**TUTORIAL N° 1**

**Modelos para Redes Modo Pacote Comutadas Orientadas a Conexão**

**1- OBJETIVOS**

O objetivo primordial do presente tutorial é o de apresentar o Modelo Overlay e o Modelo Par para a constituição de redes modo pacote comutadas orientadas a conexão, que operam por circuitos virtuais, evidenciando a prevalência atual do Modelo Par e as razões para esse fato.

Os exemplos de redes modo pacote operando no Modelo Overlay são as redes X.25, Frame Relay e ATM. No momento atual, o único exemplo de uso do Modelo Par são as redes MPLS.

Subsidiariamente, este tutorial tem os seguintes objetivos:

- Apresentar, de forma abrangente, os conceitos relativos a redes modo pacote comutadas;

- Apresentar, como fundamento e em linhas gerais, as redes modo pacote comutadas sem conexão, comparando-as com as redes modo pacote comutadas orientadas a conexão por circuitos virtuais;

-Apresentar as redes modo pacote comutadas orientadas a conexão operando no Modelo Overlay (X.25, Frame Relay e ATM);

-Apresentar as redes modo pacote comutadas orientadas a conexão operando no Modelo Par, que hoje se resumem nas redes MPLS;

- A partir das deficiências e da ineficiência das redes orientadas a conexão que operam no Modelo Overlay, apresentar as vantagens das redes modo pacote comutadas orientadas a conexão no Modelo Par, ou seja, as vantagens das redes MPLS.

A apresentação deste tutorial é original em grande parte. Para a sua elaboração, o autor baseou-se em sua experiência profissional, em conceitos estabelecidos por órgãos de padronização internacional, assim como na observação do que se passou, e ainda se passa com redes MPLS.

Buscou-se, neste tutorial, o estabelecimento de uma linha cronológica da evolução das redes modo pacote comutadas orientadas a conexão, principalmente na passagem do ATM, representando o Modelo Overlay, para o MPLS.

**2- INTRODUÇÃO**

Comutação consiste no estabelecimento, em um comutador, de uma conexão ou de uma associação entre extremidades de dois ou mais links, estando essas extremidades localizadas em portas de entrada e de saída do comutador.

 Na comutação modo circuito (c*ircuit switching*), a conexão ou associação entre as extremidades de links fica, de forma espacial ou temporal, deterministicamente estabelecida, sendo as informações comutadas automaticamente da porta de entrada para a(s) porta(s) de saída, sem que haja necessidade de qualquer identificação explícita nas informações comutadas.

 Na comutação modo pacote (*Packet Switching*), ao contrário, a associação entre extremidades de links é expressa por tabelas *cross-connect* contidas nos comutadores. Os identificadores para entrada nessas tabelas, contidos nos quadros comutados, são endereços de destino em redes modo pacote sem conexão (por datagramas), ou são labels inseridos nesses quadros em redes modo pacote orientadas a conexão.

Conforme o ITU-T, os circuitos (reais ou virtuais) comutados podem ser obtidos por comutação em demanda ou por comutação (semi) permanente.

A comutação em demanda realiza-se tipicamente por meio de sinalização, que ocorre no plano de controle da rede, no pressuposto (não obrigatório) de que as conexões (circuito reais ou virtuais) sejam de curta duração.

A comutação (semi) permanente, por sua vez, é tipicamente realizada por cross--conexão, no plano de gerenciamento, quando a comutação se realiza por comandos administrativos. Pressupõe-se, porém não obrigatoriamente, que as conexões (semi) permanentes sejam de longa duração.

Na comutação modo pacote por circuitos virtuais, por exemplo, os circuitos comutados em demanda são referidos como SVCs (*Switched Virtual Circuits*), conhecidos no Brasil como CVCs (circuitos virtuais comutados). Os circuitos obtidos por comutação (semi) permanente são referidos como PVCs (*Permanent Virtual* *Circuits*), conhecidos no Brasil como CVPs (circuitos virtuais permanentes).

**3 - COMUTAÇÃO MODO PACOTE**

As redes modo pacote comutadas podem operar sem conexão ou orientadas a conexão.

 As redes comutadas sem conexão são referidas como CLNs (c*onnectionless networks*), enquanto as redes comutadas orientadas a conexão são referidas como CONs (c*onnection-oriented networks*).

Nas CLNs, a comutação ocorre com base nos endereços de destino contidos em datagramas. Nas CONs, a comutação baseia-se em labels inseridos arbitrariamente nos cabeçalhos dos quadros, com o propósito de identificar os circuitos virtuais.

As CLNs apresentam vantagens e desvantagens com relação às CONs. Em linhas gerais, as CLNs têm na ampla conectividade o seu ponto forte, mas pecam em termos de desempenho (engenharia de tráfego, OAM robusto, comutação automática de proteção, etc...).

As CLNs possibilitam a transmissão ponto a ponto, multicast e broadcast. Além disso, as CLNs atendem naturalmente às aplicações ponto a ponto, ponto a multiponto (ou multiponto com raiz) e multiponto a multiponto.

As CONs, ao contrário das CLNs, possibilitam elevado desempenho, mas não atendem simples e eficientemente às aplicações ponto a multiponto e, principalmente, às aplicações multiponto a multiponto.

Os exemplos hoje existentes de CLNs são as redes IP e as redes Bridged Ethernet, enquanto as redes X.25, Frame Relay, ATM e MPLS representam os exemplos de CONs.

**4 - REDES MODO PACOTE COMUTADAS ORIENTADAS A CONEXÃO**

No quadro atual que se apresenta a partir das redes MPLS, as redes modo pacote comutadas orientadas a conexão passaram a ser classificadas da seguinte forma:

- Redes modo pacote comutadas orientadas a conexão no Modelo Overlay;

- Redes modo pacote comutadas orientadas a conexão no Modelo Par (*Peer Model*).

Como se verá adiante neste tutorial, o Modelo Par só é aplicável ao plano de controle de redes de camada 2 a isso destinadas. O único exemplo de rede de camada 2 operando atualmente no Modelo Par são as redes MPLS.

As redes modo pacote comutadas orientadas a conexão no Modelo Overlay (ou seja, redes X.25, redes Frame-Relay e Redes ATM) operam por NBMA (*Non-Broadcast Multiple Access*), tanto no plano de controle quanto no plano de dados.

No Modelo Par, o plano de controle opera com transmissão broadcast, por BMA, utilizando protocolos sem conexão baseados na arquitetura TCP/IP.

O plano de dados, no entanto, continua a operar em NBMA, embora com a vantagem de que os circuitos virtuais nesse tipo de rede têm as suas terminações nos comutadores de borda da rede de camada 2 de suporte. Isso significa que no plano de dados as redes MPLS são redes NBMA.

As CONs, inclusive as redes MPLS, são referidas como redes NBMA.

Vamos deixar mais clara a diferença entre a transmissão broadcast (também referida como transmissão BMA), que ocorre nas CLNs, e a transmissão NBMA, que ocorre nas CONs. Para isso vamos apresentar duas ilustrações utilizando configurações simples para melhor entendimento.

A Figura 1 ilustra a transmissão broadcast (BMA)



**Figura 1-Transmissão broadcast (BMA).**

Observa-se, nessa figura, que a transmissão BMA para múltiplos destinos ocorre pela replicação dos quadros transmitidos nos nós da rede envolvidos na transmissão. O nó (comutador ou terminal) de origem transmite apenas uma cópia de cada quadro multicast ou broadcast, cabendo à rede a sua distribuição.

A Figura 2 representa a transmissão NBMA para obter o mesmo resultado que o obtido na Figura 1 anterior.



**Figura 2-Transmissão NBMA.**

Como se verifica nessa figura, não ocorre replicação de quadros ao longo da rede. O nó de origem transmite um número de cópias de um quadro para a rede igual ao número de nós de destino (que é igual a três na figura). As três setas representam três circuitos virtuais ponto a ponto ou um circuito virtual ponto a multiponto centrado no nó A.

Na hipótese do nó A de origem ser um comutador, o terminal de origem a ele associado transmite apenas uma cópia de um quadro broadcast para esse nó de origem, que se encarrega da transmissão múltipla na rede por NBMA. Dessa forma, a transmissão NBMA não seria vista pelo usuário, que age como em uma transmissão broadcast.

Por essa razão, a transmissão NBMA é referida como transmissão pseudo - broadcast.

* 1. **Modelo Overlay**

As redes modo pacote comutadas orientadas a conexão tradicionais (X.25, Frame Relay e ATM) operam no paradigma referido como Modelo Overlay.

No Modelo Overlay, as redes de camada 2 de suporte transportam, envelopados em seus quadros, os quadros de dados e de controle das redes suportadas. É o que ocorre, por exemplo, quando o ATM transporta o IP. Outro exemplo é o transporte de Ethernet pelo Frame Relay.

Alguns campos dos quadros da rede transportada são envelopados transparentemente, ou seja, sem qualquer envolvimento da rede de camada 2 de suporte, não sofrendo qualquer alteração ao longo dessa rede. Importantes exemplos desses campos são os endereços IP de origem e de destino contidos em datagramas IP.

* + 1. **- Redes no Modelo Overlay**

 Existem três tipos de rede modo pacote comutada orientada a conexão no Modelo Overlay:

 - Redes X.25;

 - Redes Frame Relay;

 - Redes ATM.

Essas redes no Modelo Overlay, assim como o MPLS que opera no Modelo Par, utilizam *label swapping* em seus planos de dados, quando os valores de label são alterados em cada link da rede.

* + - 1. **– Redes X.25**

 As redes X.25 foram o primeiro tipo existente de CON. O auge dessas redes ocorreu na segunda metade da década de 70 e na década de 80. No Brasil, a primeira rede X.25 foi a RENPAC (Rede Nacional de Pacotes), lançada em meados da década de 80 pela EMBRATEL.

A tecnologia X.25 é extremamente robusta, no pressuposto da inexistência de redes de transporte confiáveis. As redes X.25 foram as únicas CONs operando em três camadas (camadas 1, 2 e 3).

A partir da consolidação do TCP/IP, a camada 3 em redes que suportam o IP passou a ser desnecessária, ficando o controle fim a fim das transmissões a cargo do protocolo TCP quando necessário.

O protocolo de enlace de dados utilizado na camada 2 e na camada 3 do X.25 é o LAP-B (*Link Access Procedure-Balanced Mode*).

O LAP-B é um protocolo da família HDLC (*High Level Data Link* *Control*), que opera no modo balanceado (quando em um único processo de sinalização estabelecem-se os dois sentidos de transmissão).

O LAP-B é um protocolo síncrono (por transmitir por meio de quadros sincronamente estruturados e delimitados), mas que, em termos de controle de sinalização entre terminais, opera no modo assíncrono (quando nenhum dos terminais controla a transmissão pelo outro terminal, operando ambos de forma independente).

A razão da obsolescência das redes X.25, ironicamente, é a sua robustez, que impede taxas de vazão de tráfego mais elevadas. O X.25 opera com velocidades da ordem de Kbps, com reduzidas taxas de vazão de tráfego.

Os circuitos virtuais são identificados por labels. No X.25, esses labels são referidos simplesmente como números de canal lógico.

O X.25 opera por SCVs (*Switched Virtual Circuits*) e por PVCs (*Permanent Virtual Circuits*). Os SVCs são constituídos por sinalização no plano de controle, enquanto os PVCs são constituídos por comandos administrativos, no plano de gerenciamento.

* + - 1. **– Redes Frame Relay**

Como uma nova opção ao X.25, aproximadamente na virada da década de 80 para a década de 90, foram lançadas as redes Frame Relay. O Frame Relay, que opera em velocidades da ordem de Mbps, permite taxas de vazão de tráfego mais elevadas que o X.25, taxas essas que de início satisfaziam as necessidades das aplicações da época.

O Frame Relay é o oposto ao X.25 no que se refere à robustez, e não possui a camada 3.

O protocolo de enlace de dados utilizado no Frame Relay é o *DL*-*Core* (*Data Link–Core*). O *DL-Core* resulta da retirada da função de controle do protocolo LAP-F (*LAP for Frame Relay).*

O uso do DL-Core é obrigatório apenas nos trechos DTE/DCE da rede FrameRelay. No interior da rede podem ser opcionalmente utilizadas outras tecnologias de rede, tais como ATM ou mesmo redes sem conexão.

O protocolo LAP-F é um protocolo similar ao LAP-B, mas enquanto o campo Endereço do LAP-B utiliza um octeto, o campo Endereço do LAP-F utiliza dois octetos, o que permite valores de DLCI (*Data Link Connection Identifier*) com 10 bits. O DLCI é o label utilizado em Frame Relay para a identificação de circuitos virtuais.

Embora seja possível teoricamente a constituição de SVCs por sinalização, o Frame Relay limitou-se à operação por PVCs.

O Frame Relay, por não utilizar o campo Controle do LAP-F, não oferece qualquer forma de controle de tráfego, como ocorre no X.25.

