

# Modelo de Serviço de Difusão Seletiva IP: Aperfeiçoamentos ou Mudanças?

Flávio Alencar do Rêgo Barros  
[farb@openlink.com.br](mailto:farb@openlink.com.br)

Michael Anthony Stanton  
[michael@ic.uff.br](mailto:michael@ic.uff.br)

Instituto de Computação  
Universidade Federal Fluminense  
R Passo da Pátria, 156 , bloco E, sala 350  
24210-240, Niterói, RJ

## Resumo

O modelo de Deering do serviço de comunicação em grupo pela Internet, mesmo consideradas a sua simplicidade e elegância, apresenta limitações para o completo desenvolvimento de difusão seletiva IP, seja devido à profusão de demandas contraditórias de aplicações, seja pelo pouco apoio do núcleo da rede por razões técnicas e econômicas. Se alguns destes problemas deverão ser atacados pelas camadas de transporte e aplicação, fora do escopo estrito do modelo atual, também dentro dele surgem deficiências, principalmente no que se refere ao roteamento interdomínio, envolvendo gerência de endereços, inconsciência quanto à QoS e perda de funcionalidade. A percepção destas deficiências já obtém uma resposta através do projeto MASC/BGMP que representa a transição do modelo atual. Muitos, porém, advogam que o sucesso observado nas aplicações *unidifusão* baseadas na suíte TCP/IP só se reproduzirá em difusão seletiva mediante soluções com maior simplicidade que as existentes ou com tratamentos que também envolvam inteligência do interior da rede. Neste sentido, analisamos as propostas RAMA e CLM, destinadas a responder ao argumento da simplicidade. Analisamos também AIM, voltada para a organização do grupo de receptores por semelhança de interesses. Alavancar aplicações de grupo pela Internet certamente passará por uma, outra ou ambas linhas.

## Abstract

Deering's model of Internet group communication, in spite of its simplicity and elegance, imposes limits on the complete development of IP multicast, due either to the profusion of contradictory requirements of applications, or to the reduced support provided by the network core for technical or economic reasons. Even if some of these difficulties may be resolved at the transport or application layers, thus remaining outside the scope of the present model, there also appear defects within this model, mainly due to inter-domain routing, involving address management, to QoS insensitivity and to loss of functionality. The recognition of these defects has already led to the solution presented by the MASC/BGMP project, which involves a transition from the present model. However there are many who argue that the success of unicast applications in TCP/IP will only be repeated in multicast applications through the use of much simpler solutions than the existing ones, or by including greater intelligence in the network interior. With this in mind, we analyze here the proposals RAMA and CLM, which may be seen to demonstrate greater simplicity. We also look at AIM, designed for organizing receivers into subgroups with similar interests. Leveraging Internet group applications will certainly involve one or other, or even both of these approaches.

**Palavras chave:** Internet: protocolos, serviços e aplicações; difusão seletiva; comunicação em grupo.

## 1. Introdução

Aplicações de grupo exigem novos patamares de uso da Internet e são bastante exigentes da sua infra-estrutura. Tais aplicações podem ser grupadas em classes *um-para-muitos* (distribuição escalonada de áudio e vídeo, distribuição de arquivos, etc.), *muitos-para-um* (coleta de dados e pesquisas, leilões, etc.) e *muitos-para-muitos* [QUI99] (conferência multimídia em tempo real, grupos de colaboração ou conversação, sistemas interativos distribuídos, jogos interativos, etc.), ou uma variante desta, *poucos-para-poucos*.

