desempenho da rede em termos de probabilidades de bloqueio de circuitos SDH, garantindo a tolerância a falhas através de caminhos disjuntos que protegem os circuitos SDH de falhas individuais em ligações ou nós.

Esta dissertação tem como objectivos:

- Proposta de estratégias de atribuição de custos que reflectam as características específicas da estrutura de multiplexagem SDH.
- Estudo do desempenho de algoritmos de encaminhamento robusto de custo mínimo com base nas estratégias propostas.
- Proposta de um algoritmo de reorganização de circuitos de protecção (a reorganização de caminhos de protecção, dadas as características

particulares da estrutura de multiplexagem SDH, pretende potenciar a aceitação de mais tráfego por parte da rede).

- Desenvolvimento de um simulador de eventos discretos para a análise do desempenho dos diferentes algoritmos de encaminhamento.

1.3. Estrutura da dissertação

No segundo capítulo, é apresentada a tecnologia SDH, onde são evidenciadas as principais características da tecnologia, com relevância para as questões relativas aos seus mecanismos de sobrevivência.

No terceiro capítulo, é descrita a tecnologia GMPLS, onde são apresentadas as características gerais de funcionamento bem como as características dos seus mecanismos de sobrevivência. Neste capítulo é discutida a aplicação de GMPLS a redes SDH.

O quarto capítulo apresenta as diferentes estratégias de atribuição de custos, os algoritmos de encaminhamento resultantes e o algoritmo de reorganização de caminhos de protecção proposto.

O quinto capítulo descreve o simulador de eventos discretos desenvolvido e apresenta os resultados de simulação obtidos bem como a avaliação de desempenho dos algoritmos segundo os critérios definidos.

Finalmente, no sexto capítulo, é apresentada uma síntese da dissertação, evidenciando as principais conclusões que resultam da mesma e apontando possíveis sequências deste trabalho.

Capítulo 2 – Tecnologia SDH

Actualmente existem duas tecnologias diferentes de multiplexagem em uso nas redes ópticas: *Wavelength Division Multiplexing* (WDM) e *Time Division Multiplexing* (TDM). O SDH e SONET usam a tecnologia TDM. O SDH é uma norma TDM bastante usada pelos operadores para transportar e multiplexar diferentes sinais tributários sobre ligações ópticas. O SDH tem uma estrutura de multiplexagem própria denominada estrutura de multiplexagem SDH. A norma ITU-T G.707 define a hierarquia SDH ETSI europeia.

Neste capítulo, é apresentada a tecnologia SDH, onde são evidenciadas as principais características da tecnologia, com relevância para as questões relativas aos seus mecanismos de sobrevivência.

2.1. Funcionamento da tecnologia SDH

O sinal fundamental em SDH é o STM-1 que opera à taxa de 155 Mbps. Este sinal é constituído por tramas contíguas compostas pelo cabeçalho de transporte e pelos dados a enviar. Para resolver questões de sincronização, os dados não são transportados directamente na trama de dados mas antes numa ou mais tramas internas, denominadas *Virtual Containers* (VCs), que podem flutuar entre duas tramas SDH sucessivas.

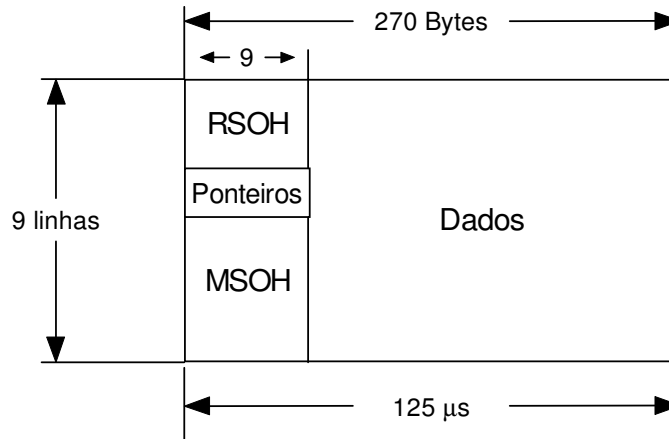


Figura 1 – Trama SDH de um sinal STM-1

A arquitectura SDH identifica três camadas diferentes, cada uma corresponde a um nível de comunicação entre equipamento SDH. Começando da mais baixa, estas são: a camada regeneradora secção/secção, a camada *multiplex section/line*, e, no topo, a camada caminho. À camada regeneradora corresponde o cabeçalho RSOH (*Regenerator Section Overhead*), à camada de multiplexagem o cabeçalho MSOH (*Multiplex Section Overhead*) e à camada de caminho corresponde o POH (*Path Overhead*).

A trama SDH é composta por 270 colunas de *bytes* por 9 linhas de *bytes* (figura 1) com uma duração de $125\mu s$. O cabeçalho principal, constituído pelas primeiras 9 colunas, inclui o cabeçalho de secção (SOH – *Section Overhead*) e os ponteiros da Unidade Administrativa (AU – *Administrative Unit*). O SOH é ainda sub-dividido pelo RSOH, composto pelas linhas um a três, e pelo MSOH composto pelas linhas cinco a nove. O RSOH, definido entre regeneradores, é usado para monitorar a qualidade da ligação (por exemplo, é com base no processamento deste cabeçalho que os equipamentos detectam falhas de transmissão). O MSOH, definido entre multiplexadores, permite monitorizar a rede e gerar alertas.

Os ponteiros AU ocupam a quarta linha de *bytes* do cabeçalho principal tendo por função a definição do *byte* de início da trama de dados. No campo de dados, cada VC inclui ainda um cabeçalho de caminho (POH - *Path Overhead*). O POH é usado nas funções necessárias ao transporte dos

dados, permitindo monitorar e controlar o endereçamento correcto do *container* (C-n) assim como identificar os conteúdos do mesmo.

O SDH pode transportar os sinais tributários europeus ETSI PDH (E1 a 2,048 Mbps, E3 a 34,368 Mbps e E4 a 139,264 Mbps) e americanos ANSI (T1 a 1,544 Mbps, T2 a 6,312 Mbps e T3 a 44,736 Mbps). A figura 2 apresenta as diferentes alternativas para a estrutura de multiplexagem em SDH dos diferentes tipos de tributários. Nesta figura, estão representadas as duas formas possíveis de multiplexar os tributários: a forma europeia e americana.

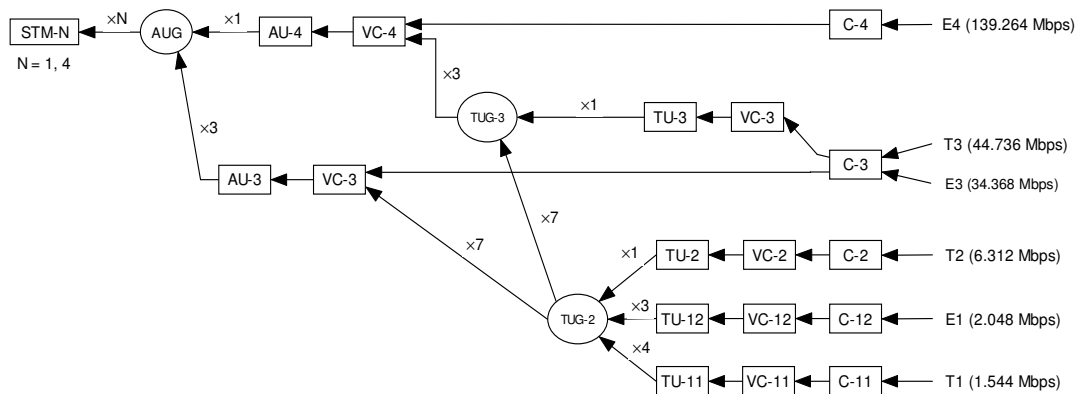


Figura 2 – Estrutura de multiplexagem SDH Europeia e Americana

No trabalho desta tese apenas são considerados os tributários da hierarquia europeia. Aos sinais tributários europeus E1, E3 e E4 correspondem os *virtual containers* VC-12, VC-3 e VC-4 respectivamente e a figura 3 apresenta a parte da figura anterior relativa à multiplexagem destes sinais tributários. Conforme se pode verificar nesta figura, a multiplexagem dos tributários E3 e E1 é efectuada através do ramo da estrutura de multiplexagem onde é gerado o TUG-3 (*Tributary Unit Group* tipo 3).

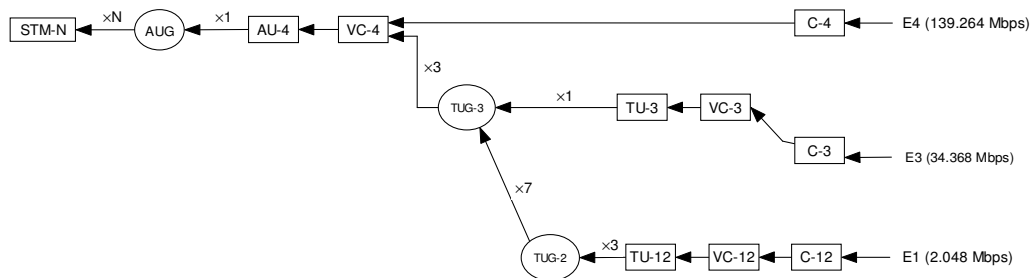


Figura 3 – Estrutura de multiplexagem SDH usada na Europa

Um STM-1 apenas pode transportar um VC-4. Cada VC-4 pode transportar um sinal tributário E4 ou três *tributary unit group* de tipo TUG-3. Um TUG-3 pode transportar um sinal tributário E3 ou até sete TUG-2. Cada TUG-2 pode transportar três sinais tributários E1 multiplexados.

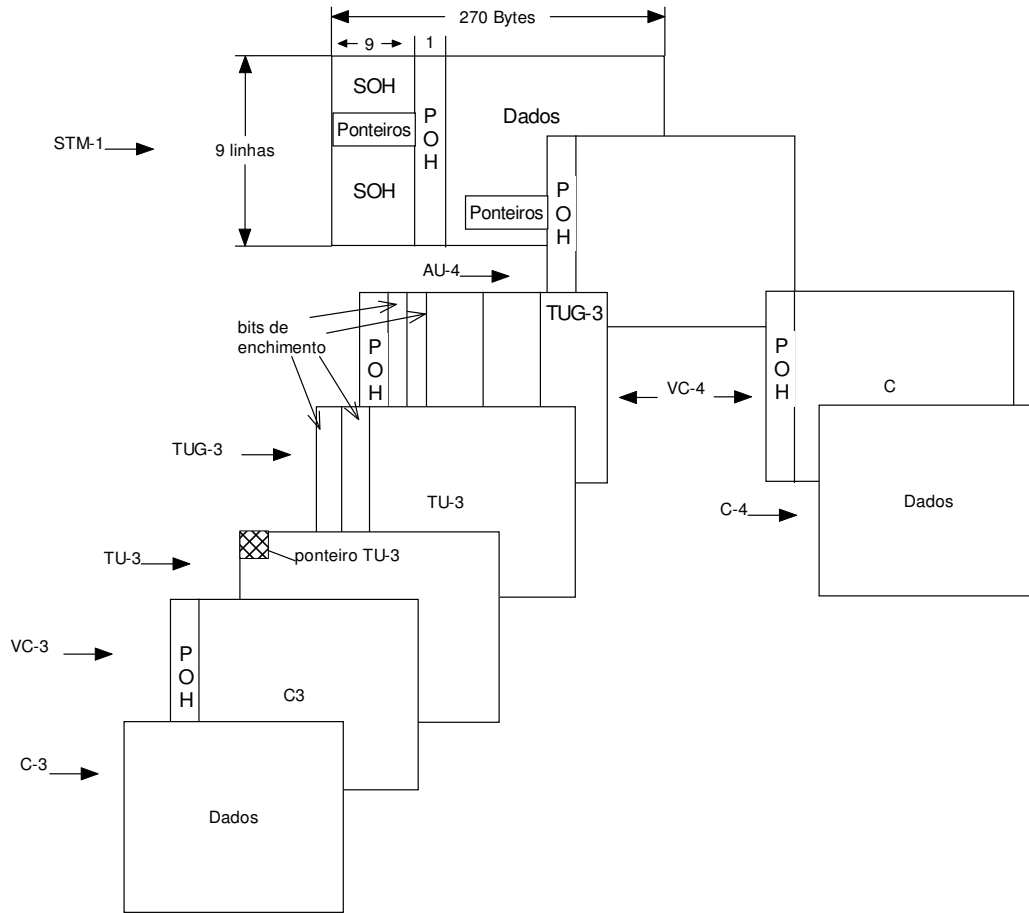


Figura 4 - Geração de um sinal STM-1 a partir de tributários E3 ou E4

A figura 4 descreve a geração de um sinal STM-1 a partir de tributários E3 ou E4. A geração de um sinal STM-1 a partir de um tributário E4 é efectuada da seguinte forma (lado direito da figura 4): ao container C-4 é associado o POH correspondente obtendo-se um VC-4, ao VC-4 são adicionados os ponteiros da Unidade Administrativa criando-se o AU-4 (Administrative Unit 4). O STM-1 é obtido juntando o cabeçalho SOH ao AU-4.

A geração de um sinal STM-1 a partir de um tributário E3 é efectuada da seguinte forma (lado esquerdo da figura 4): ao container C-3 é associado o POH correspondente obtendo-se um VC-3, com o acréscimo de um ponteiro

TU-3 é criado o TU-3 (Tributary Unit 3), o TUG-3 (Tributary Unit Group 3) é criado colocando bits de enchimento justapostos ao TU-3, posteriormente três TUG-3 são unidos e em conjunto com os bits de enchimento é criado o VC-4, ao VC-4 são adicionados os ponteiros da Unidade Administrativa criando-se o AU-4 (Administrative Unit 4). O STM-1 é obtido juntando o cabeçalho SOH ao AU-4. A geração de um STM-1 a partir de tributários E1 (figura 5) é semelhante ao caso anterior.

Como o VC-4 pode ser obtido através de diferentes combinações de tributários (figura 3), o campo de dados pode ser subdividido em sub-elementos de uma forma razoavelmente complexa. O VC-4 pode ser obtido através de um tributário E4, de três E3 ou de sessenta e três E1 ou através de combinações de sinais E3 e E1. Para a geração do sinal STM-1 com qualquer um destes três tributários é necessário o uso de ponteiros de sincronização (ponteiros da Unidade Administrativa designados por ponteiros nas figuras 4 e 5).

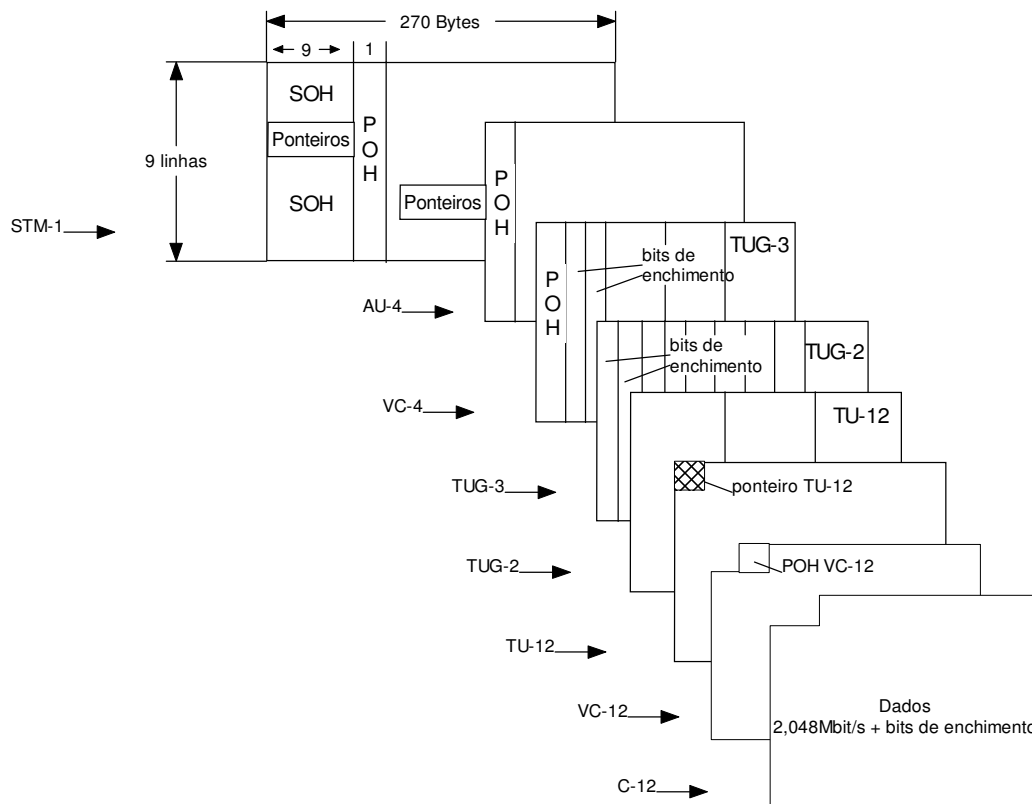


Figura 5 – Geração de um sinal STM-1 a partir da multiplexagem de tributários E1

A tecnologia SDH permite a transmissão de taxas superiores ao sinal fundamental através da criação de um sinal STM-N. Um sinal STM-N é formado por N sinais STM-1 entrelaçados *byte a byte*. Os VCs nas N frames entrelaçadas são independentes e flutuam de acordo com o seu próprio relógio¹.

Para o desenvolvimento deste trabalho foi necessário definir uma representação para a estrutura de multiplexagem SDH. Assumindo o VC-12 como unidade elementar de capacidade, tem-se que um VC-3 corresponde a ocupar 21 VC-12 e um VC-4 a ocupar 63 VC-12. Um VC-3 corresponde a um tributário E3; portanto, o pedido de um E3 pode ser visto como o pedido simultâneo de 21 E1. O pedido de um E4 (VC-4) ocupa um STM na totalidade, o mesmo acontecendo quando se tem 63 VC-12; assim o pedido de um E4 pode ser visto como 63 E1. Dado que são os *virtual-containers* que efectivamente são comutados na rede SDH, ao longo do trabalho, a menos que referido contrariamente, a referência a pedidos de *virtual-containers* corresponde ao pedido dos respectivos tributários.

Tem-se assim uma descrição da capacidade da rede SDH feita em unidades de VC-12: se o pedido for um VC-12 corresponde a uma unidade de capacidade, se o pedido for um VC-3 corresponde a 21 unidades de capacidade e se o pedido for um VC-4 corresponde a 63 unidades de capacidade.

Assim, a estrutura de multiplexagem SDH pode ser descrita de forma simples. Um STM-1 é visto como estando organizado em três pilhas de capacidade 21 VC-12 cada, ou seja, suportam 63 VC-12 conforme representado na figura 6 (cada pilha corresponde a um TUG-3). À chegada de um pedido de ligação, o tipo de pedido (VC-12, VC-3 ou VC-4) é convertido em unidades de VC-12, este valor é estabelecido na primeira pilha com capacidade suficiente para aceitar a totalidade do pedido. Assim:

- ◇ um pedido de um VC-12 ocupa uma unidade numa pilha que não esteja completa (se ela existir) ou numa pilha vazia (se ainda for possível, ou

¹ Para transportar sinais tributários maiores que as taxas básicas do sinal STM-1, os VCs podem ser concatenados mas esta funcionalidade não é abordada neste trabalho.

seja, se as três pilhas possíveis não estiverem completas);

- ◇ um pedido de um VC-3 ocupa 21 unidades numa pilha vazia se ainda existir (ou seja, torna uma pilha vazia numa pilha completamente ocupada) e
- ◇ um pedido de ligação de um VC-4 ocupa 63 unidades nas três pilhas possíveis e só pode ser condicionado apenas se as três pilhas estiverem vazias.

Conforme descrito anteriormente, um STM-4 é composto por 4 STM-1 independentes entre si pelo que um pedido de ligação VC-4 não pode ser condicionado em diferentes STM-1. Assim, podemos definir a estrutura de multiplexagem de um STM-4 por um sistema hierárquico de pilhas tal como ilustrado na figura 7. Temos 4 pilhas STM (correspondentes a cada STM-1), cada uma constituída por três pilhas (correspondentes a cada TUG-3 possível em cada STM-1). Neste caso, um pedido de ligação de um VC-4 ocupa 63 unidades nas três pilhas possíveis de um STM e só pode ser condicionado apenas se existirem três pilhas vazias num único STM.

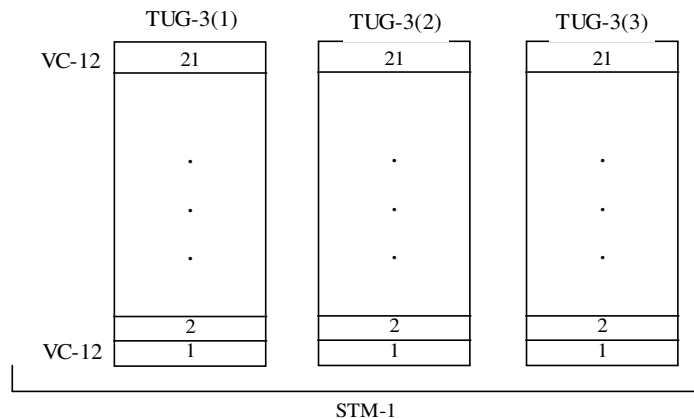


Figura 6 – Representação da estrutura de multiplexagem SDH de um STM-1

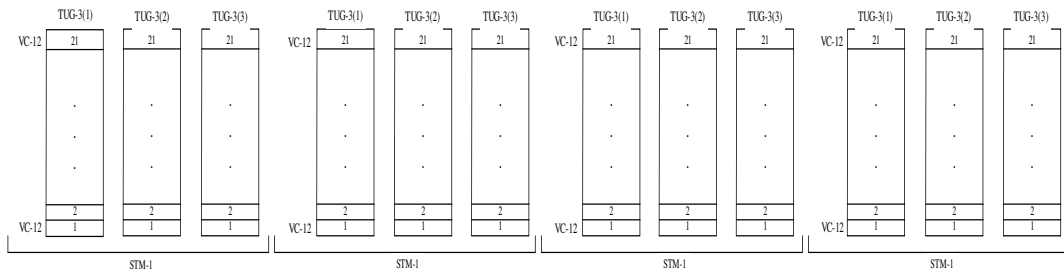


Figura 7 - Representação da estrutura de multiplexagem SDH de um STM-4

2.2. Elementos e Topologias de Rede

Em SDH os elementos de rede existentes podem ser usados para implementar diferentes tipos de topologias. De seguida é feita uma descrição dos elementos e topologias SDH [18].

2.2.1. Multiplexador Terminal

Este elemento (figura 8) é a fronteira entre a rede SDH e o equipamento do cliente. Tipicamente, numa direcção, combina os sinais tributários fornecidos, por elementos de rede de ordem inferior, num sinal agregado que é transportado pela rede. Para este sinal agregado o multiplexador gera um cabeçalho. Na direcção contrária, o multiplexador terminal separa o sinal recebido numa interface agregada nos subsinais que o constituem aos quais é extraído o cabeçalho associado. Estes sinais podem depois ser passados às interfaces tributárias associadas.

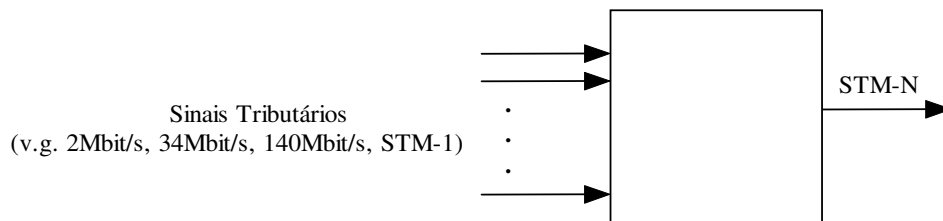


Figura 8 – Multiplexador Terminal

2.2.2. Multiplexador (Mux/Demux)

Este elemento (figura 9) multiplexa/desmultiplexa sinais STM-N em STM-M, onde $M > N$. O conteúdo da informação transportada não é alterado.

Na multiplexagem, os SOH's, de cada sinal STM-N, são terminados (lidos e avaliados). Os sinais de dados são multiplexados coluna a coluna e é gerado um novo SOH para STM-M.

Na desmultiplexagem, o SOH do sinal STM-M é terminado e os dados são distribuídos, coluna a coluna, para os canais STM-N. Para cada sinal STM-N é gerado um novo SOH.

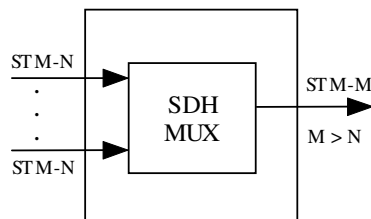


Figura 9 – Multiplexador

2.2.3. Multiplexador *Add/Drop*

O multiplexador *Add/Drop* (figura 10) é um elemento de rede que extrai um ou mais subsinais do sinal agregado STM-M e encaminha-os para a interface de tributário (função *drop*). Na direcção oposta, o multiplexador *Add/Drop* insere sinais tributários num sinal agregado STM-M (função *add*). O ADM (*Add/Drop Multiplexer*) tem a capacidade de efectuar a função *add* ou *drop* a qualquer tributário.

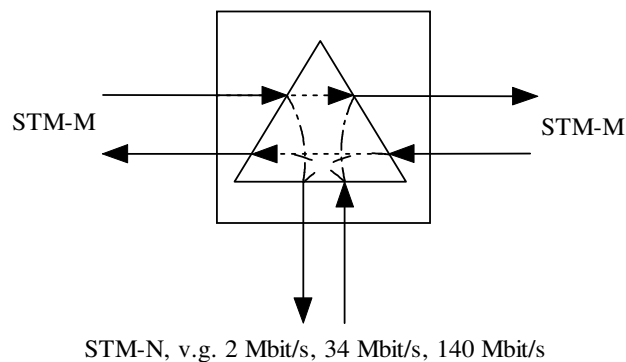


Figura 10 – Add/Drop Multiplexer

2.2.4. Digital Cross-Connect (DXC)

Nas redes SDH, o DXC (figura 11) é normalmente usado na interligação de arquitecturas de rede. O DXC interliga diversos sinais do mesmo nível hierárquico usando a função de *cross-connect*. Esta função *cross-connect* permite a comutação de qualquer sinal tributário entre os sinais agregados recebidos.

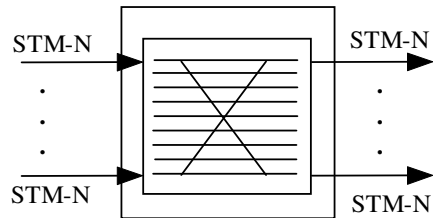


Figura 11 – Digital Cross-Connect

2.2.5. Topologias

As topologias típicas usadas para as redes SDH podem ser classificadas em quatro tipos diferentes: topologia linear ou *chain*, topologia em anel, topologia em estrela ou *hub*, topologia em malha. As diferentes topologias são obtidas com recurso aos diferentes elementos de rede descritos na secção anterior.

A topologia linear (figura 12) é usada quando não é necessária protecção e a demografia dos locais é linear. Tipicamente nesta topologia são usados os elementos multiplexador Add/Drop e multiplexador terminal.

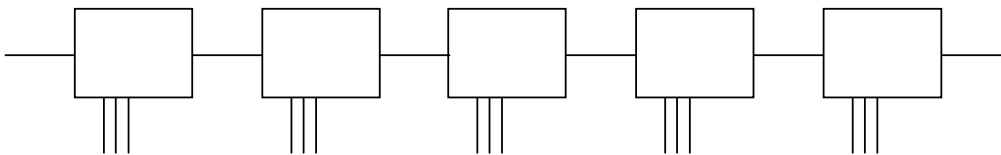


Figura 12 – Topologia Linear

A topologia em anel (figura 13) é a mais usada permitindo a implementação de mecanismos de protecção bastante fiáveis. Tipicamente nesta topologia é usado o elemento multiplexador Add/Drop.

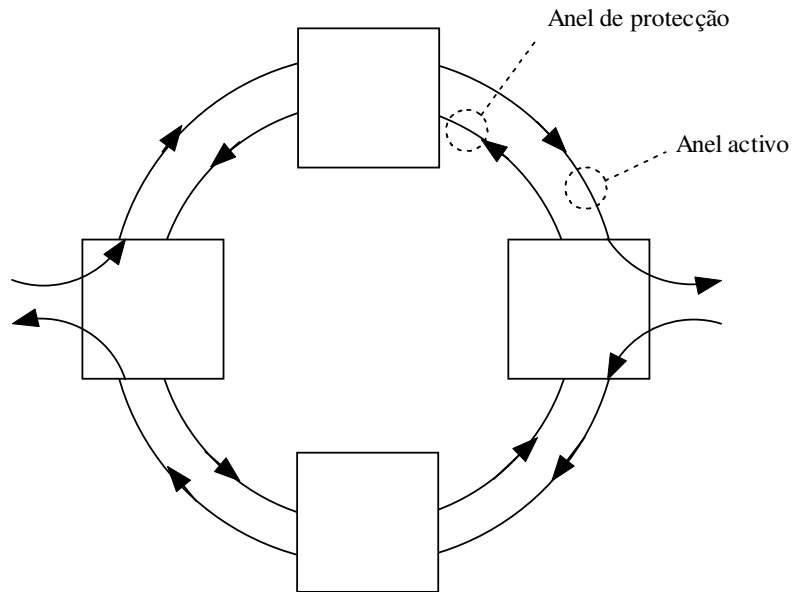


Figura 13 – Topologia em Anel

A topologia em estrela ou *hub* (figura 14) é normalmente usada para a ligação dos equipamentos terminais à rede de transporte. Tipicamente nesta topologia são usados os elementos Digital Cross Connect e multiplexador Terminal.

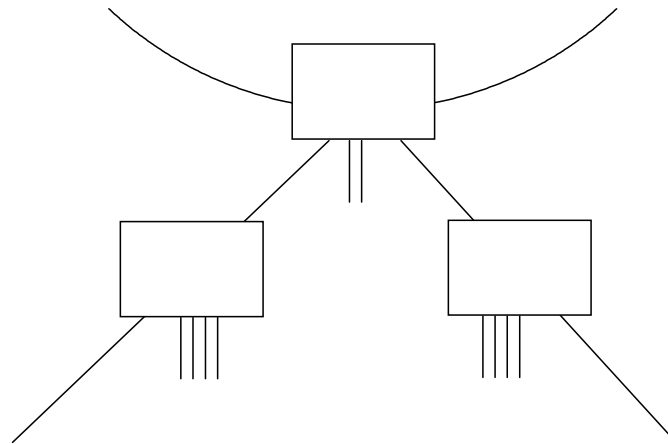


Figura 14 – Topologia em estrela

A topologia em malha (figura 15) permite uma rede com elevada flexibilidade e redundância. Tipicamente nesta topologia são usados os elementos Digital Cross connect e multiplexador Terminal. No presente trabalho a topologia em malha é a considerada.

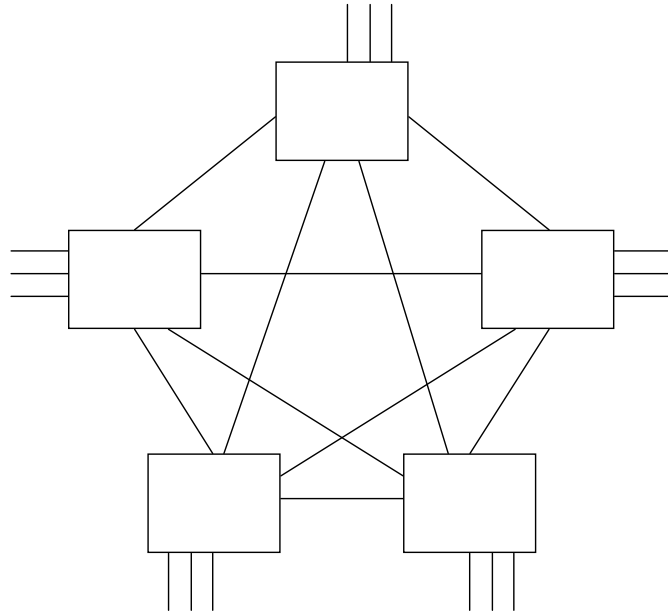


Figura 15 – Topologia em malha

2.3. Protecção SDH

O SDH permite a implementação do serviço de protecção através de *Path Protection* e de *Multiplex Section Protection* [18].

Path Protection é um serviço extremo-a-extremo que tipicamente é implementado através do envio de dois sinais iguais, um pelo caminho de serviço e outro pelo caminho de protecção. Permite também outras variantes mais complexas tais como protecção do tipo 1:N e M:N. Dependendo da escolha dos caminhos de protecção relativamente aos caminhos de serviço, este serviço permite a protecção do tráfego a falhas das ligações (se os caminhos forem disjuntos nas ligações) ou a falhas das ligações ou nós intermédios (se os caminhos forem disjuntos nos nós da rede). *Multiplex Section Protection* é um serviço de protecção a falhas nas ligações entre nós da rede e, portanto, não efectua a protecção a falhas nos nós da rede.

Ambos os serviços de protecção são possíveis tanto em redes com topologia em anel (protecção em anel) como em redes com topologia em malha (protecção linear). De seguida, são descritas apenas as técnicas de protecção linear dado serem as relevantes para o presente trabalho.

Neste trabalho pretendem-se desenvolver algoritmos que tenham capacidade de protecção extremo a extremo para falhas individuais nos elementos de rede. De entre os serviços anteriores, o serviço de *Path Protection* linear apresenta duas arquitecturas de interesse: protecção 1+1 e protecção 1:N.

Na arquitectura de protecção 1+1, o transmissor envia o sinal pelos dois canais estabelecidos, o de serviço e o de protecção. O receptor monitoriza ambos os canais e comuta entre os dois conforme o nível de sinal recebido. Nesta arquitectura não é possível o envio de tráfego extra pelo canal de protecção.

