Arquitecturas para Redes Privadas Virtuais em ATM

Jorge Carapinha, Rui Valadas

Resumo **- Este artigo analisa as principais potencialidades da tecnologia ATM para estabelecer e explorar redes privadas virtuais. São analisados três modelos básicos: redes privadas virtuais baseadas em VPCs permanentes extremo-a-extremo, redes privadas virtuais baseadas em VCCs permanentes e redes privadas virtuais baseadas em sinalização.**

Abstract **- This paper provides an overview of the main strengths of the ATM technology to establish virtual private networks (VPN) over ATM public networks. Three basic models are analysed: VPN based on permanent end-to-end VPCs, VPN based on permanent VCCs and VPN based on switched VCCs.**

I. INTRODUÇÃO

Após um período em que as redes ATM dos operadores de telecomunicações tiveram um carácter essencialmente experimental e serviram para testar e validar a tecnologia, parece ter sido atingido um nível de maturidade que permite lançar comercialmente os primeiros serviços baseados em ATM, mesmo se não explorando ainda todas as suas potencialidades.

No domínio das redes empresariais, o ATM oferece uma alternativa vantajosa às técnicas tradicionais de interligação de redes privadas, frequentemente pouco atractivas em termos económicos e carecendo da flexibilidade que é exigida pela nova realidade das empresas, muito mais dinâmica e instável do que no passado. Outras tecnologias alternativas de rede pública como RDIS, *frame relay* ou *SMDS*, embora sejam a solução para alguns problemas, estão por natureza limitadas por factores de diversa ordem (características de tráfego, largura de banda…) e têm por isso um potencial de evolução reduzido.

Apesar do elevado potencial do ATM como tecnologia integradora para um vasto leque de serviços e aplicações, o aproveitamento pleno de todas as suas potencialidades está ainda longe de ser atingido, quer pela imaturidade de algumas normas, com reflexos negativos na capacidade de interfuncionamento de diferentes sistemas, quer pelo ainda escasso número de aplicações orientadas especificamente para esta tecnologia. Neste cenário, existem motivos para supor que a introdução do ATM nas redes públicas se processará de uma forma gradual e progressiva, garantindo em cada fase a coexistência com as tecnologias tradicionais e com os serviços e aplicações nelas baseados, de forma a evitar rupturas e rentabilizar investimentos anteriores. O investimento numa nova tecnologia, como é neste caso o ATM, deve ser feito em função do seu mercado potencial.

Um serviço talhado para explorar as características do serviço público ATM na sua fase introdutória e para funcionar como alavanca para o seu desenvolvimento é o de rede privada virtual [2]. Este termo designa normalmente um serviço prestado por um fornecedor de serviços ou um operador público que consiste em oferecer a uma organização ou empresa um conjunto de facilidades de comunicação funcionalmente idênticas às de uma rede privada.

O termo *rede privada virtual*, ou RPV (na terminologia anglo-saxónica, *Virtual Private Network*, ou VPN), é utilizado em contextos muito diversos, representando conceitos nem sempre coincidentes. Uma RPV está normalmente associada à utilização de recursos de uma *rede pública*, por natureza partilhada, para oferecer um serviço funcionalmente equivalente, na perspectiva do utilizador ou cliente do serviço, ao de uma *rede privada*.

Uma RPV é antes de mais uma *rede*, no sentido em que está associada ao fornecimento de recursos de comunicação. É *privada*, uma vez que a sua utilização é supostamente restrita a um grupo fechado de utilizadores. Finalmente, é *virtual* porque os recursos em que assenta não existem enquanto entidades físicas.

A tendência para o estabelecimento de redes privadas virtuais no cenário das redes empresariais resulta de um conjunto de factores de diversa natureza: económicos, técnicos, de regulamentação, ou relacionados com a organização das empresas.

Na sua forma mais elementar, o tipo de funcionalidade suportada pelo ATM em redes empresariais pode ser a simples substituição de circuitos dedicados por circuitos virtuais ATM permanentes (também por vezes designados como "*linhas alugadas virtuais*"), ou seja, uma simples função de transporte. Este serviço básico pode ser visto como uma versão "mínima" do serviço de *rede privada virtual*. Mesmo neste cenário, o ATM oferece já um conjunto de características que o tornam uma alternativa aliciante se comparado com as soluções tradicionais. A partir deste cenário mínimo, o ATM proporciona um

conjunto de potencialidades que permitem desenvolver o conceito de RPV com graus de complexidade e sofisticação muito diversos. A sua capacidade intrínseca para suportar uma gama diversificada de serviços e aplicações constitui uma vantagem importante sobre outras tecnologias. Em cada fase do processo evolutivo das redes privadas virtuais ATM, as capacidades do serviço público que lhes serve de suporte reflectir-se-ão naturalmente nas arquitecturas que é possível estabelecer e nas funcionalidades que é possível explorar. Este trabalho faz um estudo das potencialidades do serviço público ATM na exploração de redes privadas virtuais, partindo do seu estado actual e considerando as principais fases da sua previsível evolução.

Após esta introdução, a secção II enquadra o conceito de RPV num modelo de referência geral de redes privadas de telecomunicações. A secção III apresenta os conceitos fundamentais de ATM mais relevantes na óptica deste trabalho. Na secção IV são apresentadas as potencialidades do ATM na definição e exploração de RPVs introduzidas pelo conceito de VPC (*Virtual Path Connection*). A secção V descreve três arquitecturas básicas de RPV com ATM. Finalmente, a secção VI apresenta as conclusões.

II. MODELO DE REFERÊNCIA

Uma RPV pode ser vista como uma componente de um domínio mais vasto que corresponde a uma Rede Privada de Telecomunicações, ou RPT.

Tradicionalmente, uma RPT é constituída por um conjunto de domínios privados, ou CPNs (do inglês, *Customer Premises Networks*), interligados entre si por ligações de longa distância.

Na Figura 1 é apresentado um modelo conceptual para uma RPT, constituído por cinco níveis níveis hierárquicos [8]. Partindo do nível mais elevado, cada nível resulta do anterior isolando um determinado elemento constituinte.

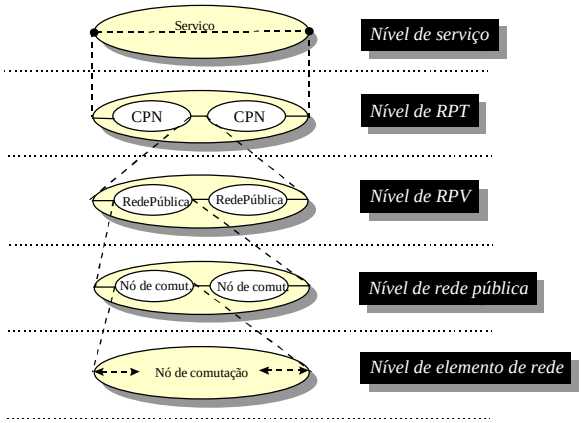

Figura 1: Modelo de referência para redes privadas.

Os cinco níveis representados acima podem ser sumariamente descritos da forma seguinte:

- *Nível de serviço*: nível de abstração mais elevado, correspondente à visão do utilizador, para o qual a topologia e os aspectos tecnológicos da rede são totalmente transparentes.
- *Nível de RPT*: nível que dá uma visão global dos recursos de telecomunicações utilizados pela rede privada para obter as facilidades de comunicação necessárias, e que pode englobar domínios pertencentes a diversas redes públicas e diversos domínios privados.
- *Nível de RPV*: nível que identifica as características topológicas e de conectividade de uma RPV, de forma transparente relativamente aos recursos da rede pública sobre os quais ela assenta.
- *Nível de rede pública*: nível que corresponde a visão dos recursos da rede pública (nós de comutação, *links* de interligação), do ponto de vista topológico e de conectividade, sobre os quais assenta uma RPV.
- *Nível de elemento de rede*: nível que identifica e caracteriza os recursos da RPV ao nível dos elementos de rede que a sustentam.