Em matéria de QoS com base em quadros transmitidos, o Frame Relay é limitado, permitindo apenas a indicação de precedência para descarte, pelo uso do bit DE (*Discard Elegibility*) contido no cabeçalho do quadro *DL-Core*.

O Frame Relay possibilita a transmissão de voz e de vídeo, ressalvados alguns cuidados especiais.

O Frame Relay seria supostamente substituído pelo ATM. No entanto, talvez pela sua qualidade e pelo fato de ter sido introduzido anteriormente, o Frame Relay coexistiu com o ATM, tendo inclusive, em alguns casos, maior longevidade que o ATM.

**4.1.1.3– Redes ATM**

 As redes ATM constituem-se na base de um amplo leque de serviços denominado RDSI-FL (Rede Digital de Serviços Integrados - Faixa Larga).

 O ATM foi especificado pelo ITU-T para redes públicas. Foi criado posteriormente o *ATM Forum,* com o propósito de coordenar, catalisar e agilizar a introdução do ATM. Como veremos no subitem 4.1.3 adiante neste tutorial, o *ATM Forum* veio a assumir um importante papel no desenvolvimento do ATM, particularmente em redes ATM privativas.

Além da oferta de diferentes serviços, o ATM opera com velocidades superiores às do Frame Relay.

* **Arquitetura ATM**

A Figura 3 apresenta a arquitetura ATM simplificada.



 **Figura 3 – Arquitetura ATM simplificada.**

Essa figura evidencia que a camada física e a camada ATM são camadas de rede, por envolverem os comutadores de toda a rede ATM. Evidencia também que a camada AAL opera fim a fim na rede ATM, não envolvendo, portanto, os comutadores no interior dessa rede.

O protocolo de enlace de dados, nos acessos e no interior da rede, é referido como protocolo ATM, que se situa na camada ATM.

 No protocolo ATM, a transmissão se realiza por quadros de pequeno tamanho, referidos como pacotes ATM, com 53 octetos, sendo também denominados células ATM. Essa transmissão envolve todos os comutadores da rede ATM.

Uma célula ATM é constituída por 5 octetos de cabeçalho e por 48 octetos de payload (dados).

Para a identificação dos circuitos virtuais no ATM, são utilizados dois labels hierarquizados, que são o VPI (*Virtual Path Identifier*) e o VCI (*Virtual Channel Identifier*).

Os circuitos virtuais no ATM, assim como no X.25 e no Frame Relay, têm as suas terminações localizadas nos terminais dessas redes.

Os VPIs possibilitam a constituição de conexões mais abrangentes, que são os caminhos virtuais. Os VCIs, que identificam os canais virtuais, por sua vez, permitem a capilarização dos caminhos virtuais, como mostra a Figura 4.



**Figura 4– Caminhos e canais virtuais no ATM.**

Nessa figura, uma interface ATM encontra-se multiplexada em caminhos virtuais (VPs), sendo exibidos os VPs com o VPI=100 e o VPI=200.

O VP com o VPI=100, por exemplo, está multiplexado em canais virtuais (VCs), sendo exibidos os VCs com o VCI=110, o VCI=120 e o VCI=130. O VPI=100 compõe com o VCI=110 o par 100/110, como mostra a figura.

A arquitetura ATM utiliza uma segunda camada, operando fim a fim acima da camada ATM, denominada camada AAL (*ATM Adaptation Layer*). Como mostra a Figura 3 apresentada anteriormente neste tutorial, a AAL não envolve os comutadores no interior da rede ATM.

A função primordial da AAL é intermediar e expandir os serviços prestados pela camada ATM, para que esses serviços se adaptem às diferentes aplicações que utilizam a rede ATM.

 Uma das missões da camada AAL é segmentação e a remontagem de quadros de dados. Os quadros AAL são segmentados no terminal ATM de origem, e, após a inserção dos cabeçalhos, esses segmentos vão constituir os pacotes ATM.

No terminal ATM de destino, a camada AAL remonta os quadros pelo reagrupamento dos respectivos pacotes.

Foram definidos pelo ITU-T as AAL 1, AAL 2, AAL 3/4 e AAL 5, para a adequada adaptação dos diferentes tipos de aplicação que utilizam o ATM.

Esses tipos de AAL destinam-se ao atendimento de aplicações como na relação abaixo:

-AAL 1: Aplicações isócronas CBR (*Constant Bit Rate*), como voz e vídeo em suas formas originais;

-AAL 2: Aplicações isócronas VBR (*Variable Bit Rate*), ou rt-VBR (*real time* *VBR*), como voz e vídeo com compressão;

-AAL ¾ e AAL 5: Aplicações anisócronas VBR, ou nrt-VBR (*non-real time* *VBR*), como as aplicações de dados em geral.

* **Serviços de Camada ATM ou ATCs**

Em redes modo pacote orientadas a conexão, a implementação de mecanismos de QoS (*Quality of Service*) pode ocorrer com base no conteúdo dos quadros ou com base em conexões virtuais. Observamos que essas duas opções não são mutuamente exclusivas em uma rede.

QoS baseada em quadros requer a disponibilidade de bits a isso destinados. Para a utilização de *Differentiated* *Service* (*DiffServ*), são necessários pelo menos três bits.

O Frame Relay e o ATM dispõem de apenas um bit em seus quadros com esse propósito, que indicam apenas a precedência para descarte. São o bit DE (*Discard* *Elegibility*) para o Frame Relay e o bit CLP (*Cell Loss Priority*) para o ATM.

Assim sendo, a aplicação de QoS nessas redes baseia-se praticamente em conexões virtuais, o que representa uma desvantagem operacional com relação a outras redes.

O MPLS, que será visto adiante neste tutorial, dispõe de três bits em seus labels genéricos, o que permite a utilização de *DiffServ*. Além disso, o MPLS faz uso intenso de QoS com base em conexões virtuais.

A aplicação de QoS com base em conexões virtuais, embora de enorme importância, engessa a aplicação de QoS, por não permitir o tratamento diferenciado para cada quadro de dados que trafega na rede. A QoS aplica-se indiscriminadamente para todos os quadros de dados na conexão virtual.

Para organizar a aplicação de QoS com base em conexões virtuais no ATM, o ITU-T e o *ATM Forum* definiram categorias de serviço de camada ATM, também referidas como ATCs (*ATM Transfer Capabilities*), destinadas ao atendimento das diferentes aplicações.

Essas categorias relacionam a aplicabilidade de parâmetros de tráfego e de QoS para as diferentes aplicações, que se refletem em comportamentos diferenciados da rede.

Infelizmente, como em outras circunstâncias, o ITT e o *ATM Forum* utilizaram diferentes terminologias e formas de definição.

Vamos apresentar abaixo a relação básica definida pelo ITU-T e pelo ATM Forum:

- DBR *(ITU-T) e* CBR *(ATM Forum);*

*-* SBR *(ITU-T) e* VBR *(ATM Forum*);

- ABR (*Available Bit Rate*), ambos;

- UBR (Unspecified Bit Rate), ambos.

É preciso atenção para não confundir aplicações CBR e VBR com ATCs CBR e VBR na nomenclatura do *ATM Forum*.

Na relação acima, DBR significa *Deterministic Bit Rate* e SBR significa *Statistical Bit Rate*.

O *ATM Forum* dividiu a classe VBR em rt-VBR e nrt-VBR, como na AAL.

As destinações das categorias DBR (CBR), SBR (VBR), rt-VBR e nrt-VBR foram apresentadas quando tratamos da AAL.

 As conexões virtuais ATM DBR e SBR compartilham enlaces físicos, utilizando a faixa passante desses enlaces físicos, com a possibilidade da existência de disponibilidade de faixa.

O propósito da definição do UBR e do ABR é a constituição de VCs que ocupem descompromissadamente (ou seja, no modo *best - effort*) essa eventual disponibilidade, otimizando dessa forma a utilização dos enlaces físicos.

+Diferentemente do UBR, contudo, no ABR é garantida uma taxa mínima, referida como MCR (*Minimum Cell Rate*) e especificado um controle de fluxo.

* **Roteamento e Sinalização**

Com o propósito de aprimorar o plano de controle do ATM, ou mesmo de aproximá-lo do Modelo Par, o *ATM Forum* emitiu, em 1996 o padrão *PNNI Draft Specification (PNNI Phase 1).*

A PNNI Fase 1 consiste na definição de dois protocolos: um protocolo de roteamento e o outro de sinalização.

O roteamento definido na PNNI Fase 1 utiliza o princípio de *constraining routing,* por disseminar, entre grupos de comutadores da rede ATM, alguns parâmetros relativos à topologia e aos recursos da rede.

Esses parâmetros envolvem a qualidade de serviço (QoS) da rede, e levam à escolha das rotas ideais para cada SVC a ser sinalizado.

O protocolo de roteamento na PNNI é considerado uma forma de protocolo *topology*-*state*.

 O roteamento na PNNI opera de forma hierarquizada, e, acompanhando o *constraining* *routing*, opera também em *source routing*. A quantidade de parâmetros conduzidos em *constraining routing* requer a realização de seu processamento de forma centralizada, conduzido ao *source routing*.

A sinalização na PNNI é utilizada como uma ponte para a transferência, no interior da rede ATM, de solicitações de SVCs geradas nas UNIs. Essa sinalização considera, também, informações sobre topologia de rede e sobre recursos providas pelo roteamento na própria PNNI.

Diferentemente da sinalização na UNI, que pode operar assimetricamente, a sinalização na PNNI é simétrica. Isso se deve ao fato de que a sinalização na PNNI ocorre entre comutadores, e não entre comutadores e terminais como na sinalização em UNIs.

Em decorrência da expectativa de atrasos na implementação da PNNI Fase 1, o *ATM Forum* emitiu, em 1995, o padrão IISP (*Interim Interswitch Protocol*), para uso provisório. O IISP, inicialmente denominado PNNI Fase 0, é um protocolo simplificado de sinalização baseado na sinalização das UNIs 3.0/3.1, utilizando roteamento manual.

* **Resolução de Endereços ATM**

São necessários processos para a resolução de endereços ATM de destino a partir dos endereços de destino da rede envelopada, processos esses diferenciados para o caso de SVCs e para o caso de PVCs.

A resolução de endereços no ATM será abordada com maiores detalhes no subitem 4.1.3 adiante neste tutorial, relativo à resolução de endereços no Modelo Overlay em geral.

* **ATM versus STM**

A denominação ATM indica o uso do modo assíncrono de transferência de informações (ou seja, do ATM), quando os quadros são transmitidos no momento em que são completados, ressalvada a disponibilidade de recursos da rede no momento.

A alternativa ao ATM é o STM (*Synchronous Transfer Mode*). No STM, um quadro só é transmitido na janela de tempo (*time-slot*) associada ao terminal transmissor. O grande exemplo de STM são os sistemas TDM (SDH e OTN, por exemplo).

A transmissão de quadros em redes de telecomunicações pode ocorrer no modo síncrono ou no modo assíncrono. No modo síncrono, ocorre uma sucessão contínua de transmissão de *time*-*slots*. No modo assíncrono, a transmissão de quadros pode ocorrer em qualquer momento em que esses quadros estejam prontos para transmissão.

No STM, a transmissão ocorre no modo síncrono e a transferência de informações ocorre também no modo síncrono. Cada terminal é associado a uma determinada janela de tempo.

Caso um terminal não tenha informações para transmitir em um instante de disponibilização de sua janela de tempo, essa janela de tempo será transmitida vazia. Isso representa ineficiência no uso da banda utilizada, mas, em contrapartida, o terminal tem sempre a possibilidade de transmitir os seus quadros.

Nas denominadas redes ATM, a transmissão é síncrona (consiste na transmissão contínua de pacotes), mas a transferência de informações ocorre no modo assíncrono (do que decorre a denominação ATM).

Transferência de informações no modo assíncrono em redes ATM, significa que um terminal, com um quadro a transmitir, pode utilizar qualquer janela de tempo (qualquer pacote) que se disponibilizar.

A rigor, a denominação genérica ATM não implica a transmissão síncrona. O X.25 e o Frame Relay, por exemplo, são formas de transmissão assíncrona, porque os quadros são transmitidos a qualquer momento. Isso implica, consequentemente, também o modo assíncrono de transferência de informações, o que significa que X.25 e Frame Relay são na realidade também formas de ATM.

O ITU-T, contudo, cunhou a denominação ATM para o caso particular de transferência de informações no modo assíncrono quando a transmissão é síncrona, cabendo a todos cumprir os desígnios do ITU-T.

* + 1. **- Restrições no Modelo Overlay**

O Modelo Overlay apresenta algumas restrições que levaram à interrupção de sua utilização, que dizem respeito particularmente aos seguintes aspectos:

-Conectividade complexa e ineficiente em aplicações ponto a multiponto, e, principalmente, em aplicações multiponto a multiponto;

- Plano de controle operando por NBMA;

- Roteamento EGP de redes IP transportadas;

- Necessidade de resolução de endereços de destino da rede de camada 2 a partir dos endereços das estações de destino da rede transportada.