A arquitectura de protecção 1:N define a existência de 1 canal de protecção para n ($n = 1, \dots, 14$) canais de serviço. Nesta arquitectura pode-se transportar tráfego extra sobre a linha de protecção, quando a linha não está a ser utilizada, i.e., quando não está a transportar tráfego de uma linha que teve uma falha. O tipo de protecção dedicada 1:1 garante um nível de protecção semelhante ao 1+1, mas tem a vantagem do canal de protecção poder transportar tráfego extra. De notar que na ocorrência de uma falha, num dos canais protegidos, o tráfego extra é interrompido para permitir a protecção do canal.

A protecção em SDH pode ser considerada unidireccional (quando os dois sentidos da comunicação estão protegidos individualmente) ou bidireccional (quando a falha de um dos sentidos de comunicação implica a comutação dos dois sentidos de comunicação para uma linha de protecção). Quando a falha é reparada, o sistema pode fazer regressar a ligação ao caminho original, neste caso, a protecção diz-se reversível.

O trabalho desenvolvido nesta tese assume que o serviço de protecção pode ser um dos seguintes casos: 1+1 unidireccional ou bidireccional, 1:1 unidireccional ou bidireccional e reversível ou não. O controlo do tipo de serviço de protecção será efectuado por GMPLS como se descreve nos capítulos seguintes.

Capítulo 3 – Redes GMPLS

Este capítulo começa por apresentar a arquitectura MPLS que permite efectuar o encaminhamento de fluxos de pacotes sobre uma rede com base numa etiqueta atribuída a cada pacote que entra na rede. Para a distribuição de etiquetas são usados os protocolos CR-LDP ou RSVP-TE. É demonstrada a capacidade do MPLS para criar ligações com sobrevivencialidade.

De seguida, é apresentada a arquitectura GMPLS que estende o conceito de MPLS para outras tecnologias de comutação, nomeadamente, TDM, fibra e comprimento de onda. São apresentadas as extensões efectuadas ao MPLS de modo a possibilitar o funcionamento de GMPLS. É dada ênfase ao uso de GMPLS em SDH e às questões relacionadas com a protecção de LSPs.

3.1. Multiprotocol Label Switching (MPLS)

O MPLS é uma tecnologia de encaminhamento de pacotes para o núcleo das redes de telecomunicações.

No encaminhamento IP tradicional, os *routers* trocam informação de encaminhamento entre eles de modo a criarem as suas tabelas de encaminhamento. As decisões de expedição de pacotes requerem uma pesquisa do tipo *longest match* na tabela de encaminhamento, que compara

o endereço destino do pacote com cada uma das entradas na tabela de encaminhamento, procedimento repetido em cada nó do percurso, desde a origem até ao destino. Embora logicamente distintos, na prática, os planos de controlo e expedição estão fortemente ligados pois é através do plano de controlo que as tabelas de encaminhamento são actualizadas.

O MPLS usa uma etiqueta (*label* em inglês) de tamanho fixo que permite efectuar encaminhamento de fluxos de tráfego . A decisão de expedição do pacote é baseada na respectiva etiqueta.

Na rede MPLS, ou domínio MPLS, os *routers* são designados de *Label Switching Routers* ou *Label Edge Routers*, dependendo do seu papel.

O *LSR* é um *router* do núcleo da rede MPLS que participa no estabelecimento de LSPs usando protocolos de distribuição de etiquetas e é capaz de efectuar a expedição de pacotes com etiquetas. O *LSR* utiliza a etiqueta como índice da tabela de expedição, obtendo assim toda a informação de que necessita para enviar o pacote – nova etiqueta e *LSR* destino.

O *LER* é um *router* que está colocada na fronteira da rede MPLS, implementando as políticas de gestão e acesso determinadas pelo administrador de rede e efectua a agregação de tráfego e classificação, inserindo (*routers* de ingresso), ou retirando (*routers* de egresso), etiquetas nos pacotes. A classificação de um pacote pode ser feita com base em informação tão diversa como o endereço origem, endereço destino, requisitos de QoS, aplicação de destino, ou o estado actual da rede.

Geralmente, utiliza-se a designação *LSR* para referir ambos os tipos de *routers* MPLS.

Um LSP (*Label Switched Path*) define o percurso de encaminhamento dos pacotes do nó de ingresso para o nó de egresso.

Um conjunto de pacotes com as mesmas características de expedição é designado *Forwarding Equivalent Class (FEC)*. A cada *FEC* é associado uma etiqueta diferente. A etiqueta é usada para determinar a interface de saída de um pacote IP sem ter de procurar o endereço na tabela de encaminhamento.

Em MPLS, a utilização da etiqueta permite separar os planos de controlo e expedição: o plano de controlo utiliza (à semelhança do protocolo IP) protocolos de encaminhamento como o OSPF, para construir e actualizar as tabelas de encaminhamento dos *routers*. A ligação entre o plano de controlo e o plano de expedição é feita através da criação de *Forwarding Equivalence Classes* que fazem corresponder as entradas na tabela de expedição dos pacotes de dados com as etiquetas a atribuir a cada pacote. Esta correspondência é realizada localmente em cada um dos LSR, sendo necessário publicitar esta informação aos LSRs vizinhos através de um protocolo apropriado. Assim, ao receber um pacote, o LSR usa a etiqueta para indexar a tabela de expedição e obter a informação necessária para o encaminhamento do pacote – interface de saída e nova etiqueta.

Com o MPLS, é possível atribuir várias FECs ao mesmo LSP, e vários LSPs à mesma FEC, flexibilizando assim a gestão dos recursos da rede. Para além disto, é também possível configurar o percurso de cada LSP quer explicitamente quer através de um qualquer protocolo de encaminhamento baseado em restrições. Estas características permitem um controlo mais preciso do tráfego na rede, por forma a obter redes mais eficientes com um controlo mais preciso na forma como cada serviço é suportado, permitindo assim realizar, efectivamente, Engenharia de Tráfego.

A associação da etiqueta LSP ao FEC pode ser efectuada de duas formas:

- *Data-driven*: a associação é efectuada pelo plano de controlo quando chega a um LSR tráfego identificado como sendo candidato a *label switching*. As associações de etiquetas a FECs só são estabelecidas quando necessário, resultando num menor número de entradas na tabela de expedição.
- *Control-driven*: as associações são feitas antes da chegada da informação a transportar através do plano de gestão e são independentes da informação a transportar.

A etiqueta tem apenas significado local, ou seja, é válida apenas numa ligação entre dois *routers*. A etiqueta pode ser transportada de diferentes formas. Por exemplo, algumas redes transportam a etiqueta na camada de

(mais um protocolo a suportar) e a sua coordenação com os protocolos de encaminhamento. O LDP foi alterado para suportar encaminhamento com restrições, dando origem ao *Constraint Routing LDP* (CR-LDP) [15].

- *Piggybacking* num protocolo existente: a informação de associação de etiquetas pode ser adicionada a um outro protocolo que seja usado na rede. Este método garante consistência na informação de expedição e evita o uso de outro protocolo. Infelizmente, nem todos os protocolos podem facilmente ser alterados para suportar *piggybacking*, pelo que este método não é uma solução completa para a distribuição de etiquetas. Entre os protocolos alterados para suportar esta funcionalidade encontra-se o *Resource reSerVation Protocol* (RSVP). A versão alterado do RSVP é o *RSVP-Traffic Engineering (TE)* [14].

O LSP é estabelecido antes de se iniciar a transmissão de dados e pode ser criado através de dois métodos:

- encaminhamento *hop-by-hop*, onde o próximo LSR é determinado através de algoritmos do tipo *shortest path*; individualmente cada LSR selecciona o próximo *hop* para um dado FEC;
- encaminhamento explícito, onde o LSP é criado com uma rota pré-determinada sobre a rede (a rota pode ser definida para satisfazer um critério de QoS); o LER de ingresso (i.e., o LER onde o fluxo de dados para a rede se inicia) especifica a lista de nós através dos quais o LSP passa.

Uma vez que a correspondência entre etiquetas é constante em cada LSR, o caminho (LSP) de um pacote dentro da rede MPLS é determinado pela sua etiqueta inicial.

3.1.1. Constraint Routing – Label Distribution Protocol

O CR-LDP é um protocolo de distribuição de etiquetas baseado em LDP. O LDP permite estabelecer um LSP associando-o a um determinado FEC. O CR-LDP é usado para estabelecer um LSP unidireccional ponto-a-ponto com

restrições de encaminhamento explícito, QoS ou outras. O LSP estabelecido com base em restrições designa-se *constraint-based routed label switched path* (CR-LSP). O CR-LSP permite, portanto, a reserva de recursos no processo de distribuição de etiquetas.

O percurso a atribuir ao CR-LSP (quer seja determinado explicitamente ou por um protocolo de encaminhamento baseado em restrições) é especificado pelo LER de ingresso. Depois de determinado o percurso, o LER cria uma mensagem de pedido de etiqueta. O percurso determinado é transportado num objecto *Type-Length-Value* (TLV) denominado *Explicit Route TLV* (ER-TLV) que consiste numa sequência ordenada de saltos que correspondem ao caminho calculado. Este objecto é inserido numa mensagem *Label_Request* e é enviado para o primeiro LSR do percurso (LSR B, figura 17). O percurso efectuado pela mensagem *Label_Request* ao longo da rede é determinado pelo conteúdo do objecto ER-TLV, e não pelo endereço de destino do pacote que a transporta. No caso do CR-LSP ter requisitos de tráfego, estes são definidos no objecto *Traffic Parameters TLV* que permite definir os parâmetros de tráfego: *Peak Data Rate*, *Peak Burst Size*, *Committed Data Rate*, *Committed Burst Size* e *Excess Burst Size*.

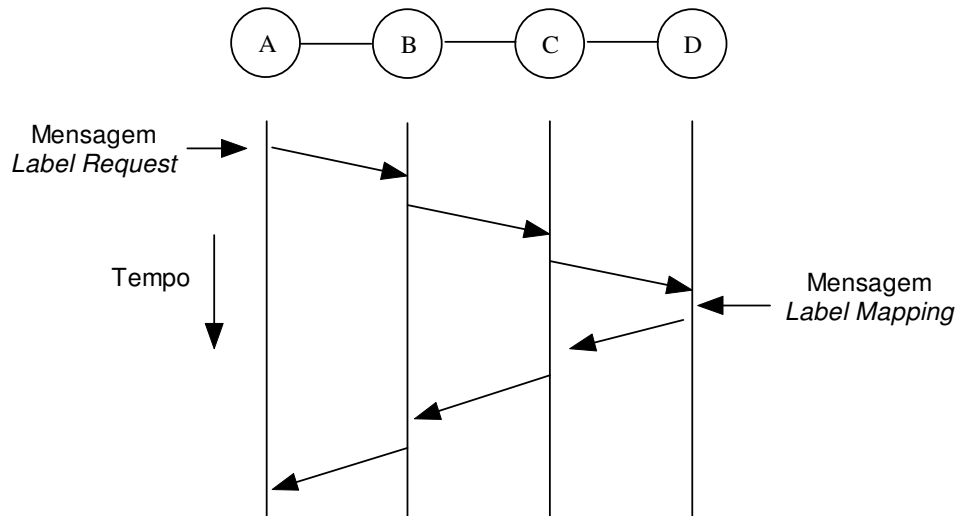


Figura 17 - Estabelecimento de LSP através de CR-LDP

O processo de estabelecimento do LSP desenvolve-se da seguinte forma. O LSR A envia a mensagem *Label_Request* para o LSR B, o primeiro no objecto ER-TLV. Como o LSR B não é o nó de egresso não pode efectuar a correspondência de uma etiqueta ao FEC até que receba a correspondência

do LSR a jusante. O LSR B recebe a mensagem *Label_Request* e reconhece que é o primeiro nó do objecto ER-TLV, e que o nó seguinte é o LSR C. O LSR C efectua o mesmo processo e envia a mensagem para o LSR D. O LSR D, de egresso, reconhece que é o último nó do ER-TLV. Selecciona uma etiqueta para o CR-LSP a estabelecer e envia o mapeamento efectuado para o LSR C através de uma mensagem de *Label_Mapping*. O LSR C recebe a mensagem *Label_Mapping*, associa-a ao pedido original, selecciona uma etiqueta para o CR-LSP e constrói uma nova mensagem *Label_Mapping* que é enviada para o LSR B. Por sua vez, o LSR B faz o processo semelhante ao LSR C, criando uma nova mensagem e enviando-a ao LSR A. O LSR A, ao receber a resposta ao pedido efectuado, preenche a tabela de encaminhamento com a correspondência apropriada, estando o LSP estabelecido e pronto a ser usado para a expedição de pacotes.

3.1.2. Resource Reservation Protocol – Traffic Engineering

O RSVP-TE é uma extensão ao RSVP que permite o estabelecimento de LSPs explícitos, com ou sem reserva de recursos, reencaminhamento de LSPs, preempção e detecção de ciclos.

O estabelecimento do LSP é efectuado através do uso das mensagens *Path* e *Resv* que foram alteradas de modo a transportarem o objecto *Explicit_Route* (ERO) e o objecto *Label* (L) respectivamente. A função e comportamento do objecto ERO é semelhante à do objecto ER no CR-LDP.

O objecto *Explicit_Route* contém o caminho explícito a estabelecer, determinado pelo LER de ingresso.

A mensagem *Path* é enviada para o LSR B (Figura 18) que determina qual o próximo nó e envia a mensagem para o LSR C. O nó C tem o mesmo procedimento. Quando o LSR D recebe a mensagem *Path* reconhece que é o nó de egresso e responde com uma mensagem *Resv*, onde é inserido o objecto *Label* com o valor de etiqueta atribuído ao FEC. A mensagem *Resv* toma o caminho inverso da mensagem *Path*. O LSR C recebe a mensagem *Resv* actualiza a sua tabela de encaminhamento, selecciona uma etiqueta para o LSP e constrói uma nova mensagem *Resv* que é enviada para o nó

LSR B. O nó B tem um procedimento semelhante ao LSR C e envia a nova mensagem *Resv* para o LSR A. O LSR A recebe a mensagem *Resv* ficando o LSP estabelecido.

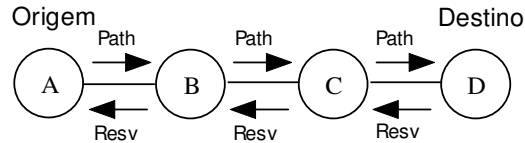


Figura 18 - Estabelecimento de LSP através de RSVP-TE

O RSVP-TE define especificações de tráfego, usando o objecto *SENDER_TSPEC* (contém características de tráfego do fluxo de dados, sendo obrigatório na mensagem *Path*) e *FLOWSPEC* (é transportado na mensagem *Resv* e contém a informação necessária para efectuar uma reserva num *router*).

3.1.3. Sobrevivencialidade em Redes MPLS

Por sobrevivencialidade de uma rede, entende-se a sua capacidade de manter ininterruptos os serviços suportados quando existem falhas nos elementos, quer sejam ligações, quer sejam nós.

Usando a tecnologia MPLS, é possível reagir a falhas na rede de forma quase instantânea: podem ser utilizados LSPs de reserva que entram em funcionamento no caso de ocorrer uma falha que impeça o normal funcionamento dos LSPs principais.

A protecção de falhas está dividida em quatro tipos: protecção de ligação, de nó, de caminho e de segmento [8].

Na protecção de ligação, pretende-se proteger um LSP de uma falha numa ligação da rede, pelo que o LSP de reserva é disjunto em ligações do LSP operacional nas ligações a proteger. Em caso de falha, o tráfego é comutado para o LSP de reserva num dos nós extremos do LSP que falhou.

Com a protecção de nó, o objectivo é proteger um LSP de falha num nó, pelo que os LSPs operacional e de reserva são disjuntos no nó que requer protecção e, consequentemente, nas ligações desse nó. O tráfego é

comutado para o LSP de protecção no nó imediatamente anterior ao que falhou.

A protecção de caminho, visa salvaguardar a falha de qualquer elemento da rede, tendo os LSPs de protecção e de serviço percursos totalmente disjuntos, em nós e em ligações. A comutação para o LSP de reserva é feita nos extremos do LSP de serviço.

Na protecção de segmento, a rede é dividida em vários domínios, sendo uma falha num domínio, reparada dentro do próprio domínio.

A relação entre os LSPs de protecção e os LSPs de serviço, pode ser:

- 1:1 – um LSP serviço é protegido por 1 LSP de protecção;
- n:1 – um LSP serviço é protegido por n LSPs de protecção;
- 1:n – um LSP de protecção protege n LSPs de serviço;
- 1+1 – o tráfego é enviado, de forma concorrente, pelos dois LSPs.

Os LSPs de protecção podem ser estabelecidos antes ou depois da falha, e os recursos necessários podem estar reservados *a priori* ou serem atribuídos a pedido depois da notificação de falha.

Os LSPs pré-estabelecidos, com recursos reservados *a priori*, garantem que, em caso de falha de rede, os compromissos de QoS sejam cumpridos. No caso de a reserva de recursos ser feita após a notificação de falha, não é possível dar quaisquer garantias quanto à QoS então prestada. No entanto, a reserva de recursos, *a priori*, implica a não utilização de todos os recursos da rede (os recursos de protecção só podem ser usados para tráfego extra) e não permite estabelecer LSPs de reserva pelo melhor caminho (no instante da falha).

3.2. Generalized MPLS

O MPLS suporta apenas comutação de pacotes. O Generalized Multi-Protocol Label Switching (GMPLS) é uma extensão ao MPLS. O GMPLS difere do MPLS, na medida em que permite suportar outros tipos de

comutação, i.e., comutação TDM, lambda e fibra. Para suportar os novos tipos de comutação, o GMPLS redefiniu algumas funções básicas do MPLS e, nalguns casos, adicionou funcionalidades. O GMPLS estende a noção de LSP por forma a permitir o encaminhamento com base em *time slots*, comprimentos de onda ou portos físicos. Assim, as interfaces dos LSRs podem ser classificadas da seguinte forma:

1. Interfaces *Packet Switch Capable* (PSC)

Interfaces que reconhecem pacotes de camada protocolar 3 e podem fazer a comutação baseando-se no conteúdo do seu cabeçalho. Um exemplo desta classe é uma interface de um *router* que encaminha pacotes IP.

2. Interfaces *Layer-2 Switch Capable* (L2SC)

Interfaces que reconhecem tramas/células de camada protocolar 2 e podem fazer a comutação com base no seu conteúdo. Um exemplo desta classe é uma interface de uma *bridge Ethernet* que encaminha as tramas com base nos seus endereços MAC ou de um *switch ATM* que encaminha as células com base nos campos VPI/VCI do seu cabeçalho.

3. Interfaces *Time-Division Multiplex Capable* (TDM)

São interfaces TDM que fazem a comutação dos dados com base no *slot* temporal dos dados. Exemplo é a interface SONET/SDH de um *Cross-Connect* (XC), *Terminal Multiplexer* (TM) ou *Add-Drop Multiplexer* (ADM).

4. Interfaces *Lambda Switch Capable* (LSC)

Interfaces ópticas que efectuem a comutação dos dados, baseando-se no comprimento de onda em que os dados são recebidos. Um exemplo é o *Photonic Cross-Connect* (PXC) ou *Optical Cross-Connect* (OXC) que podem operar ao nível do comprimento de onda individual.

5. Interfaces *Fiber-Switch Capable* (FSC)

Interfaces que fazem a comutação dos dados, com base na posição dos dados nos espaços físicos (na posição real). Exemplo desta interface é uma PXC ou OXC que opera ao nível de uma ou múltiplas fibras.

Uma ligação/circuito só pode ser estabelecida através de, ou entre, interfaces do mesmo tipo. Conforme a tecnologia usada para cada interface, podem ser usados nomes diferentes para os circuitos criados, e.g., circuito SDH, *optical trail*, *light-path*, etc. Na arquitectura GMPLS, todos estes circuitos são referidos como: *Label Switched Path* (LSP).

As interfaces estão ordenadas hierarquicamente. No topo da hierarquia tem-se a interface FCS, seguida da LSC, depois TDM, L2SC e, finalmente, PSC. Esta ordem é usada pelo GMPLS para suportar LSPs hierárquicos. A hierarquia de LSPs pode ocorrer entre interfaces do mesmo tipo ou entre interfaces diferentes. Tem-se um LSP hierárquico quando começa e termina num tipo de interface mas atravessa diferentes tipos de redes (diferentes interfaces). Este LSP pode ser encadeado com outros LSPs num LSP de ordem elevada.

Por exemplo, entre interfaces do mesmo tipo, pode-se construir uma hierarquia se uma interface tiver a capacidade de multiplexar vários LSPs da mesma tecnologia, e.g., um conjunto de LSPs SDH de baixa ordem (e.g., VC-12) é multiplexado num LSP SDH de ordem superior (e.g., VC-4). Diversos níveis de multiplexagem de sinais (LSP) são definidos para a hierarquia de multiplexagem SDH.

Para LSPs entre diferentes tipos de interfaces, um LSP que se inicia e termina numa interface PSC pode ser conduzido (conjuntamente com outros LSPs) num LSP que começa e termina numa interface L2SC. Este LSP pode também ser conduzido (conjuntamente com outros LSPs) por um LSP que tem início e termina numa interface TDM. Por sua vez, este LSP pode ser conduzido (conjuntamente com outros LSPs) por um LSP que começa e termina numa interface LSC, que por sua vez, pode ser conduzido (conjuntamente com outros LSPs) num LSP que começa e termina numa interface FSC.

A *etiqueta* toma na arquitectura GMPLS a designação de *generalized label* podendo representar um qualquer LSP das diferentes interfaces.

3.3. Plano de Controlo GMPLS

A arquitectura GMPLS separa claramente o plano de controlo do plano de expedição de dados. O plano de controlo é ainda separado em plano de sinalização, que contém os protocolos de sinalização, e plano de encaminhamento, que contém os protocolos de encaminhamento.

O GMPLS estende os planos de controlo MPLS para suportar as cinco classes de interfaces definidas na secção anterior.

O plano de controlo GMPLS suporta um modelo *overlay*, um modelo *augmented*, e um modelo *peer (integrated)* [1].

O modelo *peer* (apenas GMPLS) assume que todos os dispositivos na rede têm uma visão topológica completa, e que participam de forma semelhante no processo de encaminhamento. É um modelo semelhante ao existente nas redes IP/MPLS. Apesar deste modelo possibilitar uma optimização do uso dos recursos de rede, pode não ser apropriado se o operador não desejar expor informação crítica (largura de banda da rede, capacidade, topologia) aos operadores das camadas protocolares superiores.

O modelo *overlay* permite ao cliente (o requisitante do serviço) adicionar, modificar, apagar ligações à rede do operador, sem que o cliente tenha qualquer tipo de conhecimento da topologia de rede do operador. O modelo *overlay* mantém a separação na interface cliente-rede, continuando a existir o encaminhamento IP do cliente, os protocolos de sinalização, a distribuição topológica, e o esquema de endereçamento, independentes dos usados na rede do operador.

O modelo *augmented* fornece um mecanismo para a partilha limitada de informação, tipicamente usando *Border Gateway Protocol version 4* (BGP-4) para passar a informação de acesso entre as redes.

De modo a facilitar o encaminhamento *Constrained-Based Shortest-Path First* dos LSPs, os nós que estabelecem o LSP têm de ter mais informação sobre as ligações da rede do que aquela que os protocolos actuais das redes IP podem fornecer. Estes atributos das ligações são distribuídos usando os mecanismos de transporte já disponíveis e tidos em conta pelo algoritmo de encaminhamento do LSP.

Para transportar e codificar uniformemente a informação de caracterização das ligações, são necessárias extensões aos protocolos e algoritmos de encaminhamento tradicionais. A sinalização tem também de ser capaz de transportar os parâmetros do circuito requerido (LSP), tais como largura de banda, tipo de sinal, a protecção e/ou restauro desejado, a posição num *multiplex* em particular, etc. A maioria destas extensões foram definidas para encaminhamento *constraint-based* em interfaces PSC e L2SC em MPLS. O GMPLS define extensões adicionais adequadas às interfaces TDM, LSC e FSC.

O GMPLS estende os dois protocolos de sinalização definidos para sinalização em MPLS, i.e., RSVP-TE e CR-LDP mas não especifica qual dos dois protocolos de sinalização deverá ser usado (são os fabricantes e operadores que avaliam a melhor solução a adoptar no seu caso). O GMPLS estende também dois protocolos de encaminhamento *link-state* intra-domínio, i.e., OSPF-TE e IS-IS-TE.

As interfaces TDM, LSC e FSC introduzem novas restrições ao modelo IP de endereçamento e de encaminhamento, dado que, por exemplo, dois nós podem estar ligados por várias centenas de ligações paralelas (muitos dos operadores têm várias dezenas de comprimentos de onda por fibra entre dois nós e as novas gerações de sistemas DWDM permitirão centenas de comprimentos de onda por fibra). Nestes casos, o uso de endereços IP em cada extremo da ligação física é impraticável.

Dois mecanismos podem ser usados e combinados para aumentar a escalabilidade de endereçamento e encaminhamento: ligações inumeradas (ligações ou interfaces que não têm endereços IP) e conjunto de ligações (*link bundling*) (ligações paralelas, por exemplo *wavelengths* que são vistos

como uma única ligação). Foram introduzidas extensões aos protocolos de sinalização (RSVP-TE e CR-LDP) e de encaminhamento (OSPF-TE e IS-IS-TE) [1] para suportar estes mecanismos. No entanto, é necessário um novo protocolo para suportar as operações GMPLS, um protocolo de sinalização para gestão de ligações – *Link Management Protocol* (LMP).

Link Management Protocol (LMP)

O *Link Management Protocol* (LMP) foi especificado para efectuar as operações GMPLS, nomeadamente, na configuração e controlo de conjuntos de ligações (*link bundling*). O plano de controlo MPLS ou IP não foi concebido para poder suportar um elevado número de ligações paralelas. Portanto, para determinados casos em que o número de ligações paralelas é elevado, por exemplo DWDM, o GMPLS tem de recorrer ao LMP.

O LMP corre entre nós adjacentes no plano de dados, sendo usado para gerir as ligações. O LMP fornece mecanismos para manter a conectividade no canal de controlo (*IP Control Channel Maintenance*), verificar a conectividade física das ligações que transportam dados (*Link Verification*), correlacionar a informação das propriedades da ligação (*Link Property Correlation*), e gerir falhas da ligação (*Fault Localization e Fault Notification*). Uma particularidade do LMP é a sua capacidade para localizar falhas em redes opacas ou transparentes (i.e., independente do esquema de codificação e taxa de transmissão usada para os dados).

O LMP é definido no contexto GMPLS, mas é especificado independentemente das especificações de sinalização GMPLS dado que é um protocolo local a correr entre nós adjacentes no plano de dados. Assim, o LMP pode ser usado noutros contextos com protocolos de sinalização que não o GMPLS.

O GMPLS não especifica como é que os canais de controlo devem ser implementados, mas requer o IP para encaminhar os pacotes relativos aos protocolos de sinalização e de encaminhamento. Os canais de controlo podem ser *in-band* ou *out-of-band*, e várias soluções podem ser usadas para transportar IP. Notar que um tipo de mensagens LMP (mensagem de Teste) é usada *in-band* no plano de dados e não pode ser transportada sobre IP; isto

é um caso particular, necessário para verificar a conectividade no plano de dados.

Os canais de controlo entre dois nós, têm de ser estabelecidos para permitir a comunicação de informação de encaminhamento, de sinalização e de gestão de ligação entre nós.

Em GMPLS, os canais de controlo entre dois nós adjacentes não têm de usar o mesmo meio físico que as ligações de dados entre esses nós. Para além disso, os canais de controlo que são usados para trocar a informação do plano de controlo GMPLS existem independentemente das ligações que gerem. Desta forma, o LMP foi desenhado para gerir as ligações de dados, independentemente das capacidades de terminação dessas ligações de dados. Por exemplo, um canal de controlo pode usar um comprimento de onda ou fibra separados, uma ligação *Ethernet*, ou um túnel IP através de uma rede de gestão separada.

Uma consequência de permitir que o canal ou canais de controlo entre dois nós estejam fisicamente separados das ligações de dados associadas, é que o estado do canal de controlo não se correlaciona necessariamente com o estado das ligações de dados e vice-versa. Desta forma, foram desenvolvidos novos mecanismos em LMP para gerir as ligações, quer em termos de aprovisionamento de ligações quer em isolamento de falhas.

3.4. Extensões chave do GMPLS ao MPLS

Para além da introdução do protocolo LMP (descrito anteriormente), o GMPLS introduz várias extensões ao MPLS por forma a atingir os objectivos para os quais foi concebido (nomeadamente, permitir o controlo das camadas TDM, LSC e FSC). De seguida são enumeradas extensões chave do GMPLS em relação ao MPLS.

- Em MPLS, as ligações atravessadas por um LSP podem ser uma mistura de ligações com uma codificação de *etiqueta* heterogénea (e.g., ligações entre *routers*, ligações entre *routers* e ATM-LSR's, e ligações entre ATM-LSR's). O GMPLS estende este conceito, incluindo ligações onde a

etiqueta é codificada como um *time slot*, ou um comprimento de onda, ou uma posição (real) no espaço físico.

- Em MPLS, um LSP que transporta IP tem de começar e terminar num *router*. O GMPLS estende este conceito requerendo um LSP que comece e termine em interfaces do mesmo tipo.
- O tipo de dados que pode ser transportado em GMPLS por um LSP é estendido para permitir o transporte de sinais como SONET/SDH, Ethernet de 1GB ou 10GB, etc.
- O uso de *Forwarding Adjacencies* fornece um mecanismo que pode melhorar a utilização da largura de banda, quando a atribuição de largura de banda só pode ser efectuada em unidades discretas. Oferece também um mecanismo para agregar o estado de expedição, permitindo reduzir o número de etiquetas necessárias.
- O GMPLS permite a proposta de uma etiqueta por um nó a montante do nó a jusante, para reduzir a latência de estabelecimento do LSP. Esta proposta pode ser ignorada pelo nó a jusante mas nalguns casos, com o custo acrescido de um tempo de estabelecimento do LSP muito maior.
- O GMPLS permite a limitação do conjunto de etiquetas que podem ser seleccionados por um nó a jusante. Em GMPLS, um nó a montante pode limitar as etiquetas de um LSP ao longo de apenas um único salto ou de um caminho LSP completo. Este aspecto é útil em redes fotónicas onde a conversão de comprimentos de onda pode não estar disponível.
- Enquanto os LSPs em MPLS são unidireccionais, o GMPLS suporta o estabelecimento de LSPs bi-direccionais.
- O GMPLS suporta a terminação de um LSP num porto de saída específico, i.e., a selecção de porto no lado do destino.
- O GMPLS com RSVP-TE suporta um mecanismo específico de RSVP para a rápida notificação de falhas.

Existem ainda algumas diferenças chave entre MPLS e GMPLS:

- Para interfaces TDM, LSC e FSC, a atribuição de largura de banda para um LSP só pode ser feita em unidades discretas.
- É esperado terem-se muito menos etiquetas em ligações TDM, LSC ou FSC do que em ligações PSC ou L2SC, isto porque os primeiros são etiquetas físicas e não etiquetas lógicas.

3.5. Estabelecimento de LSPs em GMPLS

Em GMPLS, a operação de estabelecimento/requisição de LSPs efectuada através de CR-LDP ou RSVP-TE é semelhante. Os parâmetros a especificar em ambos são denominados da mesma forma sendo que em CR-LDP os parâmetros têm a forma de TLV's e em RSVP-TE têm a forma de objectos.

A operação de requisição de um LSP tem por base uma mensagem, denominada *Generalized Label Request*, sendo constituída por três campos: o *LSP Encoding Type*, o *Switching Type* e o *Generalized Payload Identifier* (G-PID). O *LSP Encoding Type* (8 bits) indica o tipo de codificação a usar com os dados associados ao LSP, i.e., o tipo de tecnologia a ser considerada (por exemplo, pode ser SDH, SONET, Ethernet, ANSI PDH, etc..). Este campo representa a natureza do LSP, e não a natureza das ligações que o LSP atravessa. Isto é usado salto-a-salto por cada nó. O *Switching Type* (8 bits) é necessário em ligações que anunciam mais do que um tipo de comutação para o LSR saber qual o tipo de comutação utilizar. O *Generalized Payload Identifier* (16 bits) é usado para identificar o tipo de carga paga transportada pelo LSP e é usado apenas pelos extremos do LSP.

Por exemplo, poderemos ter o campo *LSP Encoding Type* com o valor 5 (significa que a tecnologia usada é SDH/SONET), o campo *Switching Type* com o valor 100 (significa que a ligação tem capacidade para o tipo de comutação *Time-Division-Multiplex*) e o campo *Generalized Payload Identifier* com o valor 5 (significa que o sinal é transportado na forma *Asynchronous mapping of E4*) [5].

Os restantes parâmetros específicos da tecnologia não são transportados no objecto *Generalized Label Request* mas em objectos específicos que descrevem os parâmetros de tráfego.

Em complemento à mensagem *Generalized Label Request* tem-se o objecto *Generalized Label* que permite representar as diferentes tecnologias.

Quando o caminho é definido explicitamente, é adicionado à mensagem um objecto *Explicit Route*.

A largura de banda requerida é codificada nos parâmetros CR-LDP *Traffic Parameters* TLV ou no objecto RSVP-TE SENDER-TSPEC. Neste campo são definidos os parâmetros de tráfego específicos para uma dada tecnologia (tipo de sinal, concatenação e/ou transparência para sinais SDH).

O tipo de protecção para a ligação pode ser requerido, usando o objecto *Protection Information* (secção 3.8.2).

Se o LSP for bi-direccional, também é especificado um *Upstream Label* na mensagem de *Path/Label Request*. Esta etiqueta será usada na direcção de montante.

Adicionalmente, também podem ser incluídos na mensagem de pedido de etiqueta a informação: *Suggested Label* (para sugestão de etiqueta por parte do LSR a montante ao LSR a jusante), *Label Set* (para definição de um conjunto de etiquetas de entre os quais o LSR pode escolher) e *Waveband Label* (indica que requer uma etiqueta para um comprimento de onda).