Neste novo cenário, é possível estabelecer uma correspondência entre cada um destes níveis e os diversos agentes intervenientes. A correspondência entre cada um dos cinco níveis de abstracção representados na Figura 1 e os agentes ou entidades envolvidos no processo pode ser feita da seguinte maneira:

Nível de serviço	-	*Utilizador*
Nível de rede privada	-	*Cliente*
Nível de RPV	-	*Fornecedor de serviço RPV*
Nível de rede pública *Nível de elemento de rede*	-	*Operador de rede pública*

Relativamente aos primeiros dois agentes, refira-se a distinção, nem sempre muito clara, entre *utilizador* e *cliente* do serviço. Neste contexto, designa-se por *utilizador* o agente que efectivamente utiliza o serviço, geralmente uma pessoa ou grupo de pessoas, e designa-se por *cliente* a entidade que contrata e paga esse serviço, geralmente uma empresa ou organização. Na perspectiva deste trabalho, os agentes *cliente* e *utilizador* podem ser tomados por uma única entidade, ficando assim o modelo reduzido a três agentes fundamentais:

- o *utilizador*/*cliente* do serviço;
- o *fornecedor do serviço*;
- o *operador de rede* que na prática pode coincidir ou não com o fornecedor de serviço.

O cliente, ou utilizador, contrata um serviço de telecomunicações caracterizado por um conjunto de parâmetros de qualidade ao fornecedor de serviço, o qual por sua vez contrata ao operador público a utilização de um conjunto de recursos de rede, com um determinado nível de desempenho.

O esquema da Figura 2 identifica, relativamente ao serviço de rede privada virtual, o papel principal de cada um destes três agentes. Note-se que por cada RPV existe um cliente e um fornecedor de serviço, mas poderá haver diversos operadores de rede.

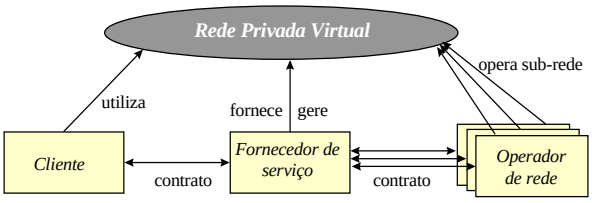

Figura 2: Agentes RPV

III. CONCEITOS FUNDAMENTAIS

O ATM é um tipo de tecnologia orientado à ligação, o que significa que a transmissão de informação é precedida do estabelecimento de uma ligação lógica entre os pontos extremos da comunicação. O ATM introduz dois conceitos fundamentais: Canal Virtual (VC de *Virtual Channel*) e Caminho Virtual ou Conduta Virtual (VP de *Virtual Path*).

Um VC corresponde a uma ligação lógica unidireccional entre duas entidades ATM, estabelecida dinamicamente ou numa base permanente, e é identificado pelo par VPI/VCI (*Virtual Path Identifier* / *Virtual Channel Identifier*) no cabeçalho da célula. Cada VC pode transportar um diferente protocolo ou tipo de tráfego. Um VP agrupa um conjunto de VCs com uma origem e um destino comuns. É identificado pelo campo VPI no cabeçalho de cada célula.

As funções de comutação executadas pelos diversos equipamentos de rede podem ser feitas com base no VPI apenas, ou com base tanto no VPI como no VCI. Por outro lado, um equipamento de rede pode fazer a comutação, quer de VPCs, quer de VCCs, usando ligações permanentes, estabelecidas no plano de gestão, ou com base em mecanismos automáticos de sinalização no plano de controlo. Ao primeiro tipo costuma dar-se o nome de *cross-connect* e ao segundo *comutador*. Normalmente, os *cross-connects* actuam apenas ao nível de VPC, enquanto os comutadores actuam aos níveis de VPC e VCC.

Com a agregação de múltiplas ligações num único VPC, mecanismos como policeamento ou CAC (*Connection Admission Control*) podem passar a ser executados apenas nos pontos extremos do VPC, libertando os nós de rede intermédios desse tipo de funções. Por outro lado, estes mecanismos passam a poder ser aplicados em bloco a um número restrito de grupos de ligações (VPCs), e não a um número elevado de ligações individuais (VCCs), como nas redes públicas comutadas convencionais.

Um mesmo meio de transmissão pode suportar diversos VPs. A Figura 3 ilustra a relação entre os conceitos de VC, VP e meio de transmissão.

Às ligações suportadas por um ou mais VCs ou VPs dá-se o nome de VCC (*VC Connection*) e VPC (*VP Connection*), respectivamente. Existe assim uma hierarquia de dois níveis na estrutura da informação nas ligações ATM: os VCCs são multiplexados nos VPCs que, por sua vez, são multiplexados nos *links* físicos. A

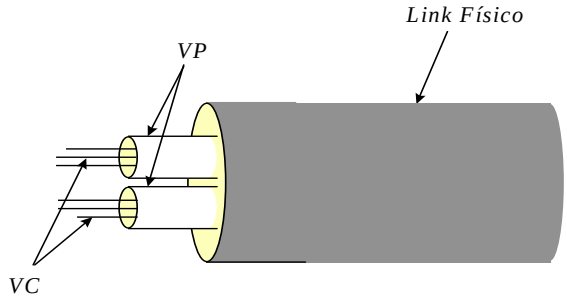

Figura 3: Relação VC / VP / link físico

Figura 4 representa a relação entre os conceitos de VCC, VPC e VP.

Podem definir-se três tipos de VPCs:

- *VPC extremo-a-extremo*: estende-se entre dois pontos de acesso à rede (entendendo-se aqui que um ponto de acesso à rede pertence ao domínio da rede privada, independentemente de ser ou não administrado pelo operador público - na prática pode corresponder a um comutador de acesso, um concentrador, um *multiplexer*, ou qualquer tipo de equipamento que permita o acesso a uma rede pública). Num VPC extremo-a-extremo todos os VCCs são transportados transparentemente ao longo da rede, o que significa que entre os seus pontos extremos só pode haver *cross-connects*, ou melhor, elementos de rede executando unicamente funções de *cross-connect* sobre esse VPC.
- *VPC Utilizador-rede:* estende-se entre um ponto de acesso à rede e um nó de rede executando terminação de VPCs (comutador ou *cross-connect* VC).
- *VPC Rede-rede:* estende-se entre dois pontos terminadores de VPCs na rede.

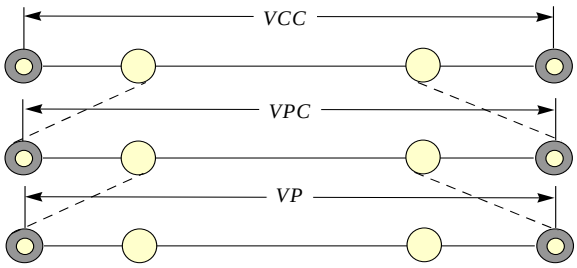

Figura 4: Relação VCC / VPC / VP

A Figura 5 clarifica a relação entre os diversos tipos de VPCs identificados acima.

Diversas estratégias para gerir recursos associados a VPs têm sido estudadas e propostas. Uma questão frequentemente discutida é a das vantagens e desvantagens da multiplexagem estatística *versus* determinística ao nível de VP e de VC. Uma solução baseada exclusivamente em multiplexagem estatística ao nível de VCCs (isto é, sem utilizar VPCs) produziria sem dúvida melhores resultados em termos de optimização de recursos, mas tornava o controlo de ligações muito mais complicado. Por outro lado, a realização de

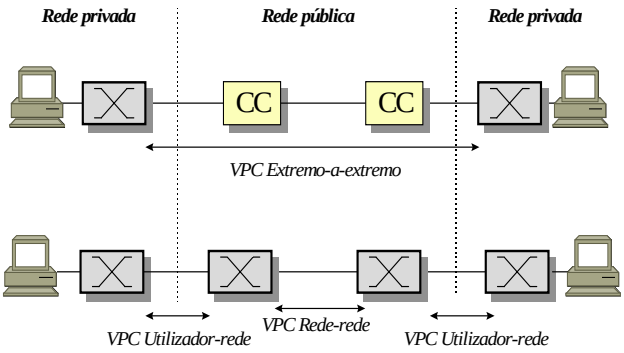

Figura 5: Tipos de VPCs numa rede pública ATM

multiplexagem determinística ao nível de VP, com a multiplexagem estatística realizada apenas ao nível de VC, implica alguma ineficiência na gestão de recursos em grau tanto maior quanto mais elevado for o número de VPs.