O Modelo Par, como será visto adiante, atenua, ou mesmo elimina em alguns casos, as restrições acima.

* + - 1. **– Aplicações Ponto a Multiponto**

 As redes modo pacote comutadas orientadas a conexão no modelo Overlay podem oferecer conexões ponto a multiponto, porém com ressalvas.

A implementação de conexões ponto a multiponto, pela dificuldade que apresenta, simplesmente não ocorreu na prática em redes X.25 e em redes Frame Relay, tanto em PVCs quanto em SVCs.

No ATM, que representa uma tecnologia de rede mais moderna e sofisticada, as conexões ponto a multiponto são utilizadas, em diversas aplicações.

O ITU-T incorporou, na B-ISUP (*Broadband Integrated Services User Part*), a sinalização para conexões ATM ponto a multiponto em redes ATM públicas.

Por outro lado, o *ATM Forum* procedeu da mesma forma tanto na sinalização na UNI quanto na PNNI. A sinalização para o estabelecimento de SVCs ponto a multiponto foi especificada nos padrões PNNI, UNI 3.0, UNI 3.1 e UNI *Signaling* 4.0.

* + - 1. **- Aplicações Multiponto a Multiponto**

 Aplicação multiponto a multiponto consiste na possibilidade de transmissões ponto a multiponto a partir de qualquer um dos pontos.

Para o pleno atendimento de uma aplicação multiponto a multiponto com **n** pontos, por circuitos virtuais, é necessária a constituição de uma malha *full*-*mesh* com **n(n-1) / 2** circuitos virtuais.

Isso representa a possibilidade da necessidade de se administrar um número elevado de circuitos virtuais, o que é complexo, tanto em PVCs quanto em SVCs. Como no Modelo Overlay os circuitos virtuais terminam nas estações finais do usuário, o número de circuitos virtuais é mais elevado que no Modelo Par, agravando o problema.

Para ilustrar essa questão, consideremos uma configuração multiponto a multiponto com 50 estações atendida por uma rede comutada no Modelo Overlay.

Serão necessários 50x49/2 circuitos virtuais, ou seja, 1.225 circuitos virtuais, o que representa um número elevado, de difícil administração.

No Modelo Par o problema com as aplicações multiponto a multiponto no plano de dados persiste. Nesse caso, porém, esse problema é atenuado pelo fato de que os circuitos virtuais passam a terminar nos comutadores de borda da rede de camada 2 de suporte (rede MPLS, como exemplo atual). Reduz-se sensivelmente, dessa forma, o número de circuitos virtuais.

* + - 1. **- Plano de Controle Operando por NBMA**

Em redes modo pacote comutadas por circuitos virtuais no Modelo Overlay, o plano de controle, assim como o plano de dados, opera em NBMA.

Em consequência, há um considerável desperdício de recursos na realização do roteamento e da sinalização nessas redes.

Na hipótese de transporte do IP, o roteamento interno na rede de camada 2 de suporte processa-se de forma totalmente independente do protocolo EGP da rede IP.

No Modelo Par, o plano de controle das redes de suporte opera por BMA, com base na arquitetura TCP/IP, o que redunda em uma considerável economia de recursos dessas redes.

**4.1.2.4 - Roteamento EGP de Redes IP**

No importante caso em que as redes de suporte de camada 2 no Modelo Overlay transportam o IP, os datagramas de roteamento EGP da rede IP transportada atravessam as redes de suporte envelopados em quadros de dados dessas redes.

Isso significa, como consequência, que o tráfego desses datagramas de roteamento EGP ocorre por NBMA, com a sua inerente ineficiência no uso dos recursos da rede.

O problema se agrava pelo fato de que, no Modelo Overlay, os circuitos virtuais das redes de camada 2 de suporte terminam nos seus terminais.

Como o número de circuitos virtuais terminando em terminais das redes é superior ao número de circuitos virtuais terminando nos comutadores de borda dessas redes como no Modelo Par, o número de vizinhanças de roteamento EGP através das redes de suporte, que acompanha o número de circuitos virtuais, é também mais elevado.

A Figura 5 mostra a constituição de uma malha full-mesh com 15 circuitos virtuais que ocorre em aplicações multiponto a multiponto, o que se reflete nas vizinhanças do roteamento EGP de redes IP que atravessa a rede de camada 2 de suporte (como redes Frame Relay ou redes ATM). Lembramos que o roteamento é também uma aplicação multiponto a multiponto.



**Figura 5 - Circuitos virtuais e vizinhanças de roteamento EGP no Modelo Overlay.**

 Observa-se que na hipótese deste subitem, a configuração dessa figura é atendida no Modelo Par por apenas três circuitos virtuais e utiliza também apenas três vizinhanças EGP através da rede MPLS. O tráfego entre os roteadores IP do usuário e os PEs da rede MPLS passa a ocorrer por IP. São estabelecidas vizinhanças de roteamento entre esses equipamentos, uma vez que, voltados para fora da rede MPLS, os PEs operam como simples roteadores IP.

Sendo o número de vizinhanças de roteamento EGP IP superior no Modelo Overlay, o tráfego de datagramas desse roteamento EGP através da rede MPLS é também superior.

Resumindo, o número de vizinhanças de roteamento EGP através das redes de suporte no Modelo Overlay é superior ao caso do Modelo Par. O tráfego de roteamento é também superior por duas razões:

- Porque esse tráfego ocorre em NBMA;

- Porque o número de vizinhanças de roteamento EGP é superior.

 É bom lembrar que esse tráfego de roteamento, que atravessa a rede de transporte envelopado em quadros de dados, pode ser eventualmente tarifado e cobrado pelo provedor dessa rede.

**4.1.2.5 - Necessidade de Resolução de Endereços**

No Modelo Overlay, as redes de camada 2 de suporte possuem endereçamentos próprios, e não existem mecanismos diretos de acoplamento entre os endereços dos comutadores de borda de destino dessas redes e os endereços das estações de destino da rede transportada.

Em consequência, há a necessidade de mecanismos de resolução de endereços de destino das redes de suporte, o que representa complexidade e sobrecarga de tráfego de overhead nessas redes.

Esses mecanismos, que variam de acordo com o tipo de rede de suporte e do tipo de rede transportada, constituem membros da família de protocolos referida como ARP (*Address Resolution Protocol*).

No caso de Ethernet sobre ATM, o *ATM Forum* desenvolveu um serviço específico, denominado LANE (*LAN Emulation over ATM*), que, dentre outras funções, permite a resolução de endereços ATM de destino a partir dos endereços MAC das estações Ethernet de destino.

Na hipótese de IP sobre Frame Relay, o IETF especificou o uso do protocolo ARP para SVCs e do protocolo InARP para PVCs (RFC 2390).

Para o caso de IP sobre ATM, o IETF e o *ATM Forum* desenvolveram diferentes mecanismos para a resolução de endereços ATM de destino a partir dos endereços IP das estações finais. Esses mecanismos estão descritos no subitem 4.1.3 deste item.

No Modelo Par, onde são definidos mecanismos de acoplamento direto entre as redes de suporte e as redes transportadas, e onde as redes de suporte não possuem endereços próprios, não existe a necessidade de resolução de endereços.

**4.1.3- Ascensão e Queda do ATM**

A partir de 1984/1985, iniciou-se, sob a égide do ITU-T, a definição da tecnologia ATM para redes públicas. Sob uma grande expectativa, o ITU-T passou a emitir uma série de recomendações relativas ao ATM a partir desse período.

 Começaram a surgir, contudo, questionamentos sobre a concepção do ITU-T para o ATM. A crítica básica era quanto à recalcitrância do ITU-T em conceber as redes modo pacote de altas velocidades como se fossem um “big telex”, mantendo a fundamentação do Modelo Overlay. O ITU-T substimou, de início, os esforços que ocorriam mundialmente, comandados pelo IETF, para a introdução da arquitetura TCP/IP.

A inadequabilidade do ATM, nos moldes concebidos pelo ITU-T, para suportar o IP era evidente. De fato, por exemplo, o roteamento IP sobre o ATM ocorre de modo complexo e oneroso, o mesmo ocorrendo com outros aspectos do ATM.

 Em 1991 foi criado o *ATM Forum*, com o propósito de coordenar, catalisar e agilizar a introdução e a consolidação do ATM.

Cedo, contudo, o IETF, e a seguir o *ATM Forum*, passaram a criar padrões objetivando atenuar a inadequabilidade do ATM para o atendimento do IP.

Pelo IETF, ocorreram as seguintes iniciativas:

- *Classical IP and ARP over ATM*, pela RFC 1577, de 1994, obsoletada e substituída pela RFC 2225;

- NHRP (*Next Hop Resolution Protocol*), pela RFC 2332, de 1998;

- MARS (*Multicast Address Resolution Server*), pela RFC 2149, de 1997.

O *ATM Forum* especificou, com esse propósito, os seguintes serviços:

- LANE (*LAN Emulation over ATM Specification Version 1*), de 1995;

- MPOA (*Multiprotocol over ATM*), em 1999.

**4.1.3.1 – Classical IP and ARP over ATM**

 A concepção denominada *Classical IP and ARP over ATM*, iniciada em1993, define os seguintes aspectos relativos à transmissão de datagramas IP sobre ATM:

- Uma técnica de encapsulamento;

- Os protocolos ATMARP e InATMARP;

- Fluxos de sinalização na UNI;

- Tamanho padrão de MTU (*Maximum Transmission Unit*).

Para englobar esses aspectos relativos à concepção *Classical IP and ARP over ATM,* foram emitidos inicialmente as seguintes RFCs:

- RFC 1483 (*Multiprotocol Encapsulation over ATM Adaptation Layer 5*), em 1993;

- RFC 1577 (*Classical IP and ARP over ATM*), em 1994;

- RFC 1626 (*Default IP MTU for Use over ATM AAL 5*), em 1994;

- RFC 1755 (*ATM Signaling Support for IP over ATM*), em 1995.

A RFC 1577 foi obsoletada e substituída pela RFC 2225, em 1998.

Para o encapsulamento e a identificação dos protocolos de camada 3 em ATM, a RFC 1483 definiu duas técnicas:

- A primeira consiste na inserção de um cabeçalho LLC/SNAP no início de cada pacote ATM, para indicar o protocolo de camada 3 envelopado. O SNAP utiliza a codificação *EtherType* com esse propósito;

- A segunda consiste no uso da multiplexação de VCs, onde é utilizado um VC ATM próprio para indicar cada um dos protocolos de camada 3 envelopados.

No que concerne a RFC 2225, destacam-se as definições do protocolo InATMARP (*Inverse ATMARP*) para a resolução de endereços em PVCs e do protocolo ATMARP para a resolução de endereços ATM para a constituição de SVCs.

Em uma rede ATM, ou em partes de uma rede ATM, pode ser constituída uma sub-rede IP, referida como uma LIS (*Logical IP Subnetwork*).

Uma LIS pode suportar múltiplos hosts e roteadores IP configurados em terminais ATM, sendo que esses hosts e roteadores possuem o mesmo prefixo de endereços IP. A transmissão entre um dado par de membros de uma LIS pela rede ATM ocorre por um PVC ou um SVC.

Observa-se que o *Classical IP and ARP over ATM* aplica-se apenas no caso de transmissão de datagramas IP unicast.

A aplicação do *Classical IP and ARP over ATM* limita-se ao âmbito de uma LIS. Para o tráfego inter-LISs nesse modelo, é necessária a interveniência de um roteador IP devidamente configurado com esse propósito.

Em redes ATM operando com PVCs, quando os circuitos virtuais já se encontram constituídos, os endereços ATM a serem resolvidos são os valores de VPI/VCI no primeiro link (entre a estação IP de origem e a rede ATM) que conduzem ao endereço IP de destino desejado.

O protocolo definido na RFC 2225 com esse propósito é o InATMARP. No InATMARP, cada uma das estações IP indaga periodicamente de cada uma das demais estações IP conectadas à rede ATM, quais endereços IP de destino encontram-se associados a cada um dos circuitos virtuais que nela terminam.

As estações IP de origem, assim como as estações IP de destino, montam então tabelas associando os endereços IP de destino informados, aos VPIs/ VCIs iniciais (entre a estação IP final de origem e a rede ATM) correspondentes. As estações IP de destino aproveitam as informações contidas nos pedidos que recebem, para montar as suas próprias tabelas InATMARP.

Como se observa, o processo para a montagem das tabelas ocorre na ordem inversa (dos endereços ATM para os endereços IP), do que decorre a denominação InATMARP.

 As consultas locais posteriores a essas tabelas, no entanto, ocorrem na ordem direta, ou seja, de endereços IP para endereços ATM.

No caso de redes ATM públicas operando com SVCs, os endereços ATM de destino a serem resolvidos são formatados conforme a Recomendação ITU-T E.164.