Nas situações em que podem ser devolvidas várias etiquetas para um único pedido, por exemplo, se for pedido um sinal SDH concatenado, o LSR a jusante enviará uma mensagem *Resv/Label Mapping* incluindo um objecto *Generalized Label* que contém diversos *Generalized Labels* [6].

Em ambos os protocolos RSVP-TE e CR-LDP, para estabelecer um LSP unidireccional do LSR A para o LSR D é usada uma mensagem de *Generalized Label Request* na direcção jusante (do LSR A para o LSR D), e uma mensagem de mapeamento na direcção montante (do LSR D para o LSR A). As etiquetas para o LSP unidireccional do LSR A para o LSR D são estabelecidas conforme a mensagem de mapeamento viaja no sentido

montante. Em GMPLS, ao contrário do que acontece em MPLS, é possível estabelecer LSPs bidireccionais com um único conjunto de mensagens de sinalização sendo apenas necessário adicionar um *upstream label* à mensagem de *Generalized Label Request*. O nó que recebe esta mensagem actualiza a sua tabela de encaminhamento com o *upstream label* e envia a mensagem com um novo *upstream label* para o nó jusante. Desta forma, conforme a mensagem de *Generalized Label Request* se propaga para o LSR D, as etiquetas para o caminho LSR D – LSR A são estabelecidas. As etiquetas para o caminho LSR A – LSR D são estabelecidas conforme a mensagem de mapeamento se propaga em direcção ao LSR A.

3.6. Extensões de Encaminhamento para Suporte de GMPLS

O MPLS faz uso de informação relacionada com o estado das ligações (v. 3.1). As características relacionadas com o estado das ligações incluem informação tal como: máxima largura de banda, máxima largura de banda reservável e largura de banda não reservada numa ligação (as características são definidas em [10] para OSPF-TE e [11] para IS-IS-TE).

Com o GMPLS todas as ligações podem ser descritas através de informação de estado de ligação. Por outro lado, um LSP pode ser visto pelo protocolo de encaminhamento como uma ligação ponto-a-ponto descrita por informação de estado de ligação (*Forwarding Adjacency*). Para melhorar a escalabilidade, um conjunto de ligações pode ser anunciada como uma única ligação com a correspondente informação de estado de ligação (*Forwarding Adjacency*) [1]. Dito de outra forma, a *Forward Adjacency* pode representar um conjunto LSP's que esteja agregado num LSP hierarquicamente superior. Neste caso, os nós intermédios vêem apenas o LSP hierarquicamente superior, não tendo de manter tabelas de encaminhamento para cada um dos LSP's internos. Isto implica menos mensagens de sinalização trocadas aumentando consideravelmente a escalabilidade da sinalização [1].

Para o GMPLS suportar o transporte da informação do estado da ligação, foram efectuadas extensões aos protocolos de encaminhamento existentes;

nomeadamente, acrescenta mais informação às extensões existentes para OSPF-TE e IS-IS-TE necessárias para MPLS.

Desta forma, as extensões de encaminhamento do GMPLS, permitem a existência de ligações *unnumbered link* em que não existem endereços IP atribuídos aos extremos da ligação; permitem o transporte da informação de *Link Protection Type* de modo que o algoritmo de cálculo de caminho possa estabelecer LSPs com as características de protecção apropriadas; permitem o transporte da informação *Shared Risk Link Group* que define um conjunto de ligações que partilham um recurso cuja falha pode afectar todas as ligações do conjunto; e definem a codificação dos valores que podem ser usados para representar características da ligação, tal como, largura de banda máxima e mínima de LSP [5]

As extensões de encaminhamento do GMPLS, para permitir o anúncio da capacidade de comutação de cada interface (PSC, L2SC, TDM, LSC ou FSC), definem um novo sub-TLV (*Type/Length/Value*) para OSPF-TE e IS-IS-TE. Este sub-TLV é designado *Interface Switching Capability Descriptor* complementando os sub-TLV's já definidos para OSPF-TE e IS-IS-TE. Para ligações bi-direccionais, as capacidades de comutação de uma interface são definidas como sendo as mesmas em ambas as direcções; quer para dados que entram no nó através da interface quer para dados a sair do nó através da interface as capacidades de comutação são as mesmas.

Os *Interface Switching Capability Descriptor(s)* são transportados no objecto *Link State Advertisement* dos protocolos OSPF-TE e IS-IS-TE. Uma interface pode ter mais do que um *Interface Switching Capability Descriptor*. Isto é usado para interfaces que suportam múltiplas capacidades de comutação, para interfaces que suportam valores de largura de banda máxima por LSP diferentes por nível de prioridade e para interfaces que suportam largura de banda descontínua.

Se uma interface for do tipo *Time-Division Multiplex (TDM)* significa que o nó que recebe dados por esta interface pode multiplexar e desmultiplexar canais nos dados SDH.

Para interfaces TDM a informação do *Interface Switching Capability Descriptor* inclui: *Maximum LSP Bandwidth*, a informação se a interface suporta *Standard* ou *Arbitrary* SDH, e a informação de *Minimum LSP Bandwidth*.

Para uma ligação simples a *Maximum LSP Bandwidth* à prioridade p é definida como a máxima largura de banda que um LSP de prioridade p pode reservar. A *Maximum LSP Bandwidth* de uma ligação *bundled* é definida em [13]. O *Minimum LSP Bandwidth* define a largura de banda mínima que um LSP pode reservar.

Os valores típicos de *Minimum LSP Bandwidth* e de *Maximum LSP Bandwidth* são enumerados em [5]. Numa interface com *Standard SDH multiplexing*, um LSP de prioridade p pode reservar qualquer valor de largura de banda permitido pela estrutura de multiplexagem SDH, com os limites a serem dados por *Minimum LSP Bandwidth* e *Maximum LSP Bandwidth* para prioridade p .

Interfaces que suportam sinais sub VC-3 podem incluir informação adicional no *Interface Switching Capability Descriptor*, no entanto, ainda não se encontra definida [12].

3.7. Parâmetros de Tráfego SDH

Em GMPLS um *Terminal Multiplexer* (TM) SDH, um *Add-Drop Multiplexer* (ADM) ou um *cross-connect* (i.e. um comutador) é designado de LSR SDH. Uma rota ou circuito SDH entre dois LSRs SDH torna-se um LSP GMPLS. Um LSP SDH é uma ligação lógica entre o ponto no qual o sinal tributário (camada do cliente) é acomodado no seu contentor virtual (VC), e o ponto no qual é extraído do seu contentor virtual.

O controlo da multiplexagem SDH, por GMPLS, é feito através do controlo dos elementos SDH que podem ser referenciados por ponteiros. Estes componentes são os sinais VC-4, VC-3, VC-2, VC-12 e VC-11 em SDH.

Para o pedido de um LSP é necessário especificar os parâmetros de tráfego pretendidos para o LSP em questão.

Para RSVP-TE, os parâmetros de tráfego SDH (Figura 19) são transportados nos objectos *SENDER_TSPEC* e *FLOWSPEC*. Não existe *Adspec* (informação adicional recolhida ao longo do caminho seguido pela mensagem *Path* em cada nó, que possibilita a alteração do pedido por parte do nó destino) associado ao *SENDER_TSPEC*. O *Adspec* ou é omitido ou é usado um valor por defeito [6]. O conteúdo do objecto *FLOWSPEC* recebido na mensagem *Resv* deve ser idêntico ao conteúdo de *SENDER_TSPEC* da correspondente mensagem de *Path*. Ou seja, o receptor não está, normalmente, autorizado a alterar os valores dos parâmetros de tráfego.

Para CR-LDP, os parâmetros de tráfego SDH são simplesmente transportados num novo *TLV*.

Os parâmetros de tráfego SDH GMPLS têm a mesma estrutura quer sejam transportados por RSVP-TE ou CR-LDP e especificam características do pedido SDH [6].

0	8	16	31
Signal Type	RCC	NCC	
NVC		Multiplier (MT)	
Transparency (T)			
Profile (P)			

Figura 19 – Parâmetros de Tráfego SDH

Signal Type (8 bits) – este campo indica o tipo de sinal SDH elementar para o LSP requisitado, e.g., VC-12, VC-4, STM-1, etc. Várias transformações podem depois ser aplicadas sucessivamente ao sinal elementar para construir o sinal final que efectivamente está a ser requisitado para o LSP. Estas transformações são obtidas através dos valores dados aos restantes campos. As transformações são opcionais e devem ser ignoradas se o valor for zero, excepto no caso do *Multiplier* em que deverá ser ignorado se tiver o valor um. Estas transformações são a concatenação contígua, a concatenação virtual, a transparência e a multiplicação. No trabalho realizado, foi assumido que não são efectuadas transformações do sinal elementar.

Requested Contiguous Concatenation (8 bits): este campo é usado para pedir a concatenação contígua SDH opcional do sinal elementar.

Number of Contiguous Components (16 bits): indica o número de VCs idênticos (i.e., sinais elementares) a concatenar da forma indicada no campo RCC (concatenação contígua).

Number of Virtual Components (16 bits): indica o número de sinais a serem virtualmente concatenados. Por definição, estes sinais são todos do mesmo tipo. São os sinais elementares (VCs) para os quais o documento [6] define tipos de sinal (VC-11, VC-12, VC-2, VC-3, VC-4).

Multiplier (16 bits): indica o número de sinais idênticos que formam o LSP, constituindo o sinal final. Os sinais podem ser sinais elementares idênticos, ou sinais concatenados de forma contígua idênticos, ou sinais concatenados virtualmente idênticos.

Transparency (32 bits): este campo é um vector de *flags* que indica o tipo de transparência requerida.

Profile (32 bits): este campo serve para indicar capacidades particulares que têm de ser suportadas pelo LSP, por exemplo, capacidades de monitorização.

3.8. Sobrevivencialidade em Redes GMPLS

À semelhança do MPLS, o GMPLS também contempla mecanismos de sobrevivencialidade.

Usando a tecnologia GMPLS, é possível reagir a falhas na rede de forma quase instantânea: podem ser utilizados LSPs de reserva que entram em funcionamento no caso de ocorrer uma falha que impeça o normal funcionamento dos LSPs principais ou os LSPs podem ser determinados após a falha.

Os mecanismos que permitem a sobrevivencialidade da rede são em geral desenhados para lidar com falhas únicas. A recuperação a múltiplas falhas

requer mais estudos [1]. Os mecanismos podem ser aplicados sobre topologias em malha e em anel.

A recuperação de uma falha na rede, incorpora diversas fases, tal como foi discutido em [8], incluindo detecção de falha, localização de falha, notificação, recuperação e a reversão do tráfego (i.e., retornar o tráfego para o LSP original ou para um LSP determinado em consequência da falha).

- A detecção de falhas é dependente da tecnologia e da implementação. Em geral, as falhas são detectadas por mecanismos da camada inferior (e.g., SONET/SDH, *Loss-of-Light* (LOL)). Quando um nó detecta uma falha, pode ser passado um alarme para a entidade GMPLS superior, que tomará as acções apropriadas, ou o alarme poderá ser propagado na camada inferior (e.g., SONET/SDH AIS).
- A localização de falhas, pode ser feita com a ajuda de GMPLS, e.g., usando LMP para localização de falhas.
- Notificação de falhas, pode também ser obtida através de GMPLS, e.g., usando notificação GMPLS RSVP-TE/CR-LDP.

3.8.1. Estratégias de Recuperação

As técnicas de recuperação de redes podem ser divididas em Protecção e Restauro (PR). Na protecção, os recursos de protecção são atribuídos antes da falha, e a conectividade após a falha é obtida simplesmente por comutação efectuada nas extremidades da ligação protegida. Por outro lado, o restauro usa sinalização após a falha, para atribuir recursos ao longo do caminho de recuperação.

- A protecção tem por objectivo tempos de reacção extremamente rápidos, podendo basear-se no uso de campos de controlo para atingir a coordenação entre extremidades. Os mecanismos de protecção podem também ser classificados pelo nível de redundância e partilha.
- Os mecanismos de restauro baseiam-se em protocolos de sinalização para coordenar as acções de comutação durante a recuperação, e podem envolver um simples re-aprovisionamento, i.e., sinalização apenas no

momento de recuperação; ou pré-sinalização, i.e., sinalização antes da recuperação.

Os mecanismos de PR podem ainda ser aplicados de forma local ou extremo-a-extremo. Na abordagem local, a PR foca-se na proximidade da falha de modo a reduzir o atraso no restauro do serviço. Na abordagem extremo-a-extremo, são os nós onde se origina e termina o LSP que controlam a recuperação.

Usando estas estratégias, podem definir-se mecanismos de recuperação.

Neste trabalho, pretende-se que os mecanismos de recuperação utilizados possam fornecer redundância aos caminhos de serviço e sejam rápidos na recuperação. Desta forma, a descrição seguinte centra-se nos esquemas de protecção.

Em termos genéricos o GMPLS permite os seguintes esquemas de protecção:

- Protecção de Ligação 1+1: dois recursos pré-aprovisionados são usados em paralelo. Por exemplo, os dados são transmitidos em simultâneo por duas ligações e um selector é usado no nó receptor para escolher a melhor fonte [9].
- Protecção de Ligação 1:N: São pré-aprovisionados recursos activos e de protecção (N activos, 1 de protecção). Se um recurso activo falha, os dados são comutados para o recurso de protecção, usando um mecanismo de coordenação. Em geral, podem-se ter N recursos activos e M recursos de protecção, para esquemas de protecção de ligação M:N [9].
- Protecção melhorada (*enhanced*): conjunção de vários mecanismos de protecção que permitem passar do nível de protecção de falha única, para protecção multifalhas.
- Protecção de LSP 1+1: transmissão simultânea de dados, nos LSPs de serviço e de protecção, sendo a selecção efectuada no nó destino [9].

3.8.2. Sinalização de Link Protection

Notar que o GMPLS anuncia as capacidades de protecção de uma ligação nos protocolos de encaminhamento OSPF-TE e IS-IS-TE. Os algoritmos de cálculo de rota, podem ter em conta esta informação, quando calculam as rotas para estabelecer LSPs.

A informação de protecção é transportada no novo objecto/TLV opcional *Protection Information* dos protocolos RSVP-TE e CR-LDP. Este indica o tipo de protecção de ligação desejada: dedicada 1+1, dedicada 1:1, partilhada 1:N ou desprotegida. Se for pedido um tipo de protecção em particular, i.e., 1+1 ou 1:N, então, o pedido de ligação, só é processado, se o tipo de protecção desejado puder ser satisfeito.

O objecto *Protection Information* indica também se o LSP é um LSP primário ou secundário. Um LSP secundário é a salvaguarda do LSP primário. Os recursos de um LSP secundário não são normalmente usados, enquanto o LSP primário não falhar, mas podem ser usados para o transporte de tráfego não prioritário. Quando o LSP primário falhar, qualquer LSP que esteja a usar os recursos do LSP secundário é terminado.

Assume-se que os mecanismos de protecção disponíveis em cada ligação são conhecidos através de mensagens de sinalização dos protocolos de encaminhamento. Isto permite que sejam apenas realizados pedidos de protecção que possam ser aceites pela ligação.

A informação do objecto *Protection Information* é definida pelos seguintes campos:

- *Secondary (S)*: campo de 1-bit que é usado para indicar que o LSP requisitado é um LSP secundário.
- *Reservado*: campo de 25-bits reservado, com todos os *bits* colocados a zero.
- *Link flags*: este campo indica o tipo de protecção desejada na ligação. Foram definidos os seguintes valores:
 - *Enhanced*: indica que deve ser usado um esquema de protecção melhor que 1+1 (i.e., 4-fiber BLSR em SDH);

- *Dedicated 1+1*: indica que deve ser usado o esquema de protecção 1+1;
- *Dedicated 1:1*: indica que deve ser usado o esquema de protecção 1:1;
- *Shared*: indica que deve ser usado o esquema de protecção *shared*;
- *Unprotected*: não é necessária protecção;
- *Extra Traffic*: indica que o LSP requerido deve usar ligações que estão a proteger outros LSPs primários. O LSP requerido pode ser interrompido se as ligações que transportam o LSP primário falharem.

Capítulo 4 – Algoritmos de Encaminhamento Propostos

Neste capítulo, são apresentados algoritmos de encaminhamento de custo mínimo com protecção, propostos para uma rede GMPLS sobre SDH. Os algoritmos têm como objectivo maximizar a aceitação de tributários (caminho de serviço e caminho de protecção) sobre uma rede SDH.

4.1. Rede GMPLS sobre SDH

A aceitação de um tributário implica o estabelecimento de um VC, como já foi visto no capítulo 2. Desta forma, quando se refere o estabelecimento de um tipo de VC sub-entende-se que teve origem no pedido do tributário correspondente. Ao longo deste capítulo o processo é referido como o pedido ou estabelecimento de VC. Notar ainda que os algoritmos são definidos apenas para os tributários E1, E3 e E4 ao que correspondem os *virtual containers* VC-12, VC-3 e VC-4 porque estes são os tributários definidos para o espaço europeu (v. cap.2). A capacidade das ligações da rede é definida como STM-1 ou STM-4 por estas serem as capacidades elementares da rede SDH no sistema europeu. Os resultados obtidos com estes valores de capacidade podem facilmente ser extrapolados para valores mais elevados

de capacidade (e.g., STM-16 a 2 Gbps e o STM-64 a 10 Gbps) que podem ser interpretados como N canais do tipo STM-4 ou STM-1.

Considere-se uma rede com controlo GMPLS sobre tecnologia SDH constituída por *Label Switched Routers* (LSRs), i.e., comutadores SDH com um plano de controlo GMPLS (de seguida designados de nós SDH/GMPLS), interligados entre si. Quando é pedido um novo VC para suportar um circuito tributário, o GMPLS faz o estabelecimento do VC (LSP), baseando-se num algoritmo robusto de percursos de custo mínimo com restrições para determinar o caminho por onde estabelecer o VC. O pedido de um VC (LSP) é efectuado recorrendo à mensagem *Generalized Label Request*. Quando se pretende estabelecer um VC entre dois comutadores SDH este é visto como um LSP. O pedido do VC é efectuado à rede do operador sem que o equipamento do cliente possa ter conhecimento da estrutura de rede do operador, portanto, é necessário um mecanismo que através da camada GMPLS (RSVP-TE) sinalize o pedido ao equipamento fronteira da rede do operador sem indicar os caminhos dentro da rede. Por outro lado, tem de estabelecer um circuito entre o equipamento do cliente e o equipamento do operador. Este circuito será constituído por um caminho de serviço e um caminho de protecção ou somente por um caminho conforme a estrutura de ligação entre os equipamentos o permitir.

As redes SDH têm, normalmente, mecanismos de protecção baseados em anéis. Este tipo de mecanismo leva à duplicação dos recursos necessários o que não é muito interessante para os operadores. Por outro lado, numa rede em malha, a protecção de caminhos é conseguida sem que se tenham de duplicar os recursos. A questão reside em conseguir algoritmos que façam uma correcta gestão dos recursos existentes na rede, de modo que seja sempre possível obter um caminho de protecção para um caminho de serviço.

O algoritmo robusto de custo mínimo tem as seguintes características: a cada interface de saída de cada ligação é atribuído um valor de custo positivo para cada tipo de VC; cada LSR, através de protocolos de encaminhamento (por exemplo, OSPF-TE ou IS-IS-TE), troca mensagens com todos os LSR's com o seu conjunto de ligações e custos para cada tipo de VC (em cada momento

todos os LSR's têm a representação topológica da rede); quando é pedido um novo VC, o LSR de origem, determina dois caminhos (um de serviço e um de protecção) através de um algoritmo de pares de percursos de custo mínimo com nós disjuntos. O algoritmo é aplicado ao grafo de rede composto pelas ligações que podem aceitar o VC pedido. De seguida os VC's disjuntos são estabelecidos de acordo com os caminhos determinados.

Dado que o estabelecimento de um caminho de serviço e de protecção corresponde, em SDH, ao estabelecimento de dois VC's, os caminhos de serviço e de protecção estabelecidos serão designados por VC de serviço e VC de protecção.

Notar que sempre que novos VC's são estabelecidos ou VC's existentes são libertados, todos os LSR's envolvidos têm de calcular os novos valores de utilização e custos e através de protocolos de encaminhamento enviar essa informação para todos os outros LSR's. Este mecanismo pode falhar se um novo circuito for pedido e os valores de utilização de uma alteração recente não tiverem ainda atingido todos os LSR's. Assume-se que, na rede GMPLS sobre SDH, o intervalo entre pedidos de circuitos tributários é na ordem de pelo menos alguns minutos, o que significa que existe sempre tempo entre dois pedidos de circuito para toda a rede actualizar o estado das ligações.

Para efectuar a requisição de um LSP (VC), recorre-se aos parâmetros de tráfego descritos em 3.7 de modo a especificar as características do VC pedido.

É requerido que para cada VC de serviço exista um VC de protecção que seja distinto do VC de serviço nos nós e arestas do grafo. O tipo de protecção desejado é transportado por RSVP-TE ou CR-LDP no objecto TLV opcional de *Protection Information*. O tipo de protecção pode ser 1+1 ou 1:1 dependendo se o operador de rede pretende usar o VC de protecção para enviar tráfego extra ou não. O envio de tráfego extra não é alvo de estudo neste trabalho.

Dada a característica distribuída do GMPLS, os algoritmos de encaminhamento de custo mínimo são também distribuídos.

A troca de informação entre os nós pode ser obtida, por exemplo, através do uso do *Link State Advertisement (LSA)* do protocolo OSPF. Os LSA's são constituídos por TLV's e sub-TLV's que transportam informação descritiva das ligações. Como visto em 3.6, uma interface pode ser descrita por mais do que um sub-TLV *Interface Switching Capability Descriptor*. Para os algoritmos em que é necessário anunciar custos diferentes para cada um dos tipos de VC's, faz-se uso do sub-TLV *Interface Switching Capability Descriptor* colocando o campo *Minimum LSP Bandwidth* com valor de VC igual ao do campo *Maximum LSP bandwidth*. Desta forma, enviando três sub-TLV's, é possível indicar três custos para a mesma interface mas para tipos de VC's diferentes.

4.2. Descrição dos Algoritmos de Encaminhamento Robusto de Custo Mínimo

Os algoritmos de encaminhamento robusto de custo mínimo propostos são estruturalmente semelhantes mas apresentam diferentes estratégias de atribuição dos custos de cada interface que servem de base para a determinação dos percursos de custo mínimo. As funções de custo estudadas são função da (i) capacidade total da ligação ou da (ii) capacidade livre da ligação ou (iii) das anteriores em conjunto com um esquema de penalizações da aceitação de determinados tipos de VC's quando a carga da ligação atinge determinados patamares. É também apresentado um algoritmo que tem por objectivo potenciar o uso dos recursos de rede, através de um mecanismo de reorganização dos VC's de protecção.

De seguida, são apresentadas as características dos diferentes algoritmos.

A primeira estratégia estudada é uma estratégia já largamente estudada noutros tipos de redes e a sua principal vantagem é a simplicidade. A estratégia consiste na atribuição de um custo constante a cada interface de saída de cada ligação, valor este inversamente proporcional à capacidade da ligação, designando-se o algoritmo resultante por InvCap.

A segunda estratégia é uma evolução natural da primeira estratégia em que os custos constantes são substituídos por custos variáveis ao longo do tempo. A estratégia consiste em atribuir a cada interface de saída de cada ligação um valor inversamente proporcional à capacidade livre da ligação, designando-se o algoritmo resultante por InvBand. Esta estratégia, embora mais complexa que a anterior, permite um melhor balanceamento do tráfego entre todas as ligações de rede (conforme os resultados comprovarão).

Os algoritmos InvCap e InvBand apresentam uma desvantagem quando aplicados a redes SDH. Esta desvantagem está relacionada com a característica de multiplexagem do SDH. Numa rede de comutação de circuitos multi-serviço, existem sempre valores de carga de ligação que, quando atingidos, não permitem acomodar os VC's de largura de banda elevada mas podem ainda acomodar VC's de menor largura de banda. Tendo em atenção a hierarquia específica da tecnologia SDH percebe-se que a aceitação de um VC de pequena capacidade impede a aceitação de VC's de maior capacidade. Por outro lado, é possível a existência de capacidade livre entre dois nós (através de diversos percursos) mas que não pode ser usada, para aceitar determinado tipo de VC de maior capacidade, dada a hierarquia. Considere-se um STM-1 inicialmente vazio. Como visto no capítulo 2, o estabelecimento de um VC-12 ou VC-3 num STM-1 impede a possibilidade de estabelecer um VC-4 no STM-1. O estabelecimento de um VC-12 impede também o estabelecimento de um VC-3. No entanto, como apenas um TUG-3 tem um VC-12 estabelecido, é ainda possível estabelecer VC-12 (no mesmo TUG-3 e nos restantes) e VC-3 (nos restantes TUG-3) nesse mesmo STM-1. Na situação em que o STM-1 tiver o equivalente a 43 VC-12 estabelecidos (situação em que no mínimo tem dois TUG-3 completos e um VC-12 estabelecido no terceiro TUG-3), o STM-1 deixa também de poder suportar VC-3 e suporta apenas VC-12.

Assim, pode-se desde já antever que, neste tipo de redes, os pedidos de VC's de largura de banda maior, obterão probabilidades de bloqueio também maiores.

Tendo em conta a desvantagem anterior é proposto um novo algoritmo baseado nos anteriores, onde é introduzido o conceito de penalizações. Esta

estratégia toma em atenção a estrutura de multiplexagem SDH e procura minimizar a diferença entre probabilidades de bloqueio de circuitos de diferentes larguras de banda, atribuindo valores de custo diferentes para diferentes tipos de VC's. A função de custo usada neste algoritmo, baseia-se nas funções dos algoritmos anteriores mas permite reflectir o impedimento de aceitar VC's de maior capacidade quando se aceitam VC's de menor capacidade. Os algoritmos tomam as designações InvCap+PEN e InvBand+PEN.

Note-se que quando se libertam os recursos atribuídos aos caminhos de protecção e serviço surgem novos caminhos entre os nós extremo de pedidos já estabelecidos que podem ter menores custos. Se se puder optar por estes novos caminhos o aproveitamento dos recursos existentes será otimizado. É, assim, proposto também um algoritmo de optimização do uso dos recursos da rede SDH que potencia a aceitação de VC's de maior capacidade. Este algoritmo faz a reorganização dos VC's de protecção já estabelecidos (os VC's de protecção são novamente calculados e re-estabelecidos). A reorganização de VC's de protecção é efectuada no momento em que se dá a libertação de recursos associados ao par de VC's de serviço e protecção.

Apenas é efectuada a reorganização dos VC's de protecção porque estes VC's, ao contrário dos VC's de serviço, não estão a ser usados para enviar tráfego prioritário. Assume-se ainda, que durante a reorganização de um VC de protecção a probabilidade de ocorrência de falhas no VC de serviço é desprezável. Desta forma, desactivar o VC de protecção não implica a perda de comunicação tendo uma sobrecarga mínima do sistema de gestão.

Este algoritmo de optimização é proposto ser centralizado, porque o nó tem de ter conhecimento de todos os caminhos de serviço e protecção estabelecidos na rede e a sua posição na estrutura de multiplexagem SDH de cada ligação.

4.2.1. Algoritmo InvCap

O algoritmo InvCap tem como função de custo o inverso da capacidade total da ligação. O valor de capacidade de um STM-1 é 63 e o valor de capacidade de um STM-4 é 252 (v. cap.2).

Assim, o custo da aresta é dado por:

$$1/63 \quad (\text{para STM-1})$$

$$1/252 \quad (\text{para STM-4})$$

Como neste algoritmo os custos das arestas são fixos, apresenta a desvantagem de obter um fraco balanceamento de carga. As ligações com baixo custo serão escolhidas até estarem completas para cada tipo de VC, este facto é sinalizado e o algoritmo deixa de ter em conta a ligação para determinar os caminhos. Para o pedido de um novo VC o algoritmo terá de escolher outras ligações de custo mínimo.

4.2.2. Algoritmo InvBand

Este algoritmo tem a função de custo da ligação dada pelo inverso da capacidade livre da ligação. Como neste algoritmo os custos não são fixos, pois variam em função da capacidade livre da aresta, em momentos distintos o caminho escolhido entre dois nós pode ser distinto. Desta forma, esta estratégia permite uma melhor distribuição dos pedidos de circuitos pela rede, resultando num melhor balanceamento de carga e, portanto, melhorando o desempenho da rede.

Assim, o custo da aresta é dado por:

$$1/[63 - (V12 + 21 \cdot V3)] \quad (\text{para STM-1})$$

$$1/[252 - (V12 + 21 \cdot V3 + 63 \cdot V4)] \quad (\text{para STM-4})$$

Nestas expressões:

- V12 é o número de VC-12 estabelecidos na aresta;
- V3 é o número de VC-3 estabelecidos na aresta;
- V4 é o número de VC-4 estabelecidos na aresta;

Notar que o valor entre parêntesis curvos é o valor da capacidade ocupada na aresta. Na primeira expressão o termo V_4 não aparece porque no caso de STM-1 quando se estabelece um VC-4, a aresta fica sem capacidade livre. A aresta é sinalizada ao algoritmo como não utilizável para o cálculo de caminhos.

Para os algoritmos InvCap e InvBand, os VC's de serviço e de protecção são determinados para cada pedido de circuito, através do algoritmo de Suurballe's com *Vertex-Splitting* (anexo B). As arestas que têm a sua capacidade totalmente ocupada são sinalizadas ao algoritmo de cálculo dos caminhos disjuntos em nós de custo mínimo como não disponíveis. No caso particular das arestas que apesar de terem capacidade livre, esta não é suficiente para aceitar determinado tipo de VC, as arestas são sinalizadas ao algoritmo como não disponíveis quando se pretende determinar um VC de serviço ou protecção desse tipo de VC. A informação trocada entre nós é o custo das arestas entre os nós. É definido um custo para cada tipo de VC.

Numa implementação prática, não é necessário o uso de *flags* indicativas de que a ligação não pode aceitar determinado tipo de VC desde que, quando isto acontece, o seu custo seja colocado a um valor elevado (não atingível pela expressão normal de custo). O próprio valor de custo indica essa situação, o valor elevado é interpretado como se de uma *flag* indicativa de impossibilidade de estabelecimento de circuito se tratasse. O valor do custo, quando colocado a 1000, por exemplo, funciona como uma *flag* indicativa de que a aresta não tem capacidade disponível para o VC pretendido. Quando a aresta está completamente ocupada, os três custos são colocados a 1000. Portanto, as arestas com *flag/custo* a 1000, não são tidas em conta pelo algoritmo. Este esquema de *flag/custo* é aplicado em todos os algoritmos.

Para o algoritmo InvCap e o algoritmo InvBand sempre que são estabelecidos novos VC's ou VC's existentes são libertados, todos os LSR's envolvidos têm de calcular os novos custos das ligações. Esta informação é enviada através dos protocolos de encaminhamento OSPF-TE ou IS-IS-TE.

4.2.3. Algoritmo InvCap+PEN

Neste algoritmo, existe um custo por cada interface para cada tipo de VC pedido. As expressões de custo têm por base as expressões de custo do algoritmo InvCap, sendo acrescentados termos que reflectem a penalização de se aceitar VC's de menor capacidade que inibem a aceitação de VC's de maior capacidade. Isto significa que o custo de aceitar um VC de menor capacidade deve ser maior quando, ao ser aceite, inibe a aceitação de um VC de capacidade maior.

Para melhor ilustração das penalizações, considere-se uma ligação STM-4 inicialmente vazia. Esta ligação pode condicionar ou 4 VC-4 ou 12 VC-3. Se for necessário estabelecer um VC-12 por esta ligação, então é criado um TUG-3 parcialmente ocupado por ele. Assim, a aceitação deste VC-12 reduz a capacidade da ligação de aceitar futuros VC-3 de 12 para 11 e a capacidade da ligação de aceitar futuros VC-4 de 4 para 3. Assim, o custo da ligação deverá ter uma penalidade que reflecta esta redução de aceitação de VC-3 e VC-4. No entanto, o TUG-3 criado pode condicionar mais 20 VC-12 (relembrar que a capacidade de um TUG-3 é de 21 VC-12) pelo que após a aceitação do VC-12 inicial, podem ser aceites até mais 20 VC-12 sem que isso reduza a capacidade da ligação de aceitar futuros VC-3 ou VC-4. Assim, nestes casos, nenhuma penalização deverá ser contemplada no custo da ligação. Se a ligação tiver 21 VC-12 aceites, a aceitação de um novo VC-12 reduz a capacidade da ligação de aceitar futuros VC-3 de 11 para 10 mas mantém a capacidade de aceitar novos VC-4. Assim, para a aceitação do VC-12 neste caso, o custo da ligação deverá ter uma penalidade que reflecta apenas a redução de aceitação de VC-3.

Portanto, é definida uma função de custo, para cada tipo de VC, que exprima a inibição de aceitar um VC de maior capacidade quando se aceita o VC pretendido.

A função de custo para um pedido de tipo VC-12 é dada pela seguinte expressão:

$$1/63 + I3/A3 + I4/A4 \quad (\text{para STM-1})$$

$$1/252 + I3/A3 + I4/A4 \quad (\text{para STM-4})$$

Nestas expressões entende-se que:

- O primeiro termo é o inverso da capacidade da ligação;
- I3 é igual a um, se a aceitação de um VC-12 reduzir o número de VC-3 possíveis de serem estabelecidos (zero, caso contrário);
- A3 é igual ao número de VC-3 que se podem estabelecer em cada momento;
- I4 é igual a um, se a aceitação de um VC-12 reduzir o número de VC-4 possíveis de serem estabelecidos (zero, caso contrário);
- A4 é igual ao número de VC-4 que se podem estabelecer em cada momento;

A aceitação de um pedido de tipo VC-3 apenas poderá inibir um pedido de tipo VC-4. Na expressão do custo apenas o termo relativo ao VC-4 é mantido.