IV. O VP COMO FERRAMENTA NA DEFINIÇÃO DE RPVS

A existência de dois níveis distintos na camada ATM, VP e VC, constitui uma ferramenta que permite definir com grande flexibilidade um conjunto diversificado de opções para a configuração de rede, com um impacto directo nas características das redes privadas virtuais sobre ela estabelecidas. Uma vantagem da utilização de VPCs, particularmente relevante no contexto deste trabalho, é a facilidade para estabelecer uma estrutura de redes lógicas sobreposta à rede física, funcionando como uma primeira aproximação ao conceito de *rede privada virtual* em ATM. A utilização de VPCs facilita a criação e a reconfiguração de redes logicamente distintas e independentes entre si sobre uma infra-estrutura física comum.

A multiplexagem determinística de VPs tem uma importante aplicação nas redes privadas virtuais por permitir executar os mecanismos de controlo e gestão de recursos dentro de cada VPC independentemente dos VPCs com que partilha os *links* físicos, com base unicamente na atribuição de um valor fixo de largura de banda a cada VP. Desta forma, é possível estabelecer RPVs tirando partido unicamente das características

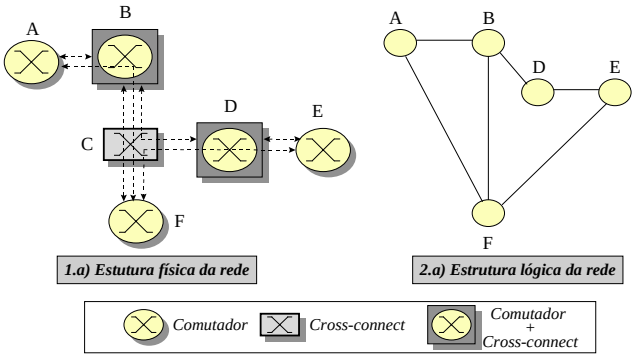

Figura 6: Comparação estrutura física / lógica de uma rede ATM

próprias da camada ATM.

A Figura 6 ilustra o estabelecimento de uma rede lógica de VPs a partir de uma rede física composta por cinco nós de três tipos: *cross-connects* de VPs, comutadores de VCs e nós mistos suportando as duas funcionalidades [10].

A título de exemplo, a Figura 7 representa uma configuração lógica alternativa à da Figura 6. Os esquemas 2.a) e 2.b) da Figura 6 e da Figura 7 representam duas estruturas lógicas diferentes para uma mesma rede física, que foram obtidas modificando apenas os VPCs estabelecidos entre os diversos comutadores, em 1.a) e 1.b). Do ponto de vista da arquitectura lógica da rede, só têm interesse os pontos terminais de cada VPC, ou seja, a função de *cross-connect* é irrelevante (note-se que o ponto C não aparece nos esquemas do lado direito).

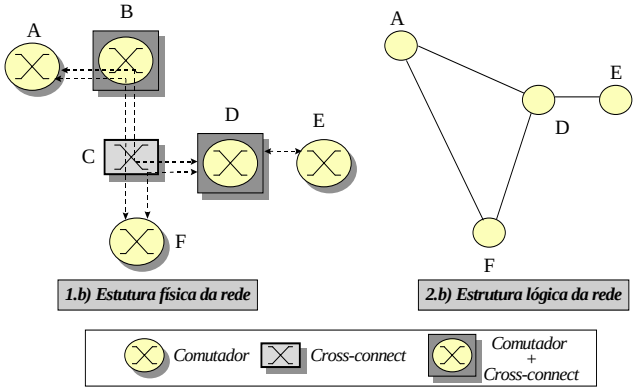

Figura 7: Configuração lógica alternativa

As duas redes lógicas representadas nas figuras anteriores constituem efectivamente redes privadas virtuais, no sentido em que definem recursos reservados da rede pública que podem ser associados exclusivamente a uma rede privada.

Neste contexto, um conceito importante é o de *nó RPV*. Um nó RPV é um nó de rede pública (isto é, um comutador) que executa funções relacionadas com uma rede privada virtual, normalmente fazendo terminação de VPCs associados à RPV. Retomando ainda os exemplos das figuras anteriores, o nó B é um nó RPV no caso da Figura 6, mas não no caso da Figura 7, uma vez que aí desempenha unicamente funções de *cross-connect*. Numa dada rede pública, o conjunto de nós RPV será assim um subconjunto de todos os nós que compõem a rede. A caracterização dos recursos ocupados por uma RPV constituída por n nós RPV e m classes de qualidade de serviço pode assim ser feita por uma matriz M de dimensão n x n x m, sendo M_{xyc} a largura de banda para tráfego da classe c entre os nós x e y (obviamente, M_{xyc} e M_{yxc} não são necessariamente iguais).

V. ARQUITECTURAS PARA RPVS ATM

O conceito de rede privada virtual está sempre associado à oferta de um serviço funcionalmente equivalente a uma rede privada, utilizando a infra-

estrutura partilhada de uma rede pública. Dependendo da tecnologia que lhe serve de suporte, esse conceito pode ser realizado de formas diversas. O ATM introduz um conjunto de novas e mais poderosas capacidades. Este capítulo pretende fazer uma avaliação dessas capacidades, em função de diversos cenários para o serviço público ATM.

A. Arquitectura baseada em VPCs permanentes extremo-a-extremo

Do ponto de vista da rede pública, nesta arquitectura de RPV todos os VPCs são extremo-a-extremo, isto é, são sempre terminados em pontos extremos da ligação e nunca em nós intermédios da rede. Esta arquitectura de RPV será característica sobretudo da primeira fase das redes públicas ATM, baseadas ainda exclusivamente em *cross-connects* de VPs, o que não significa que não seja igualmente aplicável a redes suportando funcionalidades mais avançadas (nomeadamente, redes comutadas).

Neste cenário, a interligação completa na camada ATM de todos os pares origem-destino requer uma estrutura de VPCs extremo-a-extremo em malha, como indicado na Figura 8.

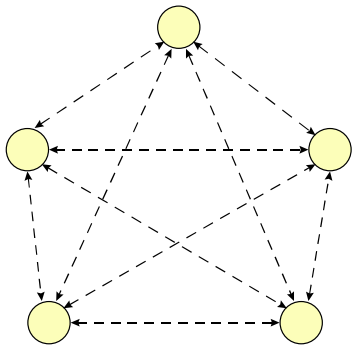

Figura 8: Rede com VPCs permanentes extremo-a-extremo em malha

Para uma rede privada virtual com *n* pontos de acesso e conectividade completa entre eles, serão necessários *n*(*n*-1)/2 VPCs bidireccionais extremo-a-extremo. Daqui resulta uma desvantagem importante deste método - a sua limitada capacidade de crescimento.

A existência de uma rede privada virtual é neste caso transparente para os nós da rede pública, os quais executam apenas funções de *cross-connect*, isto é, fazem o cruzamento das ligações em função unicamente do VPI, ignorando a existência de VCs. Isto significa que os parâmetros de qualidade de serviço garantidos pela rede são aplicáveis a VPCs e não a ligações individuais.

De certa forma, esta solução pode ser vista como a evolução das actuais redes privadas empresariais baseadas em linhas dedicadas, distinguindo-se delas essencialmente pela diferença importante de uma maior flexibilidade na gestão dos recursos da rede. Essa flexibilidade envolve dois aspectos fundamentais. Por um lado, a largura de banda em cada sentido da comunicação pode ser definida com uma granularidade virtualmente ilimitada (de 1 kbit/s até centenas de Mbit/s), ao contrário dos circuitos alugados que admitem normalmente apenas um conjunto limitado de débitos, normalmente igual nos dois sentidos. Por outro lado, a capacidade de gestão do ATM e a sua flexibilidade para suportar reconfigurações dinâmicas é muito superior à normalmente oferecida por soluções baseadas em circuitos dedicados.

Num cenário caracterizado exclusivamente por VPCs permanentes extremo-a-extremo, a entidade mais básica reconhecida pela rede é o VP, pelo que toda a informação relacionada com VCCs individuais é ignorada pela rede pública. Qualquer acção da rede susceptível de produzir uma alteração da estrutura temporal da informação (nomeadamente, *shaping* ou policeamento) pode assim ter um efeito indesejável, sobretudo se vários tipos de ligações forem multiplexados no mesmo VP. Neste cenário, será aconselhável efectuar uma segregação de classes de qualidade de serviço por VPC.

A gestão da largura de banda de uma RPV suportada por VPCs extremo-a-extremo pode ser feita ao nível de VP (entre os diversos VCs constituintes) e ao nível de grupos de VPs (no caso de uma mesma rede privada virtual ocupar vários VPs no mesmo *link*) [4]. Estes dois casos são analisados separadamente a seguir.