Para redes ATM privativas, o *ATM Forum* definiu três novos formatos destinados à identificação de usuários finais ATM que se comunicam pela utilização de UNIs ATM, que são os seguintes:

- Formato DCC (*Data Country Code*);

- Formato ICD (*International Code Designator*);

- Formato E.164 no estilo NSAP (*Network Service* *Access Point).*

Após a sua obtenção, esses endereços são utilizados na sinalização para a constituição dos circuitos virtuais que conduzem aos correspondentes endereços IP de destino.

A RFC 2225 definiu, para o caso de SVCs, o protocolo ATMARP. O ATMARP é um protocolo baseado em tabelas centralizadas em servidores ATMARP (*ATMARP Servers*), onde estações IP finais vão obter os endereços ATM de destino.

Para que o *ATMARP Server* disponha das associações entre endereços ATM e endereços IP dos membros da LIS, podem ser utilizadas duas técnicas.

Na primeira dessas técnicas, as associações são inseridas manualmente, no plano de gerenciamento da rede.

Na segunda técnica, utilizada em redes ATM de maior porte, as associações resultam da aplicação prévia do protocolo InATMARP entre o *ATMARP Server* e os clientes IP.

Para aprimorar o uso do InATMARP como no parágrafo anterior, pode ser utilizada uma conexão ATM ponto a multiponto previamente constituída entre o servidor ATMARP utilizado e as estações IP finais.

A Figura 6 ilustra a resolução de endereços ATM pelo protocolo ATMARP em uma LIS.



**Figura 6 – Resolução de endereços ATM pelo ATMARP (livro ATM and Multiprotocol Networking, McGraw Hill Series on Computer Communications).**

Como se observa nessa figura, o cliente IP#1, configurado em um terminal ATM de uma dada LIS, consulta o *ATMARP Server* para obter o endereço ATM (BBB) do cliente IP#2, localizado em outro terminal ATM nessa mesma LIS, cujo endereço IP é 176.13.11.2.

Observa-se que o prefixo de endereço IP que identifica a LIS é 176.13.11.

**4.1.3.2 – NHRP**

Para possibilitar a resolução de endereços ATM entre diferentes LISs, e possibilitar, em consequência, o estabelecimento de VCs ATM diretamente entre terminais situados em uma rede ATM, mas em diferentes LISs (sub-redes), foi emitida a RFC 2332, em 1998, definindo uma técnica referida como NHRP.

O NHRP pode ser considerado uma extensão inter-LISs do protocolo ATMARP definido na RFC 2225 para o âmbito de apenas uma LIS.

Embora de início concebido para o atendimento de IP sobre ATM, o NHRP foi estendido para possibilitar o suporte a qualquer protocolo de camada 3 sobre ATM. Dessa forma, o NHRP pode ser incorporado ao rol de técnicas que compõem o MPOA.

Uma configuração NHRP é composta pelos seguintes componentes básicos:

- NHCs (*Next Hop Clients*);

- NHSs (*Next Hop Servers*).

Os NHCs são clientes da rede de camada 3 suportada, localizados em terminais ATM devidamente configurados para a operação do NHRP.

Os NHSs, cujas funções são extensões das funções de um *ATMARP Server*, provêm os serviços NHRP para os NHCs, como, por exemplo, a resolução de endereços ATM a partir dos endereços de camada 3 dos terminais de destino (endereços IP dos terminais de destino, por exemplo).

Se o endereço de camada 3 desejado não se encontra na LIS do terminal de origem, mas em uma outra LIS na mesma rede ATM, o NHS obtém esse endereço via outros NHSs se necessário.

Dessa forma, pode ser constituído um VC inter-LISs para a comunicação almejada.

A Figura 7 ilustra o funcionamento completo do NHRP na hipótese dos dois parágrafos acima.



**Figura 7 – Funcionamento do NHRP (livro ATM and Multiprotocol Networking, McGraw Hill Series on Computer Communications).**

Observa-se, nessa figura, que se resume em uma única rede ATM, que o terminal X.1 solicitou ao NHS X o endereço ATM (BBB) do terminal Z.3, associado ao endereço IP Z3 desse terminal, sendo que o terminal Z.3 se encontra em outra LIS (*Subnet Z*).

A solicitação foi atendida pelo NHS Z, mediante a intermediação do

NHS X.

Uma vez obtido o endereço BBB, o terminal X.1 enviou uma mensagem *Setup VC*, para o estabelecimento de um VC ATM diretamente com o terminal Z.3.

Tornou-se assim possível a transmissão de quadros de dados ATM envelopando datagramas IP entre esses dois terminais através do VC ATM estabelecido.

Se o endereço de camada 3 desejado se encontra em uma outra rede ATM, o NHS obtém, via outros NHSs se necessário, o endereço ATM do roteador mais próximo do terminal de destino (ou seja, do *next hop*). Esse roteador passa a se encarregar da comunicação com o terminal no destino.

Para facilitar o funcionamento do NHRP, os NHSs devem ser configurados em roteadores da rede de camada 3 transportada pelo ATM.

-

**4.1.3.3 – MARS**

As técnicas utilizadas em *Classical IP and ARP Over ATM e em NHRP* destinam-se à resolução de endereços ATM de destino em uma LIS e em configurações inter–LISs, respectivamente. Essas técnicas, contudo, limitam-se à resolução de endereços ATM para datagramas unicast, não abrangendo, portanto, datagramas multicast (a transmissão broadcast é um caso particular de transmissão multicast que alcança a totalidade dos terminais).

Para a resolução de endereços de datagramas IP multicast, foi definida, na RFC 2022 (de 1996), a utilização de um servidor denominado MARS. Podem ser inclusive utilizados múltiplos MARS de forma distribuída.

Ressalva-se, contudo, que a utilização de um MARS, ou de múltiplos MARSs, restringe-se ao âmbito de uma dada LIS.

Na realidade, o uso do MARS não se limita ao IP, podendo ser estendido para outras tecnologias de camada 3 (como IPX, *AppleTalk*, etc...). Dessa forma, o MARS veio a se integrar à concepção do MPOA.

A arquitetura do MARS foi posteriormente detalhada na RFC 2149, de 1997.

Cada terminal ATM que atende a um endereço de grupo de assinantes de uma rede de camada 3, informa esse fato ao MARS. Dessa forma, o MARS passa a conter as associações entre endereços multicast de grupos de assinantes de camada 3 e os endereços ATM que os atendem.

Um terminal ATM que deseja transmitir um datagrama multicast pode proceder de duas formas.

Na primeira forma, referida como Modelo *VC*-*Merge*, o terminal ATM de origem obtém, do MARS, os endereços ATM associados ao endereço multicast.

O terminal ATM de origem verifica se já existe um VC ATM ponto a multiponto nele centrado para esses endereços ATM, para uso imediato.

Caso esse VC ponto a multiponto não exista, o terminal ATM de origem sinaliza para a sua constituição.

Na segunda forma, o terminal ATM de origem encaminha quadros ATM contendo datagramas multicast da rede de camada 3 para um servidor central, denominado MCS (*Multicast Server*).

O MCS, já devidamente alimentado com as associações de endereços pelo MARS, transmite os datagramas multicast para os terminais ATM associados ao grupo de assinantes, por meio de um VC ATM ponto a multiponto centrado no MCS.

Observa-se que esses dois métodos conduzem aos mesmos resultados, com vantagens e desvantagens.

**4.1.3.4 – LANE**

Redes Ethernet podem operar nativamente sobre ATM. Nesse caso, as estações Ethernet, que podem ser inclusive bridges Ethernet providas das devidas interfaces ATM, são conectadas diretamente aos comutadores ATM.

Nesse caso, terminais ATM conectados a esses comutadores ATM encontram-se impossibilitados de participar das aplicações de LAN existentes, a menos que ocorram alterações específicas nesses terminais.

Por outro lado, a única possibilidade de atendimento ao tráfego broadcast e multicast é pelo Modelo *VC*-*Merge*, o que nem sempre é desejável.

Ademais, não existe qualquer mecanismo de resolução de endereços ATM de destino a partir de endereços MAC de destino, o que demanda a necessidade de definição de esquemas não padronizados de tradução de endereços.

 O serviço Emulação de LANs sobre ATM, definido inicialmente no padrão *LAN* *Emulation over ATM Specification Version 1.0*, emitido em 1995 pelo *ATM Forum*, tem como objetivo solucionar os problemas acima mencionados.

 LANE é uma solução de software, que consiste na emulação de estações Ethernet (IEEE 802.5) ou de estações *Token-Ring* (IEEE 802.5), sobrepostas a um terminal ATM. Os terminais assim emulados são referidos como LECs (*LAN Emulation Clients*).

A aplicação de LANE se restringe a um conjunto de LECs configurados em terminais ATM, conjunto esse que constitui uma ELAN (*Emulated LAN*).

Em um LEC pode rodar uma aplicação de LAN existente, sem a necessidade que qualquer alteração.

LANE utiliza três tipos de servidores centrais:

- *LAN Emulation Configuration Server* (LECS);

- *LAN Emulation Server* (LES);

- *Broadcast / Unknown Server (Bus)*.

O LECS é responsável pelo provimento de informações de configuração para os LECs. Dentre tais informações de configuração podem ser citados o endereço ATM do LES, o tipo de LAN emulada e a MTU dos quadros transmitidos.

O LES funciona como depositário das associações entre endereços MAC e endereços ATM e como servidor de resolução entre esses endereços.

Os LECs registram seus endereços MAC e endereços ATM junto ao LES.

Os LECs podem também consultar o LES para a resolução de endereços ATM de destino a partir de endereços MAC de estações Ethernet de destino. As respostas do LES a essas consultas podem ser enviadas diretamente para os LECs que realizaram as consultas, ou podem ser encaminhadas para outros LECs caso o LEC não possua a associação de endereços solicitada. Outro LEC que possua essa associação pode enviá-la para o LEC que a solicitou.

Compete ao BUS a transmissão broadcast (NBMA, na realidade) de quadros com endereços multcast ou broadcast.

 Outra opção de funcionamento do BUS, que justifica a denominação “*Unknown*”, é a transmissão de quadros unicast na hipótese de que o LEC de origem não deseja aguardar a resposta a uma solicitação de resolução de endereços. Nesse caso, o LEC envia o quadro para o BUS, que, por desconhecer o respectivo endereço unicast, retransmite-o em broadcast para todas as estações.

O BUS utiliza um VC ATM ponto a multiponto nele centrado e conectado a todas as estações da rede.

A Figura 8 resume o relacionamento entre um LEC e os servidores centrais no serviço LANE.



**Figura 8 – Relacionamento LEC/servidores centrais (livro ATM and Multiprotocol Networking, McGraw Hill Series on Computer Communications).**

Ocorrem supostamente, nessa figura, os seguintes procedimentos:

- Para transmitir diretamente quadros unicast, o LEC solicita o endereço ATM do LES ao LECS, utilizando a C*onfiguration Direct VCC*;

- O LEC constitui a *Control Direct VCC*, pela qual obtém, do LES, o endereço ATM desejado. O LEC constitui então a VCC com o LEC de destino;

- Para transmitir um quadro MAC em broadcast, o LEC envia esse quadro para o BUS, utilizando a *Multicast Send VCC*;

- O BUS transmite o quadro em broadcast utilizando a *Multicast Forward* VCC.

**4.1.5.5 – MPOA**

MPOA, definido pelo *ATM Forum* no padrão *Multiprotocol over ATM Specification Version* *1.0,* de 1999, é uma concepção de serviço que representa uma extensão mais ampla e aprimorada de LANE.

MPOA incorpora funcionalidades dos padrões UNI 3.0, UNI 3.1 ou UNI 4.0, LANE, NHRP e MARS.

LANE destina-se à emulação de LANs Ethernet e de LANs *Token Ring* sobre redes ATM.

MPOA, por sua vez, engloba a emulação de múltiplas tecnologias de camada 3 (IP, IPX e *AppleTalk*, como principais exemplos), além de incorporar a emulação de LANs sobre redes ATM.

Os componentes do protocolo MPOA, que, a exemplo do protocolo LANE, opera em uma arquitetura cliente-servidor, são os MPCs (*MPOA* *Clients*) e os MPSs (*MPOA* *Servers*). As funções desses componentes assemelham-se, com maior complexidade, às funções dos componentes utilizados em LANE.

 Outro aprimoramento fundamental de MPOA com relação a LANE, é a abrangência de aplicação.

Enquanto LANE tem a sua operação restrita a uma ELAN, tanto em termos de configuração quanto de resolução de endereços ATM e de constituição de VCCs ATM, MPOA abrange também essas operações entre ELANs.

Para fins de comparação, vamos considerar a Figura 9, relativa à transmissão ATM em uma ELAN e entre duas ELANs, no caso de LANE.



**Figura 9– Transmissão ATM em LANE.**

Como se observa nessa figura, para a transmissão ATM entre dois LECs situados em diferentes ELANs, é necessária a utilização de diferentes VCCs intermediadas por um roteador externo (como na figura) ou por múltiplos roteadores externos.

A Figura 10 contempla a mesma configuração de rede, porém utilizando o serviço MPOA.