A função de custos para um pedido de tipo VC-3 é dada por:

$$1/63 + I4/A4 \quad (\text{para STM-1})$$

$$1/252 + I4/A4 \quad (\text{para STM-4})$$

Nestas expressões entende-se que:

- O primeiro termo é o inverso da capacidade da ligação;
- I4 é igual a um, se a aceitação de um VC-3 reduzir o número de VC-4 possíveis de serem estabelecidos (zero, caso contrário);
- A4 é igual ao número de VC-4 que se podem estabelecer em cada momento;

Como não existem VC's de maior capacidade, a aceitação de um pedido do tipo VC-4 não inibe a aceitação de qualquer tipo de VC de maior capacidade. Assim, os custos para um pedido de tipo VC-4 são dados pelo inverso da capacidade da ligação:

$$1/63 \quad (\text{para STM-1})$$

$$1/252 \quad (\text{para STM-4})$$

De notar que, com a estratégia de penalizações proposta, os termos de penalização são maiores quando a carga da aresta é maior, o que se traduz, dado o algoritmo de custo mínimo, na escolha de caminhos com penalizações menores e conseqüentemente com cargas menores. Os termos de penalização são máximos, e os correspondentes custos, quando a aceitação do tipo de VC de menor capacidade impede totalmente a aceitação do tipo de VC de maior capacidade na aresta em questão. A estratégia de penalizações resulta num maior equilíbrio das probabilidades de bloqueio entre os diferentes tipos de VC's.

4.2.4. Algoritmo InvBand+PEN

Neste algoritmo, tal como no anterior, existe um custo por cada interface para cada tipo de VC pedido. A função de custo é baseada no inverso da capacidade livre mas reflecte a inibição de aceitar VC's de maior capacidade quando se aceitam VC's de menor capacidade.

A função de custo para um pedido de tipo VC-12 é influenciada pela inibição de pedidos do tipo VC-3 e VC-4, sendo dada por:

$$1/[63 - (V12 + 21 \cdot V3)] + I3/A3 + I4/A4 \quad (\text{para STM-1})$$

$$1/[252 - (V12 + 21 \cdot V3 + 63 \cdot V4)] + I3/A3 + I4/A4 \quad (\text{para STM-4})$$

Nestas expressões entende-se que:

- O primeiro termo é o inverso da capacidade livre da ligação, onde V12 é o número de VC-12 estabelecidos e V3 o número de VC-3 estabelecidos;
- I3 é igual a um, se a aceitação de um VC-12 reduzir o número de VC-3 possíveis de serem estabelecidos (zero, caso contrário);
- A3 é igual ao número de VC-3 que se podem estabelecer em cada momento;
- I4 é igual a um, se a aceitação de um VC-12 reduzir o número de VC-4 possíveis de serem estabelecidos (zero, caso contrário);

- A4 é igual ao número de VC-4 que se podem estabelecer em cada momento;

Na expressão seguinte, apenas o termo referente ao pedido de VC-4 é mantido porque a aceitação de um pedido VC-3 pode inibir a aceitação de um pedido VC-4. Os custos para um pedido de tipo VC-3 são dados por:

$$1/[63 - (V12 + 21 \cdot V3)] + I4/A4 \quad (\text{para STM-1})$$

$$1/[252 - (V12 + 21 \cdot V3 + 63 \cdot V4)] + I4/A4 \quad (\text{para STM-4})$$

Nestas expressões entende-se que:

- O primeiro termo é o inverso da capacidade livre da ligação, onde V12 é o número de VC-12 estabelecidos e V3 o número de VC-3 estabelecidos;
- I4 é igual a um, se a aceitação de um VC-3 reduzir o número de VC-4 possíveis de serem estabelecidos (zero, caso contrário);
- A4 é igual ao número de VC-4 que se podem estabelecer em cada momento;

Como a aceitação do pedido de um VC-4 não inibe a aceitação de pedidos de VC maiores, os custos para um pedido de tipo VC-4 são dados pelo inverso da capacidade livre da ligação, onde V12 é o número de VC-12 estabelecidos e V3 o número de VC-3 estabelecidos :

$$1/[63 - (V12 + 21 \cdot V3)] \quad (\text{para STM-1})$$

$$1/[252 - (V12 + 21 \cdot V3 + 63 \cdot V4)] \quad (\text{para STM-4})$$

Os VC's de serviço e protecção são calculados através do algoritmo de Suurballe's com *Vertex-Splitting* para cada pedido de um VC com protecção. Para este algoritmo, as arestas que têm a sua capacidade totalmente ocupada ou ocupada para um tipo de VC são sinalizadas ao algoritmo de cálculo dos VC's de serviço e protecção para o pedido desse VC como não disponíveis.

Esta estratégia de penalizações obriga a uma maior complexidade de computação dada a necessidade de cálculo dos custos nos nós. Os parâmetros trocados entre nós são o custo para cada tipo de VC. Sempre

que são estabelecidos novos VC's, ou VC's existentes são libertados, todos os LSR's envolvidos têm de calcular os novos custos das ligações e enviá-los através de mensagens dos protocolos de encaminhamento.

4.2.5. Reorganização de VC's de protecção

Através da representação da multiplexagem SDH apresentada na secção 2.1, verifica-se que, quando um par de VCs (um VC de serviço e o correspondente VC de protecção) é libertado, podem surgir na estrutura de multiplexagem “buracos de capacidade”. Estes “buracos de capacidade” podem ser definidos como a capacidade livre vista em cada TUG-3. Os “buracos de capacidade” aparecem porque, para cada pedido de VC, a posição na estrutura de multiplexagem é dada pelo STM e TUG-3 correspondente dentro da estrutura. Como os “buracos de capacidade” estão em TUG-3 diferentes e são de valor de capacidade reduzido, não podem ser correctamente aproveitados. Por exemplo, podem-se ter 21 “buracos de capacidade” de capacidade VC-12 distribuídos por diferentes TUG-3 e STM's que não podem ser usados para aceitar um VC-3. Se os diversos “buracos de capacidade” existentes na estrutura de multiplexagem forem aglomerados num só, cria-se um bloco maior de capacidade livre que permite a aceitação de um VC-3. Este processo permite potenciar o número de VC's de capacidade maior que podem ser aceites pela rede. Para efectuar esta tarefa é proposto o algoritmo de reorganização de VC's de protecção.

A reorganização dos VC's de protecção é invocada quando um par de VCs (um VC de serviço e o correspondente VC de protecção) é libertado, o que poderá permitir a reorganização dos VC's de protecção estabelecidos. Um algoritmo deste tipo faz sentido porque o tempo entre pedidos de circuitos ou entre a libertação de pares de VCs é considerada razoavelmente grande.

O algoritmo de reorganização de VC's de protecção é executado de forma centralizada. O nó central recebe informação da rede para construir um grafo representativo do estado da rede. Sobre este grafo são efectuados todos os cálculos auxiliares à reorganização dos caminhos existentes. Um caminho de protecção só é alterado na rede, se também o for no grafo. Como é

necessária a criação de um grafo, implica o conhecimento de todos os circuitos já estabelecidos (e dos caminhos que lhes foram atribuídos) e do respectivo estado de ocupação da estrutura de multiplexagem SDH apresentada nas figuras 6 e 7. Portanto, para a reorganização de VC's de protecção, a informação da rede pode ser obtida através de mensagens trocadas entre os nós e o nó central. Esta informação enviada para o nó central exige um protocolo de gestão específico. O protocolo deve enviar a informação sempre que um pedido de VC é aceite ou é libertado, da informação deve constar a mesma informação que o RSVP-TE ou CR-LDP usam para o estabelecimento de um VC. O par de VC's é calculado e estabelecido sobre o grafo. Desta forma o nó central tem sempre a representação actual do estado de ocupação da rede. Este fluxo de informação poderá ser considerável para redes com um número de nós elevado. Este algoritmo continua a efectuar a troca de custos entre nós como em InvCap+PEN e InvBand+PEN.

A reorganização dos VC's de protecção é efectuada, começando pelos VC's de protecção de circuitos com capacidade VC-12, depois os VC's de protecção de circuitos com capacidade VC-3 e, finalmente, são reorganizados os VC's de protecção de circuitos VC-4. A reorganização dos VC's de protecção é efectuada por esta ordem porque, como os custos associados às arestas resultam do algoritmo de penalizações, os VC's de protecção estarão homogeneamente distribuídos pela rede. Assim, para o estado estacionário da rede, e sabendo que a rede recebe maior número de fluxos de capacidade VC-12, a ocupação da rede terá maior quantidade de "buracos de capacidade" provocados por VC-12 depois por VC-3 e finalmente por VC-4. Portanto, se se começar por reorganizar os VC's de protecção dos fluxos VC-12, o número de "buracos de capacidade" desse tamanho, tende a reduzir ou a anular-se, criando com isso, "buracos de capacidade" de maiores capacidades. Estes "buracos de capacidade", ao serem maiores, podem ser do tipo VC-3 ou VC-4, permitindo a reorganização dos VC's de protecção de fluxos VC-3 e VC-4. Ao efectuar-se de seguida a reorganização de fluxos de VC-3, o número de "buracos de capacidade" desse tamanho, tende a reduzir.

O algoritmo de reorganização de VC's de protecção é descrito da seguinte forma (Figura 20):

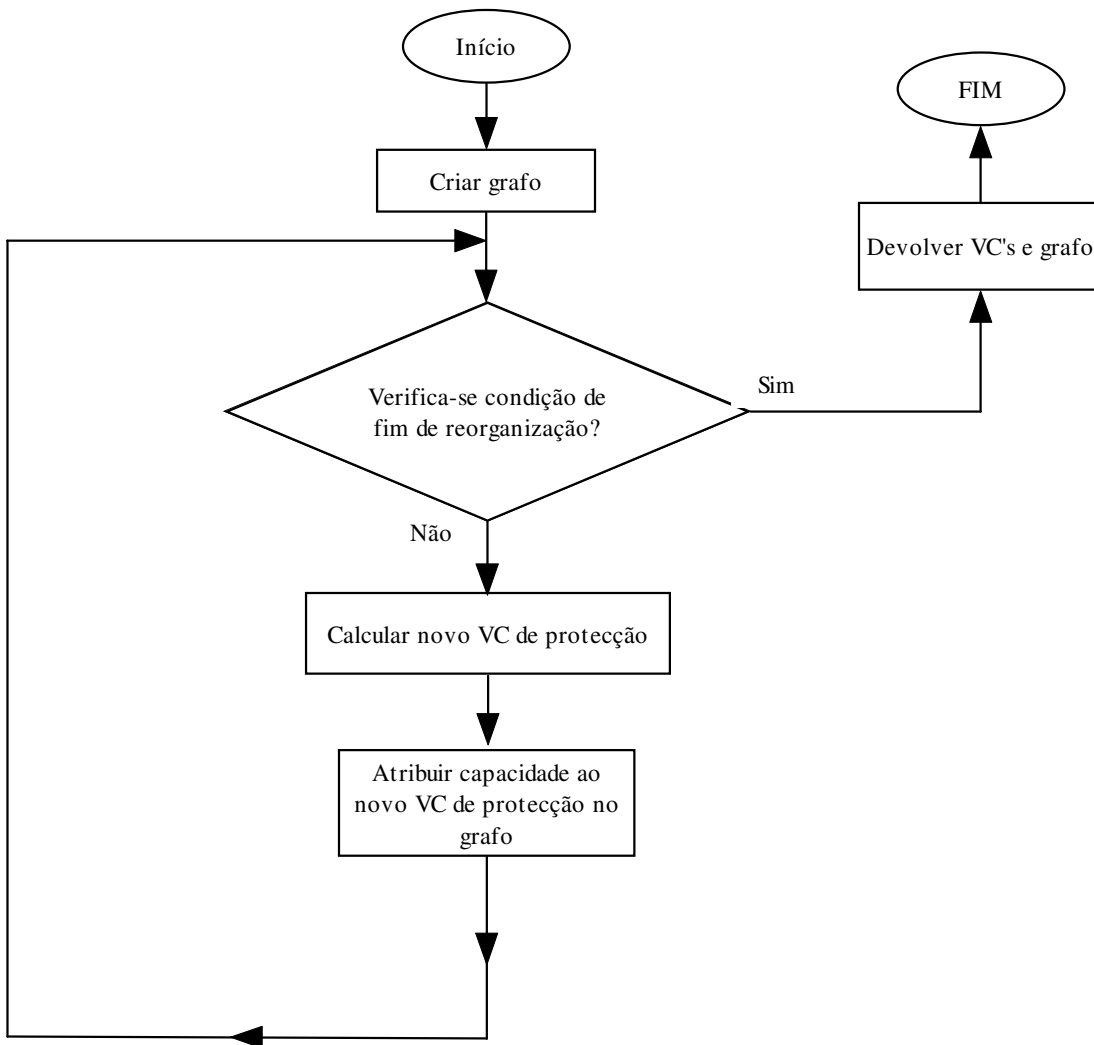


Figura 20 – Diagrama de blocos do algoritmo de Reorganização de VC's de protecção.

A reorganização de um VC de protecção consiste em libertar os seus recursos no grafo libertando todas as capacidades de aresta relativas ao VC e efectuar a respectiva actualização de custos (só possível tendo a informação completa do estado de ocupação da aresta em causa). De seguida, determina-se um caminho de custo mínimo sobre o grafo não considerando as arestas usadas pelo VC de serviço associado. O caminho determinado, que no pior caso é igual ao inicial, é o novo VC de protecção. De notar que, dada a estrutura de multiplexagem SDH, se o VC de protecção determinado coincidir com o original no percurso

mas tiver pelo menos uma ligação em que usa uma posição da estrutura de multiplexagem diferente, este é considerado um novo VC de protecção. O novo VC de protecção é estabelecido nas mesmas arestas que o VC de protecção original mas em posições diferentes na estrutura de multiplexagem das arestas em causa. Esta situação é considerada como uma reorganização do VC de protecção. Por exemplo, tendo um VC-12 estabelecido na pilha TUG-3(2) e existindo um VC-12 livre na pilha TUG-3(1), a reconfiguração do VC-12 vai permitir ocupar a pilha TUG-3(1) libertando a TUG-3(2). Este processo pode ser efectuado entre pilhas de diferentes STM's. O processo de reconfiguração é repetido até que nenhum VC de protecção seja alterado ou até um máximo de dez corridas deste processo. Foi definido o valor de dez corridas porque se verificou que a partir deste número de corridas os resultados não sofrem alterações significativas.

O algoritmo InvCap+PEN+RP tem a mesma função de custo do algoritmo InvCap+PEN, a diferença reside na capacidade de reorganizar os VC's de protecção.

O algoritmo InvBand+PEN+RP tem a mesma função de custo do algoritmo InvBand+PEN mas é efectuada a reorganização de VC's de protecção.

Para ambos os algoritmos é efectuada a reorganização dos VC's de protecção, através do sistema centralizado descrito anteriormente. Esta reorganização dos VC's de protecção tem por objectivo possibilitar a aceitação de mais tráfego na rede.

O mecanismo de reorganização de protecções não é aplicado aos algoritmos InvCap e InvBand porque estes algoritmos, como se irá verificar, obtêm os piores desempenhos. Desta forma, a optimização que se pretende com este mecanismo não seria obtida em toda a sua extensão para estes algoritmos.

Capítulo 5 – Avaliação de Desempenho dos Algoritmos

Neste capítulo é feita a avaliação do desempenho dos algoritmos de encaminhamento robusto apresentados no capítulo anterior. Esta avaliação é baseada em resultados de simulação, para os quais foi desenvolvido um simulador apropriado. Assim, este capítulo começa por descrever o simulador desenvolvido. De seguida, apresenta os casos de estudo considerados, os resultados obtidos bem como a sua análise e respectivas conclusões.

5.1. Descrição do Simulador

No âmbito deste trabalho foi desenvolvido um simulador de eventos discretos, na linguagem de programação C++, para estimar o desempenho de uma rede SDH com controlo GMPLS, usando os algoritmos descritos no capítulo anterior.

5.1.1. Parâmetros de Entrada do Simulador

Os parâmetros de entrada do simulador são:

- Rede SDH com a enumeração dos nós e a capacidade de cada aresta.

- Fluxos de tráfego em que cada fluxo é definido por:
 - os seus nós extremo
 - taxa de pedidos de circuito λ (em número pedidos por hora)
 - duração média de cada circuito $1/\mu$ (em horas)
 - tipo de circuito.

Nos casos de estudo considerados, assumiu-se que:

- Cada ligação da rede pode ser um STM-1 ou um STM-4.
- Os pedidos de circuito são do tipo VC-12, VC-3 ou VC-4 por correspondência aos tributários E-1, E-3 e E-4 respectivamente.
- O processo de chegada de pedidos de cada tipo de circuito é um processo de Poisson.
- A duração de cada circuito segue uma distribuição exponencial.

A capacidade de uma ligação STM-1 é 63 e a capacidade de uma ligação STM-4 é 252 (v. cap.2). As capacidades dos VC-12, VC-3 e VC-4 são respectivamente 1, 21 e 63.

O simulador recebe os parâmetros de entrada e devolve os resultados através de ficheiros (o anexo C apresenta uma descrição da forma como os ficheiros são construídos).

5.1.2. Critério de Paragem de Simulação

A todos os pedidos de circuito aceites é atribuído um VC de serviço e um VC de protecção, determinados segundo um algoritmo robusto de custo mínimo.

Para terminar a simulação é necessária a definição de um critério de paragem de simulação que defina o momento em que a simulação deve ser terminada.

Como o objectivo principal da simulação é estimar as probabilidades de bloqueio de cada fluxo, no caso geral, um critério de paragem apropriado é

assumir que todos os fluxos têm de cumprir um valor X de eventos-chegadas e Y de pedidos bloqueados. No entanto, dada a especificidade da rede SDH, constata-se que a probabilidade de bloqueio dos circuitos de maior capacidade são muito mais elevados do que a probabilidade de bloqueio dos circuitos de menor capacidade. Conforme se verá nos resultados computacionais, os circuitos VC-12 têm uma probabilidade de bloqueio desprezável quando comparados com a probabilidade de bloqueio dos circuitos VC-3 ou VC-4. Além disto, assumiu-se nos casos de estudo que a taxa de pedidos dos circuitos de menor capacidade é maior do que a dos outros (reflectindo a facto de o operador cobrar mais os circuitos de maior capacidade pelo que os clientes só os solicitam se a capacidade adicional for necessária).

Considere-se por exemplo que existem dois fluxos: (i) para o fluxo A de maior capacidade o valor X é atingido e o valor Y também e (ii) para o fluxo B de menor capacidade o valor X é largamente ultrapassado mas ainda não tem qualquer pedido bloqueado. Isto significa que o valor de probabilidade de bloqueio do fluxo B é muito menor quando comparado com a probabilidade de bloqueio do fluxo A. Se se pretender obrigar que o fluxo B cumpra os Y pedidos bloqueados isto irá obrigar a um tempo de processamento demasiado excessivo. A informação associada a este valor é irrelevante para o simulador porque o objectivo da simulação é estudar os valores das piores probabilidades de bloqueio. Desta forma, mesmo que o fluxo B não cumpra as especificações em termos de pedidos bloqueados, pode-se dizer que a sua probabilidade de bloqueio é consideravelmente menor que a probabilidade de bloqueio do fluxo A.

Assim, considere-se para um qualquer instante de tempo simulado o número de eventos-chegada do fluxo i dado por X_i e o número de pedidos bloqueados do fluxo i dado por Y_i . O objectivo principal do simulador é determinar as probabilidades de bloqueio de cada fluxo pelo que, no caso geral, para cada fluxo seria necessário que $X_i \geq X$ e $Y_i \geq Y$ para qualquer fluxo i . No entanto, como ilustrado pelo exemplo anterior, obter $Y_i = Y$ para alguns fluxos implica um tempo elevado de processamento e não acrescenta validade estatística aos resultados. Desta forma, os fluxos são divididos em dois grupos: os que

cumprem os X eventos-chegadas e Y pedidos bloqueados e os que cumprem apenas os X eventos-chegadas. No entanto, em cada momento é necessário verificar se os fluxos que estão no segundo grupo podem ser realmente considerados como tendo probabilidade de bloqueio muito menor que os do primeiro grupo. Esta verificação é efectuada recorrendo à relação Y/X para obter o patamar mínimo de probabilidade de bloqueio. De seguida é determinado de entre os fluxos que cumprem as especificações qual o fluxo com maior probabilidade de bloqueio. Este valor é usado como termo de comparação para verificar se a probabilidade de bloqueio dos fluxos que não cumprem Y número de pedidos bloqueados pode ser considerada desprezável. No presente trabalho, considera-se que a probabilidade de bloqueio de um fluxo i é desprezável se o seu valor actual Y_i / X_i for pelo menos cem vezes menor que a pior probabilidade de bloqueio de entre todos os fluxos. No caso da probabilidade de bloqueio de um fluxo ser considerada desprezável o fluxo não tem de cumprir os Y número de pedidos bloqueados. A simulação termina quando todos os fluxos que não cumprem os Y número de pedidos bloqueados tiverem probabilidades de bloqueio pelo menos cem vezes menores que a maior probabilidade de bloqueio dos fluxos que cumprem a especificação. Caso não se verifique o critério anterior, a simulação termina ao fim de quatro horas.

Para o presente trabalho os valores de X e Y foram determinados através de testes preliminares iniciais. Os valores determinados permitem obter uma boa confiança estatística dos resultados através de intervalos de confiança bastante apertados. Os valores determinados são $X = 50000$ eventos-chegadas e $Y = 10$ pedidos bloqueados ao que corresponde o patamar mínimo de probabilidade de bloqueio de 0,0002%.

De forma sucinta, apresenta-se o critério de paragem de simulação:

- Uma corrida da simulação termina quando todos os fluxos tiverem obtido um mínimo de dez pedidos bloqueados e um mínimo de cinquenta mil chegadas ou quando atingido um mínimo de cinquenta mil chegadas para todos os fluxos e os fluxos que não tenham obtido um mínimo de dez pedidos bloqueados tenham bloqueios desprezáveis. O processo evolui da seguinte forma:

- Para todos os fluxos, com um mínimo de dez pedidos bloqueados e um mínimo de cinquenta mil chegadas, é determinado o maior bloqueio de entre os diversos fluxos.
- Para os fluxos que tenham menos que dez pedidos bloqueados verifica-se se o bloqueio de cada fluxo é desprezável quando comparado com o bloqueio máximo determinado.
- A simulação termina se todos os pedidos que não cumprem a especificação de dez pedidos bloqueados tiverem bloqueios de pelo menos cem vezes menos que o pior bloqueio dos pedidos que cumprem a especificação.
- Se não se verificar o critério anterior, a simulação termina ao fim de quatro horas.

5.1.3. Medidas de Desempenho do Simulador

O simulador foi desenvolvido por forma a obter as seguintes medidas de desempenho:

- Probabilidade de bloqueio de cada fluxo estimada como sendo o número de pedidos do fluxo bloqueados a dividir pelo número total de pedidos do fluxo efectuados.
- Probabilidade de bloqueio de cada tipo de circuito, VC-12, VC-3 e VC-4, estimada como sendo o número de pedidos de circuito bloqueados a dividir pelo número total de pedidos de circuito efectuados.
- Probabilidade média de bloqueio global estimada como a média das probabilidades médias, de todos os fluxos, de cada corrida.
- O número médio de ligações usadas por cada fluxo dado pela média do número de ligações usadas pelo caminho de serviço e pelo caminho de protecção.
- O número médio de ligações usadas por cada tipo de circuito, VC-12, VC-3 e VC-4 dado pela média do número de ligações usadas pelo caminho de serviço e pelo caminho de protecção.

- A ocupação média das ligações, dada pela ocupação de cada ligação dada pela capacidade ocupada da ligação pelos circuitos estabelecidos a multiplicar pelo tempo entre dois eventos chegada e/ou partida a dividir pelo tempo de simulação da corrida.

5.1.4. Funcionamento do Simulador

Os diversos algoritmos apresentados no capítulo anterior têm um funcionamento similar entre si. A diferença reside na forma de cálculo do custo de cada aresta e na informação a trocar entre nós. Desta forma, e como as diferenças em termos de funções de custo e informação trocada foram já abordadas no capítulo anterior, nesta secção é descrita o modo de funcionamento dos algoritmos. A descrição seguinte é aplicável a qualquer um dos algoritmos.

Os eventos considerados são:

- o evento-chegada, definido como o instante de tempo de pedido da ligação, o tipo de VC pedido e os nós extremo;
- o evento-partida, definido como o instante de tempo de terminação da ligação estabelecida, o tipo de VC pedido e os nós extremo;

Os instantes de ocorrência dos eventos são armazenados numa lista de eventos. Nesta lista os eventos estão ordenados por ordem de ocorrência.

As variáveis consideradas são de três tipos: relógio de simulação, contadores estatísticos e variáveis de estado [16].

Relógio de Simulação:

É a variável que indica, em cada instante, o tempo de simulação decorrido, permitindo indexar cronologicamente os eventos.

Contadores estatísticos:

Para cada fluxo são usados dois contadores: um que contabiliza o número de pedidos bloqueados e outro que contabiliza os pedidos tentados; destes é estimado no fim da simulação a probabilidade de bloqueio por fluxo e por tipo de circuito.

Para cada aresta é usado um contador que contabiliza a sua área de ocupação determinada da seguinte forma: no instante de cada evento, é somado a este contador a capacidade ocupada do *link* multiplicada pelo intervalo de tempo entre o instante actual e o instante do evento anterior; este contador, quando dividido pelo tempo simulado, permite determinar a ocupação média de cada aresta.

Para cada fluxo é usado um contador que contabiliza o número médio de ligações usadas no estabelecimento dos respectivos circuitos (o número de ligações do percurso de serviço mais o número de ligações do percurso de protecção a dividir por dois); este contador permite determinar o número médio de ligações usadas para estabelecer um circuito por fluxo e por tipo de fluxo.

É ainda usado um contador para contabilizar a quantidade de tráfego suportada pela rede: no instante de cada evento, é somado a este contador a largura de banda total actualmente suportada pela rede multiplicada pelo intervalo de tempo entre o instante actual e o instante do evento anterior: este contador, quando dividido pelo tempo simulado, permite determinar a quantidade de tráfego média suportada pela rede.

Variáveis de estado:

- largura de banda ocupada no instante simulado presente em cada *slot* (um *slot* representa um TUG-3) de cada aresta;
- estado de ocupação da aresta dado pela atribuição e libertação de capacidade referente aos circuitos estabelecidos através da aresta;
- estado de ocupação da rede dado pela atribuição e libertação de capacidade referente aos circuitos estabelecidos sobre a rede (cada circuito contribui apenas com o valor do tipo de circuito do fluxo, não tendo qualquer relação com o número de ligações que tenha de usar para ser estabelecido);

O funcionamento do algoritmo robusto de custo mínimo é descrito da seguinte forma (conforme ilustrado na Figura 21):

São inicializados os contadores estatísticos e é agendado o primeiro evento-chegada de cada fluxo sendo criada a lista de eventos.

É determinado o próximo evento. No caso de ser um evento-chegada (na primeira vez é sempre um evento-chegada) é agendado o próximo evento-chegada para este fluxo (eliminando-se o actual da lista de eventos) e incrementa-se o número de pedidos efectuados deste fluxo. Desde que seja determinado um caminho de serviço e um de protecção, é agendado o respectivo evento-partida e as capacidades requeridas ao longo dos caminhos de serviço e protecção são atribuídas, obtendo-se o VC de serviço e o VC de protecção. Os contadores estatísticos são actualizados. É criada uma estrutura com os VC's de serviço e protecção que, juntamente com a nova partida agendada, é colocada numa estrutura referente aos diversos pedidos existentes. No caso de não ser possível alocar recursos para um ou para ambos os caminhos, o pedido é bloqueado, incrementando-se o respectivo contador.

No caso do evento ser uma partida é libertada a capacidade, referente ao pedido, ao longo dos VC's de serviço e de protecção e é actualizada a ocupação de rede. O evento-partida é retirado da lista de eventos, retorna-se ao teste de evento. O algoritmo de reorganização de protecções é invocado caso se esteja num algoritmo em que este está definido.

De seguida é verificado o critério de paragem de simulação. Se o teste de paragem de simulação for negativo, retorna-se ao teste de evento.

Quando se faz a atribuição de capacidades aos VC's de serviço e de protecção são actualizados os contadores de número de arestas usados por pedido. O contador relativo à ocupação das arestas é actualizado quando se efectua a atribuição e a libertação das capacidades referentes ao pedido.

Quando, através do critério de paragem de simulação, se verifica o final da corrida, as medidas de desempenho referentes à corrida são armazenadas. No fim das corridas pré-determinadas, é apresentado no ecrã e em formato de ficheiro, um relatório das medidas de desempenho.

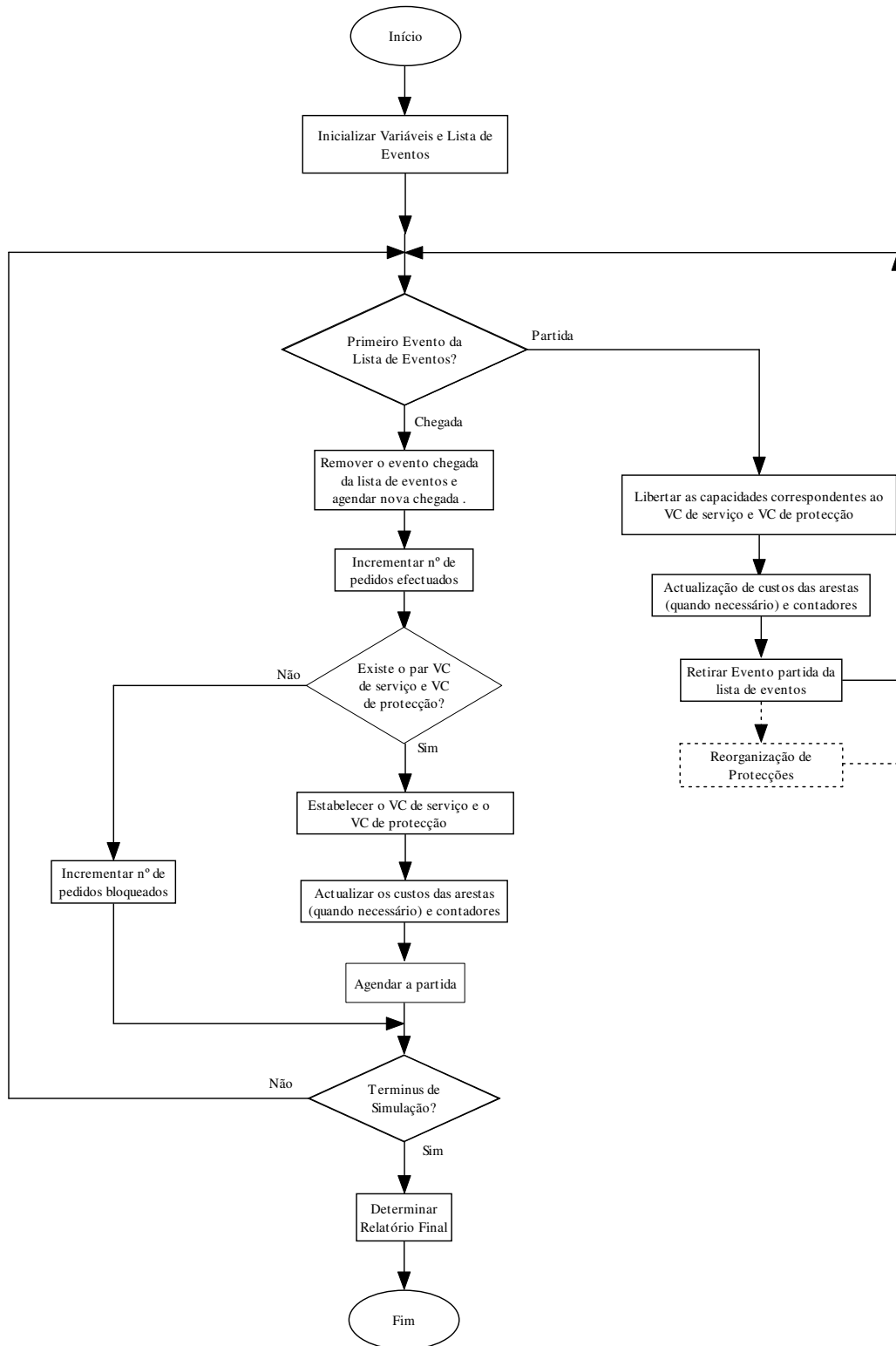


Figura 21 – Diagrama de blocos dos Algoritmos

5.2. Casos de Estudo

Os estudos de simulação foram efectuados a três casos de estudo. As topologias de rede dos casos de estudo são apresentadas de seguida.

Em relação ao tráfego, em todos os casos de estudo são consideradas distribuições exponenciais para o tempo de serviço com média de 6 horas para VC-12, 2 horas para VC-3 e 1 hora para VC-4.

Para todos os casos assume-se que todos os circuitos de serviço requerem circuito de protecção pelo que um circuito é bloqueado se um dos dois VC's não puder ser estabelecido.

5.2.1. Caso de Estudo A

Os casos de estudo A e B representam duas redes correctamente dimensionadas para o tráfego esperado. Nesta situação demonstra-se que os algoritmos de encaminhamento robusto melhoram os resultados obtidos com algoritmos de encaminhamentos já conhecidos.

No caso de estudo A e para o tipo VC-12, os valores de taxa de pedidos λ para cada fluxo foram gerados aleatoriamente com uma distribuição uniforme entre $[0,0-5,0]$. Para o tipo VC-3, os valores foram gerados aleatoriamente com uma distribuição uniforme entre $[0,0-0,3]$. Para o tipo VC-4, os valores foram gerados aleatoriamente com uma distribuição uniforme entre $[0,0-0,05]$.