A.1 Gestão de recursos por VP

A gestão de tráfego por VPC, e não por VCCs individuais, simplifica os mecanismos da rede, mas pode ter igualmente alguns efeitos negativos. É o que acontece no caso em que há descarte de células em resultado de uma acção de policeamento da rede, afectando VCCs que não contribuiram para essa situação. Uma vez que a rede pública só reconhece a existência de VPs, o descarte das células afectará indiscriminadamente todas as ligações. Para atenuar este problema, poderão ser usados alguns métodos que permitem gerir dinamicamente a largura de banda associada a cada VP. De um modo geral, o que se pretende com a gestão dinâmica de recursos é estabelecer mecanismos de controlo de acesso a um determinado recurso partilhado da rede de forma a garantir a sua justa utilização, em função das necessidades em cada momento, evitando desperdícios ou sub-utilização de recursos e ao mesmo tempo prevenindo situações de sobrecarga. Dois métodos possíveis são a aplicação de um túnel de sinalização extremo-a-extremo (*PVP Tunneling*) e a utilização de mecanismos de controlo de fluxo.

A primeira destas soluções consiste no estabelecimento e libertação de circuitos dentro de um VPC permanente extremo-a-extremo entre um par origem-destino, utilizando um canal de sinalização com VCI=5. Entre redes privadas pode ser utilizado qualquer protocolo de sinalização suportado pelos respectivos comutadores, por exemplo, IISP ou um qualquer protocolo proprietário. Sempre que for necessário estabelecer, modificar ou libertar uma ligação extremo-a-extremo, é feita a troca de mensagens de sinalização entre comutadores de acesso, de forma a verificar se há recursos

disponíveis, no caso de se pretender utilizar mais recursos, ou libertar recursos anteriormente utilizados. Esta solução é simples de implementar e a sua transparência relativamente à rede pública permite a utilização de protocolos proprietários entre os dois extremos da ligação. Sendo os VPCs multiplexados deterministicamente ao longo da rede, pelo facto de as ligações serem extremo-a-extremo, os nós origem e destino têm a capacidade de controlar as ligações sem necessidade de intervenção dos nós intermédios da rede pública.

Uma solução alternativa consiste na utilização, nos VPCs atribuído à RPV, de mecanismos de controlo de fluxo do tipo ABR (*Available Bit Rate*) [7, 14]. Estes mecanismos têm algumas vantagens e limitações. Para tipos de tráfego caracterizados pela alternância entre períodos de "rajadas" e períodos de "silêncio", estes protocolos oferecem uma elasticidade muito maior em comparação com o método anterior, havendo nesses casos vantagem na sua utilização. As principais desvantagens do ABR são o facto de o controlo da execução do processo estar localizado nos pontos extremos da ligação, e não na rede e ainda a sua reduzida eficiência em *loops* de controlo muito longos. Deve notar-se que o ponto extremo da ligação, na perspectiva do protocolo ABR, não corresponde necessariamente ao equipamento terminal, mas pode ser desempenhado por um equipamento de acesso intermédio, podendo existir "por trás" desse equipamento um qualquer outro protocolo.

A.2 Gestão de recursos por GVP

Em diversos trabalhos (por exemplo, [4], [5], [6]) é proposto um esquema de gestão de recursos de uma RPV com base em Grupos de VPs (GVPs). Um GVP pode ser visto como uma entidade lógica que agrega um grupo de VPs (um ou mais VPs) reservados para utilização de uma mesma entidade, neste caso uma rede privada virtual. A Figura 9 ilustra este conceito.

O fornecedor de serviço associa uma dada largura de banda a um GVP, definindo assim a capacidade máxima total que pode ser ocupada por todos os VPs que constituem o GVP, ou seja, os recursos atribuídos à RPV nesse *link*, podendo o cliente do serviço ter a capacidade de reconfigurar cada VP individualmente. Neste caso, a rede pública executa os mecanismos de policeamento, não sobre cada VP individualmente, mas sobre o bloco completo de VPs que constituem o GVP. Uma tal abordagem corresponde na prática a criar na estrutura da informação do ATM um nível adicional ao de VP e VC (GVP), exigindo dos nós da rede a capacidade para executar mecanismos de controlo, nomeadamente policeamento, sobre essa nova entidade.

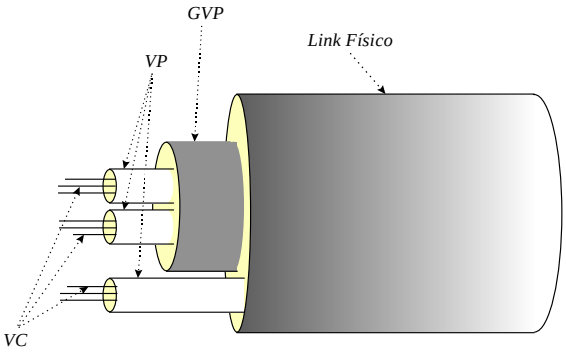

Figura 9: Relação entre link físico, GVP, VP e VC

Um modelo de RPV baseado em GVPs é exemplificado na Figura 10, em que a largura de banda de cada GVP é partilhada por diversos pares origem-destino da mesma RPV.

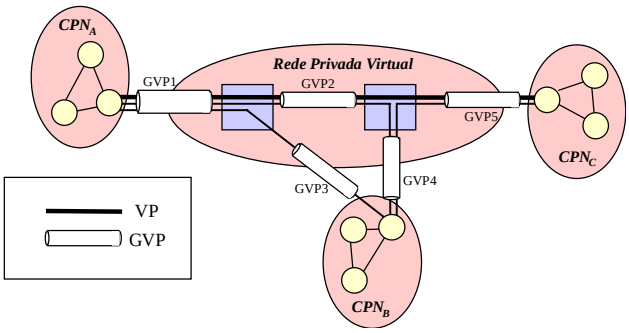

Figura 10: RPV baseada em GVPs

Obviamente, para evitar potenciais pontos de congestionamento no interior da rede deverá garantir-se que o somatório das larguras de banda dos GVPs à entrada e à saída de cada nó são iguais. Tomando como exemplo a RPV representada na Figura 10, a largura de banda de GVP1 deve ser igual à soma das larguras de banda de GVP2 e GVP3.

Os GVPs e correspondentes VPs são estabelecidos inicialmente pelo sistema de gestão do operador de rede na fase de configuração da RPV. O uso de GVPs não tem impacto nos mecanismos de comutação de células nos *cross-connects*, nos quais só é relevante o valor do VPI.

B. Arquitectura baseada em VCCs permanentes

O modelo de rede privada virtual apresentado atrás tira partido da capacidade intrínseca do ATM de criar redes lógicas virtuais unicamente pela utilização de VPCs permanentes extremo-a-extremo. A vantagem principal desse modelo reside no facto de não exigir funcionalidades específicas por parte da rede - para criar uma rede privada virtual basta fazer a interligação dos vários pontos de acesso por VPCs extremo-a-extremo, sendo a existência de VCCs ignorada pela rede pública. Essa simplicidade é paga com a necessidade de estabelecer um número de VPCs que cresce muito rapidamente com o aumento do número de pares origem-destino. Isto significa que uma solução baseada em VPCs extremo-a-extremo é viável apenas para valores de *n* não muito elevados.

Uma solução alternativa consiste na terminação de VPCs da rede privada virtual em nós intermédios da rede pública, a que chamámos anteriormente nós RPV. A

terminação de VPCs em nós intermédios da rede implica que seja feita nesses pontos a comutação de VCCs, e as respectivas funções de agregação e desagregação de ligações em VPCs. Deixa assim de ser necessário estabelecer uma estrutura em malha ao nível de VPC entre todos os possíveis pares origem-destino da RPV.

Tal como no caso anterior, supõe-se que a rede pública não suporta sinalização, o que significa que o controlo das ligações - estabelecimento, libertação, modificação - é executado por procedimentos no plano de gestão.

Numa configuração deste tipo, todos os pares origem-destino estão interligados por um ou mais VCCs suportados por uma sequência de VPCs utilizador-rede e rede-rede reservados para utilização da RPV.

A Figura 11 ilustra este conceito para uma RPV com quatro pontos de acesso (A, B, C, D) e um nó RPV executando terminação de VPCs.