**Figura 10 – Transmissão ATM em MPOA.**

 Como se verifica nessa figura, a transmissão entre o MPC A e o MPC B, situados em diferentes ELANs, ocorre por um VC ATM conectando diretamente esses dois MPCs. Esse VC (VC AB) resultou, como uma hipótese, da resolução do endereço ATM do MPC B, situado na ELAN 2, realizada pelo MPC A, situado na ELAN A. Nessa hipótese, uma vez obtido o endereço ATM do MPC B, o MPC A supostamente constituiu o VC AB por sinalização.

Quando da especificação do MPOA, no final da década de 90, existiam aplicações correntes das demais concepções de suporte ao ATM, como *Classical IP and ARP over ATM,* NHRP, MARS e LANE. O serviço MPOA, no entanto, praticamente não foi utilizado.

A especificação do serviço MPOA foi um dos últimos padrões, se não o último, definido pelo *ATM Forum*. O *ATM Forum* perdeu a razão de sua existência a partir dessa época.

**4.1.5.6 – Final do ATM e Surgimento do MPLS**

 Em face da inadequabilidade do ATM para o atendimento do TCP/IP, iniciaram-se os estudos para a criação de uma nova tecnologia de comutação modo pacote no Modelo Par, para substituir o ATM. Essa nova tecnologia veio a denominar-se MPLS (*Multiprotocol Label Switching*).

No início da década de 2000, o ATM chegou praticamente ao seu final. As razões para isso, em resumo, foram as seguintes:

- As deficiências do Modelo Overlay em que se baseia o ATM;

- Desigualdade entre o ATM privativo aprimorado criado pelo IETF e, principalmente, pelo *ATM Forum*, e o ATM público definido pelo ITU-T;

- Iminência do lançamento do MPLS, operando no Modelo Par.

Em sucessão a algumas iniciativas isoladas de fabricantes de redes MPLS, o IETF emitiu, em janeiro de 2001, uma série de seis RFCs (RFC 3031, RFC 3032, RFC 3034, RFC 3035, RFC 3036 e RFC 3037), dando início ao processo de padronização para o lançamento do MPLS.

* 1. **-Modelo Par**

O Modelo Par, cujo primeiro e único exemplo de utilização no momento é o MPLS, fundamenta-se no uso do modo sem conexão baseado no TCP/IP exclusivamente para o plano de controle da rede de camada 2 utilizada. São envolvidos, portanto, os processos de roteamento e de sinalização.

O envolvimento do plano de dados da rede de camada 2 no Modelo Par não tem sentido. Dessa forma recairíamos em redes sem conexão, quando o que se deseja é o aprimoramento de redes orientadas a conexão por circuitos virtuais.

Em resumo, o que se almeja com o Modelo Par é unir a facilidade e a eficiência da conectividade de redes sem conexão no plano de controle, com o elevado nível de desempenho de redes orientadas a conexão por circuitos virtuais no plano de dados.

A rede de camada 2 de suporte no Modelo Par utiliza protocolos usuais ou aprimorados de roteamento IP como protocolo IGP. Para a sinalização são também utilizados protocolos baseados na arquitetura TCP/IP, associados aos protocolos IGP adotados.

A operação da rede de camada 2 de suporte no modo sem conexão no Modelo Par, embora ocorra exclusivamente no plano de controle, reflete-se no respectivo plano de dados, tornando-o mais simples, independente e eficiente.

Esse aprimoramento de desempenho do plano de dados decorre do fato de que, no Modelo Par, os circuitos virtuais têm os seus pontos de terminação localizados nos comutadores de borda da rede de camada 2 de suporte, e não nos equipamentos terminais da rede transportada como no Modelo Overlay.

Como vimos no subitem 4.1.1.3 anterior neste tutorial, houve uma tentativa do *ATM Forum*, mediante a emissão do padrão *PNNI Draft Specification* (*PNNI Phase 1*), em 1996, para a definição de uma forma de antecipação de alguns aspectos do Modelo Par para o ATM.

A PNNI constituiu-se certamente em um importante embasamento para a definição do Modelo Par, particularmente do MPLS. Como de fato ocorreu, alguns conceitos e princípios adotados no MPLS foram, de alguma forma, aplicados na PNNI.

Por exemplo, o conceito do vetor DTL (*Designated Transit List*) constituiu-se na base para o conceito do objeto ERO (*Explicit Route Object*) definido na RFC 3209 para uso no protocolo RSVP-TE referente à sinalização no MPLS-TE.

 Esses dois conceitos referem-se a uma lista completa de componentes da rede que explicita o caminho a ser seguido pela solicitação de SVC, lista essa definida pelo comutador de origem com base nas informações providas pelo roteamento.

**4.2.1- Características do Modelo Par**

O Modelo Par possui as seguintes características:

- O plano de controle da rede da camada 2 (MPLS, como único exemplo atual) opera em BMA, como em uma rede IP, consequentemente no modo sem conexão. Em decorrência, o roteamento nessa rede de camada 2 passa a ser um roteamento IGP (*Interior Gateway Protocol*).

- O plano de dados da rede de camada 2, embora continue a operar em NBMA, apresenta a vantagem de que os circuitos virtuais terminam nos comutadores de borda dessa rede;

- No caso de transporte do IP pela rede de camada 2 de suporte, os pontos de vizinhança do roteamento EGP da rede IP também se localizam nos comutadores de borda da rede de camada 2, o que se reflete na simplificação administrativa e na redução do tráfego de roteamento EGP através dessa rede de camada 2;

- Não existe a necessidade do complexo e oneroso processo de resolução de endereços de camada 2 a partir de endereços dos terminais de destino da rede transportada (como IP e Ethernet, por exemplo).

**4.2.2 – Vantagens do Modelo Par**

As vantagens do Modelo Par representam a eliminação, ou a atenuação, das restrições no Modelo Overlay apresentadas no subitem 4.1.2 anterior neste tutorial.

Tais vantagens podem ser resumidas na seguinte relação:

- Menor número de circuitos virtuais;

 - Atendimento mais eficiente de aplicações ponto a multiponto e de aplicações multiponto a multiponto;

- Maior adequabilidade e eficiência no processo de roteamento;

- Eliminação da necessidade de resolução de endereços.

Essas vantagens, que decorrem das características do Modelo Par apresentadas no subitem anterior, serão evidenciadas na apresentação das redes MPLS nos próximos subitens deste tutorial.

**4.3– MPLS**

O MPLS (*Multiprotocol Label Switching*) é uma tecnologia de rede modo pacote comutada por circuitos virtuais, ou seja, uma tecnologia de rede NBMA, na qual, como em Frame Relay e em ATM, a comutação ocorre com base em labels contidos nos respectivos quadros.

Diferentemente do Frame Relay e do ATM, contudo, o MPLS possui inerentemente diferentes aplicações que suportam especificamente múltiplos tipos de rede de acesso. Além disso, o MPLS é um único tipo de rede NBMA no Modelo Par no momento presente de conhecimento do autor deste tutorial.

As redes MPLS representam, certamente, o ápice de redes modo pacote comutadas orientadas a conexão na atualidade, não deixando espaço para outras redes desse tipo, como redes Frame Relay e redes ATM.

Dada a complexidade das opções de tipos de rede e das categorias de aplicações do MPLS, é inviável falar-se do MPLS em termos gerais sem especificar claramente o contexto abordado.

**4.3.1 - Concepção do MPLS**

Os comutadores MPLS são referidos como LSRs (*Label Switching Routers*). Os LSRs de borda são referidos como PEs (*Provider Edge Equipments*) ou LERs (*Label Edge Routers*), enquanto os LSRs no interior da rede MPLS são referidos como Ps (*Provider Equipments*) ou simplesmente como LSRs.

Os circuitos virtuais no MPLS são referidos como LSPs (*Label Switching Paths*).

Na realidade, o MPLS surgiu como mais uma forma para tentar salvar o ATM (e também o Frame Relay, por extensão).

O MPLS consistia em uma rede ATM com o seu plano de dados e o seu interfaceamento físico, porém com um novo plano de controle. Esse novo plano de controle é baseado no TCP/IP e opera no Modelo Par, livrando assim o ATM das limitações do plano de controle no Modelo Overlay.

Cedo, contudo, foi notado que essa concepção trazia algumas limitações, parte delas inerentes aos formatos dos VPIs/VCIs (e dos DLCIs).

Os VPIs/VCIs e os DLCIs não possuem a disponibilidade de três bits para uso na indicação de QoS, o que impede a utilização de *Differentiated Services* (*DiffServ*). Não possuem tampouco a estrutura adequada para a constituição de pilhas de labels (*labels stacks*).

Mais problemática ainda era a dificuldade de utilização de comutadores ATM (e Frame Relay) adaptados para operar como LSRs. Isso decorre de fato de que, sendo baseado no TCP/IP, o plano de controle do MPLS apresenta grande diferença para as características desses comutadores.

Surgiu então a ideia de tornar o MPLS realmente uma nova tecnologia, com planos de dados e de controle próprios.

Para isso, foram definidos novos labels de túnel com formato próprio, independentemente de qualquer outra tecnologia. Esse novo formato foi denominado formato genérico, que será apresentado adiante neste tutorial.

Como o MPLS foi concebido sem interfaceamento físico, tornou-se necessária a utilização do interfaceamento físico de outras redes de camada 2 na arquitetura do MPLS quando da utilização de labels genéricos. Passou-se então a utilizar o interfaceamento físico do PPP e de Ethernet com esse propósito.

O interfaceamento físico do PPP é utilizado na hipótese de roteadores IP adaptados como LSRs. Como o plano de controle do MPLS é TCP/IP, essa adaptação ocorre com a maior facilidade. Além disso, roteadores IP são normalmente providos com interfaces PPP.

Lembramos que quando da utilização do MPLS sobre ATM ou Frame Relay, o interfaceamento físico do MPLS é o das próprias redes ATM ou Frame Relay.

Atualmente, redes MPLS com suporte em ATM e em Frame Relay não são mais implantadas. A solução mais utilizada é o uso do interfaceamento físico PPP, sendo os LSRs construídos como roteadores IP adaptados.

**4.3.2 – Labels no Plano de Dados**

Os labels no plano de dados do MPLS podem existir isoladamente ou podem ser constituídas pilhas de labels (*label stacks*), que são arquiteturas de labels.

Uma alternativa usualmente utilizada de arquitetura de labels no plano de dados do MPLS encontra-se na Figura 11.

**Figura 11 – Arquitetura usual de labels no plano de dados do MPLS.**

Os labels na parte inferior dessa arquitetura são genericamente referidos como *top labels* (por se encontrar na parte superior quando se desenha verticalmente os quadros no plano de dados do MPLS). Especificamente, esses labels são referidos como labels de túnel, labels de túnel LSP, labels de LSP ou labels IGP.

Uma sucessão de labels de túnel para os links da rede a partir de um PE define um LSP. Recordamos que ocorre *swapping* nesses labels.

Quando o MPLS tem o Frame Relay ou o ATM como rede de suporte, os labels de túnel são, respectivamente, os DLCIs e os VPIs / VCIs.

Quando o MPLS é suportado pelo PPP ou pela Ethernet, quando não existem labels, define-se os labels de túnel com um formato específico, denominado formato genérico, como mostra a Figura 12.

**Figura 12 - Formato genérico de labels no MPLS.**

Os labels na parte superior da Figura 11 anterior são genericamente referidos como *botton labels*, que representam os labels específicos para as diferentes aplicações do MPLS.

Os labels de aplicação utilizam o formato genérico em qualquer hipótese de interfaceamento físico (PPP ou Ethernet) e de rede de suporte (Frame Relay ou ATM).

Serão vistos adiante neste tutorial os *botton labels* utilizados para as seguintes aplicações do MPLS: MPLS IP VPNs, VPWS e VPLS. A aplicação Serviço MPLS Público utiliza exclusivamente os labels de túnel.

A atribuição e a distribuição de labels de túnel no MPLS ocorrem normalmente no modo *solicited downstream assignment*. Isso significa que o LSR *upstream* (*LSR Ru*) solicita labels de túnel e o LSR *downstream* (*LSR Rd*) atribui e envia para o *LSR Ru* um ou dois labels

Em LSPs unidirecionais, constituidos ou em constituição, o *LSR Ru* em um dado par de LSRs é aquele responsável pela transmissão do tráfego de dados para o outro LSR. Nesse tipo de LSP, é atribuído e enviado um único label, referido como label *downstream*.

Em LSPs bidirecionais, constituidos ou em constituição, o *LSR Ru* em um dado par de LSRs é aquele que se situa mais proximamente ao PE *upstream* no LSP. O PE *upstream*, nesse caso*,* é aquele responsável pelo processamento das informações de roteamento, pelo cálculo de rotas e pela inicialização do processo de sinalização, independentemente do sentido do tráfego.

Observamos que no MPLS-TE e no MPLS–TP, o PE *upstream* é mais propriamente referido também como *head end LSR*, enquanto o PE *downstream* o é como *tail end LSR*.