Este caso de estudo tem por base a seguinte rede (Figura 22) (os nós extremo de fluxos estão assinalados a sombreado):

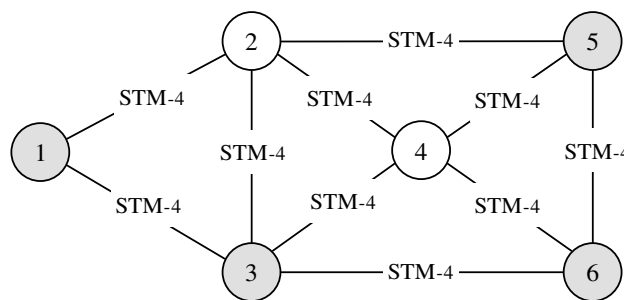


Figura 22 – Grafo do caso de estudo A

Os valores gerados são os que se mostram na tabela seguinte:

Nós Extremo		Tipo de VC	λ (circuitos/hora)	$1/\mu$ (horas)
1	3	VC-12	1,40	6
		VC-3	0,08	2
1	5	VC-12	2,20	6
		VC-3	0,20	2
		VC-4	0,03	1
1	6	VC-12	3,00	6
		VC-3	0,272	2
		VC-4	0,02	1
3	5	VC-12	4,60	6
		VC-3	0,12	2
		VC-4	0,04	1
3	6	VC-12	4,20	6
		VC-3	0,168	2
		VC-4	0,06	1
5	6	VC-12	3,00	6
		VC-3	0,104	2

Tabela 1 – Mapa de tráfego da rede do caso de estudo A

5.2.2. Caso de Estudo B

Este caso de estudo apresenta um maior número de nós e um correspondente aumento de tráfego gerado. Pretende-se assim verificar a validade dos algoritmos em redes de maiores dimensões e que suportem maiores níveis de tráfego.

No caso de estudo B e para o tipo VC-12, os valores de taxa de pedidos λ para cada fluxo foram gerados aleatoriamente com uma distribuição uniforme entre [0,0–4,0]. Para o tipo VC-3, os valores foram gerados aleatoriamente com uma distribuição uniforme entre [0,0–0,2]. Para o tipo VC-4, os valores foram gerados aleatoriamente com uma distribuição uniforme entre [0,0–0,04].

Este caso de estudo tem por base a seguinte rede (Figura 23) (os nós extremo de fluxos estão assinalados a sombreado):

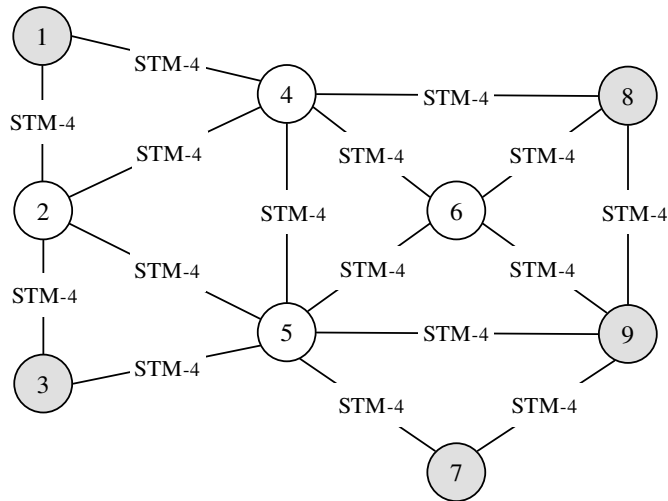


Figura 23 – Grafo do caso de estudo B

Os valores gerados são os que se mostram na tabela seguinte:

Nós Extremo	Tipo de VC	λ (circuitos/hora)	$1/\mu$ (horas)
1 3	VC-12	1,26	6
	VC-3	0,06	2
	VC-4	0,02	1
1 7	VC-12	3,22	6
	VC-3	0,19	2
	VC-4	0,05	1
1 8	VC-12	2,10	6
	VC-3	0,11	2
	VC-4	0,03	1
1 9	VC-12	1,54	6
	VC-3	0,14	2
	VC-4	0,01	1
3 7	VC-12	2,94	6
	VC-3	0,08	2
3 8	VC-12	1,68	6
	VC-3	0,09	2
	VC-4	0,03	1
3 9	VC-12	2,66	6
	VC-3	0,14	2
	VC-4	0,02	1
7 8	VC-12	1,96	6
	VC-3	0,16	2
7 9	VC-12	0,98	6
	VC-3	0,09	2
8 9	VC-12	3,08	6
	VC-3	0,18	2
	VC-4	0,03	1

Tabela 2 – Mapa de tráfego da rede do caso de estudo B

5.2.3. Caso de Estudo C

Por contraponto ao caso de estudo A, este caso de estudo pretende demonstrar que quando a rede é incorrectamente dimensionada, os algoritmos robustos de encaminhamento não conseguem obter melhores resultados que os algoritmos tradicionais.

Este caso de estudo tem por base a seguinte rede (Figura 24) (os nós extremo de fluxos estão assinalados a sombreado):

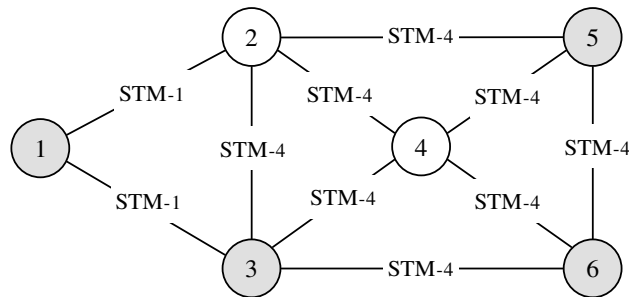


Figura 24 – Grafo do caso de estudo C

Esta rede diferencia-se do caso de estudo A por possuir duas ligações (1-2 e 1-3) que têm capacidade STM-1 enquanto no caso de estudo A têm capacidade STM-4. Esta diferença tem influência no tráfego que pode ser suportado pela rede quer com origem no nó 1 quer no tráfego originado por outros nós dado que o percurso constituído pelos nós 2 – 1 – 3 não tem a mesma capacidade de aceitação de fluxos que a restante rede.

O número médio de pedidos de circuitos por hora foi gerado aleatoriamente para todos os pares de tráfego e para todos os tipos de VC's. Para este caso de estudo, dado que a largura de banda do grafo não é homogénea, foram definidos dois grupos de intervalos para a geração com distribuição uniforme dos valores de tráfego. O primeiro grupo define as taxas de chegada para os fluxos com origem no nó 1 que tem ligações STM-1. Para este grupo assume-se que não são efectuados pedidos do tipo VC-4 porque o seu pedido e a correspondente satisfação implicaria que mais nenhum outro fluxo pudesse ser estabelecido enquanto o fluxo estivesse activo ou, no caso de se ter pedidos de um fluxo tipo VC-4 este teria um bloqueio muito elevado porque o estabelecimento de um VC-12 ou VC-3 impede a aceitação do fluxo VC-4. Por outro lado, os valores das taxas de chegada dos fluxos VC-12 e VC-3

têm de ser reduzidos (quando comparados com os fluxos com origem nos restantes nós) para que a seu bloqueio seja aceitável. O segundo grupo define as taxas de chegada para os fluxos com origem nos nós que têm ligações STM-4.

Os pedidos que têm início no nó com arestas de largura de banda STM-1 têm os seguintes intervalos: para o fluxo tipo VC-12 [0,0 – 0,9] e para o fluxo tipo VC-3 [0,0 – 0,1]. Em relação aos restantes pedidos, os valores de tráfego são gerados com distribuição uniforme com base nos intervalos: para fluxos tipo VC-12 [2,8 – 3,8], para fluxos tipo VC-3 [0,1 – 0,5] e para fluxos tipo VC-4 [0,0 – 0,05].

A esta rede é aplicado o seguinte mapa de tráfego:

Nós Extremo	Tipo de VC	λ (circuitos/hora)	$1/\mu$ (horas)	
1	3	VC-12	0.71	6
		VC-3	0.05	2
1	5	VC-12	0.55	6
		VC-3	0.08	2
1	6	VC-12	0.8	6
		VC-3	0.02	2
3	5	VC-12	3.416	6
		VC-3	0.36	2
		VC-4	0.044	1
3	6	VC-12	3.716	6
		VC-3	0.23	2
		VC-4	0.046	1
5	6	VC-12	3.094	6
		VC-3	0.49	2
5	6	VC-4	0.031	1

Tabela 3 - Mapa de Tráfego da rede do caso de estudo C

5.3. Apresentação e Discussão de Resultados

Todos os casos de estudo foram simulados com todos os algoritmos usando o simulador desenvolvido com o critério de paragem anteriormente descrito. As simulações foram executadas num PC com processador Pentium 4 a 2.8GHz e com 512Mbytes de memória Ram. Para cada algoritmo em cada caso, o simulador foi executado 10 vezes e, com os resultados obtidos, foram calculados os valores médios bem como os respectivos intervalos de confiança. Os resultados detalhados de todas as simulações são

apresentados no Anexo D. De seguida, são apresentados os resultados de simulação obtidos e a respectiva análise.

O primeiro critério de comparação dos diversos algoritmos é o tráfego médio suportado pela rede, dado pelo número médio de unidades de VC-12 aceites pela rede. A Tabela 4 apresenta a largura de banda média que não foi bloqueada por cada estratégia em cada caso de estudo (os valores são dados em unidades de VC-12).

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
A	158,97	159,33	159,36	159,42	159,43	159,47
B	191,77	191,84	191,85	192,04	192,26	192,35

Tabela 4 – Largura de Banda Média suportada pela rede por cada estratégia

A largura de banda média submetida foi de 159,50 unidades de VC-12 para o caso de estudo A e de 192,57 de unidades de VC-12 para o caso de estudo B. Os resultados da tabela anterior mostram que, quer a estratégia InvBand, quer a InvBand+PEN permitem a melhoria da largura de banda média não bloqueada pela rede para os casos de estudo A e B. A reorganização de VC's de protecção, para os melhores resultados, InvBand+PEN, aumenta a largura de banda média suportada pela rede.

Como segundo critério de comparação de resultados, para os algoritmos descritos anteriormente, a Tabela 5 apresenta a probabilidade média de bloqueio global obtida para os casos de estudo A e B.

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
A	0,843%	0,310%	0,253%	0,179%	0,146%	0,131%
B	1,467%	1,368%	1,216%	0,968%	0,650%	0,537%

Tabela 5 – Probabilidade média de bloqueio global

Os valores apresentados nesta tabela confirmam os valores da tabela anterior. Verifica-se mais uma vez que a estratégia InvBand melhora substancialmente os resultados obtidos através da estratégia InvCap. Isto é devido à variação de custos das arestas existente na estratégia InvBand que permite uma melhor distribuição do tráfego na rede.

Quando se acrescenta a estratégia de penalizações aos algoritmos InvCap e InvBand o valor das probabilidades de bloqueio decresce substancialmente

em ambos os casos de estudo e para ambos os algoritmos. Notar que a melhoria obtida para o caso A através de InvBand é menor que através de InvCap, no entanto, o valor da probabilidade média de bloqueio é menor para o algoritmo InvBand+PEN. Isto significa que o algoritmo de penalizações consegue melhorar o desempenho do algoritmo InvCap e também do algoritmo InvBand que obtém valores inferiores ao algoritmo InvCap+PEN. Para o caso B o algoritmo de penalização obtém melhores resultados para a estratégia InvBand dado que a estratégia InvCap é penalizada com o aumento de tráfego/nós de uma rede.

O algoritmo de reorganização de protecções consegue para ambos os casos de estudo a diminuição da probabilidade de bloqueio obtida através do algoritmo de penalizações. No entanto, verifica-se que a diminuição da probabilidade de bloqueio não é tão significativa como a registada do algoritmo sem penalizações para o algoritmo com a estratégia de penalizações, o que, dadas as complexidades acrescidas a este algoritmo, nomeadamente a informação a enviar para o nó central, pode não compensar o decréscimo obtido na probabilidade de bloqueio.

A Tabela 6 apresenta a probabilidade média de bloqueio de cada tipo de VC para os casos de estudo A e B. Como esperado, dado que os fluxos VC-4 e VC-3 exigem maior largura de banda, os fluxos VC-4 têm as piores probabilidades de bloqueio, de seguida, os fluxos VC-3 e os fluxos VC-12 não têm uma probabilidade de bloqueio relevante (estes resultados põem em evidência a enorme diferença em termos de probabilidade de bloqueio existente entre os fluxos VC-12 de baixa largura de banda e os restantes fluxos).

Caso de Estudo	Tipo de VC	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
A	12	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%
	3	0,097%	0,065%	0,096%	0,011%	0,014%	0,018%
	4	4,009%	1,351%	1,027%	0,702%	0,517%	0,433%
B	12	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%
	3	0,136%	0,248%	0,367%	0,072%	0,060%	0,067%
	4	5,372%	4,657%	3,936%	3,244%	1,688%	1,298%

Tabela 6 – Probabilidade média de bloqueio de cada tipo de circuito VC

Os resultados confirmam que a estratégia InvBand é melhor que a estratégia InvCap: a probabilidade média de bloqueio dos fluxos tipo VC-4 reduziu de 4,009% para 0,702% (caso de estudo A) e de 5,372% para 3,244% (caso de estudo B) e a probabilidade média de bloqueio dos fluxos tipo VC-3 foi reduzida de 0,097% para 0,011% (caso de estudo A) e de 0,136% para 0,072% (caso de estudo B). A probabilidade média de bloqueio do fluxo tipo VC-12 não sofre alteração através dos algoritmos InvCap e InvBand.

Estes resultados confirmam também que a estratégia de penalizações tem a capacidade de melhorar as probabilidades de bloqueio quando combinada com a estratégia InvCap ou InvBand. Quando aplicada à melhor estratégia (a estratégia InvBand), a estratégia de penalizações permitiu diminuir a probabilidade média de bloqueio de fluxos tipo VC-4 de 0,702% para 0,517% (caso de estudo A) e de 3,244% para 1,688% (caso de estudo B). Notar que, em todos os casos, a estratégia de penalizações consegue melhorar a probabilidade de bloqueio dos fluxos VC-4. No entanto, apenas melhora a probabilidade média de bloqueio do fluxo VC-3 para o caso B. Estes resultados não são contrários ao esperado pois, com a diminuição da probabilidade de bloqueio do fluxo VC-4, é possível a penalização da probabilidade de bloqueio dos outros fluxos.

Verifica-se que, a estratégia de reorganização de VC's de protecção, melhora a probabilidade média de bloqueio dos fluxos tipo VC-4 quer no algoritmo InvCap+PEN quer em InvBand+PEN. No caso de estudo A, as melhoras podem não ser proporcionais à complexidade do sistema, mas, no caso de estudo B para o algoritmo InvBand+PEN, passa-se de 1,688% para 1,298%, o que poderá compensar a complexidade, devido ao sistema ser centralizado. Por outro lado, a reorganização de VC's de protecção, degrada ligeiramente a probabilidade de bloqueio dos fluxos VC-3.

A Tabela 7 apresenta os intervalos de confiança obtidos pelas 10 simulações de cada caso relativas aos resultados da Tabela 6 anterior. Conforme se pode constatar, os intervalos de confiança são suficientemente pequenos para validar as conclusões retiradas dos resultados da Tabela 6.

Caso de Estudo	Tipo de VC	InvCap		InvCap +PEN		InvCap +PEN +RP		InvBand		InvBand +PEN		InvBand +PEN +RP	
A	12	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%
	3	0,0903%	0,0960%	0,0614%	0,0684%	0,0934%	0,0991%	0,0101%	0,0116%	0,0129%	0,0145%	0,0165%	0,0192%
	4	4,0214%	4,1509%	1,3103%	1,3914%	0,9808%	1,0726%	0,6794%	0,7247%	0,4976%	0,5356%	0,4103%	0,4561%
B	12	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%	0,000%
	3	0,1316%	0,1398%	0,2418%	0,2538%	0,3604%	0,3746%	0,0684%	0,0746%	0,0581%	0,0623%	0,0628%	0,0703%
	4	5,3324%	5,4125%	4,6135%	4,7009%	3,8895%	3,9829%	3,2139%	3,2732%	1,6654%	1,7107%	1,2717%	1,3251%

Tabela 7 - Intervalo de confiança da probabilidade média de bloqueio de cada tipo de circuito VC

Para cada tipo de circuito VC pode também ser observado o número médio de ligações usadas para estabelecer cada circuito de cada tipo de VC. Da Tabela 8 evidencia-se que os circuitos de maior largura de banda, para os algoritmos InvCap e InvBand, usam um maior número de ligações. Quando se aplica a estratégia de penalizações e a estratégia de reorganização de circuitos continua a verificar-se este facto. Como se verificou anteriormente, a probabilidade de bloqueio dos circuitos VC-12 é desprezável. Por outro lado, a estrutura de multiplexagem SDH implica que por cada VC-12 estabelecido possam ser estabelecidos mais 0 a 62 circuitos por cada STM-1 dependendo do estado da ligação. Assim, o estabelecimento de um circuito VC-12 através de um percurso curto obriga a que os circuitos VC-4 tenham de determinar percursos, através de outras ligações, que não são os mais curtos em número de ligações utilizadas. De notar que com a aplicação dos algoritmos de penalização e de reorganização de protecções obtém-se uma ligeira diminuição do comprimento do circuito VC-4 com o consequente aumento dos comprimentos dos circuitos VC-3 e VC-12. Esta constatação vem corroborar o funcionamento dos algoritmos que pretendem favorecer o desempenho dos pedidos de circuitos VC-4. Por outro lado, a diminuição do número de ligações usadas reflecte-se, como verificado anteriormente, no aumento da largura de banda média suportada pela rede.

Caso de Estudo	Tipo de VC	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
A	12	1,92	1,94	1,99	1,92	1,94	1,99
	3	1,92	2,10	2,11	1,92	2,06	2,09
	4	2,16	2,14	2,14	2,14	2,13	2,13
B	12	2,70	2,71	2,74	2,70	2,72	2,73
	3	2,71	2,88	2,91	2,71	2,82	2,84
	4	2,85	2,82	2,82	2,82	2,80	2,79

Tabela 8 – Número médio de ligações usadas para estabelecer cada tipo de circuito VC

Comparando os valores de pior probabilidade de bloqueio para cada algoritmo (apresentados na Tabela 9) verificam-se as conclusões já obtidas anteriormente. Para o caso de estudo A e B os melhores resultados são obtidos para o algoritmo InvBand+PEN+RP. No entanto, a diferença para o algoritmo InvBand+PEN pode não ser suficiente para se optar pelo algoritmo InvBand+PEN+RP dada a sua maior complexidade.

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
A	5,857%	1,623%	1,354%	0,989%	0,746%	0,651%
B	11,424%	9,383%	7,943%	6,371%	2,629%	1,953%

Tabela 9 – Piores valores de bloqueio para cada algoritmo

As diferentes estratégias podem também ser avaliadas através da carga média das arestas da rede. As probabilidades médias de bloqueio são principalmente impostas pelas piores cargas das arestas (as que têm uma maior probabilidade de ficarem totalmente ocupadas). As figuras 25 e 26 comparam as percentagens médias de carga por aresta para os casos de estudo A e B entre a pior (InvCap) e as duas melhores estratégias (InvBand+PEN e InvBand+PEN+RP).

Verifica-se pela análise destas figuras que para os três casos de estudo o algoritmo InvBand+PEN permite baixar a carga das arestas com piores cargas, arestas 2-5, 3-6 e 5-6 para o caso de estudo A e arestas 4-8, 5-9 e 8-9 para o caso de estudo B. As restantes cargas de aresta aumentam, resultando num melhor desempenho de probabilidade de bloqueio e de utilização da rede.

A estratégia InvBand+PEN+RP mantém esta situação sem alterações significativas para os dois casos de estudo o que reflecte a pequena variação obtida nas probabilidades de bloqueio.

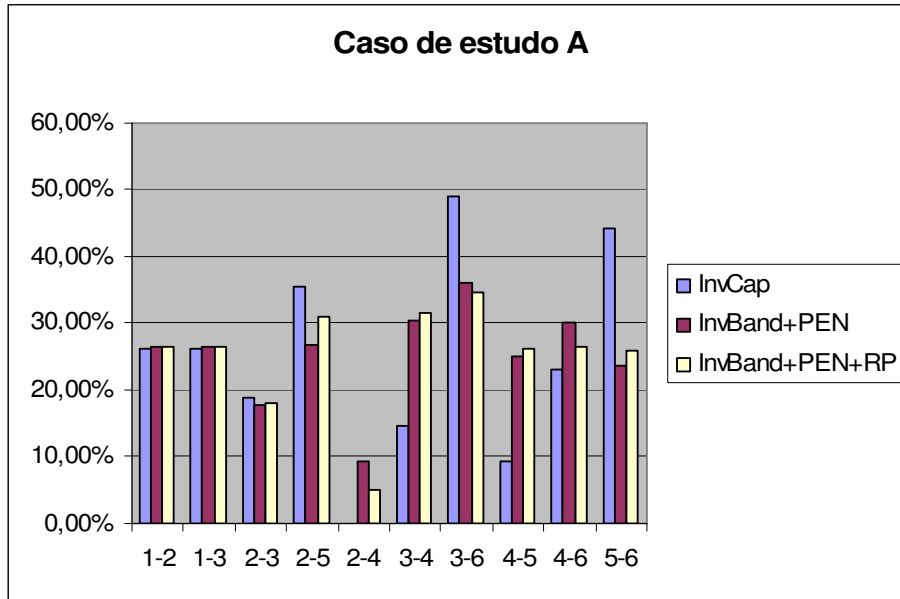


Figura 25 – Carga de cada ligação (em percentagem) do caso de estudo A para os algoritmos InvCap, InvBand+PEN e InvBand+PEN+RP

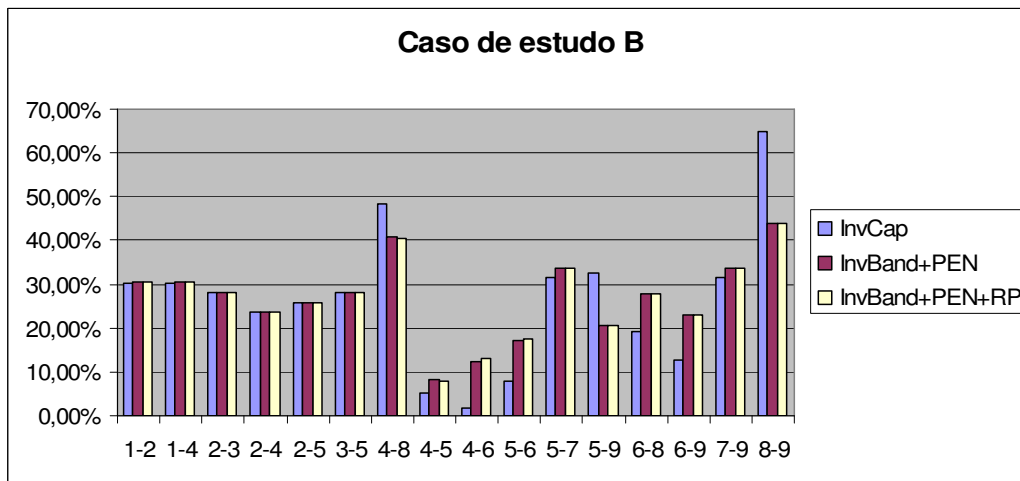


Figura 26 – Carga de cada ligação (em percentagem) do caso de estudo B para os algoritmos InvCap, InvBand+PEN e InvBand+PEN+RP

O caso de estudo C é um exemplo de uma rede incorrectamente dimensionada para o tráfego a que pretende responder. Este estudo, em conjunto com os anteriores, demonstra que os algoritmos aqui propostos obtêm os resultados esperados desde que a rede esteja correctamente dimensionada.

Observando a largura de banda suportada pela rede (Tabela 10), e ao contrário dos resultados obtidos nos casos de estudo A e B, a estratégia de

penalização não permitiu o aumento da largura de banda média suportada pela rede. Para a estratégia de reorganização de protecções existe uma pequena diminuição da largura de banda média suportada mas que é obtida à custa da penalização dos fluxos tipo VC-3 (conforme se verá na Tabela 12).

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
C	132,64	132,50	132,50	132,68	132,57	132,50

Tabela 10 – Largura de Banda Média suportada pela rede por cada estratégia para o caso de estudo C

Quanto à probabilidade média de bloqueio global (Tabela 11), verifica-se mais uma vez que, ao contrário dos casos de estudo A e B, a probabilidade média de bloqueio global aumenta quando se aplicam os algoritmos de penalização e de reorganização de protecções.

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
C	1,348%	2,169%	2,374%	1,359%	2,157%	2,475%

Tabela 11 – Probabilidade média de bloqueio global para o caso de estudo C

Através da probabilidade média de bloqueio obtida para cada tipo de VC (valores apresentados na Tabela 12) constata-se que ao contrário dos resultados obtidos para os casos de estudo A e B, o fluxo tipo VC-3 apresenta a pior probabilidade de bloqueio, o que fica a dever-se à configuração da rede: as arestas com apenas STM-1 de largura de banda e os fluxos que têm como extremo o nó 1, influenciam fortemente o valor da probabilidade média de bloqueio dos fluxos VC-3. Assim, os resultados desta tabela permitem as seguintes conclusões: (i) a estratégia InvBand é ainda assim melhor que a estratégia InvCap (melhora a probabilidade de bloqueio dos VC-4 mantendo a probabilidade de bloqueio dos VC-3) e (ii) a estratégia das penalizações conduz a um pior desempenho global dado que beneficia os fluxos VC-4 em prejuízo dos fluxos VC-3 que são os que têm à partida a pior probabilidade de bloqueio.

Caso de Estudo	Tipo de VC	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
C	12	0,001%	0,001%	0,001%	0,000%	0,001%	0,002%
	3	2,213%	3,567%	3,934%	2,213%	3,544%	4,094%
	4	0,847%	0,369%	0,203%	0,326%	0,215%	0,093%

Tabela 12 – Probabilidade média de bloqueio de cada tipo de circuito VC

Neste caso de estudo, os circuitos VC-4 têm percursos mais curtos em número de ligações usadas (ver resultados apresentados na Tabela 13), e os circuitos VC-12 percursos maiores. Esta conclusão contrária à obtida nos casos de estudo anteriores é devida ao incorrecto dimensionamento da rede. Este resultado confirma os valores de probabilidade média de bloqueio de cada tipo de circuito VC porque o circuito VC-3 obtém os piores valores de probabilidade de bloqueio e os percursos mais compridos.

Caso de Estudo	Tipo de VC	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
C	12	1,92	1,94	1,98	1,92	1,94	1,99
	3	1,92	2,08	2,10	1,92	2,07	2,09
	4	1,68	1,67	1,67	1,67	1,67	1,67

Tabela 13 – Número médio de ligações usadas para estabelecer cada tipo de circuito VC

Os valores de pior probabilidade de bloqueio evoluem de forma contrária aos casos de estudo A e B. Face aos resultados anteriores, este resultado era esperado dado que a largura de banda aceite diminui e a probabilidade média de bloqueio global aumenta para este caso de estudo.

Caso de Estudo	InvCap	InvCap +PEN	InvCap +PEN +RP	InvBand	InvBand +PEN	InvBand +PEN +RP
C	4,416%	7,136%	7,884%	4,441%	7,089%	8,195%

Tabela 14 – Piores valores de bloqueio para cada algoritmo

Por último, o parâmetro da carga de cada ligação também não obtém resultados satisfatórios (Figura 27). As ligações mais sobrecarregadas veem a sua carga diminuir, mas não na mesma percentagem que nos casos de estudo A e B. Por outro lado, esta diminuição não corresponde a uma distribuição equitativa da carga pelas ligações. Com os algoritmos de penalização e de reorganização de protecções ficam sobrecarregadas outras ligações, ou seja, não é efectuada uma distribuição uniforme da carga como nos casos de estudo A e B.

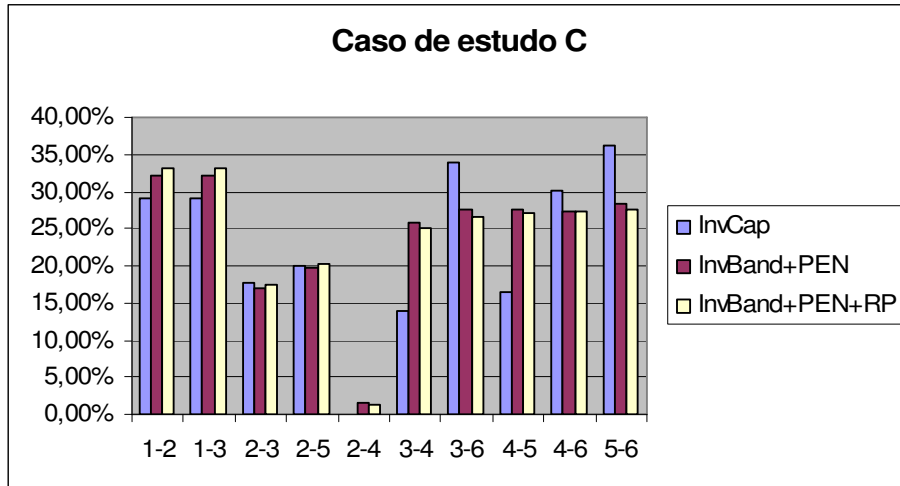


Figura 27 – Carga de cada ligação (em percentagem) do caso de estudo C para os algoritmos InvCap, InvBand+PEN e InvBand+PEN+RP

Como se constatou os resultados obtidos para o caso de estudo C não estão de acordo com os resultados obtidos para os casos de estudo A e B. Este facto é devido ao incorrecto dimensionamento da rede do caso de estudo C.

Portanto, os algoritmos apresentados conseguem atingir os objectivos propostos desde que as redes estejam correctamente dimensionadas: melhoram a probabilidade de bloqueio de circuitos que requerem elevada largura de banda e melhoram a utilização da rede. Por outro lado, não necessitam de qualquer conhecimento antecipado do tráfego a ser suportado para obterem melhores desempenhos. Finalmente, são uma solução totalmente distribuída sem qualquer necessidade de um sistema de gestão centralizado, excepto para o caso específico da reorganização de protecções.

Pode-se evidenciar o algoritmo InvBand+PEN como o que melhores resultados obteve, uma vez que apesar do algoritmo InvBand+PEN+RP ter obtido melhores resultados para algumas situações, a melhoria pode não ser significativa quando comparada com a maior complexidade deste algoritmo.

Capítulo 6 – Considerações Finais

Neste capítulo são apresentadas as principais conclusões resultantes do trabalho efectuado e são apontados tópicos considerados importantes para trabalho futuro.

6.1. Conclusões

A presente dissertação teve como principais objectivos a proposta/concepção e avaliação de desempenho de algoritmos de encaminhamento robusto de custo mínimo no âmbito de redes GMPLS (*Generalized MultiProtocol Label Switching*) sobre a tecnologia SDH (*Synchronous Digital Hierarchy*).

O problema estudado considerou a perspectiva de uma rede SDH em malha com ligações de capacidade STM-1 ou STM-4 entre os nós e com pedidos de tributários do tipo E-1, E-3 e E-4. Foi estudada a forma como a norma GMPLS permite efectuar a gestão distribuída da rede SDH.

Por algoritmo de encaminhamento robusto de custo mínimo, entendeu-se um algoritmo de custo mínimo que determina um par de percursos disjuntos em nós para cada pedido de circuito. Um percurso é o conjunto de nós e ligações que suportam o circuito virtual de serviço e o outro o conjunto de nós e

ligações que suportam o circuito virtual de protecção. A observação da estrutura de multiplexagem SDH permitiu propor algoritmos robustos de custo mínimo baseados na carga das arestas e no número e tipo de VC's estabelecidos em cada momento. Os algoritmos desenvolvidos pretendem otimizar o desempenho da rede e garantir tolerância a falhas individuais em arestas ou nós.

Os algoritmos robustos de custo mínimo propostos podem ser divididos em três grupos: algoritmos robustos de custo mínimo com função de custo simples, algoritmos robustos de custo mínimo baseados na estrutura de multiplexagem SDH e algoritmos robustos de custo mínimo com reorganização de caminhos de protecção.

Os algoritmos robustos de custo mínimo, com função de custo simples, têm como função de custo para cada aresta o inverso da capacidade total da aresta (InvCap) e o inverso da capacidade livre da aresta (InvBand). Estes algoritmos servem basicamente de termo de comparação para se verificar a evolução dos restantes.

Dada a estrutura de multiplexagem SDH verifica-se que a aceitação de um tributário E-1 pode, por exemplo, inibir a aceitação de um tributário E-3 ou E-4. Os algoritmos robustos de custo mínimo com função de custo baseada na estrutura de multiplexagem SDH adoptam uma estratégia de penalizações, na função de custo, que penaliza a aceitação de tributários de menor capacidade quando a sua aceitação impede a aceitação de tributários de maior capacidade (InvCap+PEN e InvBand+PEN). A estratégia de penalizações pretende garantir uma menor desigualdade de acesso, aos recursos existentes na rede, por parte dos diferentes tipos de VC's.

A última abordagem assenta nos algoritmos anteriores, acrescentando a estratégia de reorganização de protecções (InvCap+PEN+RP e InvBand+PEN+RP). Dada a estrutura de multiplexagem SDH verifica-se que, numa aresta, pode existir um total de capacidade livre suficiente para aceitar determinado tributário, mas dado que a capacidade livre está distribuída por diferentes TUG-3 da estrutura de multiplexagem, a aceitação do tributário não é possível. A estratégia de reorganização de protecções tenta contrair este

facto reorganizando os VC's de protecção o que potencia o aparecimento de "buracos de capacidade" contíguos de maior tamanho e conseqüentemente a aceitação de um maior número de tributários de maior capacidade.

Todos os algoritmos são distribuídos, apenas a estratégia de reorganização de caminhos de protecção é centralizada. A informação que serve de base ao cálculo dos caminhos (custo das arestas) é trocada entre os nós GMPLS/SDH através dos protocolos de encaminhamento OSPF-TE ou IS-IS-TE, por exemplo. O RSVP-TE ou CR-LDP são usados para o estabelecimento dos VC's de serviço e de protecção (LSP's).