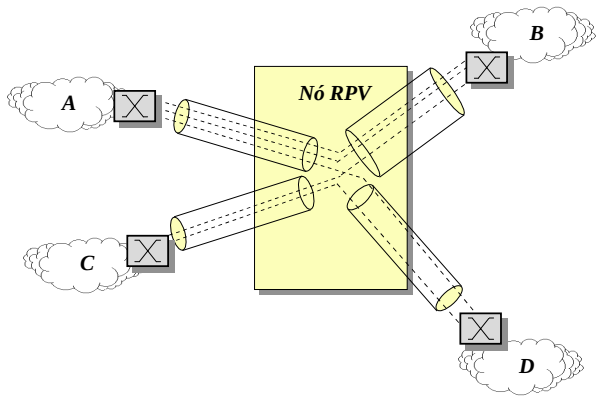

Figura 11: Nó RPV com comutação de VCCs

Ao contrário do cenário anterior, em que a cada VPC estava associado um e um só par origem-destino, um mesmo VPC pode neste caso ser partilhado por diversos pares origem-destino. Daqui resulta a possibilidade de organizar os recursos da rede de uma forma mais eficaz, em função unicamente do tipo de tráfego que transporta, independentemente dos seus pontos origem e destino. Por outro lado, é possível obter com este método uma economia significativa no número de VPCs necessários para uma RPV. Numa situação em que uma RPV com n pontos de acesso suportasse m tipos de tráfego distintos, segregados por VPC, teríamos de acordo com a arquitectura anterior que recorrer a $n\cdot(n\text{-}1)\cdot m$ VPCs extremo-a-extremo distintos, enquanto neste caso seriam necessários apenas $n\cdot m$ VPCs utilizador-rede. Obviamente, esta vantagem é tanto mais significativa quanto maior for o valor de n.

Cada par origem-destino é neste caso ligado, não por um, mas por uma sequência de VPCs. Este facto complica a gestão dos recursos da rede e do controlo de tráfego, nomeadamente ao nível dos mecanismos de CAC e policeamento. Em termos de CAC, a dificuldade deste método resulta do facto de os pontos extremos de cada ligação, ao contrário da arquitectura com VPCs extremo-a-extremo, não poderem ter um conhecimento completo dos recursos disponíveis em todos os VPCs ao longo do percurso de uma determinada ligação. Por este motivo, o método do túnel de sinalização não é aplicável neste caso.

No que respeita ao policeamento, o facto de nós da rede pública funcionarem como terminadores de VPCs complica consideravelmente o processo. No caso da arquitectura anterior, em que existiam apenas VPCs permanentes extremo-a-extremo, a rede pública só tinha que executar funções de policeamento para cada par origem-destino num único ponto, em princípio no ponto de acesso à rede pública, ignorando os VCCs transportados por esse VPC. Neste caso, o policeamento terá que ser efectuado em vários pontos da rede pública.

Sempre que dois ou mais VCCs partilham o mesmo VPC à saída de um nó da rede pública, sendo a soma das larguras de banda máximas desses VCCs superior à largura de banda do VPC respectivo, existirá potencialmente um problema de sobrecarga.

A Figura 12 ilustra o caso de um nó de rede fazendo a terminação dos VPCs identificados como VPC1, VPC2 e VPC3, com uma largura de banda de x Mbit/s bidireccionais e com origem nas CPNs 1, 2 e 3 respectivamente, transportando VCCs indicados na figura por linhas a tracejado. Se o tráfego entre os três pontos de acesso for razoavelmente balanceado, uma configuração deste tipo funcionará sem problemas. Supondo que em determinada circunstância, por exemplo, as CPNs 1 e 2 tentam transmitir simultaneamente informação para CPN3 com débitos y_1, y_2, tais que $y_1 + y_2 > x$, ocorrerá nesse caso uma situação de congestionamento no *buffer* de saída 3 do *cross-connect*, apesar de cada um dos VPCs 1 e 2 ter cumprido o respectivo contrato de tráfego (isto é, os débitos nos VPCs 1 e 2 serem inferiores a x Mbit/s). Isto significa que, pelo facto de existir uma interdependência no tráfego entre diferentes VPCs, um policeamento com base em VPCs individuais não é neste caso aplicável.

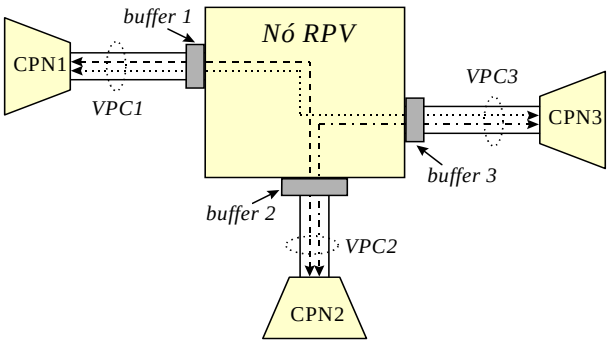

Figura 12: Terminação de VPCs num nó RPV

Uma forma possível de circunscrever o problema do congestionamento a uma RPV, garantindo que a qualidade de serviço dos VPCs que partilham o mesmo *link* não é afectada, consiste na execução de policeamento em *buffers* de saída por VP. Este tipo de solução, embora eficaz do ponto de vista do controlo de congestionamento, é no entanto pouco satisfatório do ponto de vista do utilizador, uma vez que uma situação de sobrecarga em

qualquer nó da rede gera necessariamente perda de células e consequentemente degradação do serviço. Em alternativa, ou complementarmente a este tipo de solução, podem ser utilizados métodos preventivos que reduzem a probabilidade de ocorrência de situações de congestionamento. A ausência de mecanismos de sinalização nos nós de rede, que é um pressuposto deste modelo, limita as possibilidades de um controlo efectivo, nomeadamente através de CAC pelos nós da rede. Em [1] são analisadas algumas formas possíveis de fazer um controlo preventivo contra situações de congestionamento em nós intermédios da rede.

A superioridade das técnicas baseadas em comutação de VCCs sobre o modelo de VPCs permanentes extremo-a-extremo, é avaliada em [9] com base em simulações computacionais entre 2 e 20 vezes. Esse trabalho confirma ainda que as diferenças de custo entre o método baseado na utilização de VPCs extremo-a-extremo e os métodos baseados na comutação de VCCs na rede é tanto mais significativa quanto maior for o número de pares origem-destino na RPV.

C. Arquitectura baseada em sinalização

As soluções anteriores são formas relativamente simples de implementar uma RPV sobre uma infra-estrutura de rede pública ATM. Essa simplicidade é no entanto paga com um certo grau de ineficiência na utilização dos recursos da rede.

A capacidade da rede pública para suportar mecanismos de sinalização constitui o principal factor de distinção entre este modelo e os anteriores. A utilização de ligações comutadas em vez de ligações permanentes permite um nível de eficiência muito mais elevado na utilização dos recursos da rede.

À semelhança das arquitecturas anteriores, o VPC pode ser usado como entidade básica delimitadora dos recursos da RPV numa rede pública. A existência de comutação de VCCs nos nós da rede pública implica que seja efectuada nesses pontos terminação de VPCs. Contudo, ao contrário do caso anterior em que os VCCs eram estabelecidos estaticamente por mecanismos de gestão, neste caso as ligações são estabelecidas dinamicamente "a pedido", por procedimentos de sinalização. Isto implica que cada nó de rede que efectua terminação de VPCs associados a uma rede virtual deve ter o conhecimento dos recursos a ela associados.

Em relação às arquitecturas de RPV anteriores, a sinalização introduz ainda a capacidade importante de estabelecer ligações de e para pontos localizados física e administrativamente fora do domínio da RPV.

Apesar de nesta arquitectura todo o processo de estabelecimento de ligações ser baseado em mecanismos de sinalização, a reserva de recursos de uma RPV pode continuar a ser feita com base em VPCs.

A Figura 13 ilustra uma configuração típica de uma RPV baseada em ligações comutadas, composta pelos domínios privados CPN1, CPN2 e CPN3. As linhas contínuas representam *links* físicos entre cada par de nós de rede e as linhas a tracejado representam VPCs associados a essa RPV particular.