No caso de LSPs bidirecionais, o *LSR Rd* atribui e distribui, mediante solicitação do *LSR Ru*, também o label *upstream*, além do label *downstream*, o que possibilita a bidirecionalidade do tráfego de dados.

**4.3.3 – Modalidades de Rede MPLS**

O MPLS representa hoje três diferentes modalidades de rede:

- MPLS (ou MPLS Básico);

- MPLS-TE (*MPLS Traffic Engineering*);

- MPLS-TP (*MPLS Transport Profile*).

A primeira dessas modalidades, que foi utilizada no início do funcionamento do MPLS, não recebeu uma denominação específica pelo IETF, que a ele se refere simplesmente como MPLS. Como o termo MPLS denota também o MPLS como um todo, é comum a ocorrência de desentendimentos.

Por essa razão, estamos utilizando neste tutorial a denominação MPLS Básico para esse primeiro tipo de MPLS, ressalvando, contudo, que essa denominação não foi especificada pelo IETF.

Utiliza-se hoje o termo IP/MPLS, não definido formalmente pelo IETF, para representar o conjunto formado pelo MPLS Básico e pelo MPLS-TP (ou seja, excluindo o MPLS-TP). Evitaremos o uso da expressão IP/MPLS neste tutorial.

**4.3.3.1 - MPLS Básico**

O MPLS Básico tem a limitação do IP em termos de roteamento, por utilizar, como protocolo IGP, o protocolo OSPF (*Open Shortest Path First*) ou o protocolo IS-IS (*Intermediate Systems-to-Intermediate System*s), ambos sendo protocolos de roteamento IGP convencionais utilizados por redes IP. Tanto o OSPF quanto o IS-IS utilizam a métrica *link-state* de roteamento.

Enquanto o OSPF distribui as informações de roteamento utilizando PDUs denominadas LSAs (*Link State Advertisements*), o IS-IS o faz por meio de LSPs (*Link State Packets*).

 É preciso atenção para não se confundir LSPs da família IS-IS com os caminhos virtuais LSPs do MPLS.

O protocolo de sinalização utilizado no MPLS Básico é o LDP (*Label*

*Distribution Protocol*). O LDP é um protocolo simples, que consiste basicamente em um processo de atribuição e distribuição de labels entre LSRs.

O MPLS-TE e o MPLS-TP são tecnologias de rede que utilizam engenharia de tráfego (TE). Os respectivos protocolos de roteamento IGP são do tipo *constraining routing*, quando a definição de rotas é condicionada por uma série de atributos, referidos como objetos, tais como capacidades de links, disponibilidades momentâneas de banda, características de links em termos de delays e de variações de delays, etc...

**4.3.3.2 - MPLS-TE**

No MPLS-TE, o roteamento IGP utiliza o protocolo OSPF-TE (*OSPF Traffic Engineering*) ou o protocolo ISIS-TE (*IS-IS Traffic Engineering*).

O OSPF-TE e o ISIS-TE utilizam *constraining routing* e *source routing*.

 Em *constraining routing,* que utiliza um tipo de métrica *link state* aprimorada, são utilizados, além dos custos usuais, diferentes parâmetros (*constraints*) que condicionam a definição das rotas a serem adotadas.

 *Source routing* significa que os parâmetros de roteamento são conduzidos para pontos centralizados (os PEs no MPLS), onde são processados para a definição de rotas.

 A sinalização, que acompanha a sofisticação do roteamento, utiliza o protocolo RSVP-TE (*Resource Reservation Protocol Traffic Engineering*).

O plano de controle do MPLS-TE foi utilizado como base referencial para o desenvolvimento de um amplo plano de controle de uso generalizado, denominado GMPLS (*Generalized MPLS*).

**4.3.3.3 – MPLS-TP**

O MPLS-TP utiliza o GMPLS como plano de controle.

O GMPLS utiliza como protocolo de roteamento IGP o protocolo GMPLS OSPF-TE ou o protocolo GMPLS ISIS-TE. Na sinalização, o GMPLS utiliza o protocolo GMPLS RSVP-TE.

O GMPLS atende tanto a redes modo circuito (SDH, OTN, WDM, etc...) quanto a redes modo pacote (cujo exemplo atual é o MPLS-TP).

Em redes que utilizam o GMPLS como plano de controle, é possível tanto conexões reais ou virtuais unidirecionais quanto conexões reais ou virtuais ponto a ponto bidirecionais co-roteadas constituídas em um único processo de sinalização. O MPLS-TP faz uso dessas duas alternativas.

 Outra característica importante do GMPLS é total separação entre a rede utilizada no plano de dados e a rede onde se processa o plano de controle, ou seja, onde se processa o GMPLS.

A Figura 13 exibe um exemplo da separação entre os planos de dados e de controle que ocorre em redes utilizando o GMPLS.



**Figura 13 – Separação entre os planos de dados e de controle no GMPLS (livro GMPLS – Architecture and Applications, Morgan Kaufmann Publishers)**

O GMPLS representa uma antecipação da concepção de constituição de redes denominada SDN (*Software Defined Networking*), cuja essência é justamente a transferência do processamento das funções de controle para o exterior da rede onde se encontra o plano de dados.

O MPLS-TP representa o mais importante exemplo, se não o único no momento atual, de uma concepção de rede modo pacote referida como PTN (*Packet Transport Network*).

As PTNs representam uma opção às redes de transporte modo circuito, como, por exemplo, as redes SDH e OTN, gozando, no entanto, da economicidade das redes modo pacote para aplicações com tráfego intermitente não muito intenso.

O MPLS-TP opera nos moldes de redes SDH e de redes OTN, mediante o uso da aplicação ponto a ponto do MPLS denominada VPWS, que será vista no subitem 4.2.4.4 adiante neste tutorial.

Para a plena funcionalidade objetivada para o MPLS-TP, foi necessária a eliminação de algumas funções utilizadas no MPLS Básico e no MPLS-TE (ou seja, no IP/MPLS), que descaracterizam o perfil de transporte almejado para o MPLS-TP.

Dentre tais funções podem ser citadas o *label merging* (fusão de labels), PHP (*Penultimate Hop Popping*) e ECMP *(Equal-Cost Multi-Path).*

Ocorreu, recentemente, um movimento objetivando a definição de uma tecnologia de rede bridged Ethernet orientada a conexão por circuitos virtuais, denominada PBB-TE (*Provider Backbone Bridging-Traffic Engineering*).

O objetivo do PBB-TE é o de constituir-se em outra opção de PTN para concorrer com o MPLS-TP. A introdução do PBB-TE, contudo, foi interrompida em face da prevalência esmagadora do MPLS-TP.

**4.3.4 – Aplicações do MPLS**

O MPLS oferece as seguintes principais aplicações:

- Serviço MPLS Público;

- BGP / MPLS IP VPNs, referida também como MPLS IP VPNs ou MPLS L3 VPNs;

- VPWS (*Virtual Private Wire Service*);

- VPLS (*Virtual Private LAN Service*).

Todas as modalidades de rede MPLS suportam, teoricamente, todas essas quatro aplicações. Na prática, todavia, ocorrem algumas exceções.

**4.3.4.1 – Serviço MPLS Público**

No Serviço MPLS Público, onde se utiliza apenas o label de túnel na arquitetura de labels, a rede MPLS representa simplesmente uma extensão orientada a conexão da rede IP global atendida (rede Internet Pública, por exemplo).

A Figura 14 exibe um exemplo de utilização do Serviço MPLS Público.



**Figura 14 – Exemplo de Serviço MPLS Público.**

Nessa figura, foi constituido um LSP entre os dois LERs (PEs) representados. A figura mostra a transmissão de um datagrama IP do site IP da esquerda para o site IP da direita.

No LER de origem (LER 2) foi acrescentado o label de túnel atribuído ao LSP utilizado, com o seu valor. Esse valor foi encontrado com base no endereço IP de destino contido no datagrama IP recebido, endereço esse que, direta (pelo seu prefixo) ou indiretamente, representa um elemento de FEC associado aos labels do LSP.

 Os valores de label de túnel foram alterados nos dois LSRs (Ps) ao longo do LSP (*label swapping*), alcançando assim o LER de destino (LER 4).

No LER 4 foi retirado o último label de túnel (operação *popping)*, do que resulta novamente o datagrama IP. O lado IP do LER 4 (lado externo) transmite então o datagrama para a estação IP de destino, utilizando os procedimentos IP usuais.

Observa-se que, por se tratar do Serviço MPLS Público, não foram utilizados *botton labels*, o que ocorreria nas demais aplicações do MPLS.

O serviço MPLS iniciou com o MPLS Básico prestando o Serviço MPLS Público. Essa associação objetivava tão somente prover uma extensão da rede IP usufruindo das vantagens operacionais das redes orientadas a conexão, tais como a simplicidade da comutação por labels e a possibilidade de uso de OAM mais robusto e de comutação automática de proteção.

Posteriormente, com a introdução do MPLS-TE e do MPLS–TP, o Serviço MPLS Público passou a usufruir das vantagens oferecidas pela engenharia de tráfego, tais como LSPs com reserva de banda passante e LSPs diferenciados para as classes de serviço.

Na fase inicial de associação do MPLS Básico e do Serviço MPLS Público, o protocolo IGP do MPLS (OSPF ou IS-IS) consistia em uma simples extensão do roteamento IP da rede global. Isso significa que a rede MPLS se resumia em um AS (*Autonomous System*) do roteamento da rede IP global (na realidade, o IETF especificou inclusive que esse AS consistia em apenas uma Área de Roteamento).

Em consequência, as rotas utilizadas no IGP do MPLS eram os prefixos de endereço IP das estações IP de destino, trazidos via protocolo BGP-4 para o interior da rede MPLS. Nos termos do IETF, isso significa que as FECs (*Forwarding Equivalence Classes*) no IGP eram os prefixos de endereço IP das estações IP de destino.

 Esse processo de roteamento refletia-se na sinalização da rede MPLS, uma vez que o protocolo LDP distribui labels com base nas FIBs (*Forwarding* *Information Bases*) do protocolo de roteamento utilizado (OSPF ou IS-IS, no caso), que associam as FECs aos próximos roteadores IP (*next-hops*).

Esse modo operacional representa uma série de problemas e de limitações, como os seguintes:

- O número de rotas transmitidas no IGP do MPLS é elevado;

- O MPLS fica atrelado ao IP como rede externa, impedindo aplicações como o VPWS e o VPLS;

- Não existe a possibilidade de *constraining routing*, e consequentemente de engenharia de tráfego em nível elevado, o que impede a existência de redes como o MPLS-TE e o MPLS-TP;

- Os LSPs constituídos são exclusivos para um serviço, não podendo ser utilizados por instâncias de outros serviços.

Para solucionar essa grave condição, o IETF definiu um mecanismo denominado *Hierarchy of Routing Knowledge* (HRK).

A ideia básica do HRK, muito simples, aliás, é a utilização dos endereços IP dos PEs como rotas para o roteamento IGP do MPLS. Em outras palavras, com o HRK os endereços IP dos PEs de destino passam a ser elementos de FEC.

Dessa forma, o IGP do MPLS torna-se totalmente independente da rede externa, que pode ser constituída por qualquer tecnologia. Assim, aplicações como o VPWS e o VPWS tornaram-se possíveis.

 Todas as demais limitações no processo de roteamento IGP do MPLS inicial são eliminadas com o uso do HRK. Possibilitou-se a introdução do MPLS-TE e do MPLS-TP. Além disso, os LSPs passaram a ser de uso irrestrito, inclusive por instâncias de serviço de diferentes aplicações.

Além de sua utilização obrigatória em qualquer aplicação do MPLS no MPLS-TE e no MPLS-TP, o HRK passou a ser utilizado também no MPLS Básico, inclusive no Serviço MPLS Público, pelas vantagens que apresenta.

**4.3.4.2 – MPLS IP VPNs**

Na aplicação MPLS IP VPNs, assim como no Serviço MPLS Público, as redes externas transportadas são redes IP.

Em MPLS IP VPNs, que utiliza HRK em qualquer tipo de rede MPLS de suporte, o protocolo IGP roda independentemente do protocolo EGP da rede IP. As estações finais, e consequentemente as rotas de destino, são os PEs de destino. Em consequência, os LSPs são constituídos com um mínimo de transmissão de rotas e de modo totalmente independente da rede externa.

Dessa forma, um LSP pode ser utilizado por diferentes MPLS IP VPNs, inclusive juntamente com instâncias de VPWS e/ou de VPLS. Esse LSP pode transportar também o Serviço MPLS Público para isso as *Default Forwarding* Tables.

Para a constituição de uma MPLS IP VPN, são configuradas, em cada um dos PEs envolvidos nessa VPN, instâncias virtuais de roteamento IP, referidas como VRFs (*Virtual Routing and Forwarding Tables*).

O subconjunto de VRFs configuradas na totalidade de PEs envolvidos em uma MPLS IP VPN define essa VPN.