Para o caso da estratégia de reorganização de caminhos de protecção, é necessário o desenvolvimento de um protocolo específico para a troca de informação entre os nós e o nó central. O nó central tem de ter conhecimento topológico da rede, das posições ocupadas na estrutura de multiplexagem SDH e dos respectivos fluxos que a ocupam.

Os algoritmos foram avaliados através de um simulador desenvolvido para o efeito em C++. Através dos casos de estudo simulados, constatou-se que os algoritmos que obtêm melhores resultados para os critérios de desempenho definidos (probabilidade média de bloqueio de cada tipo de fluxo; ocupação média das arestas; probabilidade de bloqueio do fluxo com pior probabilidade de bloqueio; probabilidade média de bloqueio do simulador) são os InvBand+PEN e InvBand+PEN+RP.

A estratégia de penalizações consegue diminuir bastante as probabilidades de bloqueio média e de pior caso dos casos de estudo A e B. A probabilidade de bloqueio dos fluxos VC-4 obtêm também uma redução mas à custa de um agravamento da probabilidade de bloqueio dos fluxos VC-3. A probabilidade de bloqueio dos fluxos VC-12 mantém-se desprezável.

Para InvBand+PEN+RP a probabilidade média de bloqueio do VC de maior largura de banda (VC-4) melhora quando comparada com os melhores resultados obtidos para InvBand+PEN. No entanto, como o sistema é centralizado, envolve uma maior complexidade para o funcionamento da rede. É necessário ter ganhos consideráveis para compensar a complexidade necessária à implementação deste tipo de sistema. Dependendo do objectivo

do operador da rede, a complexidade do sistema pode ser compensada pela diminuição da probabilidade média de bloqueio dos fluxos VC-4.

De notar que, apesar do trabalho ter sido desenvolvido para os tributários E-1, E-3 e E-4 (os usados na Europa), as estratégias são facilmente adaptadas para um esquema em que se tenha de usar toda a granularidade da estrutura de multiplexagem SDH. Nesse caso, como o menor tributário é o T-1 ao que corresponde o circuito virtual VC-11, as funções de custo seriam alteradas de modo a que um STM-1 fosse representado por 84 VC-11.

6.2. Trabalho Futuro

O algoritmo InvBand+PEN+RP obtém resultados que não permitem concluir se a sua aplicação será compensatória nas redes reais. Observando os diferentes casos de estudo, poder-se-á dizer que este tipo de estratégia está ligada a redes de maior tamanho. Quanto maior for a rede mais caminhos existem entre o nó-origem e o nó-destino, possibilitando tirar maior rendimento da estratégia de reorganização de protecções. Esta linha de raciocínio poderá ser verificada em futuros trabalhos.

Um outro tópico de investigação é o estudo de como um esquema de reserva de recursos pode ser combinado com os algoritmos propostos de modo a melhorar as probabilidades de bloqueio dos circuitos de elevada largura de banda. No entanto, esta abordagem tem os seus próprios custos. Primeiro, requer um sistema centralizado para calcular a quantidade correcta de recursos a reservar em cada aresta para cada tipo de VC e para configurar os valores em cada LSR. Segundo, a reserva de recursos irá necessariamente reduzir a utilização de rede dado que quando alguns recursos de transmissão estão reservados para alguns fluxos de tráfego, a utilização total da rede é sempre diminuída.

Neste trabalho a relação entre os termos de penalização das funções de custo não foi trabalhada. Os termos de penalização são somados com peso unitário. Uma outra abordagem seria estudar formas de dar pesos diferentes, através de constantes, aos termos de penalização. Os pesos diferentes

permitiriam criar um esquema de penalizações com o objectivo de melhorar a probabilidade de bloqueio dos fluxos tipo VC-4 e fluxos tipo VC-3.

Para a reorganização de protecções foi definido que o algoritmo era executado no momento do evento-partida, no entanto, a execução do algoritmo no momento em que se estabelece um circuito ou em ambos os momentos não foi testada. Como trabalho futuro poder-se-ia verificar ambos os casos, por um lado, efectuar a reorganização de protecções quando se estabelece um circuito e por outro, efectuar a reorganização de protecções quando se estabelece um circuito e quando ocorre o evento partida. Esta última abordagem exige mais poder de processamento o que terá de ser contraposto por uma significativa melhoria dos resultados.

A concatenação SDH não foi abordada neste trabalho; no entanto, decorre alguma investigação que permite oferecer serviços baseados em concatenação SDH, nomeadamente, permitem que o cliente possa ter tributários de valores diferentes dos pré-estabelecidos. Seria interessante a aplicação dos algoritmos anteriores à concatenação SDH para verificar se se confirmam os resultados agora obtidos.

Referências

- [1] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", IETF RFC3945, Outubro de 2004
- [2] G.Bernstein, E.Mannie, V. Sharma, E. Gray, "Framework for Generalized Multi-Protocol Label Switching (GMPLS) – based Control of Synchronous Digital Hierarchy/ Synchronous Optical Networking (SDH/SONET) Networks", IETF RFC 4257, Dezembro 2005
- [3] E. Rosen, A. Viswanathan and R. Callon., "Multi-Protocol Label Switching Architecture", RFC 3031, IETF, Jan. 2001
- [4] G.707, "Network Node Interface for the Synchronous Digital Hierarchy (SDH)", ITU-T, Março 1996
- [5] Berger, L. (Editor), "Generalized MPLS – Signaling Functional Description", RFC 3471, Janeiro 2003
- [6] Mannie, E., Ed. And Papadimitriou D., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Extensions for Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) Control", RFC 3946, Outubro 2004
- [7] Lai,W. and D.McDysan, "Network Hierarchy and Multilayer Survivability", RFC 3386, Novembro 2002
- [8] Sharma, V., F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS) – based Recovery", RFC 3469, Fevereiro 2003
- [9] Lang, J.P., Ed., B. Rajagopalan, Ed., D. Papadimitriou, "Generalized MPLS Recovery Functional Specification", RFC 4426, Março 2006
- [10] D. Katz, K. Kompella, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC3630, Setembro 2003

- [11] H. Smit, T. Li, "Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)", RFC3784, Junho 2004
- [12] K. Kompella, Y. Rekhter, "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC4202, Outubro 2005
- [13] K. Kompella, Y. Rekhter, "Link Bundling in MPLS Traffic Engineering (TE)", RFC4201, Outubro 2005
- [14] D. Awduche, L. Berger, D. Gan e outros, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC3209, Dezembro 2001
- [15] B. Jamoussi, L. Andersson, R. Callon e outros, "Constraint-Based LSP Setup using LDP", RFC3212, Janeiro 2002
- [16] Elizabeth Fernandez, Rui Valadas, "Demonstrador Animado das Técnicas de Programação de Simuladores de Eventos Discretos, utilizando o MATLAB", Revista do DETUA, Vol. 2, Nº 3, Setembro 1998
- [17] Amaro F. de Sousa, "Algoritmos Eficientes para Problemas de Grafos", Apontamentos da disciplina de Sistemas de Telecomunicações, DET - UA, Setembro 2006
- [18] J.P. Vasseur, M. Pickavet e Piet Demeester, "Network Recovery, Protection and Restoration of Optical, Sonet/SDH, IP, and MPLS", Morgan Kaufman Publishers, 2004

Bibliografia

- Hui Zang, "WDM Mesh Networks: Management and Survivability", Kluwer Academic Publishers, 2003
- Hussein T. Mouftah, Pin-Han Ho, "Optical Networks: Architecture and Survivability", Kluwer Academic Publishers, 2002
- Rao Lingampalli et al, "Performance of Protection and Restoration in IP/Optical Core Networks with GMPLS Protocols", Calient Networks, 2002.
- Jonathan P. Lang, John Drake, "Mesh Network Resiliency Using GMPLS", Proceedings of the IEEE, Vol. 90, No. 9, pp. 1559-1564, Setembro 2002.
- Lei Lei, et al, "A Joint Resilience Scheme with Interlayer Backup Resource Sharing in IP over WDM Networks", IEEE Communications Magazine, Janeiro 2004.
- S. Ramamurthy, et al, "Survivable WDM Mesh Networks", Journal of Lightwave Technology, Vol. 21, No. 4, Abril 2003
- Jong T. Park, "Resilience in GMPLS Path Management: Model and Mechanism", IEEE Communications Magazine, Julho 2004
- Jing Zhang and Biswanath Mukherjee, "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges", IEEE Network, Março 2004
- Berger, L. (Editor), "Generalized MPLS Signaling RSVP-TE Extensions", RFC 3473, Janeiro 2003
- Ramesh Bhandari, "Survivable Networks: Algorithms for Diverse Routing", pág. 86 a 91, Kluwer Academic Publishers, 1998
- J. Lang, "Link Management Protocol (LMP)", RFC4204, Outubro 2005
- K. Kompella, Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC4203, Outubro 2005

Harry G. Perros, "Connection-Oriented Networks : SONET/SDH, ATM, MPLS and Optical Networks", Wiley, Fevereiro 2005

H. M. Deitel, P. J. Deitel, C++ How to Program, Pearson Education, 4^a Ed., 2003

Acrónimos

ADM	<i>Add Drop Multiplex</i>
AIS	<i>Alarm Indicating Signal</i>
ANSI	<i>American National Standards Institute</i>
ATM	<i>Asynchronous Transfer Mode</i>
AU	<i>Administrative Unit</i>
BGP	<i>Border Gateway Protocol</i>
CoS	<i>Class of Service</i>
CR-LDP	<i>Constraint Routing Label Distribution Protocol</i>
CR-LSP	<i>Constraint Routing Label Switch Path</i>
DWDM	<i>Dense Wavelength Division Multiplexing</i>
E1	<i>Ligação a 2 Mbps da hierarquia PDH europeia</i>
E3	<i>Ligação a 34 Mbps da hierarquia PDH europeia</i>
E4	<i>Ligação a 139 Mbps da hierarquia PDH europeia</i>
ETSI	<i>European Telecommunications Standards Institute</i>
FEC	<i>Forward Error Correction</i>
FSC	<i>Fiber Switch Capable</i>
GMPLS	<i>Generalised Multi-Protocol Label Switching</i>
IGP	<i>Interior Gateway Protocol</i>
IP	<i>Internet Protocol</i>

IS-IS-TE	<i>Intermediate System - Intermediate System - Traffic Engineering</i>
ITU-T	<i>International Telecommunications Union Telecommunication Standardization Sector</i>
L2SC	<i>Layer-2 Switch Capable</i>
LAN	<i>Local Area Network</i>
LDP	<i>Label Distribution Protocol</i>
LER	<i>Label Edge Router</i>
LMP	<i>Link Management Protocol</i>
LOL	<i>Loss of Light</i>
LSA	<i>Link State Advertisement</i>
LSC	<i>Lambda Switch Capable</i>
LSP	<i>Label Switched Path</i>
LSR	<i>Label Switching Router</i>
MAN	<i>Metropolitan Area Network</i>
MPLS	<i>Multi-Protocol Labelling Switching</i>
MSOH	<i>Multiplex Section Overhead</i>
OSI	<i>Open Systems Interconnection</i>
OSPF	<i>Open Shortest Path First</i>
OSPF-TE	<i>Open Shortest Path First Traffic Engineering</i>
PDH	<i>Plesiochronous Digital Hierarchy</i>
POH	<i>Path Overhead</i>
PR	<i>Protecção e Restauo</i>
PSC	<i>Packet Switch Capable</i>
RSOH	<i>Regenerator Section Overhead</i>
QoS	<i>Qualidade de Serviço</i>
RSVP	<i>Resource Reservation Protocol</i>
RSVP-TE	<i>Resource Reservation Protocol Traffic Engineering</i>
SDH	<i>Synchronous Digital Hierarchy</i>
SOH	<i>Section Overhead</i>
SONET	<i>Synchronous Optical Networking</i>

STM	<i>Synchronous Transport Module</i>
STM-1	<i>Ligação a 155 Mbps da hierarquia SDH</i>
STM-4	<i>Ligação a 622 Mbps da hierarquia SDH</i>
TDM	<i>Time Division Multiplexing</i>
TE	<i>Traffic Engineering</i>
TLV	<i>Type-Length-Value</i>
TM	<i>Terminal Multiplexer</i>
TTL	<i>Time To Live</i>
TU	<i>Tributary Unit</i>
TUG	<i>Tributary Unit Group</i>
VC	<i>Virtual Container</i>
VCI	<i>Virtual Channel Identifier</i>
VPI	<i>Virtual Path Identifier</i>
WAN	<i>Wide Area Network</i>
WDM	<i>Wavelength Division Multiplex</i>

Anexos

Anexo A – Algoritmo de Dijkstra [17]

Dado um grafo $G = (N, A)$, onde N é o conjunto de nós e A o conjunto das arestas do grafo, e dado um custo $l(i,j)$ atribuído a cada aresta $\{i,j\} \in A$, o algoritmo Dijkstra determina um caminho de menor custo de um dado nó origem o para um dado nó destino d . Considere-se as seguintes variáveis

$c(i)$ – custo do percurso de custo mínimo do nó origem s até ao nó i ($c(s) = 0$)

$p(i)$ – nó predecessor do nó i no percurso de custo mínimo do nó origem s até ao nó i

S – um subconjunto dos nós da rede ($S \subset N$)

O algoritmo Dijkstra pode ser descrito da seguinte forma:

```

1   $S = \{s\}$ 
2   $c(s) = 0$ 
3   $p(s) = \text{NULL}$ 
4  for  $i \in N \setminus \{s\}$  do:
5       $c(i) = +\infty$ 
6       $p(i) = \text{NULL}$ 
7  while  $t \notin S$  do:
8      escolher  $i \in N \setminus S$  tal que  $c(i) = \min_{j \in N \setminus S} c(j)$ 
9       $S = S \cup \{i\}$ 
10     for  $(i,j) \in A$  tal que  $j \notin S$  do:
11         if  $c(j) > c(i) + l(i,j)$  do:
12              $c(j) = c(i) + l(i,j)$ 
13              $p(j) = i$ 

```

O conjunto S contém os nós i para os quais foi encontrado um percurso de custo mínimo do nó origem s até i . No início este conjunto está vazio (passo 1) e o algoritmo termina quando este conjunto inclui o nó destino t (passo 7). As variáveis $p(i)$ são inicializadas a NULL (passos 3 a 6) dado que ainda não foi determinado nenhum predecessor e as variáveis $c(i)$ são inicializadas a $+\infty$ (passo 5) dado que ainda não foram determinados os custos dos percursos de custo mínimo do nó origem s para qualquer outro nó i .

Em cada uma das iterações do ciclo *while* (passos 7 a 13): primeiro escolhe-se o nó i (dos que ainda não pertencem a S) cujo $c(i)$ é o menor de todos (passo 8), depois acrescenta-se o nó i ao conjunto S (passo 9) e depois actualizam-se os custos e os predecessores de todos os outros nós j que ainda não pertencem a S (passos 10 a 13). Esta actualização é feita do seguinte modo: para cada arco (i,j) em que o i é o nó escolhido na iteração actual e j é um nó que ainda não pertence a S (passo 10), se o custo actual do nó j for maior que o custo do nó i mais o custo do arco (i,j) (passo 11), então o custo do nó j é actualizado com o valor do custo do nó i mais o custo do arco (i,j) (passo 12) e o predecessor do nó j é actualizado com o nó i (passo 13).

No fim do algoritmo, a variável $c(t)$ indica o custo do percurso encontrado e o conteúdo das variáveis dos predecessores $p(i)$ permitem reconstruir o percurso completo.

Dado apenas o nó origem s , o algoritmo de Dijkstra permite também determinar um percurso de custo mínimo deste nó para cada um dos outros nós da rede. Para isso, basta que se garanta que o algoritmo é executado até o conjunto S conter todos os nós da rede, ou seja, basta substituir o passo 7 anterior por:

while $|S| < |N|$ **do:**

No fim do algoritmo, as variáveis $c(i)$ indicam os custos dos percursos encontrados para cada nó i e o conteúdo das variáveis dos predecessores $p(i)$ permitem reconstruir os percursos do nó origem s para cada um dos nós destino i . Nesta variante, o algoritmo executa exactamente $|N|$ iterações.

Anexo B – Algoritmo de Suurballe's [17]

Considere-se o conjunto N dos nós da rede. Considere-se que estes nós estão ligados por ligações ponto-a-ponto. Uma ligação entre o nó $i \in N$ e o nó $j \in N$ é representada pelo par não ordenado $\{i,j\}$ ou, em alternativa, por dois pares ordenados: o arco (i,j) que representa a ligação $\{i,j\}$ no sentido de i para j e o arco (j,i) que representa a ligação $\{i,j\}$ no sentido de j para i . Considere então o grafo $G = (N,A)$ em que N é o conjunto dos nós da rede e A é o conjunto dos arcos da rede. A cada arco (i,j) é associado um custo w_{ij} . Considere-se no grafo G , o nó origem $s \in N$ e o nó destino $t \in N$. Pretende-se determinar dois percursos disjuntos, ambos com origem em s e destino em t , tal que a soma dos seus custos seja mínima.

Dois percursos são disjuntos nos nós se não passarem por nós comuns excepto os nós origem e destino (note-se que dois percursos disjuntos nos nós são também disjuntos nas ligações).

O algoritmo de Suurballe's que determina o par de percursos de custo mínimo disjuntos nos nós é dado por:

- 1 Determinar o conjunto M_1 de arcos que constitui um percurso de custo mínimo do nó origem s para o nó destino t .
- 2 Determinar os custos c_i dos percursos de custo mínimo do nó origem s para cada um dos outros nós i .
- 3 Determinar um novo conjunto de custos w'_{ij} para cada arco $(i,j) \in A$ de acordo com a seguinte transformação:

$$w'_{ij} = \begin{cases} +\infty & , \text{ se } (i,j) \in M_1 \\ w_{ij} + c_i - c_j & , \text{ se } (i,j) \notin M_1 \text{ e } (j,i) \notin M_1 \\ 0 & , \text{ se } (j,i) \in M_1 \end{cases}$$

- 4 Determinar um novo grafo $G' = (N',A')$ com as seguintes regras:
 - i) considerar um segundo nó (designado por nó duplicado) para cada nó intermédio do percurso definido por M_1 e considerar o conjunto N' constituído por todos os nós de N mais todos os nós duplicados
 - ii) para cada arco (i,j) do grafo original cujo custo $w'_{ij} \neq +\infty$, fazer corresponder no grafo G' com o mesmo custo w'_{ij} o arco $(i,d[i])$ se (j,i) pertencer a M_1 ou o arco $(d[i],j)$ se (j,i) não pertencer a M_1 ($d[i]$ designa o nó duplicado de i se este nó tiver sido duplicado ou o próprio nó i se este nó não tiver sido duplicado)
 - iii) acrescentar ao grafo G' os arcos $(d[i],i)$ com custo 0

- 5 Determinar o conjunto M'_2 de arcos que constitui um percurso de custo mínimo do nó origem s para o nó destino t no grafo G' .
- 6 Determinar M_2 fazendo a correspondência inversa de cada arco de M'_2 no grafo original.
- 7 Determinar o conjunto $M = M_1 \cup M_2$.
- 8 Retirar do conjunto M o conjunto de todos os pares de arcos que representam a mesma ligação, e.g., que tenham os mesmos nós extremo.

No fim do algoritmo, o conjunto M contém os arcos de um par de percursos de menor custo disjuntos nos nós. Nos passos 1 e 2 é executado um algoritmo de percursos de custo mínimo seguido de uma transformação dos custos (passo 3). No passo 4, aplica-se uma técnica de duplicação de nós aos nós intermédios do percurso de custo mínimo determinado anteriormente e o segundo percurso de custo mínimo é determinado no grafo resultante G' (passo 5). No passo 6, determina-se no grafo original G o percurso correspondente ao segundo percurso de custo mínimo. Nos passos 7 e 8 é realizado um processamento final para a determinação dos dois percursos finais com base nos percursos de custo mínimo determinados anteriormente.

Anexo C – Ficheiros de Entrada e Saída do Simulador

Os parâmetros de entrada do simulador são passados ao simulador na forma de ficheiros de texto. As medidas de desempenho obtidas pelo simulador são apresentadas pelo simulador através de um relatório na forma de ficheiro de texto.

Os parâmetros de entrada são passados ao simulador através de dois ficheiros, um que descreve a rede sobre a qual o simulador vai operar e o outro que descreve os pedidos a simular.

No ficheiro que descreve a rede (*rede.txt*) cada linha indica a aresta e a capacidade da mesma em número de STM's.

No ficheiro de pedidos (*pedidos.txt*) cada linha diz respeito a um par de nós extremo tendo a seguinte informação separada por espaços: um nó extremo, outro nó extremo, capacidade requerida (tipo de VC pretendido), taxa de chegadas (em chamadas por hora) e taxa de serviço (em horas).

Os resultados obtidos através de simulação são colocados num ficheiro de texto cujo nome é dado pela data e hora justapostas à palavra resultados. Os resultados são obtidos para 10 corridas. As corridas são executadas automaticamente. No ficheiro de resultados tem-se: a descrição do grafo, os pedidos, e por cada simulador o bloqueio médio de cada VC, a probabilidade de pico estimada por fluxo, a probabilidade média estimada do algoritmo, o tráfego suportado pela rede, o tempo simulado e o tempo de simulação por cada corrida.

De seguida é apresentado um exemplo dos ficheiros dos parâmetros de entrada e dos resultados.

O ficheiro de entrada, *rede.txt*, com a descrição da rede tem a seguinte apresentação:

No1	No2	Aresta (STM) #
1	2	1
1	3	1
2	3	4
2	4	4
3	4	4

Figura 28 – Conteúdo do ficheiro *rede.txt*

A primeira linha é considerada pelo simulador como um comentário não sendo interpretada. Cada uma das linhas seguintes representa uma aresta do grafo. Os dois primeiros valores representam os nós extremo de uma aresta e o terceiro valor a largura de banda da aresta em STM's (1 para STM-1 e 4 para STM-4).

O segundo ficheiro de entrada é *pedidos.txt* que descreve os pedidos de fluxos sobre a rede.

Origem	Destino	Container	Lambda	Inv_Niu	#
1	3	12	1.1	6	
1	3	3	0.08	2	
1	2	12	0.9	6	
1	2	3	0.1	2	
4	3	12	3.71	6	
4	3	3	0.15	2	
4	3	4	0.02	1	
4	2	12	3.91	6	
4	2	3	0.21	2	
4	2	4	0.021	1	

Figura 29 – Conteúdo do ficheiro *pedidos.txt*

A primeira linha é interpretada pelo simulador como um comentário. As linhas seguintes descrevem cada um dos fluxos. O primeiro valor é um nó extremo, o segundo o outro nó extremo, o terceiro valor indica o tipo de VC requisitado (12 para VC-12, 3 para VC-3 e 4 para VC-4), o quarto representa a taxa de chegadas e o quinto a taxa de serviço.

O terceiro ficheiro apresenta os resultados obtidos após a simulação. Aqui são apenas apresentados os resultados para o algoritmo InvCap, para os restantes seria apresentado o mesmo tipo de informação.

```

SedGraf 2.0
Critério de Paragem 50000

Grafo
1 2 1
1 3 1
2 3 4
2 5 4
2 4 4
3 4 4
3 6 4
4 5 4
4 6 4
5 6 4

Pedidos
1 3 12 0.71 6
1 3 3 0.05 2
1 5 12 0.55 6
1 5 3 0.08 2
1 6 12 0.8 6
1 6 3 0.02 2
3 5 12 3.416 6
3 5 3 0.36 2
3 5 4 0.044 1
3 6 12 3.716 6
3 6 3 0.23 2
3 6 4 0.046 1
5 6 12 3.094 6
5 6 3 0.49 2
5 6 4 0.031 1

InvCap

Prob media de bloqueio global
0.0120505 0.013508 0.0149656

Tráfego médio suportado pela rede
132.603 132.617 132.632

Prob média de bloqueio dos VC12 - N. médio de links usados pelos VC12
7.39704e-006 7.58209e-006 7.76715e-006 - 1.91667 1.91667 1.91667

Prob média de bloqueio dos VC3 - N. médio de links usados pelos VC3
0.0220558 0.0221752 0.0222947 - 1.91705 1.91706 1.91706

Prob média de bloqueio dos VC4- N. médio de links usados pelos VC4
0.00829136 0.00834367 0.00839599 - 1.67998 1.68008 1.68017

Probabilidade de bloqueio por fluxo N. médio de links usados pelo fluxo
1 3 0.71 6 1 0.000154438 0.000160468 0.000166497 - 1.5 1.5 1.5
1 3 0.05 2 21 0.0438754 0.0441115 0.0443476 - 1.5 1.5 1.50001
1 5 0.55 6 1 0.000156987 0.000161807 0.000166628 - 2.5 2.5 2.5
1 5 0.08 2 21 0.0441152 0.0442867 0.0444581 - 2.5 2.5 2.5
1 6 0.8 6 1 0.000150005 0.000155373 0.000160741 - 2.5 2.5 2.5
1 6 0.02 2 21 0.0437811 0.044278 0.0447749 - 2.50027 2.50029 2.50031
3 5 3.416 6 1 0 0 0 2 2 2
3 5 0.36 2 21 2.40376e-005 2.57814e-005 2.75252e-005 - 2 2 2
3 5 0.044 1 63 0.00182724 0.00190074 0.00197424 - 2 2 2
3 6 3.716 6 1 0 1.08233e-008 2.6927e-008 - 1.5 1.5 1.5
3 6 0.23 2 21 0.000166122 0.000175036 0.000183949 - 1.50079 1.5008 1.50082
3 6 0.046 1 63 0.0114116 0.0115543 0.011697 - 1.51367 1.51383 1.514
5 6 3.094 6 1 0 1.30179e-008 3.23869e-008 - 1.5 1.5 1.5
5 6 0.49 2 21 0.000168558 0.000174358 0.000180158 - 1.50121 1.50123 1.50125
5 6 0.031 1 63 0.0114554 0.011576 0.0116966 - 1.52615 1.52639 1.52663

Ocupacao Média por link
1 2 1 2 63 29.1693% 18.3693 18.3767 18.384
1 3 1 3 63 29.1693% 18.3693 18.3767 18.384
2 3 2 3 252 17.7554% 44.7278 44.7435 44.7592
2 5 2 5 252 20.0751% 50.5721 50.5892 50.6064
2 4 2 4 252 0.000379097% 0.000894087 0.000955323 0.00101656
3 4 3 4 252 13.8831% 34.9746 34.9854 34.9962
3 6 3 6 252 33.8075% 85.1826 85.1949 85.2072
4 5 4 5 252 16.3595% 41.2163 41.226 41.2357
4 6 4 6 252 30.0898% 75.8119 75.8263 75.8407
5 6 5 6 252 36.2611% 91.3609 91.3779 91.3949

TSimulado(horas) TSimulacao(segundos)
2.48221e+006 2407.36
2.50528e+006 2815.82
2.49949e+006 2450.12
2.49854e+006 2224.11
2.47355e+006 2230.1

```

2.51927e+006	2272.31
2.48641e+006	2246.72
2.50393e+006	2254.25
2.51925e+006	2445.91
2.50614e+006	2452.88

Figura 30 – Conteúdo do ficheiro de resultados para o algoritmo InvCap

A primeira linha indica a versão do simulador em uso. De seguida é indicado o número de chegadas usado para o critério de paragem de simulador, este valor e o número de corridas (dez corridas para as simulações efectuadas) são introduzidos como parâmetros na linha de comandos quando se executa o simulador. O bloco de informação constituído por *Grafo* e *Pedidos* descreve o grafo da rede e os fluxos a simular (é igual ao conteúdo dos ficheiros de entrada), de seguida são apresentados os resultados afectos ao algoritmo *InvCap*. Os primeiros resultados apresentam a probabilidade de bloqueio média global e o intervalo de confiança obtido, depois o tráfego médio suportado pela rede e de seguida as probabilidades de bloqueio médias para cada tipo de circuito estabelecido assim como o número médio de ligações usadas para o seu estabelecimento. O segundo grupo de resultados apresentam a probabilidade média de bloqueio por fluxo e o número médio de ligações usadas no estabelecimento de cada circuito do fluxo. Assim, tem-se para a primeira linha o fluxo com nó extremo 1 e nó extremo 3, uma taxa de chegadas de 0,71 e uma taxa de serviço de 1/6 para um VC de tipo VC-12. Notar que o tipo de VC é dado em unidades de VC-12. Os três valores seguintes representam o extremo inferior do intervalo de confiança, a probabilidade média de bloqueio do fluxo e o extremo superior do intervalo de confiança. Os últimos três valores representam o número médio de arestas utilizado por cada VC estabelecido e o respectivo intervalo de confiança.

O bloco de informação seguinte apresenta a ocupação média das arestas. É descrita a aresta, os nós extremo, a largura de banda em número de VC-12 e é apresentada a ocupação média da aresta e o respectivo intervalo de confiança. A ocupação média é também dada em percentagem.

O último bloco descreve o tempo simulado (em horas) e o tempo de simulação (em segundos) por cada corrida do simulador.

Os intervalos de confiança são obtidos a 90%.