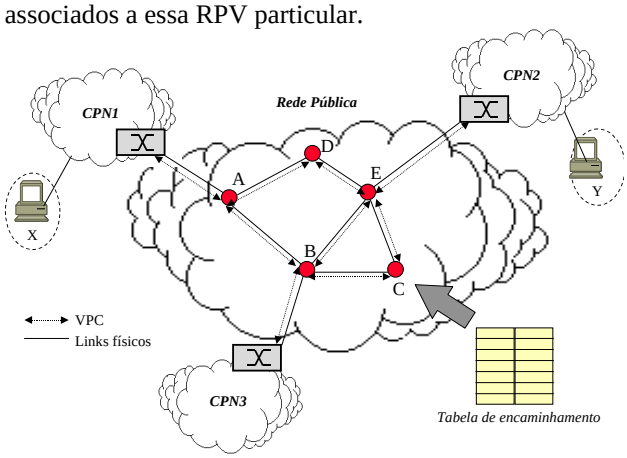

Figura 13: Exemplo de configuração de uma RPV baseada em sinalização

Quando o utilizador *X* localizado em CPN1 pretende estabelecer uma ligação com o utilizador *Y* localizado em CPN2, o comutador de acesso à rede pública em CPN1 estabelece os procedimentos normais de ligação à rede pública.

No estabelecimento da ligação entre X e Y, todos os nós RPV envolvidos devem identificar a associação entre a chamada e a respectiva RPV e aplicar o encaminhamento adequado tendo em conta os recursos reservados para essa RPV. Neste caso, um determinado nó de rede poderá ter a possibilidade de escolher entre vários caminhos alternativos para uma determinada ligação, em função de um determinado critério, por exemplo a carga momentânea de cada um dos *links*. No caso da Figura 13, o nó *A* poderia optar por um dos *links A-B* ou *A-D*.

Normalmente, numa rede ATM comutada a decisão sobre o encaminhamento de uma chamada tem como variáveis de entrada o endereço do destino, a classe de qualidade de serviço da ligação e as condições de tráfego em cada *link* nesse instante. No caso de uma RPV, os algoritmos de CAC e encaminhamento têm como restrição adicional o facto de a chamada dever ser encaminhada utilizando os recursos reservados para essa RPV específica, ou seja, os VPCs associados a essa RPV. Isto implica, por exemplo, rejeitar o estabelecimento de uma ligação se não houver recursos reservados para a RPV, mesmo que haja recursos disponíveis na rede. Os comutadores de rede envolvidos, ou seja, os nós RPV, têm assim que "conhecer" a existência de redes privadas virtuais.

Uma questão que se coloca neste processo é a forma como os nós da rede detectam que uma determinada ligação pertence a uma RPV específica, de forma a aplicar os procedimentos de CAC e encaminhamento adequados. Uma solução possível é a análise do endereço do destino, eventualmente em conjugação com o da origem. Neste caso, os endereços associados a RPVs poderiam ter uma característica particular que permitisse a sua identificação (por exemplo, um prefixo). Outra solução, preconizada

em [4], é a inclusão na sinalização do plano de controlo de informação específica sobre redes privadas virtuais.

Ao contrário do modelo baseado em VCCs permanentes, neste caso os mecanismos de CAC executados pelos comutadores da rede pública garantem um controlo eficaz sobre os recursos da RPV e minimizam a probabilidade de ocorrência de situações de congestionamento.

Neste cenário, a utilização de um plano de numeração próprio pode ser feita desde que os comutadores de acesso do lado da rede privada estabeleçam a correspondência entre os dois tipos de endereços.

C.1 Tipos de acesso à RPV

Um factor distintivo importante desta arquitectura relativamente às anteriores é a possibilidade de alargar o acesso à RPV a pontos situados fisica e administrativamente fora do seu domínio, ou seja, definir acessos "*on-net*" e "*off-net*". O acesso "*on-net*" é feito a partir de um ponto registado na rede, utilizando recursos dedicados da RPV ou uma ligação comutada. O acesso "*off-net*" é feito a partir de um ponto não registado, logo requerendo procedimentos de controlo de acesso e autenticação adequados num qualquer nó RPV da rede. Esta facilidade possibilita o acesso a uma RPV a partir de um ponto qualquer da rede pública, e não apenas de pontos localizados em domínios pertencentes à rede privada. Em função deste critério, podem assim distinguir-se os três tipos de ligações representados na Figura 14.

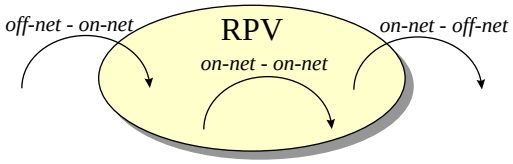

Figura 14: Tipos de acesso a uma RPV

Para ilustrar o mecanismo básico do acesso "*off-net*" (ou seja, duma ligação *off-net* - *on-net*), retomemos o exemplo da Figura 13, supondo que se pretende estabelecer agora um acesso à RPV a partir de um ponto Z, como representado na Figura 15. O nó F, que não pertence à RPV, identifica o pedido de ligação como fazendo parte de uma RPV e limita-se a fazer prosseguir o pedido até ao primeiro nó RPV que tenha capacidade para o processar. Aí, se Z for um ponto de acesso registado, o nó RPV poderá fazer uma validação em função unicamente dos endereços origem e destino. Se Z não for um acesso registado (ou seja, *off-net*) o nó RPV deve executar um conjunto de procedimentos que permitam validar com segurança que o utilizador Z é de facto autorizado a aceder a essa RPV, nesse caso através de informação específica que permita autenticar a sua identificação. Deve notar-se que um acesso "*off-net*", por aceder à RPV através de uma ligação comutada normal da rede pública, não tem qualquer tipo de garantia de qualidade de serviço no troço da ligação localizado fora do domínio da RPV.

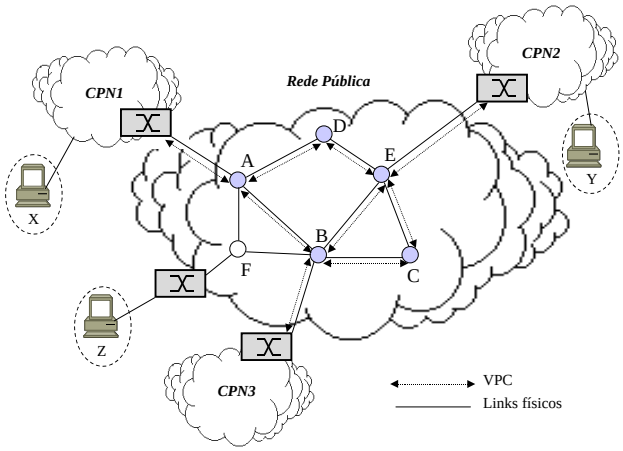

Figura 15: Acesso "off-net" a uma RPV

C.2 Gestão de recursos

Tirando partido das potencialidades da sinalização e da capacidade para executar encaminhamento dinâmico, esta arquitectura permite um grau de flexibilidade na gestão de recursos muito maior do que nos casos anteriores.

Nesta arquitectura, o fornecedor de serviço gere essencialmente recursos "virtuais", no sentido em que, embora mapeáveis directamente em recursos físicos da rede, estes são-lhe transparentes. Relativamente à conectividade entre dois pontos de acesso à rede, a um fornecedor de serviço interessa apenas conhecer as suas características em termos de largura de banda e qualidade de serviço. Pelo contrário, a perspectiva do operador de rede será sobretudo a das características físicas e topológicas da rede necessárias para oferecer o serviço solicitado.

A Figura 16 representa um troço de uma rede pública suportando uma RPV entre dois pontos A e G, interligados por três VPCs: [ad1, de, ef, fg1], [ad2, df, fg2] e [ab, bc, cg] (por razões de simplicidade, admitamos que todos os VPCs suportam a mesma classe de qualidade de serviço). Sempre que o comutador no ponto *A* recebe um pedido de ligação para *G* no âmbito da RPV, pode optar por qualquer um dos três VPCs, em função de um conjunto de critérios que o operador definir. Um esquema deste tipo permite ao operador gerir os recursos da sua rede com muito maior flexibilidade do que seria possível com os métodos anteriores. Por outro lado, a distribuição dos recursos associados a uma RPV por vários *links* permite atenuar os potenciais reflexos negativos resultantes da indisponibilidade desses recursos para o tráfego normal.