O que se chama modelo de serviço atual de difusão seletiva<sup>1</sup> na Internet (ou *difusão seletiva à moda Deering* ou ainda *difusão seletiva IP*) funda-se em extensões ao protocolo IP, referindo-se às questões da camada de rede que suportem comunicação de grupo utilizando endereços classe D. Ele é derivado fundamentalmente de dois componentes: o *Modelo de Grupo de Estações* e um *Protocolo de Roteamento de Difusão Seletiva* [DEE91]. Enquanto o primeiro se preocupa com a organização de grupos de estações consumidoras do tráfego do grupo (uma fonte emissora não necessita fazer parte do grupo, precisa *apenas* conhecer o endereço do grupo a que ela se propõe transmitir dados), o segundo necessita de um protocolo de roteamento de difusão seletiva para construir e manter uma árvore de distribuição que permita o encaminhamento dos pacotes. Este protocolo é de interesse principalmente dos provedores de serviços de rede. É nestes dois componentes, protocolo de roteamento e modelo de grupo de estações, que se fundamenta a diferente natureza da difusão seletiva perante a *unidifusão*<sup>2</sup> e é a partir destes dois componentes que todas pesquisas, propostas e implementações têm sido feitas nesta última década. A estes dois modelos se pode atribuir as dificuldades e carências das quais difusão seletiva padece (e unidifusão não!).

Resolver as questões de difusão seletiva é, primariamente, resolver as questões de roteamento, em particular as questões de roteamento interdomínio, porque em domínios diferentes podem ser estabelecidas políticas e escolhas (administrativas ou técnicas) diferentes, e estas escolhas podem acarretar problemas de escalabilidade e custos para estações e para a rede. Mas não é só isso. As questões colocadas por aplicações de comunicação de grupo pela Internet quanto a confiabilidade, desempenho, controle de fluxo e congestionamento, segurança, gerenciamento e coordenação de grupo e outros mais, fazem a difusão seletiva envolver, para além do modelo de serviço atual, as camadas de aplicação e transporte e até mesmo a camada de enlace.

Na seção 2 estaremos identificando as bases do modelo de serviço atual de difusão seletiva IP, na seção 3, analisaremos a transição que ora se verifica com vistas a seu aprimoramento, para, a seguir, na seção 4 fazermos uma avaliação deste modelo de serviço e suas anunciadas extensões, identificando demandas não cobertas, seguindo na seção 5 a análise de propostas que têm sido feitas para superar algumas destas limitações. As conclusões são apresentadas na seção 6.

## 2. O Modelo de Serviço Atual

A proposta original de Deering [DEE89] se baseia em transmissões de difusão seletiva IP para um grupo de estações caracterizado por um endereço classe D, onde a entrega dos datagramas se dá com a mesma confiabilidade “melhor esforço” da entrega de datagramas por unidifusão IP. O endereço de grupo é permanente, mas os membros podem não ser. Membros entram e saem do grupo segundo sua própria conveniência. O modelo diz respeito a extensões ao IP, definindo o protocolo IGMP (*Internet Group Management Protocol*).

O IGMP tem apenas dois tipos de mensagens, de *pedidos* e de *anúncios*. Roteadores locais difundem periodicamente na rede local a mensagem de pedido para descobrir quais grupos de estações receptoras têm membros em sua rede local. As estações respondem com mensagens de *anúncios* imediatamente (membro sem temporizador) ou depois de temporizar

---

<sup>1</sup> *Difusão Seletiva*, originalmente *multicast*. “*Multicasting*” é um método que admite cópias de um único pacote serem passadas para um subconjunto selecionado de possíveis destinatários [COM95].

<sup>2</sup> *Unicast* é o termo original. “*Unicasting*” é uma técnica pela qual um pacote é enviado a um único destinatário. Chamaremos *unidifusão*.

aleatoriamente (membro com temporizador), para reduzir a chance de acúmulo de *anúncios* no roteador. É possível ainda uma estação efetuar um “*join*”<sup>3</sup> a um novo grupo, e, nesta circunstância, o processo de associação é imediato.