Anexo D – Resultados de Simulação dos Casos de Estudo

Caso de Estudo A

InvCap

Prob media de bloqueio global
0.00735814 0.00842961 0.00950108

Tráfego médio suportado pela rede
158.908 159.047 159.186

Prob média de bloqueio dos VC12				N. médio de links usados pelos VC12								
0	2.70621e-008	5.67509e-008	-	1.91667	1.91667	1.91667	-					
Prob média de bloqueio dos VC3				N. médio de links usados pelos VC3								
0.000903517	0.000931775	0.000960033	-	1.91855	1.91861	1.91866	-					
Prob média de bloqueio dos VC4				N. médio de links usados pelos VC4								
0.0402148	0.0408622	0.0415097	-	2.15712	2.15779	2.15845	-					
Probabilidade de bloqueio por fluxo												
1	3	1.4	6	1	0	7.81574e-007	1.94445e-006	-	1.5	1.5	1.5	1.5
1	3	0.08	2	21	1.10375e-007	1.36633e-005	2.72162e-005	-	1.5	1.5	1.5	1.5
1	5	2.2	6	1	0	2.48787e-007	6.18948e-007	-	2.5	2.5	2.5	2.5
1	5	0.2	2	21	0.000302089	0.000360706	0.000419322	-	2.50019	2.50021	2.50024	2.50024
1	5	0.03	1	63	0.0224475	0.0233593	0.0242711	-	2.5004	2.50049	2.50058	2.50058
1	6	3	6	1	2.94105e-009	3.63808e-007	7.24675e-007	-	2.50001	2.50001	2.50001	2.50001
1	6	0.272	2	21	0.00152528	0.001592	0.00165872	-	2.50325	2.50335	2.50345	2.50345
1	6	0.02	1	63	0.0567308	0.0585701	0.0604093	-	2.54244	2.54379	2.54515	2.54515
3	5	4.6	6	1	0	0	0	-	2	2	2	2
3	5	0.12	2	21	0.000364675	0.000399024	0.000433373	-	2	2	2	2
3	5	0.04	1	63	0.0222188	0.0231513	0.0240837	-	2	2.00001	2.00002	2.00002
3	6	4.2	6	1	0	1.29302e-007	3.21686e-007	-	1.50001	1.50002	1.50003	1.50003
3	6	0.168	2	21	0.00152455	0.00163474	0.00174493	-	1.50653	1.5067	1.50688	1.50688
3	6	0.06	1	63	0.0576716	0.0583683	0.0590651	-	1.58528	1.58685	1.58842	1.58842
5	6	3	6	1	0	1.81439e-007	4.51397e-007	-	1.50001	1.50001	1.50001	1.50001
5	6	0.104	2	21	0.00147502	0.00159052	0.00170601	-	1.50122	1.50137	1.50152	1.50152

Prob de pico estimada por fluxo
0.0567308 0.0585701 0.0604093

Ocupacao Média por link

1	2	1	2	252	26.1096%	65.7114	65.7962	65.881
1	3	1	3	252	26.1096%	65.7114	65.7962	65.881
2	3	2	3	252	18.739%	47.1617	47.2223	47.2829
2	5	2	5	252	35.4985%	89.3695	89.4561	89.5427
2	4	2	4	252	0.019883%	0.0481954	0.0501053	0.0520151
3	4	3	4	252	14.5537%	36.6265	36.6754	36.7243
3	6	3	6	252	49.0827%	123.594	123.688	123.783
4	5	4	5	252	9.15763%	23.0518	23.0772	23.1026
4	6	4	6	252	23.1638%	58.311	58.3729	58.4347
5	6	5	6	252	44.093%	111.029	111.114	111.2

Tsimulado(horas) Tsimulacao(segundos)

183425	165.703
184492	163.235
183666	164.031
182895	162.109
182303	161.688
183951	162.781
184239	163.078
182509	161.047
183046	162
183178	161.844

Caso de Estudo A

InvBand

Prob media de bloqueio global
0.00172785 0.00178539 0.00184293

Tráfego médio suportado pela rede
159.349 159.42 159.491

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12							
2.73919e-011	6.23189e-009	1.24364e-008	-	1.91667	1.91667	1.91667					
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3							
0.000101195	0.000108648	0.000116101	-	1.91956	1.9196	1.91964					
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4							
0.00679355	0.00702049	0.00724742	-	2.13977	2.14003	2.1403					
Probabilidade de bloqueio por fluxo											
1	3	1.4	6	1	0	1.4406e-007	3.58402e-007	-	1.5	1.50001	1.50001
1	3	0.08	2	21	6.08046e-005	0.000105198	0.000149592	-	1.50001	1.50002	1.50003
1	5	2.2	6	1	0	0	0	-	2.5	2.5	2.5
1	5	0.2	2	21	0.000155877	0.000175131	0.000194385	-	2.50187	2.50196	2.50206
1	5	0.03	1	63	0.00704207	0.00745505	0.00786803	-	2.50225	2.50245	2.50264
1	6	3	6	1	0	2.48549e-007	5.25478e-007	-	2.5	2.5	2.5
1	6	0.272	2	21	0.000146369	0.000180342	0.000214314	-	2.50606	2.50618	2.50629
1	6	0.02	1	63	0.00900959	0.00989239	0.0107752	-	2.51855	2.51926	2.51997
3	5	4.6	6	1	0	0	0	-	2	2	2
3	5	0.12	2	21	3.05501e-005	4.54105e-005	6.02709e-005	-	2.0002	2.00023	2.00026
3	5	0.04	1	63	0.00326334	0.00363399	0.00400464	-	2.00029	2.00033	2.00037
3	6	4.2	6	1	0	0	0	-	1.5	1.50001	1.50001
3	6	0.168	2	21	7.88607e-005	9.77849e-005	0.000116709	-	1.50887	1.50908	1.50929
3	6	0.06	1	63	0.00672772	0.00710051	0.0074733	-	1.53742	1.53809	1.53876
5	6	3	6	1	0	0	0	-	1.5	1.5	1.50001
5	6	0.104	2	21	3.1047e-005	4.8021e-005	6.49951e-005	-	1.50009	1.50011	1.50013

Prob de pico estimada por fluxo
0.00900959 0.00989239 0.0107752

Ocupacao Média por link

1	2	1	2	252	26.1465%	65.8436	65.8891	65.9346
1	3	1	3	252	26.1465%	65.8436	65.8891	65.9346
2	3	2	3	252	18.4962%	46.5868	46.6103	46.6338
2	5	2	5	252	30.7323%	77.3952	77.4455	77.4957
2	4	2	4	252	4.57959%	11.5072	11.5406	11.5739
3	4	3	4	252	21.1836%	53.3393	53.3827	53.426
3	6	3	6	252	42.941%	108.165	108.211	108.258
4	5	4	5	252	15.7389%	39.6226	39.6621	39.7016
4	6	4	6	252	27.7809%	69.9516	70.0079	70.0642
5	6	5	6	252	33.2153%	83.6576	83.7025	83.7475

TSimulado(horas) TSimulacao(segundos)

289084	255.094
266068	234.063
234931	207.125
184268	162.25
240486	211.828
183469	161.797
495124	434.562
184733	162.969
185031	162.281
249188	219.594

Caso de Estudo A

InvCap+PEN

Prob media de bloqueio global
0.00282326 0.0030994 0.00337554

Tráfego médio suportado pela rede
159.241 159.329 159.417

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12		
9.14425e-008	1.24373e-007	1.57303e-007	-	1.93532	1.93539	1.93545
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3		
0.000614499	0.00064922	0.000683942	-	2.09932	2.09988	2.10044
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4		
0.0131032	0.0135088	0.0139144	-	2.14144	2.14177	2.1421
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo		
1 3	1.4	6 1	0	7.77433e-007	1.93415e-006	- 1.51933 1.51948 1.51963
1 3	0.08	2 21	3.64858e-005	7.49383e-005	0.000113391	- 1.77196 1.7741 1.77624
1 5	2.2	6 1	4.02324e-009	4.97434e-007	9.90846e-007	- 2.50754 2.5077 2.50786
1 5	0.2	2 21	0.000461767	0.000520165	0.000578563	- 2.61077 2.61136 2.61194
1 5	0.03	1 63	0.010539	0.0115359	0.0125328	- 2.50098 2.50113 2.50128
1 6	3	6 1	1.29426e-006	2.17328e-006	3.05229e-006	- 2.51857 2.51873 2.51889
1 6	0.272	2 21	0.000907448	0.000982	0.00105655	- 2.61619 2.61658 2.61696
1 6	0.02	1 63	0.016234	0.0174245	0.018615	- 2.52029 2.52122 2.52215
3 5	4.6	6 1	8.45065e-008	4.74887e-007	8.65267e-007	- 2.00064 2.00065 2.00066
3 5	0.12	2 21	0.000401238	0.00045258	0.000503921	- 2.07645 2.07708 2.07771
3 5	0.04	1 63	0.00815207	0.00872727	0.00930247	- 2 2.00001 2.00002
3 6	4.2	6 1	6.56565e-007	1.55667e-006	2.45677e-006	- 1.53298 1.53317 1.53336
3 6	0.168	2 21	0.000803052	0.000889693	0.000976335	- 1.7947 1.79596 1.79721
3 6	0.06	1 63	0.015805	0.0163475	0.0168901	- 1.54393 1.54473 1.54553
5 6	3	6 1	1.36828e-006	2.35578e-006	3.34328e-006	- 1.53238 1.5326 1.53281
5 6	0.104	2 21	0.000859347	0.000975945	0.00109254	- 1.72272 1.72421 1.7257

Prob de pico estimada por fluxo
0.016234 0.0174245 0.018615

Ocupacao Média por link

1 2 1 2	252	26.4648%	66.6243	66.6914	66.7585
1 3 1 3	252	26.4648%	66.6243	66.6914	66.7585
2 3 2 3	252	17.8702%	44.9975	45.033	45.0684
2 5 2 5	252	33.4487%	84.1933	84.2906	84.388
2 4 2 4	252	2.72418%	6.82587	6.86493	6.90399
3 4 3 4	252	19.6229%	49.399	49.4498	49.5007
3 6 3 6	252	46.477%	117.041	117.122	117.203
4 5 4 5	252	14.7549%	37.1303	37.1825	37.2346
4 6 4 6	252	24.651%	62.0591	62.1204	62.1817
5 6 5 6	252	41.1521%	103.654	103.703	103.753

TSimulado(horas) TSimulacao(segundos)

184163	179.297
182879	177.625
182442	177.312
183051	178.391
185988	180.5
184620	179.922
184981	178.954
184065	179
182736	176.609
183261	177.125

Caso de Estudo A

InvBand+PEN

Prob media de bloqueio global
0.00138547 0.00146051 0.00153555

Tráfego médio suportado pela rede
159.32 159.425 159.529

Prob média de bloqueio dos VC12		-	N. médio de links usados pelos VC12	
0	1.36934e-008	2.86953e-008	-	1.93598 1.93604 1.9361
Prob média de bloqueio dos VC3		-	N. médio de links usados pelos VC3	
0.000129157	0.000137191	0.000145225	-	2.06115 2.06147 2.06179
Prob média de bloqueio dos VC4		-	N. médio de links usados pelos VC4	
0.00497566	0.00516628	0.0053569	-	2.1307 2.13096 2.13123
Probabilidade de bloqueio por fluxo			N. médio de links usados pelo fluxo	
1 3	1.4	6 1	0	0 - 1.51352 1.51361 1.51371
1 3	0.08	2 21	8.52554e-005	0.00012901 0.000172765 - 1.68516 1.68629 1.68741
1 5	2.2	6 1	4.02397e-009	4.98419e-007 9.92815e-007 - 2.50947 2.50963 2.50978
1 5	0.2	2 21	0.000154891	0.000182491 0.00021009 - 2.58444 2.58513 2.58582
1 5	0.03	1 63	0.00599156	0.0064982 0.00700483 - 2.50092 2.50107 2.50122
1 6	3	6 1	0	3.64262e-007 9.06236e-007 - 2.51267 2.51274 2.51281
1 6	0.272	2 21	0.000218717	0.000251342 0.000283967 - 2.55503 2.55557 2.55561
1 6	0.02	1 63	0.00681467	0.00745725 0.00809983 - 2.50549 2.50599 2.50649
3 5	4.6	6 1	0	0 - 2.00157 2.00158 2.0016
3 5	0.12	2 21	6.04231e-005	8.59382e-005 0.000111453 - 2.08702 2.08765 2.08827
3 5	0.04	1 63	0.00272096	0.00308788 0.00345479 - 2.0001 2.00014 2.00018
3 6	4.2	6 1	0	0 - 1.5416 1.54178 1.54196
3 6	0.168	2 21	0.000102575	0.00012754 0.000152506 - 1.71693 1.71768 1.71843
3 6	0.06	1 63	0.00339738	0.00362179 0.00384621 - 1.5159 1.51666 1.51742
5 6	3	6 1	0	0 - 1.53673 1.5369 1.53708
5 6	0.104	2 21	2.53727e-005	4.68229e-005 6.82731e-005 - 1.73509 1.7365 1.7379

Prob de pico estimada por fluxo
0.00681467 0.00745725 0.00809983

Ocupacao Média por link

1 2 1 2	252	26.4465%	66.5723	66.6452	66.718
1 3 1 3	252	26.4465%	66.5723	66.6452	66.718
2 3 2 3	252	17.7606%	44.7157	44.7567	44.7977
2 5 2 5	252	26.8679%	67.6355	67.7072	67.7789
2 4 2 4	252	9.37537%	23.5786	23.6259	23.6732
3 4 3 4	252	30.4181%	76.5967	76.6536	76.7105
3 6 3 6	252	35.9188%	90.4385	90.5155	90.5925
4 5 4 5	252	25.1973%	63.4111	63.4973	63.5836
4 6 4 6	252	30.2564%	76.1747	76.2462	76.3177
5 6 5 6	252	23.761%	59.8101	59.8778	59.9454

TSimulado(horas) TSimulacao(segundos)

183266	178.468
184258	179.844
183894	179.797
183824	179.109
183772	179.25
184146	179.344
183245	178
184359	179.328
182220	188.406
276549	270.094

Caso de Estudo A

InvCap+PEN+RP

Prob media de bloqueio global
0.00229407 0.00252515 0.00275623

Tráfego médio suportado pela rede
159.281 159.364 159.447

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12		
1.91919e-007	2.57982e-007	3.24045e-007	-	1.98718	1.98743	1.98767
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3		
0.000933723	0.000962162	0.0009906	-	2.11077	2.1112	2.11162
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4		
0.00980803	0.0102671	0.0107261	-	2.14151	2.1418	2.1421
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo		
1	3	1.4	6	1	0	0 - 1.52867 1.52902 1.52937
1	3	0.08	2	21	3.42772e-005	5.45887e-005 7.49003e-005 - 1.73092 1.73227 1.73363
1	5	2.2	6	1	1.79383e-007	7.39987e-007 1.30059e-006 - 2.51159 2.51171 2.51183
1	5	0.2	2	21	0.000766069	0.000833668 0.000901267 - 2.62348 2.62395 2.62443
1	5	0.03	1	63	0.00808279	0.00881897 0.00955516 - 2.50045 2.50055 2.50065
1	6	3	6	1	3.44554e-006	5.26471e-006 7.08388e-006 - 2.54926 2.54989 2.55052
1	6	0.272	2	21	0.00134589	0.001384 0.00142211 - 2.67676 2.67766 2.67856
1	6	0.02	1	63	0.0127069	0.0135428 0.0143787 - 2.52136 2.52212 2.52288
3	5	4.6	6	1	0	7.09659e-007 1.46066e-006 - 2.00378 2.00385 2.00391
3	5	0.12	2	21	0.000517693	0.0006107 0.000703706 - 2.07629 2.07682 2.07736
3	5	0.04	1	63	0.00586703	0.0065042 0.00714102 - 2 2 2
3	6	4.2	6	1	3.02248e-006	4.27497e-006 5.52747e-006 - 1.64654 1.64725 1.64795
3	6	0.168	2	21	0.00142323	0.00150981 0.00159639 - 1.82876 1.83033 1.83189
3	6	0.06	1	63	0.0116703	0.0122025 0.0127347 - 1.54378 1.54455 1.54532
5	6	3	6	1	3.53299e-006	5.26353e-006 6.99407e-006 - 1.68193 1.68284 1.68376
5	6	0.104	2	21	0.00129779	0.00138021 0.00146262 - 1.72448 1.72615 1.72782

Prob de pico estimada por fluxo
0.0127069 0.0135428 0.0143787

Ocupacao Média por link

1	2	1	2	252	26.4323%	66.5424	66.6094	66.6765
1	3	1	3	252	26.4323%	66.5424	66.6094	66.6765
2	3	2	3	252	17.6255%	44.3883	44.4162	44.4441
2	5	2	5	252	33.0661%	83.2582	83.3267	83.3951
2	4	2	4	252	2.33404%	5.85977	5.88178	5.90379
3	4	3	4	252	18.9105%	47.6126	47.6545	47.6964
3	6	3	6	252	47.3614%	119.285	119.351	119.417
4	5	4	5	252	13.6011%	34.2436	34.2747	34.3058
4	6	4	6	252	24.5437%	61.7971	61.85	61.9029
5	6	5	6	252	42.0095%	105.793	105.864	105.935

TSimulado(horas) TSimulacao(segundos)

183802	3783.53
183360	3773.74
183237	3772.01
183959	3777.31
183953	3793.94
182878	3746.05
183938	3783.28
183681	3771.23
184476	3789.36
183688	3790.11

Caso de Estudo A

InvBand+PEN+RP

Prob media de bloqueio global
0.00121046 0.00130775 0.00140503

Tráfego médio suportado pela rede
159.391 159.471 159.55

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12		
0	0	0	-	1.99475	1.99499	1.99522
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3		
0.00016521	0.000178799	0.000192387	-	2.09041	2.09092	2.09143
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4		
0.00410343	0.00433217	0.00456091	-	2.12971	2.12984	2.12997
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo		
1 3	1.4	6 1	0	0 - 1.55711	1.5577	1.55828
1 3	0.08	2 21	6.99337e-005	0.000129274	0.000188614	- 1.7542 1.75637 1.75855
1 5	2.2	6 1	0	0	0 - 2.51136	2.51147 2.51159
1 5	0.2	2 21	0.000258783	0.000305292	0.000351801	- 2.59137 2.5919 2.59244
1 5	0.03	1 63	0.00604172	0.00650872	0.00697571	- 2.50251 2.5027 2.5029
1 6	3	6 1	0	0	0 - 2.54844	2.54872 2.549
1 6	0.272	2 21	0.000238803	0.000279637	0.000320472	- 2.61173 2.61234 2.61295
1 6	0.02	1 63	0.00511452	0.00570499	0.00629545	- 2.50374 2.50414 2.50455
3 5	4.6	6 1	0	0	0 - 2.00316	2.00321 2.00326
3 5	0.12	2 21	0.000108324	0.000149559	0.000190794	- 2.09524 2.09597 2.09671
3 5	0.04	1 63	0.00221999	0.00251562	0.00281126	- 2.00052 2.00061 2.00071
3 6	4.2	6 1	0	0	0 - 1.66638	1.66704 1.6677
3 6	0.168	2 21	0.000148854	0.000177561	0.000206267	- 1.74206 1.74298 1.74391
3 6	0.06	1 63	0.00242917	0.00259935	0.00276952	- 1.51141 1.51189 1.51238
5 6	3	6 1	0	0	0 - 1.68104	1.6818 1.68255
5 6	0.104	2 21	1.41251e-005	3.14701e-005	4.88151e-005	- 1.74457 1.74594 1.74732

Prob de pico estimada por fluxo
0.00604172 0.00650872 0.00697571

Ocupacao Média por link

1 2 1 2	252	26.4653%	66.6291	66.6926	66.7561
1 3 1 3	252	26.4653%	66.6291	66.6926	66.7561
2 3 2 3	252	17.8999%	45.0675	45.1077	45.1479
2 5 2 5	252	30.9727%	77.9773	78.0512	78.1252
2 4 2 4	252	5.02918%	12.6252	12.6735	12.7219
3 4 3 4	252	31.613%	79.6146	79.6648	79.7149
3 6 3 6	252	34.6895%	87.3746	87.4175	87.4605
4 5 4 5	252	26.3218%	66.2805	66.3309	66.3813
4 6 4 6	252	26.5593%	66.8622	66.9294	66.9966
5 6 5 6	252	25.7971%	64.9545	65.0087	65.063

TSimulado(horas) TSimulacao(segundos)

184163	4250.06
184729	4267.81
183385	4240.27
183492	4245.61
182744	4218.38
183022	4212.52
183549	4234.86
187746	4356.52
183554	4226.13
185358	4276.16

Caso de Estudo B

InvCap

Prob media de bloqueio global
0.0145114 0.0146713 0.0148313

Tráfego médio suportado pela rede
191.699 191.769 191.839

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12								
5.31544e-009	8.35985e-009	1.14043e-008	-	2.70002	2.70003	2.70003					
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3								
0.00131637	0.0013571	0.00139784	-	2.70854	2.70862	2.70869					
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4								
0.0533242	0.0537248	0.0541253	-	2.85351	2.85401	2.85451					
Probabilidade de bloqueio por fluxo						N. médio de links usados pelo fluxo					
1	3	1.26	6	1	4.86536e-009	6.01685e-007	1.1985e-006	-	2.5	2.5	2.5
1	3	0.06	2	21	0.000396697	0.000461579	0.000526462	-	2.5	2.5	2.5
1	3	0.02	1	63	0.0114775	0.0125489	0.0136203	-	2.5	2.5	2.5
1	7	3.22	6	1	1.40074e-006	2.59214e-006	3.78355e-006	-	3.5	3.5	3.5
1	7	0.19	2	21	0.00058268	0.000652	0.00072132	-	3.5	3.5	3.5
1	7	0.05	1	63	0.015349	0.0158856	0.0164221	-	3.50014	3.50017	3.5002
1	8	2.1	6	1	4.89899e-007	1.08472e-006	1.67953e-006	-	3.00001	3.00001	3.00001
1	8	0.11	2	21	0.00275407	0.00291818	0.00308228	-	3.0012	3.00129	3.00137
1	8	0.03	1	63	0.11275	0.114243	0.115736	-	3.00371	3.00411	3.00451
1	9	1.54	6	1	0	2.45628e-007	6.1109e-007	-	3	3	3
1	9	0.14	2	21	0.000402818	0.000462637	0.000522455	-	3.0001	3.00012	3.00014
1	9	0.01	1	63	0.00946619	0.0102896	0.011113	-	3.0047	3.00507	3.00544
3	7	2.94	6	1	1.99195e-007	9.02048e-007	1.6049e-006	-	3.5	3.5	3.5
3	7	0.08	2	21	0.000296211	0.000354959	0.000413706	-	3.5	3.5	3.5
3	8	1.68	6	1	1.64591e-007	6.7897e-007	1.19335e-006	-	3	3.00001	3.00001
3	8	0.09	2	21	0.0026518	0.00282582	0.00299984	-	3.00122	3.0013	3.00139
3	8	0.03	1	63	0.107361	0.109068	0.110775	-	3.00401	3.00421	3.00441
3	9	2.66	6	1	0	0	0	-	3	3	3
3	9	0.14	2	21	8.84162e-005	0.000102861	0.000117307	-	3.00009	3.00011	3.00012
3	9	0.02	1	63	0.00363211	0.00408188	0.00453164	-	3.00471	3.00496	3.00521
7	8	1.96	6	1	3.0409e-007	7.74601e-007	1.24511e-006	-	2.50008	2.50008	2.50009
7	8	0.16	2	21	0.00273802	0.00285833	0.00297864	-	2.52749	2.52768	2.52786
7	9	0.98	6	1	0	1.54917e-006	3.30983e-006	-	1.5	1.5	1.5
7	9	0.09	2	21	0.000191085	0.000232414	0.000273743	-	1.50009	1.50012	1.50014
8	9	3.08	6	1	0	1.23167e-007	3.06424e-007	-	1.50015	1.50016	1.50017
8	9	0.18	2	21	0.00259057	0.00270227	0.00281398	-	1.55488	1.55554	1.55562
8	9	0.03	1	63	0.108663	0.109957	0.111251	-	1.95639	1.95955	1.96271

Prob de pico estimada por fluxo
0.11275 0.114243 0.115736

Ocupacao Média por link

1	2	1	2	252	30.3141%	76.3483	76.3914	76.4346
1	4	1	4	252	30.3141%	76.3483	76.3914	76.4346
2	3	2	3	252	28.142%	70.8792	70.9178	70.9563
2	4	2	4	252	23.648%	59.5701	59.593	59.6159
2	5	2	5	252	25.8201%	65.0187	65.0667	65.1146
3	5	3	5	252	28.142%	70.8792	70.9178	70.9563
4	8	4	8	252	48.4924%	122.153	122.201	122.249
4	5	4	5	252	5.11383%	12.8592	12.8868	12.9144
4	6	4	6	252	1.59692%	4.00583	4.02424	4.04265
5	6	5	6	252	7.968%	20.0419	20.0794	20.1168
5	7	5	7	252	31.5708%	79.5138	79.5584	79.6031
5	9	5	9	252	32.5713%	82.0402	82.0797	82.1191
6	8	6	8	252	19.113%	48.116	48.1647	48.2135
6	9	6	9	252	12.7045%	31.9909	32.0152	32.0395
7	9	7	9	252	31.5708%	79.5138	79.5584	79.6031
8	9	8	9	252	64.7805%	163.198	163.247	163.296

TSimulado(horas) TSimulacao(segundos)

263906	444.312
261889	439.844
263739	441.203
262219	439.266
263624	440.312
263925	439.531
262287	437.469
263504	439.594
264605	442.562
263830	444.875

Caso de Estudo B

InvBand

Prob media de bloqueio global
0.00917718 0.00968286 0.0101885

Tráfego médio suportado pela rede
191.95 192.041 192.132

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12								
2.29201e-009	3.38152e-009	4.47103e-009	-	2.70001	2.70001 2.70002						
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3								
0.000684129	0.000715085	0.000746041	-	2.71154	2.71161 2.71168						
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4								
0.0321391	0.0324359	0.0327327	-	2.81806	2.81827 2.81849						
Probabilidade de bloqueio por fluxo N. médio de links usados pelo fluxo											
1	3	1.26	6	1	0	3.00379e-007	7.47303e-007	-	2.5	2.50002	2.50004
1	3	0.06	2	21	0.000515264	0.000579883	0.000644502	-	2.50006	2.50009	2.50012
1	3	0.02	1	63	0.0133197	0.0143843	0.015449	-	2.5	2.50002	2.50004
1	7	3.22	6	1	0	1.16947e-007	2.90949e-007	-	3.5	3.5	3.5
1	7	0.19	2	21	0.000463854	0.000534	0.000604146	-	3.5	3.5	3.5
1	7	0.05	1	63	0.0157703	0.0161204	0.0164704	-	3.50022	3.50027	3.50031
1	8	2.1	6	1	1.8118e-007	9.01708e-007	1.62224e-006	-	3.00001	3.00002	3.00002
1	8	0.11	2	21	0.00136999	0.00149963	0.00162926	-	3.0143	3.01453	3.01477
1	8	0.03	1	63	0.0623634	0.0637083	0.0650533	-	3.02129	3.02182	3.02236
1	9	1.54	6	1	1.79779e-007	7.41648e-007	1.30352e-006	-	3.00001	3.00001	3.00001
1	9	0.14	2	21	0.000301314	0.000358008	0.000414702	-	3.00139	3.00145	3.0015
1	9	0.01	1	63	0.010568	0.0109609	0.0113539	-	3.00177	3.00204	3.00232
3	7	2.94	6	1	2.16284e-007	6.45324e-007	1.07436e-006	-	3.5	3.5	3.5
3	7	0.08	2	21	0.000270335	0.000327419	0.000384503	-	3.5	3.5	3.5
3	8	1.68	6	1	0	2.24556e-007	5.58665e-007	-	3.00001	3.00001	3.00001
3	8	0.09	2	21	0.00102391	0.00111952	0.00121513	-	3.01473	3.01491	3.01509
3	8	0.03	1	63	0.058214	0.0597808	0.0613476	-	3.02175	3.0223	3.02285
3	9	2.66	6	1	0	1.42118e-007	3.53571e-007	-	3.00001	3.00001	3.00001
3	9	0.14	2	21	9.96245e-005	0.000127253	0.000154882	-	3.00146	3.00152	3.00157
3	9	0.02	1	63	0.00453282	0.00508017	0.00562752	-	3.00141	3.00162	3.00183
7	8	1.96	6	1	0	3.86616e-007	9.6185e-007	-	2.50002	2.50003	2.50004
7	8	0.16	2	21	0.00117511	0.00123525	0.0012954	-	2.54942	2.54975	2.55007
7	9	0.98	6	1	0	0	0	-	1.5	1.5	1.50001
7	9	0.09	2	21	0.000153572	0.000197406	0.000241239	-	1.50147	1.50158	1.50169
8	9	3.08	6	1	0	0	0	-	1.50003	1.50004	1.50004
8	9	0.18	2	21	0.00107464	0.00117248	0.00127032	-	1.53195	1.53227	1.53259
8	9	0.03	1	63	0.0559725	0.0570164	0.0580602	-	1.67819	1.67985	1.6815

Prob de pico estimada por fluxo
0.0623634 0.0637083 0.0650533

Ocupacao Média por link

1	2	1	2	252	30.3241%	76.3619	76.4168	76.4718
1	4	1	4	252	30.3241%	76.3619	76.4168	76.4718
2	3	2	3	252	28.1825%	70.9747	71.0198	71.0648
2	4	2	4	252	23.6863%	59.6547	59.6895	59.7243
2	5	2	5	252	25.828%	65.0372	65.0865	65.1358
3	5	3	5	252	28.1825%	70.9747	71.0198	71.0648
4	8	4	8	252	48.7415%	122.762	122.828	122.895
4	5	4	5	252	9.66115%	24.3179	24.3461	24.3743
4	6	4	6	252	5.94022%	14.9314	14.9694	15.0074
5	6	5	6	252	6.96583%	17.5179	17.5539	17.5899
5	7	5	7	252	31.5571%	79.4776	79.5239	79.5701
5	9	5	9	252	28.6123%	72.0725	72.103	72.1335
6	8	6	8	252	18.4115%	46.3396	46.3971	46.4545
6	9	6	9	252	17.0761%	42.9763	43.0318	43.0872
7	9	7	9	252	31.5571%	79.4776	79.5239	79.5701
8	9	8	9	252	57.0462%	143.691	143.756	143.822

TSimulado(horas) TSimulacao(segundos)

262577	441.391
264484	442.672
265387	444.594
265281	464.031
262447	440.265
261547	436.657
264461	442.875
263388	441.562
262631	442.094
263741	441.656

Caso de Estudo B

InvCap+PEN

Prob media de bloqueio global
0.0133175 0.0136752 0.0140329

Tráfego médio suportado pela rede
191.761 191.842 191.923

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12								
1.35583e-008	1.85486e-008	2.35389e-008	-	2.71426	2.71443	2.71461					
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3								
0.0024179	0.00247801	0.00253811	-	2.87644	2.87763	2.87882					
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4								
0.0461346	0.0465715	0.0470085	-	2.81941	2.8198	2.82019					
Probabilidade de bloqueio por fluxo			N. médio de links usados pelo fluxo								
1	3	1.26	6	1	5.02439e-007	1.50032e-006	2.49821e-006	-	2.52189	2.52321	2.52454
1	3	0.06	2	21	0.000406636	0.000501241	0.000595847	-	2.54568	2.54688	2.54809
1	3	0.02	1	63	0.0130449	0.0137521	0.0144592	-	2.5	2.5	2.5
1	7	3.22	6	1	2.53093e-006	3.54394e-006	4.55695e-006	-	3.50015	3.50016	3.50017
1	7	0.19	2	21	0.00076115	0.00082	0.00087885	-	3.51384	3.51408	3.51431
1	7	0.05	1	63	0.0217374	0.0223562	0.022975	-	3.50015	3.50019	3.50022
1	8	2.1	6	1	1.20391e-006	2.16738e-006	3.13086e-006	-	3.00076	3.00078	3.00079
1	8	0.11	2	21	0.00519826	0.00547848	0.00575869	-	3.10952	3.11032	3.11112
1	8	0.03	1	63	0.0923	0.0938341	0.0953683	-	3.011	3.01145	3.01189
1	9	1.54	6	1	8.28125e-007	2.46291e-006	4.09769e-006	-	3.02205	3.02232	3.02259
1	9	0.14	2	21	0.000354139	0.000404188	0.000454238	-	3.3205	3.32408	3.32767
1	9	0.01	1	63	0.00997938	0.0106485	0.0113175	-	3.00057	3.0008	3.00104
3	7	2.94	6	1	8.98341e-007	2.32253e-006	3.74672e-006	-	3.50006	3.50007	3.50007
3	7	0.08	2	21	0.000555256	0.000614055	0.000672855	-	3.50592	3.50608	3.50624
3	8	1.68	6	1	9.70988e-007	1.81539e-006	2.65978e-006	-	3.0008	3.00081	3.00083
3	8	0.09	2	21	0.00499988	0.00523296	0.00546605	-	3.11306	3.11446	3.11587
3	8	0.03	1	63	0.0898965	0.0912416	0.0925867	-	3.01092	3.01141	3.0119
3	9	2.66	6	1	1.01421e-007	5.70613e-007	1.03981e-006	-	3.02208	3.02227	3.02246
3	9	0.14	2	21	0.000122328	0.000154615	0.000186902	-	3.31849	3.32189	3.3253
3	9	0.02	1	63	0.00363902	0.00389946	0.0041599	-	3.00042	3.00056	3.0007
7	8	1.96	6	1	6.71441e-007	2.31815e-006	3.96486e-006	-	2.50212	2.50215	2.50218
7	8	0.16	2	21	0.00554789	0.00571668	0.00588548	-	2.64528	2.64622	2.64716
7	9	0.98	6	1	0	1.16142e-006	2.39005e-006	-	1.52428	1.52449	1.52469
7	9	0.09	2	21	0.000449712	0.000502018	0.000554324	-	1.78576	1.78991	1.79406
8	9	3.08	6	1	5.34305e-007	1.11255e-006	1.69079e-006	-	1.54794	1.54806	1.54819
8	9	0.18	2	21	0.00524791	0.00535582	0.00546372	-	1.90034	1.90234	1.90434
8	9	0.03	1	63	0.0885386	0.0902689	0.0919991	-	1.71163	1.7142	1.71678

Prob de pico estimada por fluxo
0.0923 0.0938341 0.0953683

Ocupacao Média por link

1	2	1	2	252	30.3277%	76.3707	76.4258	76.4808
1	4	1	4	252	30.3277%	76.3707	76.4258	76.4808
2	3	2	3	252	28.229%	71.0968	71.1372	71.1776
2	4	2	4	252	23.6736%	59.6176	59.6576	59.6975
2	5	2	5	252	25.7723%	64.9011	64.9462	64.9912
3	5	3	5	252	28.229%	71.0968	71.1372	71.1776
4	8	4	8	252	49.0776%	123.615	123.676	123.736
4	5	4	5	252	6.79002%	17.0945	17.1108	17.1271
4	6	4	6	252	3.05633%	7.65546	7.70195	7.74845
5	6	5	6	252	10.9791%	27.5889	27.6672	27.7456
5	7	5	7	252	34.1283%	85.9201	86.0034	86.0866
5	9	5	9	252	28.0797%	70.6007	70.7608	70.9208
6	8	6	8	252	21.3726%	53.8087	53.8589	53.909
6	9	6	9	252	15.7757%	39.6892	39.7547	39.8202
7	9	7	9	252	34.1283%	85.9201	86.0034	86.0866
8	9	8	9	252	60.6511%	152.806	152.841	152.876

TSimulado(horas) TSimulacao(segundos)

262822	482.297
263122	479.672
262295	478.094
263804	483.687
263460	479.735
263193	480.156
261055	475.797
261348	478.531
264321	482.344
264107	482.859

Caso de Estudo B

InvBand+PEN

Prob media de bloqueio global
0.00554082 0.00645826 0.00737569

Tráfego médio suportado pela rede
192.18 192.256 192.331

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12		
5.6007e-009	8.60959e-009	1.16185e-008	-	2.71494	2.71503 2.71511
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3		
0.000569096	0.000601082	0.000633068	-	2.8154	2.81569 2.81598
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4		
0.016584	0.0169589	0.0173338	-	2.7956	2.79571 2.79582
Probabilidade de bloqueio por fluxo			N. médio de links usados pelo fluxo		
1 3	1.26 6 1	1.29005e-007	1.50959e-006	2.89017e-006	- 2.50422 2.50459 2.50496
1 3	0.06 2 21	0.000527066	0.000617655	0.000708245	- 2.52643 2.52713 2.52784
1 3	0.02 1 63	0.0127045	0.0133768	0.0140491	- 2.5 2.5 2.5
1 7	3.22 6 1	1.48261e-006	2.47707e-006	3.47153e-006	- 3.50002 3.50002 3.50003
1 7	0.19 2 21	0.000741645	0.00082	0.000898355	- 3.50176 3.5018 3.50184
1 7	0.05 1 63	0.0211097	0.0217831	0.0224566	- 3.50015 3.50017 3.5002
1 8	2.1 6 1	7.73942e-008	9.035e-007	1.72961e-006	- 3.00787 3.00794 3.00801
1 8	0.11 2 21	0.000882793	0.000957229	0.00103166	- 3.09042 3.09127 3.09212
1 8	0.03 1 63	0.0259455	0.0270221	0.0280987	- 3.0128 3.01331 3.01382
1 9	1.54 6 1	0	7.41157e-007	1.52595e-006	- 3.02349 3.02373 3.02397
1 9	0.14 2 21	0.00041244	0.000456642	0.000500844	- 3.17899 3.17963 3.18027
1 9	0.01 1 63	0.00961701	0.0106265	0.0116359	- 3.00068 3.00076 3.00085
3 7	2.94 6 1	4.06203e-007	1.03215e-006	1.6581e-006	- 3.5 3.5 3.5
3 7	0.08 2 21	0.000453232	0.000504753	0.000556274	- 3.5001 3.50013 3.50016
3 8	1.68 6 1	0	4.52984e-007	1.12696e-006	- 3.0081 3.00818 3.00826
3 8	0.09 2 21	0.000561182	0.000601624	0.000642066	- 3.09473 3.09541 3.09609
3 8	0.03 1 63	0.0222155	0.0228028	0.0233901	- 3.01319 3.01372 3.01424
3 9	2.66 6 1	0	1.4286e-007	3.55416e-007	- 3.02348 3.02364 3.02381
3 9	0.14 2 21	0.000131304	0.00015706	0.000182816	- 3.17616 3.17672 3.17727
3 9	0.02 1 63	0.00324318	0.00370383	0.00416448	- 3.00028 3.00036 3.00044
7 8	1.96 6 1	6.08665e-007	1.5483e-006	2.48794e-006	- 2.50955 2.50963 2.50971
7 8	0.16 2 21	0.000787302	0.000893133	0.000998964	- 2.58935 2.58984 2.59034
7 9	0.98 6 1	0	0	0	- 1.52435 1.52456 1.52478
7 9	0.09 2 21	0.000406229	0.000443406	0.000480583	- 1.64816 1.64883 1.6495
8 9	3.08 6 1	0	0	0	- 1.54774 1.54795 1.54817
8 9	0.18 2 21	0.000508049	0.000559317	0.000610584	- 1.84526 1.84617 1.84708
8 9	0.03 1 63	0.0185643	0.0193972	0.02023	- 1.54092 1.54163 1.54234