Neste novo cenário, os planos de intervenção do operador de rede e do fornecedor de serviço RPV são claramente distintos. O fornecedor de serviço passa a gerir um conjunto de recursos da rede, abrangendo domínios de um ou mais operadores públicos, sobre os quais pode

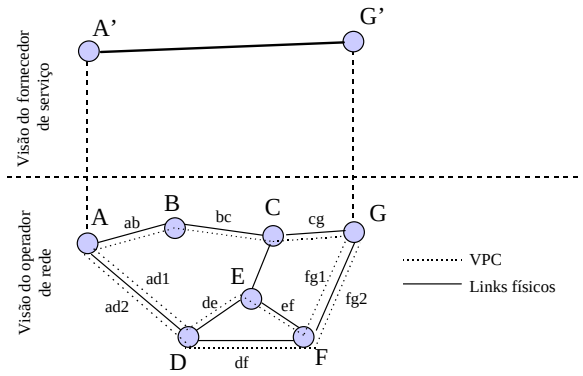

Figura 16: Visão da rede pública para fornecedor de serviço e operador de rede

desenvolver e explorar diferentes RPVs fornecidas a diferentes clientes. Um ponto crítico neste cenário é o interfuncionamento entre sistemas de gestão do fornecedor de serviço e do operador ou operadores de rede.

Apesar de esta arquitectura ser baseada em ligações comutadas, a delimitação dos recursos de uma RPV pode continuar a ser feita, como nos casos anteriores, por VPCs permanentes. Uma vez que os recursos da rede pública são limitados, é necessário garantir um conjunto mínimo de recursos para uma RPV, de forma a protegê-la de situações de sobrecarga na rede. Na perspectiva oposta, a existência de VPCs pode representar um limite ao volume de recursos ocupados por uma RPV. Uma solução de compromisso pode ser encontrada usando o esquema representado na Figura 17. Suponhamos que a largura de banda de um determinado *link* é partilhada por três RPVs como mostra a figura. Para cada uma das três RPVs indicadas existe um conjunto de recursos que podem ser designados por "zona garantida". Se em determinada circunstância é feito um pedido de chamada, por exemplo em RPV1, e não há recursos disponíveis dentro da sua "zona reservada", isso não significa necessariamente a rejeição da chamada pelo mecanismo de CAC, uma vez que a chamada pode ser estabelecida na zona de tráfego não-RPV. Desta forma garante-se um conjunto de recursos mínimo por RPV, mas a RPV poderá fazer uso de recursos fora da zona "garantida", se for necessário.

Dependendo das características do tráfego, a utilização de mecanismos de sinalização para controlar o estabelecimento e a libertação de ligações pode ter

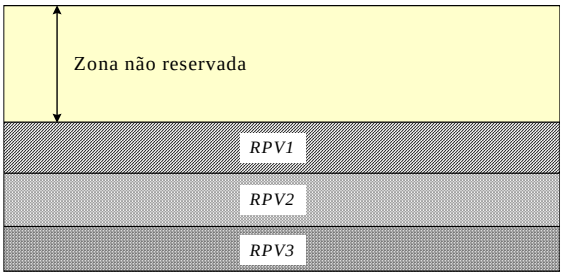

Figura 17: Reserva de recursos com várias RPVs

igualmente consequências negativas. De um modo geral, uma reduzida taxa de pedidos de chamada de elevada capacidade tende a afectar o desempenho da rede de transporte. Pelo contrário, uma elevada taxa de pedidos de chamada de reduzida capacidade tende a degradar a capacidade de resposta da rede de sinalização. Em [3] é demonstrado que uma carga excessiva na rede de sinalização pode impôr uma sub-utilização da rede de transporte, ou seja, uma sub-utilização de recursos. Nas redes ATM, os VPCs constituem uma forma de simplificar o mecanismo de estabelecimento de ligações, à custa de alguma ineficácia na gestão de recursos da rede associada à reserva de recursos em cada VP. Os VPCs são por isso uma peça fundamental na determinação do ponto de equilíbrio entre a eficácia da gestão de recursos e a carga exigida à rede pelos mecanismos de sinalização.

C.3 Características da sinalização

Existem fundamentalmente dois sistemas de sinalização de rede para ATM: o B-ISUP, baseado no SS#7 e desenvolvido pelo ITU-T [13], e o PNNI desenvolvido pelo ATM Forum [12]. O primeiro sistema está sobretudo associado às redes públicas e o segundo às redes privadas, o que não significa que uma rede pública não possa suportar PNNI. Haverá no entanto uma forte probabilidade de que redes públicas e privadas suportem tipos de sinalização diferentes. Neste cenário, assumindo que o PNNI se deverá impôr como solução para o domínio das redes privadas, uma questão da maior importância é a avaliação dos possíveis cenários para a sinalização em RPVs.

À medida que o protocolo PNNI for sendo usado num maior número de redes privadas, colocar-se-à o problema da interligação de domínios privados baseados em PNNI através de redes públicas, normalmente não baseadas em PNNI, e utilizando outros métodos de encaminhamento. Fundamentalmente, o problema que se coloca é o de saber como será possível executar os mecanismos do protocolo PNNI descritos anteriormente, tendo pelo meio uma rede que não está preparada para os suportar.

Numa primeira aproximação, a rede pública pode ser vista como um sub-domínio da rede privada, sobre o qual é passada informação de sinalização e encaminhamento transparentemente por *PVP tunneling*, e o respectivo PVPC tratado com um *link* virtual PNNI. Este é contudo um método limitado que impede um uso eficiente e flexível dos recursos da rede pública, além de ser uma solução pouco robusta na ocorrência de falhas.

A oferta de um serviço comutado por parte da rede pública ATM pode resolver algumas dessas limitações. Deve contudo ser encontrada uma forma de ultrapassar, ou pelo menos minimizar, a provável incapacidade das redes públicas para suportar PNNI. Nesse sentido, é de prever que o PNNI venha a incorporar algumas funcionalidades que permitam um mais fácil interfuncionamento com redes não baseadas em PNNI.

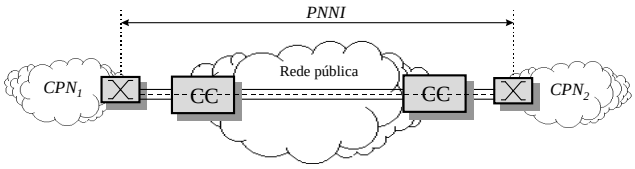

Figura 18: PNNI através de túnel de sinalização

São a seguir consideradas vários cenários de interfuncionamento entre redes privadas e rede pública.

- Rede pública não suporta sinalização

Neste caso, a única forma de transportar informação de sinalização através da rede pública consiste no chamado túnel de sinalização já referido atrás. Assim, não existe um verdadeiro interfuncionamento entre rede privada e pública, uma vez que esta se limita a passar transparentemente a informação de sinalização no VC com VCI=5 de cada VP até ao comutador de entrada no domínio privado remoto. Duas redes suportando PNNI podem ser interligadas utilizando este método, como mostra a Figura 18. O VPC extremo-a-extremo é visto na perspectiva do PNNI como um *link* normal, igual a qualquer outro *link* no domínio privado.

Este procedimento, embora aceitável como solução transitória numa altura em que a rede pública não suporta ainda sinalização, tenderá a ser substituída por soluções efectivas de interfuncionamento com redes privadas, à medida que for sendo introduzida sinalização na rede pública.

- Rede pública suporta sinalização mas não PNNI

Neste caso, cada CPN da RPV estará ligada à rede pública por um interface UNI. Uma diferença essencial entre as redes públicas e as redes privadas ATM consiste na utilização de esquemas de endereçamento distintos: enquanto as redes públicas usam normalmente o formato E.164, as redes privadas baseiam-se no formato NSAP. É assim necessário executar funções de mapeamento entre os dois tipos de endereçamento nos equipamentos de acesso à rede pública. A Figura 19 [11] ilustra este processo - os terminais origem e destino com endereços NSAP *A* e *B* estão ligados a domínios privados diferentes, interligados por uma rede pública ATM através de interfaces de acesso com endereços públicos E.164 *A* e *B*. O mapeamento entre os dois tipos de endereçamento poderá ser feito, pelo menos numa fase inicial, através da configuração manual dos comutadores de acesso à rede pública.