Um site IP do usuário que participa de uma MPLS IP VPN é conectado diretamente à VRF dessa VPN no PE local. Essa conexão é referida como *attachment circuit (AC).*

Um PE pode conter múltiplas tabelas de encaminhamento. Uma dessas tabelas é a *default forwarding table*, e as demais são as VRFs destinadas às diferentes MPLS IP VPNs.

A *default forwarding table* destina-se ao tráfego *non-VPN*, ou seja, ao tráfego público. Um datagrama IP entrante em um PE por um AC que não se encontra associado a nenhuma VRF, é conduzido à *default forwarding table* desse PE para transmissão.

Para a associação entre os endereços IP de destino e os endereços dos PEs de destino de um LSP, assim como para a associação entre VRFs e as respectivas MPLS IP VPNs, foi definida, pela RFC 4760, uma extensão do protocolo MP-BGP (*Multiprotocol BGP*), que, por sua vez, é uma extensão do protocolo BGP-4.

Por essa extensão, cada um dos PEs de entrada em uma MPLS IP VPN altera, na respectiva VRF, os endereços IP de destino dos datagramas IP recebidos através do respectivo AC. Essa alteração consiste na inclusão de um cabeçalho adicional nos endereços IP de destino.

Esses endereços IP alterados são referidos como endereços VPN-IP (embora o que importa sejam apenas os respectivos prefixos VPN-IP, que realmente representam as rotas consideradas). O IETF definiu inicialmente apenas os endereços VPN- IPv4.

O valor contido em um campo denominado RD (*Route Distinguisher*), definido na VRF de entrada e localizado no cabeçalho dos endereços VPN-IP, passa a identificar a respectiva MPLS IP VPN no plano de controle.

O valor do campo RD possibilita aos demais PEs participantes da MPLS IP VPN, identificar as VRFs associadas a essa VPN.

Cada VRF de destino, contida no seu respectivo PE, é identificada no plano de dados por meio de um botton label, referido como label de VPN, ou label de BGP, atribuído e distribuído anteriormente, no plano de controle, por esse próprio PE.

A aplicação MPLS IP VPNs suporta também a possibilidade de constituição de grupos fechados de usuários IP em uma MPLS IP VPN. Essa facilidade é possibilitada pela utilização, no plano de controle, de um campo adicional contido no cabeçalho dos endereços VPN-IP. Esse campo denomina-se *Route Target Community* (RT).

No plano de dados, a identificação dos grupos fechados requer o uso de labels adicionais, sobrepostos aos labels de VPN na arquitetura de labels no plano de dados.

O BGP-4, por meio de outra extensão definida na RFC 3107, permite a distribuição de labels. Dessa forma, não há a necessidade de um protocolo próprio para sinalização desses labels.

No plano de dados, onde não são utilizados os endereços VPN-IP, um quadro MPLS de uma MPLS IP VPN é enviado no devido LSP, contendo o label de VPN e o label identificador do grupo fechado se for o caso. O PE de destino encaminha o quadro MPLS recebido para a devida VRF e para o devido grupo fechado, com base nesses labels.

 A partir da VRF de destino, o PE envia o datagrama IP, no modo IP usual, já sem o label de túnel, o label de VPN e o eventual label de grupo fechado, para a estação ou para as estações IP de destino.

 **4.3.4.3 – Conexões Virtuais Fim A Fim**

Conexões virtuais fim a fim são associações ponto a ponto ou multiponto estabelecidas entre instâncias de entidade pares situadas em sistemas distintos. Essas associações podem ser estabelecidas administrativamente ou por sinalização. Esse conceito não impõe qualquer restrição quanto ao tipo de rede interligando os pontos.

Circuitos virtuais, da forma em que são conceituados, representam uma sucessão de conexões virtuais fim a fim entre pares de comutadores sucessivos que os formam.

O número de circuitos virtuais ou de conexões virtuais fim a fim sobre um circuito real, não altera a capacidade de vazão de tráfego desse circuito real. Essa capacidade é limitada apenas pela velocidade de transmissão do circuito real.

O papel de qualquer tipo de conexão virtual é o de separar fluxos de tráfego de diferentes processos, entre dois ou mais pontos.

Para exemplificar, vamos admitir a necessidade de separar os fluxos de tráfego de 10 diferentes processos entre dois pontos.

Se for utilizado o modo circuito, seriam necessários 10 circuitos reais, o que pode ser obviamente oneroso.

Se forem constituídos 10 circuitos virtuais sobre um único circuito real, os 10 fluxos de tráfego serão igualmente atendidos. Ressalva-se, contudo, a necessária verificação da capacidade do circuito real para o atendimento do somatório de tráfego de todos os 10 processos.

Ocorre, contudo, que a constituição de circuitos virtuais demanda a montagem de tabelas de roteamento em todos os comutadores da rede envolvidos nos circuitos virtuais. No caso de uso de sinalização, essa montagem requer o uso de elaborados processos de sinalização. Isso significa sobrecarga de tráfego de controle e sobrecarga no uso de memória, na rede.

Surgiu então a ideia de se utilizar conexões virtuais fim a fim sobre circuitos virtuais, sobre conectividades BMA ou mesmo sobre circuitos reais. Essa ideia é antiga, na realidade, pois já vem sendo utilizada no protocolo TCP. O TCP é um protocolo de transporte fim a fim orientado a conexão entre estações finais na arquitetura TCP/IP, que opera sobreposto a uma conectividade IP.

Assim, por exemplo, se são constituidos 10 conexões virtuais fim a fim em um circuito virtual, é possível (ressalvada ainda a capacidade de tráfego do circuito real), o atendimento dos 10 fluxos de tráfego de processos do exemplo anterior nesse único circuito virtual.

No caso de uso de circuitos virtuais, que são identificados por labels, para suporte a conexões virtuais fim a fim, também identificados por labels, deve ser utilizada uma arquitetura de labels, como no MPLS, onde os labels de conexão virtual fim a fim (*botton labels)* devem ser sobrepostos aos labels dos circuitos virtuais de suporte (*top labels*) nessa arquitetura.

Existem diferentes formas para a constituição de conexões virtuais fim a fim. Nas MPLS IP VPNs, por exemplo, as conexões virtuais fim a fim são constituídas com base nas extensões do protocolo BGP-4 apresentadas no subitem 4.3.4.2 anterior. No plano de dados, as conexões virtuais entre VRFs são identificadas pelos labels de VPN.

Uma forma notória de constituição de conexões virtuais fim a fim ocorre pela utilização da arquitetura PWE 3, especificada na RFC 3985. As conexões virtuais fim a fim constituídas de acordo com a arquitetura PWE 3 são denominadas *pseudowires* (PWs).

A arquitetura PWE 3 permite a constituição de PWs emulando diferentes tecnologias (Ethernet e ATM, por exemplo), sobre diferentes tipos de PSN (*Packet Switching Network*). O MPLS é uma das PSNs que suportam a arquitetura PWE 3, por meio das aplicações VPWS e VPLS.

Os PWs, que podem ser ponto a ponto ou multiponto, podem terminar em pontos de terminação de PW (comunicação ponto a ponto), como no VPWS, ou terminar em portas de instâncias de comutação virtual localizadas nos comutadores de borda da PSN, como no VPLS.

Cada terminação de PW, referente a qualquer tecnologia de rede transportada, é conectada a um AC (*attachment circuit*) que conduz ao site da rede do usuário que utiliza o PW.

Os ACs podem ser ACs físicos ou ACs virtuais sobre um AC físico. Os ACs físicos atendem indiscriminadamente a todo o tráfego de dados intercambiado entre os sites da rede do usuário e as terminações de PW, independentemente de qualquer identificação nos quadros trafegados.

Os ACs virtuais, por outro lado, podem intercambiar discriminadamente diferentes fluxos de tráfego gerados no site, ou por ele recebido, sendo esses fluxos de dados identificados por algum parâmetro contido nos quadros trafegados.

No caso de transporte de Ethernet por PWs, por exemplo, os ACs virtuais são identificados por agrupamentos discriminados de VLAN IDs correspondentes às VLANs que participam de cada um dos ACs virtuais. Esses agrupamentos discriminados podem consistir da totalidade dos VLAN IDs, de subgrupos de VLAN IDs ou de apenas um VLAN ID.

O acesso de um AC físico a uma terminação de PW é referido como acesso no *raw-mode*, ou acesso baseado em porta (*port-based*). No acesso no *raw-mode*, todo o tráfego originado ou destinado ao site é transmitido no PW, independentemente de qualquer identificação nos quadros transmitidos.

O acesso de um AC virtual a uma terminação de PW é referido como acesso no *tagged-mode*. Um PW assim terminado destina-se exclusivamente ao tráfego de quadros contendo o identificador ou o conjunto de identificadores associado a esse PW.

No exemplo de PWs Ethernet, o acesso no *tagged-mode* é também referido como acesso *VLAN-based*.

Outro tipo de rede que utiliza conexões virtuais fim a fim são as redes Carrier Ethernet. A essência de Carrier Ethernet é a Camada Ethernet (*ETH-Layer*), que consiste no uso de conexões virtuais fim a fim, referidas como EVCs (*Ethernet Virtual Connections*), associando instâncias de serviço configuradas em UNIs.

As UNIs localizam-se nas bordas de alguma rede de transporte que as interliga. Essas redes de transporte constituem a Camada de Transporte (*TRAN-Layer*).

A *TRAN-Layer* evidencia a amplitude da variedade de tipos de rede que podem suportar conexões virtuais fim a fim. De fato, são utilizadas na *TRAN-Layer* redes modo circuito (SDH e OTN, por exemplo), redes modo pacote orientadas a conexão (VPWS, VPLS e MPLS-TP, por exemplo) e redes modo pacote sem conexão (PB e PBB, por exemplo). PB significa *Provider Bridging*, enquanto PBB significa *Provider Backbone Bridging*.

**4.3.4.4 – VPWS (Virtual Private Wire Service)**

O VPWS é uma aplicação que utiliza PWs ponto a ponto entre pontos de terminação de PW localizados em comutadores de borda de PSNs, como, por exemplo, de redes MPLS.

Os PWs constituídos no VPWS podem ser diferenciados entre si, com o propósito de suportar o transporte de diferentes tecnologias de rede, como Ethernet, ATM, Frame Relay, PPP/HDLC, etc...

No caso do MPLS como PSN, a aplicação VPWS é referida como MPLS VPWS. No contexto de redes MPLS, contudo, a simples denominação VPWS indica o MPLS VPWS.

No VPWS, os ACs podem acessar os pontos de terminação de PW no *raw*-*mode* ou no *tagged-mode*. Como cada um dos ACs é conectado a um ponto de terminação de PW, e como um PW ponto a ponto representa uma conexão virtual ponto a ponto entre pontos de terminação de PW, todo o link entre os dois sites do usuário distantes representa uma conexão ponto a ponto.

Assim, um quadro enviado por um site no AC associado a um PW, será transmitido diretamente para o site distante associado a esse PW e ao LSP que o suporta, sem a necessidade de consulta a qualquer parâmetro contido no quadro.

Vamos exemplificar a operação do VPWS por meio de Ethernet PWs, onde os ACs virtuais são identificados por VLAN IDs.

Nos ACs físicos, onde o acesso aos pontos de terminação de PW ocorre no *raw-mode (port-based),* pode ser intercambiado indiscriminadamente tráfego de todas as VLANs existentes nos dois sites Ethernet do usuário, sem qualquer consulta aos respectivos VLAN IDs.

No *tagged-mode*, cada um dos ACs virtuais, identificado de modo discriminado por um VLAN-ID, por um subconjunto de VLAN IDs ou pela totalidade de VLAN IDs, é associado a um ponto de terminação de PW.

A Figura 15 mostra um exemplo de rede VPWS utilizando Ethernet PWs no *tagged-mode*.

**Figura 15 - Utilização de Ethernet PWs no tagged-mode.**

Nessa figura, o PW 1 e o PW 2, assim como os correspondentes AC 1 e AC 2 no lado esquerdo e AC 4 e AC 5 no lado direito, são individualmente identificados, respectivamente, pelo VLAN ID A e pelo VLAN ID B.

Na parte inferior da figura, o PW 3 e os correspondentes AC 3 e AC 6 são identificados pelo subconjunto {VLAN ID C, VLAN ID D}, ou seja, pelo VLAN ID C ou pelo VLAN ID D.

No plano de dados do VPWS, os PWs são identificados por meio de labels de PW, que se posicionam como *bottom* *labels* na arquitetura de labels do MPLS.

Cada PW é rigidamente associado a um LSP, não sendo necessário, portanto, qualquer mecanismo dinâmico de associação como ocorre no VPLS.

A sinalização para o estabelecimento de PWs, e para a correspondente distribuição de labels de PW, utiliza uma extensão do protocolo LDP definida na RFC 4447.

Não há a necessidade de resolução de endereços no VPWS, até mesmo porque a rede externa não é uma rede IP, não se utilizando, consequentemente, qualquer protocolo EGP.