Prob de pico estimada por fluxo
0.0259455 0.0270221 0.0280987

Ocupacao Média por link

1 2 1 2	252	30.3683%	76.488	76.5281	76.5683
1 4 1 4	252	30.3683%	76.488	76.5281	76.5683
2 3 2 3	252	28.2399%	71.1153	71.1646	71.2138
2 4 2 4	252	23.7299%	59.7526	59.7993	59.846
2 5 2 5	252	25.8583%	65.1319	65.1629	65.1938
3 5 3 5	252	28.2399%	71.1153	71.1646	71.2138
4 8 4 8	252	40.9745%	103.197	103.256	103.314
4 5 4 5	252	8.17798%	20.5899	20.6085	20.6271
4 6 4 6	252	12.517%	31.5152	31.5428	31.5704
5 6 5 6	252	17.247%	43.4302	43.4625	43.4947
5 7 5 7	252	33.7378%	84.9733	85.0194	85.0654
5 9 5 9	252	20.6701%	52.0549	52.0886	52.1223
6 8 6 8	252	27.8319%	70.0917	70.1363	70.1809
6 9 6 9	252	22.8751%	57.6008	57.6453	57.6898
7 9 7 9	252	33.7378%	84.9733	85.0194	85.0654
8 9 8 9	252	44.0586%	110.975	111.028	111.081

TSimulado(horas) TSimulacao(segundos)

263711	484.031
262742	484.625
262076	482.437
264352	487.032
263154	483.968
263298	485.516
262891	482.687
262915	484.438
262984	483.11
263894	488.156

Caso de Estudo B

InvCap+PEN+RP

Prob media de bloqueio global
0.0118424 0.0121607 0.012479

Tráfego médio suportado pela rede
191.765 191.845 191.926

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12								
3.8622e-008	4.54154e-008	5.22089e-008	2.73533	2.73549	2.73565						
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3								
0.00360381	0.00367472	0.00374564	2.90543	2.90627	2.90711						
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4								
0.0388947	0.0393617	0.0398287	2.81529	2.81587	2.81645						
Probabilidade de bloqueio por fluxo			N. médio de links usados pelo fluxo								
1	3	1.26	6	1	0	9.06664e-007	1.86409e-006	-	2.54386	2.54506	2.54626
1	3	0.06	2	21	0.000354628	0.000450638	0.000546648	-	2.55311	2.55475	2.55639
1	3	0.02	1	63	0.0118632	0.0124381	0.0130131	-	2.5	2.5	2.5
1	7	3.22	6	1	7.54657e-007	1.52261e-006	2.29056e-006	-	3.50072	3.50075	3.50078
1	7	0.19	2	21	0.000895946	0.000943126	0.000990306	-	3.52969	3.53007	3.53045
1	7	0.05	1	63	0.0191453	0.0197912	0.0204371	-	3.50004	3.50008	3.50012
1	8	2.1	6	1	6.0923e-006	8.78801e-006	1.14837e-005	-	3.00202	3.00207	3.00212
1	8	0.11	2	21	0.00814062	0.00854171	0.0089428	-	3.1351	3.13591	3.13672
1	8	0.03	1	63	0.078086	0.0794302	0.0807745	-	3.00688	3.00727	3.00767
1	9	1.54	6	1	3.98905e-009	4.94003e-007	9.84018e-007	-	3.04291	3.04335	3.04379
1	9	0.14	2	21	0.000355364	0.000412682	0.000469999	-	3.35479	3.35706	3.35934
1	9	0.01	1	63	0.00908877	0.00961496	0.0101411	-	3.00027	3.00043	3.0006
3	7	2.94	6	1	7.6651e-007	2.2005e-006	3.63449e-006	-	3.50043	3.50044	3.50046
3	7	0.08	2	21	0.000513856	0.000579679	0.000645502	-	3.51576	3.51604	3.51632
3	8	1.68	6	1	7.38379e-006	9.62626e-006	1.18687e-005	-	3.00213	3.00215	3.00218
3	8	0.09	2	21	0.00771663	0.00807029	0.00842395	-	3.1397	3.14081	3.14192
3	8	0.03	1	63	0.0738089	0.0754764	0.0771439	-	3.00662	3.00704	3.00746
3	9	2.66	6	1	0	0	0	-	3.04276	3.04326	3.04376
3	9	0.14	2	21	0.000124503	0.000146478	0.000168453	-	3.34697	3.3489	3.35082
3	9	0.02	1	63	0.00354676	0.00394183	0.0043369	-	3.00035	3.00046	3.00056
7	8	1.96	6	1	8.0739e-006	1.03231e-005	1.25722e-005	-	2.50689	2.50698	2.50706
7	8	0.16	2	21	0.0084219	0.00865192	0.00888195	-	2.68725	2.68821	2.68916
7	9	0.98	6	1	2.19467e-007	2.0924e-006	3.96533e-006	-	1.5528	1.55342	1.55404
7	9	0.09	2	21	0.000336901	0.000424026	0.00051115	-	1.82352	1.82637	1.82922
8	9	3.08	6	1	7.97891e-006	1.05065e-005	1.30341e-005	-	1.65718	1.65744	1.65769
8	9	0.18	2	21	0.00834037	0.0085267	0.00871302	-	1.96288	1.96458	1.96628
8	9	0.03	1	63	0.0741501	0.0748392	0.0755283	-	1.69175	1.69578	1.69981

Prob de pico estimada por fluxo
0.078086 0.0794302 0.0807745

Ocupacao Média por link

1	2	1	2	252	30.3291%	76.3584	76.4294	76.5005
1	4	1	4	252	30.3291%	76.3584	76.4294	76.5005
2	3	2	3	252	28.3356%	71.364	71.4057	71.4473
2	4	2	4	252	23.6743%	59.6313	59.6592	59.6871
2	5	2	5	252	25.6678%	64.6267	64.6829	64.7392
3	5	3	5	252	28.3356%	71.364	71.4057	71.4473
4	8	4	8	252	49.6382%	125.035	125.088	125.142
4	5	4	5	252	6.49538%	16.3401	16.3684	16.3967
4	6	4	6	252	2.20593%	5.5432	5.55895	5.57471
5	6	5	6	252	10.2038%	25.6726	25.7136	25.7546
5	7	5	7	252	33.9505%	85.512	85.5552	85.5985
5	9	5	9	252	27.9203%	70.2663	70.3591	70.4519
6	8	6	8	252	20.3774%	51.3034	51.3511	51.3988
6	9	6	9	252	15.192%	38.2438	38.2838	38.3239
7	9	7	9	252	33.9505%	85.512	85.5552	85.5985
8	9	8	9	252	62.3948%	157.17	157.235	157.3

TSimulado(horas) TSimulacao(segundos)

162736	7857.84
261975	12688.2
259926	12618.7
252399	12222.6
262849	12737
206293	10006.1
261215	12684.7
263705	12787.5
264661	12843.7
224593	10896.8

Caso de Estudo B

InvBand+PEN+RP

Prob media de bloqueio global
0.00449665 0.00537156 0.00624646

Tráfego médio suportado pela rede
192.273 192.348 192.423

Prob média de bloqueio dos VC12			N. médio de links usados pelos VC12								
5.28896e-009	8.08213e-009	1.08753e-008	-	-	-						
			-	2.73357	2.73371 2.73385						
Prob média de bloqueio dos VC3			N. médio de links usados pelos VC3								
0.000628431	0.000665566	0.000702702	-	-	-						
			-	2.83767	2.83791 2.83815						
Prob média de bloqueio dos VC4			N. médio de links usados pelos VC4								
0.0127172	0.0129841	0.013251	-	-	-						
			-	2.7927	2.79285 2.793						
Probabilidade de bloqueio por fluxo											
1	3	1.26	6	1	2.15114e-007	1.20823e-006	2.20134e-006	-	2.54443	2.54507	2.5457
1	3	0.06	2	21	0.000500332	0.000623178	0.000746024	-	2.53583	2.53661	2.53739
1	3	0.02	1	63	0.0129294	0.0137222	0.014515	-	2.5	2.5	2.5
1	7	3.22	6	1	1.15106e-006	2.12362e-006	3.09618e-006	-	3.50027	3.50028	3.50029
1	7	0.19	2	21	0.000797104	0.000858	0.000918896	-	3.50788	3.5081	3.50831
1	7	0.05	1	63	0.0189867	0.0195336	0.0200805	-	3.50009	3.50012	3.50015
1	8	2.1	6	1	7.90632e-008	9.06783e-007	1.7345e-006	-	3.00935	3.00939	3.00944
1	8	0.11	2	21	0.00100109	0.00108867	0.00117626	-	3.11701	3.11765	3.11829
1	8	0.03	1	63	0.0172661	0.0178835	0.0185009	-	3.00953	3.00982	3.01012
1	9	1.54	6	1	1.06603e-006	2.21647e-006	3.36691e-006	-	3.03969	3.03979	3.0399
1	9	0.14	2	21	0.000353539	0.000399774	0.000446008	-	3.20264	3.20333	3.20402
1	9	0.01	1	63	0.0104169	0.0112055	0.0119941	-	3.00035	3.00048	3.00061
3	7	2.94	6	1	2.09463e-009	2.5905e-007	5.16006e-007	-	3.5	3.5	3.5
3	7	0.08	2	21	0.000443402	0.000513191	0.00058298	-	3.50356	3.50362	3.50368
3	8	1.68	6	1	0	0	0	-	3.00971	3.00977	3.00984
3	8	0.09	2	21	0.00079531	0.000881214	0.000967119	-	3.12239	3.12313	3.12387
3	8	0.03	1	63	0.0136036	0.013965	0.0143264	-	3.01006	3.01051	3.01096
3	9	2.66	6	1	0	0	0	-	3.03935	3.03954	3.03974
3	9	0.14	2	21	0.000122976	0.000154927	0.000186877	-	3.19807	3.19871	3.19934
3	9	0.02	1	63	0.00338031	0.00359958	0.00381884	-	3.00028	3.00036	3.00045
7	8	1.96	6	1	2.81031e-007	1.16679e-006	2.05255e-006	-	2.51019	2.51029	2.5104
7	8	0.16	2	21	0.00099898	0.0010453	0.00109163	-	2.62064	2.62124	2.62183
7	9	0.98	6	1	0	3.87081e-007	9.63006e-007	-	1.54205	1.54234	1.54263
7	9	0.09	2	21	0.000364361	0.000423806	0.00048325	-	1.66809	1.66927	1.67044
8	9	3.08	6	1	0	0	0	-	1.64	1.64064	1.64128
8	9	0.18	2	21	0.000624252	0.000667597	0.000710943	-	1.89626	1.89747	1.89869
8	9	0.03	1	63	0.0103756	0.0109793	0.011583	-	1.52763	1.52864	1.52966

Prob de pico estimada por fluxo
0.0189867 0.0195336 0.0200805

Ocupacao Média por link

1 2 1 2	252	30.4084%	76.6005	76.6292	76.6579
1 4 1 4	252	30.4084%	76.6005	76.6292	76.6579
2 3 2 3	252	28.2868%	71.2405	71.2828	71.3251
2 4 2 4	252	23.7312%	59.7607	59.8025	59.8443
2 5 2 5	252	25.8528%	65.1247	65.149	65.1732
3 5 3 5	252	28.2868%	71.2405	71.2828	71.3251
4 8 4 8	252	40.4996%	101.964	102.059	102.154
4 5 4 5	252	7.87953%	19.8349	19.8564	19.878
4 6 4 6	252	12.8952%	32.4259	32.4959	32.5659
5 6 5 6	252	17.3195%	43.6073	43.6452	43.6832
5 7 5 7	252	33.4759%	84.3222	84.3592	84.3963
5 9 5 9	252	20.4693%	51.5486	51.5826	51.6167
6 8 6 8	252	27.7357%	69.8337	69.8939	69.954
6 9 6 9	252	23.0072%	57.9235	57.9781	58.0326
7 9 7 9	252	33.4759%	84.3222	84.3592	84.3963
8 9 8 9	252	43.9432%	110.651	110.737	110.822

TSimulado(horas) TSimulacao(segundos)

264475	13494.5
261875	13384.5
261729	13344.3
263189	13395.8
259583	13214.1
263373	13446.8
264850	13514.9
261980	13360.1
263298	13470.6
263929	13490.2

Caso de Estudo C

InvCap

Prob media de bloqueio global
0.012041 0.0134832 0.0149255

Tráfego médio suportado pela rede
132.613 132.635 132.657

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12		
7.6737e-006	7.84326e-006	8.01281e-006	-	1.91667	1.91667	1.91667
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3		
0.02220039	0.0221259	0.0222479	-	1.91705	1.91705	1.91706
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4		
0.00841021	0.00846601	0.00852181	-	1.68004	1.68012	1.6802
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo		
1 3	0.71 6 1	0.000161334	0.000165537	0.000169739	-	1.5 1.5 1.5
1 3	0.05 2 21	0.0438106	0.0440988	0.044387	-	1.5 1.50001 1.50001
1 5	0.55 6 1	0.000164487	0.000167893	0.000171299	-	2.5 2.5 2.5
1 5	0.08 2 21	0.0438217	0.044158	0.0444944	-	2.5 2.5 2.50001
1 6	0.8 6 1	0.00015495	0.000160669	0.000166388	-	2.5 2.5 2.5
1 6	0.02 2 21	0.0435982	0.044138	0.0446778	-	2.50027 2.5003 2.50033
3 5	3.416 6 1	0	0	0	-	2 2 2
3 5	0.36 2 21	2.02609e-005	2.25233e-005	2.47857e-005	-	2 2 2
3 5	0.044 1 63	0.00184223	0.00192091	0.00199959	-	2 2 2
3 6	3.716 6 1	0	0	0	-	1.5 1.5 1.5
3 6	0.23 2 21	0.000159155	0.000165146	0.000171136	-	1.50078 1.5008 1.50081
3 6	0.046 1 63	0.0114931	0.0116496	0.0118062	-	1.51374 1.51387 1.51401
5 6	3.094 6 1	0	2.59048e-008	6.44478e-008	-	1.5 1.5 1.5
5 6	0.49 2 21	0.000165772	0.000173038	0.000180304	-	1.50119 1.5012 1.50121
5 6	0.031 1 63	0.0116073	0.0118275	0.0120477	-	1.52628 1.52649 1.52669

Prob de pico estimada por fluxo
0.0438217 0.044158 0.0444944

Ocupacao Média por link

1 2 1 2	63	29.1778%	18.3742	18.382	18.3898
1 3 1 3	63	29.1778%	18.3742	18.382	18.3898
2 3 2 3	252	17.76%	44.7387	44.7553	44.772
2 5 2 5	252	20.078%	50.5771	50.5965	50.616
2 4 2 4	252	0.000427036%	0.00100294	0.00107613	0.00114932
3 4 3 4	252	13.8837%	34.9742	34.9868	34.9995
3 6 3 6	252	33.8101%	85.1853	85.2015	85.2177
4 5 4 5	252	16.3625%	41.2219	41.2334	41.2449
4 6 4 6	252	30.0916%	75.8161	75.8309	75.8458
5 6 5 6	252	36.2653%	91.3643	91.3886	91.4129

TSimulado (horas) TSimulado (segundos)

2.51404e+006	1479.14
2.50287e+006	1475.48
2.49214e+006	1456.84
2.49886e+006	1458.41
2.51572e+006	1476.19
2.52001e+006	1474.52
2.51024e+006	1474.19
2.49547e+006	1465.06
2.49054e+006	1465.61
2.50464e+006	1474.39

Caso de Estudo C

InvBand

Prob media de bloqueio global
0.0115794 0.0135901 0.0156008

Tráfego médio suportado pela rede
132.662 132.682 132.703

Prob média de bloqueio dos VC12		-	N. médio de links usados pelos VC12								
7.66262e-006	7.87431e-006	8.086e-006	-	1.91667 1.91667 1.91667							
Prob média de bloqueio dos VC3		-	N. médio de links usados pelos VC3								
0.0219938	0.0221303	0.0222668	-	1.918 1.918 1.91801							
Prob média de bloqueio dos VC4		-	N. médio de links usados pelos VC4								
0.00321808	0.00326156	0.00330504	-	1.67202 1.67207 1.67212							
Probabilidade de bloqueio por fluxo N. médio de links usados pelo fluxo											
1	3	0.71	6	1	0.00016231	0.000168252	0.000174194	-	1.5	1.5	1.5
1	3	0.05	2	21	0.0438107	0.0441724	0.0445341	-	1.50017	1.50018	1.50019
1	5	0.55	6	1	0.000161302	0.000167468	0.000173634	-	2.5	2.5	2.5
1	5	0.08	2	21	0.0442016	0.044409	0.0446165	-	2.50007	2.50007	2.50008
1	6	0.8	6	1	0.000154461	0.000160336	0.000166211	-	2.5	2.5	2.5
1	6	0.02	2	21	0.0433517	0.044124	0.0448963	-	2.50006	2.50007	2.50008
3	5	3.416	6	1	0	0	0	-	2	2	2
3	5	0.36	2	21	2.30133e-005	2.52001e-005	2.7387e-005	-	2.00001	2.00001	2.00001
3	5	0.044	1	63	0.0025642	0.00267434	0.00278448	-	2.00001	2.00002	2.00002
3	6	3.716	6	1	0	0	0	-	1.5	1.5	1.5
3	6	0.23	2	21	2.11638e-005	2.47039e-005	2.8244e-005	-	1.50328	1.50331	1.50333
3	6	0.046	1	63	0.00324679	0.00330663	0.00336647	-	1.50667	1.50678	1.50689
5	6	3.094	6	1	0	2.57871e-008	6.41549e-008	-	1.5	1.5	1.5
5	6	0.49	2	21	2.52216e-005	2.65414e-005	2.78611e-005	-	1.50437	1.50438	1.5044
5	6	0.031	1	63	0.00371354	0.00380371	0.00389387	-	1.5093	1.50941	1.50951

Prob de pico estimada por fluxo
0.0442016 0.044409 0.0446165

Ocupacao Média por link

1	2	1	2	63	29.1754%	18.3729	18.3805	18.388
1	3	1	3	63	29.1754%	18.3729	18.3805	18.388
2	3	2	3	252	17.2322%	43.4147	43.425	43.4354
2	5	2	5	252	19.29%	48.6044	48.6108	48.6173
2	4	2	4	252	0.267355%	0.671895	0.673735	0.675574
3	4	3	4	252	21.0698%	53.0819	53.0959	53.1099
3	6	3	6	252	27.2731%	68.7179	68.7283	68.7388
4	5	4	5	252	23.4991%	59.2018	59.2177	59.2336
4	6	4	6	252	30.2762%	76.2777	76.296	76.3143
5	6	5	6	252	29.4348%	74.1586	74.1757	74.1927

TSimulado (horas) TSimulacao (segundos)

2.5024e+006	1454.25
2.48708e+006	1447.05
2.5149e+006	1462.61
2.50789e+006	1454.97
2.50692e+006	1454.42
2.49426e+006	1451.31
2.49085e+006	1443.7
2.48565e+006	1449.69
2.49574e+006	1450.45
2.51498e+006	1477.48

Caso de Estudo C

InvCap+PEN

Prob media de bloqueio global
0.0184024 0.0216883 0.0249741

Tráfego médio suportado pela rede
132.474 132.501 132.527

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12							
1.33984e-005	1.36177e-005	1.3837e-005	-	1.93988	1.9399	1.93993					
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3							
0.0355314	0.035672	0.0358126	-	2.0829	2.08308	2.08327					
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4							
0.0036544	0.00369019	0.00372598	-	1.67244	1.67252	1.67259					
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo							
1	3	0.71	6	1	0.00028225	0.000288571	0.000294892	-	1.5387	1.53884	1.53898
1	3	0.05	2	21	0.0707159	0.0710816	0.0714472	-	1.67668	1.67716	1.67764
1	5	0.55	6	1	0.000280421	0.000287013	0.000293605	-	2.5021	2.50214	2.50218
1	5	0.08	2	21	0.070885	0.0712006	0.0715162	-	2.60523	2.60552	2.60581
1	6	0.8	6	1	0.000275367	0.000281969	0.000288571	-	2.51776	2.51783	2.51789
1	6	0.02	2	21	0.0707267	0.07136	0.0719933	-	2.6394	2.63998	2.64057
3	5	3.416	6	1	1.89493e-010	2.34328e-008	4.66761e-008	-	2.00031	2.00031	2.00032
3	5	0.36	2	21	5.75747e-005	6.21421e-005	6.67096e-005	-	2.08025	2.08042	2.08059
3	5	0.044	1	63	0.00228278	0.00232052	0.00235827	-	2	2.00001	2.00001
3	6	3.716	6	1	6.68369e-008	1.29157e-007	1.91478e-007	-	1.53798	1.53804	1.5381
3	6	0.23	2	21	0.000154189	0.000163642	0.000173095	-	1.79008	1.79051	1.79094
3	6	0.046	1	63	0.00412995	0.00420047	0.004271	-	1.507	1.50708	1.50716
5	6	3.094	6	1	1.41377e-007	2.06734e-007	2.72091e-007	-	1.54214	1.54226	1.54237
5	6	0.49	2	21	0.000158193	0.000163982	0.00016977	-	1.70465	1.7049	1.70516
5	6	0.031	1	63	0.00447384	0.00454958	0.00462533	-	1.51025	1.51046	1.51067

Prob de pico estimada por fluxo
0.0707267 0.07136 0.0719933

Ocupacao Média por link

1	2	1	2	63	32.5736%	20.51	20.5214	20.5328
1	3	1	3	63	32.5736%	20.51	20.5214	20.5328
2	3	2	3	252	16.8385%	42.4226	42.433	42.4435
2	5	2	5	252	19.752%	49.7614	49.7749	49.7884
2	4	2	4	252	1.10186%	2.77044	2.77668	2.78293
3	4	3	4	252	19.9626%	50.2826	50.3057	50.3288
3	6	3	6	252	33.1183%	83.4446	83.4581	83.4716
4	5	4	5	252	22.25%	56.0526	56.0701	56.0876
4	6	4	6	252	27.575%	69.4639	69.489	69.5142
5	6	5	6	252	34.2987%	86.4151	86.4328	86.4505

TSimulado (horas) TSimulacao (segundos)

2.50992e+006	1612.61
2.49361e+006	1598.03
2.49399e+006	1602.94
2.50126e+006	1604.08
2.51595e+006	1614.33
2.51474e+006	1612.5
2.50792e+006	1608.31
2.49529e+006	1598.75
2.49378e+006	1599.22
2.50025e+006	1614.41

Caso de Estudo C

InvBand+PEN

Prob media de bloqueio global
0.0181447 0.0215695 0.0249942

Tráfego médio suportado pela rede
132.547 132.566 132.585

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12							
1.33138e-005	1.35392e-005	1.37647e-005	-	1.94119	1.94123	1.94127					
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3							
0.035358	0.0354417	0.0355254	-	2.06645	2.06665	2.06685					
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4							
0.002116	0.0021547	0.00219341	-	1.67085	1.67091	1.67097					
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo							
1	3	0.71	6	1	0.0002844	0.000292511	0.000300621	-	1.52892	1.52913	1.52933
1	3	0.05	2	21	0.0705823	0.0707454	0.0709084	-	1.69195	1.69258	1.69321
1	5	0.55	6	1	0.000274145	0.000278629	0.000283114	-	2.50373	2.50377	2.50381
1	5	0.08	2	21	0.0706765	0.0708587	0.0710408	-	2.59432	2.59457	2.59482
1	6	0.8	6	1	0.000273852	0.000281809	0.000289766	-	2.5229	2.52293	2.52297
1	6	0.02	2	21	0.070417	0.070894	0.071371	-	2.59044	2.59086	2.59128
3	5	3.416	6	1	0	1.16647e-008	2.90201e-008	-	2.00056	2.00057	2.00057
3	5	0.36	2	21	5.44012e-005	5.71445e-005	5.98877e-005	-	2.07202	2.07212	2.07222
3	5	0.044	1	63	0.00222702	0.00228651	0.002346	-	2.00002	2.00003	2.00003
3	6	3.716	6	1	0	1.07522e-008	2.675e-008	-	1.54755	1.54762	1.5477
3	6	0.23	2	21	4.22797e-005	4.66057e-005	5.09317e-005	-	1.73785	1.73808	1.73832
3	6	0.046	1	63	0.00183763	0.00187504	0.00191245	-	1.50571	1.50583	1.50595
5	6	3.094	6	1	0	0	0	-	1.54332	1.54336	1.54341
5	6	0.49	2	21	4.48771e-005	4.81848e-005	5.14925e-005	-	1.71151	1.71169	1.71186
5	6	0.031	1	63	0.00221188	0.00230255	0.00239323	-	1.50668	1.50687	1.50705

Prob de pico estimada por fluxo
0.070417 0.070894 0.071371

Ocupacao Média por link

1	2	1	2	63	32.1498%	20.2502	20.2544	20.2586
1	3	1	3	63	32.1498%	20.2502	20.2544	20.2586
2	3	2	3	252	16.9985%	42.8231	42.8363	42.8494
2	5	2	5	252	19.7571%	49.7763	49.7878	49.7993
2	4	2	4	252	1.43661%	3.61245	3.62026	3.62806
3	4	3	4	252	25.9402%	65.352	65.3693	65.3866
3	6	3	6	252	27.5379%	69.3753	69.3956	69.4158
4	5	4	5	252	27.6388%	69.633	69.6497	69.6664
4	6	4	6	252	27.246%	68.6485	68.6598	68.6711
5	6	5	6	252	28.3963%	71.5384	71.5587	71.579

TSimulado (horas) TSimulacao (segundos)

2.50908e+006	1618.63
2.50308e+006	1612.77
2.50525e+006	1614.59
2.47585e+006	1594.55
2.49527e+006	1602.73
2.48606e+006	1604
2.50686e+006	1616.92
2.4928e+006	1607.39
2.50888e+006	1616.25
2.50479e+006	1609.95

Caso de Estudo C

InvCap+PEN+RP

Prob media de bloqueio global
0.0200028 0.0237425 0.0274822

Tráfego médio suportado pela rede
132.431 132.495 132.559

Prob média de bloqueio dos VC12			-	N. médio de links usados pelos VC12							
1.43743e-005	1.47919e-005	1.52094e-005	-	1.9842	1.98431	1.98442					
Prob média de bloqueio dos VC3			-	N. médio de links usados pelos VC3							
0.0391293	0.0393374	0.0395455	-	2.10021	2.10054	2.10088					
Prob média de bloqueio dos VC4			-	N. médio de links usados pelos VC4							
0.00200268	0.00203376	0.00206483	-	1.67085	1.67098	1.6711					
Probabilidade de bloqueio por fluxo				N. médio de links usados pelo fluxo							
1	3	0.71	6	1	0.000308374	0.000317224	0.000326075	-	1.55583	1.55622	1.55662
1	3	0.05	2	21	0.0780374	0.0788448	0.0796522	-	1.67463	1.67545	1.67628
1	5	0.55	6	1	0.000291777	0.000308221	0.000324665	-	2.50366	2.5037	2.50374
1	5	0.08	2	21	0.0776319	0.0783134	0.0789949	-	2.58025	2.58069	2.58114
1	6	0.8	6	1	0.000293948	0.000304855	0.000315763	-	2.53263	2.53276	2.5329
1	6	0.02	2	21	0.077659	0.0782992	0.0789394	-	2.66894	2.67018	2.67142
3	5	3.416	6	1	0	3.71677e-008	9.24682e-008	-	2.00272	2.00275	2.00278
3	5	0.36	2	21	4.79971e-005	5.63147e-005	6.46322e-005	-	2.09992	2.1001	2.10028
3	5	0.044	1	63	0.000903706	0.000980474	0.00105724	-	2	2	2
3	6	3.716	6	1	1.40496e-007	4.43649e-007	7.46802e-007	-	1.65003	1.65027	1.65051
3	6	0.23	2	21	0.000235965	0.000250582	0.0002652	-	1.83728	1.83791	1.83853
3	6	0.046	1	63	0.00238084	0.0024886	0.00259636	-	1.5049	1.50515	1.5054
5	6	3.094	6	1	7.65319e-007	1.10625e-006	1.44719e-006	-	1.65982	1.66015	1.66049
5	6	0.49	2	21	0.000248048	0.000260091	0.000272135	-	1.73846	1.73893	1.73941
5	6	0.031	1	63	0.00248378	0.00263219	0.00278061	-	1.50755	1.50778	1.508

Prob de pico estimada por fluxo
0.0780374 0.0788448 0.0796522

Ocupacao Média por link

1	2	1	2	63	32.9131%	20.7211	20.7353	20.7494
1	3	1	3	63	32.9131%	20.7211	20.7353	20.7494
2	3	2	3	252	16.4894%	41.5284	41.5533	41.5782
2	5	2	5	252	19.2534%	48.4863	48.5185	48.5506
2	4	2	4	252	0.978432%	2.45601	2.46565	2.47529
3	4	3	4	252	18.9049%	47.6045	47.6403	47.6761
3	6	3	6	252	33.6807%	84.8307	84.8753	84.92
4	5	4	5	252	20.9002%	52.627	52.6685	52.7101
4	6	4	6	252	27.5277%	69.328	69.3698	69.4115
5	6	5	6	252	35.1851%	88.6223	88.6665	88.7108

TSimulado (horas) TSimulacao (segundos)

1.56104e+006	14400
1.56013e+006	14400
1.56171e+006	14400
1.56123e+006	14400
1.56175e+006	14400
1.56196e+006	14400
1.56519e+006	14400
1.56144e+006	14400
1.56122e+006	14400
1.56192e+006	14400

Caso de Estudo C

InvBand+PEN+RP

Prob media de bloqueio global
0.0207212 0.0247533 0.0287854

Tráfego médio suportado pela rede
132.451 132.5 132.548

Prob média de bloqueio dos VC12				-	N. médio de links usados pelos VC12				
1.48631e-005	1.54119e-005	1.59606e-005		-	1.99368	1.9938	1.99392		
Prob média de bloqueio dos VC3				-	N. médio de links usados pelos VC3				
0.0406317	0.0409392	0.0412466		-	2.09219	2.09245	2.09272		
Prob média de bloqueio dos VC4				-	N. médio de links usados pelos VC4				
0.000881648	0.000933656	0.000985665		-	1.66916	1.66923	1.6693		
Probabilidade de bloqueio por fluxo					N. médio de links usados pelo fluxo				
1	3	0.71	6	1	0.00030759	0.000319923	0.000332257 - 1.56289	1.56336	1.56383
1	3	0.05	2	21	0.0812371	0.0819545	0.082672 - 1.71319	1.71409	1.71499
1	5	0.55	6	1	0.000306515	0.000321355	0.000336194 - 2.50386	2.50391	2.50397
1	5	0.08	2	21	0.0816009	0.0819366	0.0822722 - 2.60368	2.60415	2.60463
1	6	0.8	6	1	0.000314541	0.000329325	0.000344109 - 2.5402	2.54042	2.54065
1	6	0.02	2	21	0.0802092	0.0815906	0.082972 - 2.6114	2.61223	2.61306
3	5	3.416	6	1	0	1.63926e-007	3.50243e-007 - 2.00149	2.0015	2.00151
3	5	0.36	2	21	5.47812e-005	6.22035e-005	6.96258e-005 - 2.10379	2.10406	2.10434
3	5	0.044	1	63	0.000949739	0.00101838	0.00108702 - 2.00001	2.00002	2.00004
3	6	3.716	6	1	0	0	0 - 1.66659	1.66691	1.66724
3	6	0.23	2	21	4.2469e-005	4.80885e-005	5.37081e-005 - 1.7887	1.78928	1.78986
3	6	0.046	1	63	0.000799915	0.000868497	0.00093708 - 1.50314	1.50326	1.50337
5	6	3.094	6	1	1.46311e-009	1.80901e-007	3.60339e-007 - 1.68645	1.68671	1.68696
5	6	0.49	2	21	3.67259e-005	4.31493e-005	4.95727e-005 - 1.7306	1.7309	1.7312
5	6	0.031	1	63	0.000798369	0.00091409	0.00102981 - 1.50424	1.50441	1.50457

Prob de pico estimada por fluxo
0.0812371 0.0819545 0.082672

Ocupacao Média por link

1	2	1	2	63	33.101%	20.836	20.8536	20.8712
1	3	1	3	63	33.101%	20.8361	20.8536	20.8712
2	3	2	3	252	17.4444%	43.9301	43.9598	43.9895
2	5	2	5	252	20.236%	50.9612	50.9947	51.0283
2	4	2	4	252	1.27285%	3.19654	3.20758	3.21863
3	4	3	4	252	25.1726%	63.3997	63.4349	63.4702
3	6	3	6	252	26.496%	66.7298	66.7698	66.8099
4	5	4	5	252	27.0551%	68.154	68.1789	68.2038
4	6	4	6	252	27.4303%	69.1126	69.1245	69.1363
5	6	5	6	252	27.6942%	69.7573	69.7894	69.8216

TSimulado (horas) TSimulacao (segundos)

1.56194e+006	14400
1.56010e+006	14400
1.56131e+006	14400
1.56343e+006	14400
1.56125e+006	14400
1.56156e+006	14400
1.56510e+006	14400
1.56131e+006	14400
1.56159e+006	14400
1.56177e+006	14400