Se a rede pública suportar apenas o formato E.164, o domínio privado deverá indicar o endereço E.164 na respectiva mensagem de sinalização para a rede pública,

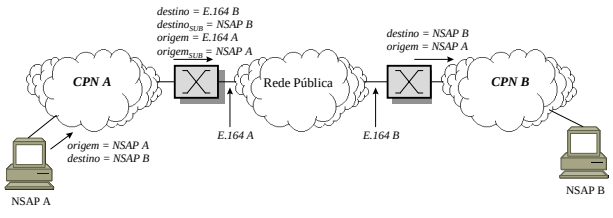

Figura 19: Interfuncionamento de sinalização pública / privada

podendo o endereço privado ser transportado transparentemente pela rede pública no sub-endereço. Se, pelo contrário, a rede pública suportar endereçamento com formato NSAP, esse tipo de endereço pode ser transportado no respectivo elemento de informação de endereço (*Called Party Number*).

- Rede pública suporta PNNI como interface externo

Neste caso, a rede pública é baseada internamente num protocolo de rede que poderá não ser PNNI (provavelmente SS#7/B-ISUP) mas tem interfaces externos PNNI que possibilitam o interfuncionamento com redes privadas com base neste protocolo. Do ponto de vista do protocolo PNNI, a rede pública passará então a funcionar globalmente como um *peer group* PNNI. A Figura 20 ilustra esta situação para o caso em que quatro domínios privados correspondentes a outros tantos *peer groups* PNNI estão interligados através da rede pública.

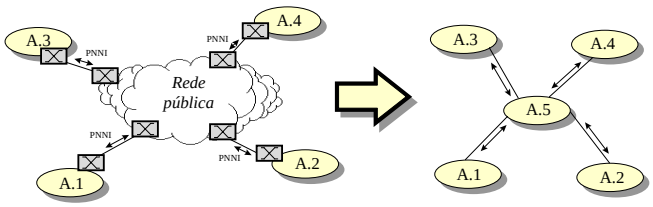

Figura 20: Rede pública como "peer group" PNNI

Neste caso, uma vez que toda a rede pública corresponde a um *peer group* único, a sua estrutura não tem que ser dada a conhecer externamente.

- Rede pública suporta PNNI internamente

Na solução anterior a rede pública suportava PNNI apenas como interface externo. Não é necessariamente de excluir a utilização de PNNI internamente na rede pública. No caso de isso acontecer, a rede pública poderia funcionar do ponto de vista dos mecanismos de sinalização e encaminhamento como um ou mais domínios privados, dando inclusivamente à rede privada a possibilidade de tomar decisões sobre encaminhamento na rede pública, em função da informação divulgada pelo protocolo de encaminhamento PNNI. Naturalmente, esta funcionalidade choca com o modelo tradicional das redes públicas, em que a sua estrutura interna é sempre invisível do ponto de vista dos utilizadores, e não é claro que venha efectivamente a ser realizada.

VI. CONCLUSÕES

A tecnologia ATM surge como a solução mais adequada para suportar os crescentes requisitos das novas redes empresariais, baseadas num largo espectro de serviços e aplicações, e ao mesmo tempo a forma mais flexível de gerir e controlar os recursos de redes privadas virtuais.

Em particular, o conceito de VPC como elemento delimitador de recursos da rede e agregador de ligações confere ao ATM um conjunto de capacidades de grande

relevância para o estabelecimento de redes privadas virtuais.

Sendo o ATM uma tecnologia complexa, a sua introdução nas redes públicas será efectuada de uma forma faseada. Partindo de um cenário mínimo, o ATM tenderá evoluir no sentido de suportar um número crescente de funcionalidades. À medida que novas capacidades vão sendo introduzidas nas redes públicas ATM, vai sendo igualmente possível criar redes privadas virtuais com um crescente grau de sofisticação. Um marco fundamental neste processo, que permitirá dar um salto importante nas potencialidades das redes privadas virtuais sobre ATM, será a introdução da capacidade de sinalização e o controlo automático de ligações nas redes públicas.

Na secção IV foram descritos três modelos de rede privada virtual sobre redes públicas ATM e identificados os requisitos básicos impostos à infra-estrutura de rede pública por cada um:

- Rede privada virtual baseada em VPCs permanentes extremo-a-extremo;
- Rede privada virtual baseada em VCCs permanentes;
- Rede privada virtual baseada em redes com sinalização.

A primeira destas arquitecturas constitui a forma mais simples de explorar uma rede privada virtual sobre uma infra-estrutura de rede pública, com base apenas em VPCs extremo-a-extremo. Na sua forma mais elementar, a implementação de uma rede privada virtual sobre ATM pode assentar unicamente na capacidade dos VPCs para delimitar recursos. A existência de uma rede privada virtual é neste caso transparente para a rede pública, cabendo aos sistemas no domínio privado fazer a gestão da fracção dos recursos da rede pública que que lhe estão reservados e, eventualmente, aplicar procedimentos de sinalização.

A segunda arquitectura pode ser vista como uma evolução da primeira, distinguindo-se dela fundamentalmente pela possibilidade de fazer terminação de VPCs da rede privada virtual em nós de comutação intermédios da rede pública. Evita-se desta forma a utilização exclusiva de VPCs extremo-a-extremo, e os custos daí decorrentes, mas a gestão de recursos da rede privada virtual torna-se mais complexa e deixa de ser transparente para o operador de rede.

A terceira arquitectura exige à rede pública a capacidade para suportar sinalização, o que, salvo raras excepções, ainda não se verifica. Em contrapartida, só este terceiro modelo permite um conjunto de funcionalidades importantes numa RPV. Do ponto de vista dos utilizadores, refira-se a capacidade para estabelecer ligações de e para pontos exteriores à RPV, mediante mecanismos de controlo de acesso adequados. Do ponto de vista dos operadores, passa a ser possível distinguir claramente os planos da infra-estrutura física da rede e dos recursos da RPV - donde resulta uma distinção clara entre os papéis do operador e do fornecedor de serviços. Um problema relevante neste caso é o interfuncionamento entre sistemas de sinalização privados, sendo o PNNI o protocolo dominante, e sistemas de sinalização públicos, orientados para o modelo do sistema de sinalização nº7 do ITU-T.

REFERÊNCIAS

[1] "Redes Privadas Virtuais em ATM", Jorge Carapinha, Dissertação de Mestrado, Departamento de Electrónica e Telecomunicações da Universidade de Aveiro, Abril 1998

[2] "A New Direction for Broadband ISDN", Stephen Walters, IEEE Communications Magazine, Setembro 1991

[3] "Virtual Path Control for ATM Networks with Call Level Quality of Service Guarantees", Nikolaos Anerousis, Aurel A. Lazar, IEEE/ACM Transactions on Networking, Abril 1998

[4] "Some Traffic Issues in the Design of Virtual Private Networks Over ATM", Fabrice Guillemin, Isabelle Hamchaoui, International Journal of Communication Systems, 1996

[5] "Resource Management in Virtual Private Networks Over ATM", Isabelle Hamchaoui, Fabrice Guillemin, IEEE ATM'97, Maio 1997

[6] "Customer Management and Control of Broadband VPN Services", M. C. Chan, A. A. Lazar, R. Stadler, International Symposium on Integrated Network Management (IM'97), San Diego, Maio 1997

[7] "ATM Traffic and Bandwidth Management using Virtual Private Networks", Mario Gerla, Shivi Fotedar, 3rd International Telecommunications Congress, Fevereiro 1995

[8] "A Generic Architecture for VPN Configuration Management", Jean-Paul Gaspoz, Jean-Pierre Hubaux, Simon Znaty, Journal of Network and Systems Management, Vol. 4, Nº. 4, Dezembro 1996

[9] "ATM Virtual Private Networks", Shivi Fotedar, Mario Gerla, Paola Crocetti, Luigi Fratta, Communications of the ACM, Fevereiro 1995

[10] "Resource Management with Virtual Paths in ATM Networks", V. J. Friesen, J. J. Harms, J. W. Wong, IEEE Network, Setembro/Outubro 1996

[11] "ATM Internetworking", Anthony Alles, Cisco Systems Inc., http://www.cisco.com/warp/public/614/12.html, Maio 1995

[12] "Private Network-Network Interface Specification Version 1.0 (PNNI 1.0)", ATM Forum, Março 1996

[13] ITU-T Recommendation Q.2761-4 "Broadband Integrated Services Digital Network (B-ISDN), Signalling System No.7 B-ISDN User Part (B-ISUP), 1995

[14] ITU-T Recommendation I.371 "Traffic Control and Congestion Control in B-ISDN", Dezembro 1995