**4.3.4.5 – VPLS (Virtual Private LAN Service)**

 O VPLS é uma aplicação do MPLS que utiliza comutação fim a fim entre instâncias virtuais emuladas de switches Ethernet, utilizando PWs para a interconexão dessas instâncias.

De forma assemelhada à aplicação MPLS IP VPNs, onde são constituídas VPNs IP, no VPLS são constituídas VPNs bridged Ethernet, referidas como VPLS VPNs.

As instâncias virtuais emuladas no VPLS são referidas como VSIs (*Virtual Switching Instances*), que se localizam nos PEs participantes da respectiva VPLS VPN.

Como as redes MPLS operam por circuitos virtuais, ou seja, por LSPs, as VSIs transmitem quadros Ethernet multicast e broadcast por NBMA. Para alcançar cada uma das demais VSIs da VPLS VPN é requerido o uso de um LSP.

As VSIs de uma VPLS VPN são interconectadas por Ethernet PWs, que como no VPWS são identificados por labels de PW.

 Os conceitos de *raw-mode* e de *tagged-mode* são aplicados. No caso de *tagged-mode*, são utilizados, como no VPWS, os VLAN IDs das VLANs existentes nos dois sites de usuário como identificadores de ACs virtuais e de PWs virtuais.

A sinalização para a constituição de PWs no VPLS pode ocorrer com base em dois diferentes protocolos:

- Extensão específica do BGP-4 para sinalização e *auto-discovery* de PWs (RFC 4761);

- Extensão específica do LDP para sinalização de PWs (RFC 4762).

Na rede MPLS de suporte roda, de forma independente, o protocolo IGP correspondente ao tipo de rede MPLS utilizado. Os LSPs são constituídos da mesma forma que nas demais aplicações do MPLS, podendo ser inclusive de uso comum para essas aplicações.

Como no VPWS, os PWs no VPLS são também mapeados em LSPs da rede MPLS de suporte. Cada VSI é conectada às demais VSIs de uma VPLS VPN por meio de dois LSPs unidirecionais ou de um LSP bidirecional, nos quais se encontram mapeados os correspondentes PWs.

Na transmissão, em uma VPLS VPN, de um quadro MAC multicast/broadcast ou de um quadro MAC unicast cujo endereço de destino não tenha sido aprendido, a VSI de origem insere os devidos PWs e transmite o quadro por todos os LSPs que nela terminam.

Caso tenha ocorrido a aprendizagem do endereço MAC unicast de destino do quadro, esse quadro será transmitido direcionadamente para a VSI de destino, contendo o correspondente PW e utilizando o LSP que conduz à VSI de destino.

A identificação do LSP a ser utilizado em uma transmissão direcionada de um quadro MAC unicast resulta do processo de aprendizagem de endereços MAC de destino. Dessa forma, a VSI de origem é capaz de identificar o devido LSP para a transmissão do quadro unicast.

 Não ocorre obviamente resolução de endereços MPLS no VPLS, da mesma forma que não ocorre no VPWS.

**4.3.5 - MPLS no Modelo Par**

 A aplicação do Modelo Par abrange todos os tipos de redes MPLS e todas as suas aplicações. O roteamento interno na rede MPLS ocorre na arquitetura TCP/IP, constituindo-se então em um roteamento IGP. Os circuitos virtuais do plano de dados terminam nos comutadores de borda (nos PEs) e não ocorre resolução de endereços.

Caso a rede externa transportada pelo MPLS seja uma rede IP, os datagramas do protocolo EGP dessa rede atravessam a rede MPLS incorporados ao plano de controle TCP/IP da rede MPLS. Lembramos que no Modelo Overlay esses datagramas atravessam a rede MPLS envelopados em quadros de dados da rede de camada 2 de suporte.

O protocolo EGP através do MPLS depende da aplicação do MPLS utilizada. O serviço MPLS Público utiliza o BGP-4 como EGP através da rede MPLS, enquanto a aplicação MPLS IP VPNs utiliza uma extensão do protocolo MP-BGP, que por sua vez é uma extensão do BGP- 4 com esse intento.

Nas aplicações VPWS e VPLS não existem obviamente protocolos EGP através da rede MPLS.

Como vimos no subitem 4.3.4.1 anterior deste tutorial, no MPLS Básico o OSPF distribui as informações de roteamento por meio de LSAs, enquanto o IS-IS as distribui utilizando LSPs.

Nos protocolos OSPF-TE e GMPLS OSPF-TE, que operam por *source routing*, são utilizadas LSAs opacas, que são processadas apenas pelos PEs. O mesmo ocorre com os protocolos ISIS-TE e GMPLS ISIS-TE, que utilizam LSPs opacas.

 No LDP, que opera no modo descentralizado, as solicitações para a obtenção de labels, realizadas individualmente pelos LSRs, indicam as FECs (*Forwarding Equivalence Classes*) a serem associadas aos labels que irão definir cada LSP.

No RSVP-TE e no GMPLS RSVP-TE, que operam centralizadamente, as solicitações de labels são incorporadas às mensagens *RSVP Path*, no sentido *downstream*, por meio do *LABEL\_REQUEST Object*. As rotas a serem utilizadas pelos LSPs encontram-se explicitadas nessas mensagens, pelo *Explicit\_ Route Object (*ERO)

A distribuição dos labels solicitados ocorre no sentido *upstream*, por meio do *LABEL Object*, contido em mensagens *RSVP Resv*.

**5 – CONSIDERAÇÔES FINAIS**

 Como visto ao longo deste tutorial, as redes modo pacote comutadas orientadas a conexão podem ser constituídas no Modelo Overlay ou no Modelo Par.

 O Modelo Overlay foi o adotado nas tecnologias modo pacote orientadas a conexão iniciais, que são o X.25, o Frame Relay e o ATM.

 Essas redes passaram por um processo evolutivo por um período de aproximadamente 20 anos, partindo do X.25 para o Frame Relay e, supostamente, do Frame Relay para o ATM. Na realidade, essa última transição foi nebulosa, tendo a sobrevida do Frame Relay ultrapassado a do ATM em alguns casos.

 Devido a algumas considerações, particularmente no que diz respeito à adequabilidade ao TCP/IP, as redes no Modelo Overlay chegaram aos seus limites no final do século passado, dando ensejo à definição e ao predomínio do MPLS, já operando no Modelo Par.

 O MPLS, cuja aceitação foi muito grande, representa o único exemplo atual de uso do Modelo Par.

 Essa tecnologia, que de início representava apenas uma solução para aprimorar o ATM pela adoção de um novo plano de controle sem conexão baseado no TCP/IP, passou por uma evolução acelerada em termos de facilidades adicionais, de novos tipos de rede e de novas aplicações.

 Partindo do MPLS Básico, limitado pelo suporte no OSPF ou no IS-IS, evolui-se para o MPLS-TE, já com constraining routing e engenharia de tráfego, e daí para o MPLS-TP, com o mesmo embasamento do MPLS-TE, mas concebido com um perfil de transporte para a sua utilização como PTN.

 Como vimos, o MPLS-TP adota o GMPLS como plano de controle.

 As aplicações do MPLS, que de início se resumiam à constituição de extensões orientadas a conexão de redes IP (como a Internet, por exemplo), evoluíram, ainda para o atendimento de redes IP, no sentido de possibilitar a constituição de MPLS IP VPNs.

 Nas MPLS IP VPNs, a rede MPLS emula IP VPNs mediante a constituição de instâncias virtuais de roteadores IP nos PEs da rede, instâncias essas referidas como VRFs.

 A seguir, graças à concepção HRK, evoluiu-se para a libertação do MPLS das garras do IP, pela definição dos serviços VPWS e VPLS.

 No VPWS, a rede MPLS comporta-se como um conjunto de conexões virtuais ponto a ponto, conexões essas destinadas ao transporte de diferentes tipos de rede de camada 2, como ATM, Frame Relay, Ethernet, PPP e HDLC. O VPWS possibilita também o transporte de sequências de bits estruturadas ou não estruturadas.

 No VPLS, a rede MPLS emula VPNs bridged Ethernet mediante a constituição de instâncias virtuais de bridges (switches) Ethernet nos PEs da rede, instâncias essas referidas como VSIs.

**6– REFERÊNCIAS**

**6.1 – Livros:**

 – ENNE, A. J. F. – TCP/IP sobre MPLS. Rio de Janeiro: Ciência Moderna 2009.

 – ENNE, A. J. F. – Frame Relay: Redes, Protocolos e Serviços. Rio de Janeiro: Axel Books e Embratel, 1998.

 – FARREL, A., BRYNSKIN, I. – GMPLS: Architecture and Applications. San Francisco, USA: Morgan and Kaufmann, 2006.

-FARREL, A., DAVIE, B. S. – MPLS: Next Steps. San Francisco, USA: Morgan and Kaufmann, 2008.

- DAVIE, B. S., RECKHTER, Y. – MPLS: Technology and Applications. San Francisco, USA: Morgan and Kaufmann, 2000.

- CAVANAGH, J. P. – Frame Relay Applications. San Francisco, USA: Morgan and Kaufmann, 1998.

- SACKET, G. C., METZ, C. Y. – ATM and Multiprotocol Networking, New York, USA: McGraw Hill, 1997.

**6.2 – Recomendações do ITU-T**

- Y.311: B-ISDN General Network Aspects, 1993.

- Y.321: B-ISDN Protocol Reference and its Applications, 1991.

- Y.327: B-ISDN Functional Architecture, 1993.

- Y.361: B-ISDN ATM Layer Specification, 1993.

**6.3– Padrões do ATM Forum:**

- ATM User-Network Interface (UNI) Specification Version 3.1, 1995.

- LAN Emulation over ATM Version 1.0, 1995.

- LAN Emulation over ATM Version.

- P-NNI Draft Specification, 1996.

- Baseline Text for MPOA, 1996.

- UNI Signaling 4.0, 1995.

**6.4– Padrões do IETF (RFCs):**

- RFC 3031: Multiprotocol Label Switching Architecture.

- RFC 3032: MPLS Label Stack Encoding.

- RFC 3036: LDP Specification.

- RFC 3209: RSVP-TE – Extensions to RSVP for LSP Tunnels.

-RFC 3985: Pseudowire Emulation Edge-to-Edge (PWE 3) Architecture.

- RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

- RFC 4761: VPLS Using BGP for Auto-Discovery and Signaling.

- RFC 4762: VPLS Using LDP Signaling.

**7– TESTE SEU ENTENDIMENTO**

7.1 – O protocolo DL-Core utilizado no Frame Relay resulta da seguinte medida:

A) Retirada da função de controle do LAP-B.

B) Retirada da função de endereço do LAP-F.

C) Retirada da função de controle do LAP-F porque o campo Endereço do LAP-F possui dois octetos.

D) Retirada da função de controle do LAP-F porque o LAP-F é mais robusto que o LAP-B.

7.2 – Qual a frase correta?

A) O serviço DBR (CBR) de camada ATM destina-se à transmissão de pacotes no modo best-effort.

B) Os serviços ABR e UBR são best-effort, mas apenas o ABR garante uma taxa mínima de transmissão e utiliza controle de fluxo.

C) O serviço ABR destina-se às aplicações isócronas com taxas de bit variáveis.

D) Nenhuma delas.

7.3– Qual a frase correta?

A) A camada AAL do ATM é responsável pela adaptação das aplicações para o atendimento pela camada ATM.

B) A camada AAL do ATM é responsável pela aplicação de QoS na rede.

C) A camada AAL é interpretada por todos os comutadores da rede ATM, inclusive pelos que se encontram no seu interior.

D) Nenhuma delas.

7.4– Qual a frase correta?

A) No MPLS sobre ATM utiliza-se labels de túnel no formato genérico.

B) No MPLS sobre Frame Relay o campo DLCI perde a sua função.

C) Quando se utiliza o PPP como suporte ao MPLS são utilizados labels de túnel no formato genérico.

D) Quando se utiliza Ethernet como suporte ao MPLS a comutação ocorre com base nos endereços MAC.

7.5– Qual a frase correta?

A) Na aplicação Serviço MPLS Público é necessário apenas o label de túnel.

B) No MPLS Básico é necessário apenas o label de túnel.

C) O VPLS pode operar com apenas o label de túnel, sem o label de PW.

D) O VPWS destina-se exclusivamente ao transporte de Ethernet.

7.6– Qual a frase correta?

A) O GMPLS destina-se exclusivamente a controlar o MPLS-TP.

B) O GMPLS cursa obrigatoriamente pela mesma rede em que cursa o plano de dados da rede por ele controlada.

C) São utilizados labels de túnel no plano de dados de redes modo circuito controladas pelo GMPLS.

D) Nenhuma delas.

 **ATENÇÃO: RESPOSTAS NA PRÓXIMA PÁGINA**

**RESPOSTAS**:

7.1 - C

7.2 - B

7.3 - A

7.4 - C

7.5 - A

7.6 - D