O processo de um membro se juntar ou sair de um grupo compete ao IGMP, porém, são necessárias informações adicionais para um membro potencial decidir juntar-se ou não ao grupo. Um grupo de trabalho da IETF, o MMUSIC (*Multiparty Multimedia Session Control*), é o responsável por desenvolver protocolos de anúncio de conteúdo de grupo. Existem atualmente duas formas de lidar com a questão [MIL98]. A forma mais corriqueira é usar o modelo “*teledifusão*”, tendo sido desenvolvido para isto o SAP (*Session Announcement Protocol*), protocolo para enviar um fluxo de endereços “bem conhecidos” para orientar potenciais receptores. SAP utiliza o protocolo SDP (*Session Description Protocol*) para descrever o conteúdo das sessões que estão sendo anunciadas, e ambos são ferramentas bastante usadas em teledifusão pelo Mbone<sup>4</sup>. Este modelo, semelhante à TV aberta, é fracamente acoplado, pois os emissores de sessão não conhecem quem possa estar “escutando” suas transmissões.

Outro enfoque, também desenvolvido dentro do grupo de trabalho da IETF MMUSIC, é representado pelo SIP (*Session Initiation Protocol*), usado para convidar membros para conferências de alguma espécie, sendo muito utilizado para aplicações de vídeo/áudio conferências.

Além do IGMP, feito para gerenciar entrada e saída de estações no grupo, são necessários dois protocolos: um para roteamento no interior de um domínio (chamado MIGP<sup>5</sup> [SAH00]) e outro usado em roteadores de fronteira conectando domínios. Protocolos de roteamento de difusão seletiva (do tipo MIGP) baseados no modelo de serviço atual constroem árvores de distribuição para difusão seletiva usando um mecanismo que reflete a forma na qual candidatos se associam: ou usam mecanismos de junção explícita ao grupo com a manutenção de estado *soft*<sup>6</sup> nos roteadores (chamados protocolos de *modo esparsos*) ou usam mecanismos de difusão de associação ou, ainda, mecanismos de inundação e poda (protocolos de *modo denso*). As propostas práticas de árvore de distribuição em difusão seletiva convergem em dois tipos: o primeiro tipo, árvore baseada na fonte, apropriada para aplicações *um-para-muitos* ou suas variantes que demandem alta taxa de dados e baixo retardo com controle de acesso por fonte em cenários similares à teledifusão. O outro tipo, árvore compartilhada, é próprio para aplicações com muitas fontes de baixa taxa de dados, mas pouco exigentes de retardo de entrega, ou, ainda, em cenários de uso de árvores baseadas na fonte que se caracterizem por grande superposição de caminhos. O uso de protocolos baseados em fonte implica na manutenção de estados de grupo nos roteadores da rede da forma (*endereço da fonte, endereço classe D*), enquanto em árvores compartilhadas, os roteadores deverão manter estados da forma (\*, *endereço classe D*), e a localização dos

---

<sup>3</sup> A interface de serviço IP é estendida de modo prover duas novas operações: *JoinHostGroup* e *LeaveHostGroup*.

<sup>4</sup> **Multicast Backbone**. Rede virtual suportando pacotes de difusão seletiva IP, em funcionamento desde 1992 [WAN00b][MIL98].

<sup>5</sup> **Multicast Internal Group Protocol**. Poderia ser qualquer um dos protocolos intradomínio, por exemplo, PIM-SM ou DVMRP.

<sup>6</sup> Manter estado *soft* em roteadores significa manter registros para encaminhamento de dados dos membros de um grupo de difusão seletiva por tempo limitado, à espera de alguma atualização ou, expirado o tempo, do descarte. Influencia significativamente no custo de manter estado *soft* os mecanismos de escalonamento e gerência de filas em roteadores e esquemas de ordenamento e de descarte em receptores. Manter estado *soft* nos roteadores é considerado preferível a manter estado *hard* por uma série de fatores, como a flexibilidade, administração algorítmica, tolerância à falhas, e outros.

núcleos poderá ser administrativamente configurada ou poderá ser utilizado um serviço de diretório para este fim.

Quanto a políticas de encaminhamento, existem duas possíveis modalidades: com a árvore construída o tráfego pode ser encaminhado de modo *unidirecional*, quando parte sempre da raiz da árvore em direção aos consumidores, ou *bidirecional*, quando pacotes podem ser encaminhados em qualquer direção em um roteador da árvore.

No campo das árvores baseadas em fonte, o protocolo DVMRP (*Distance Vector Multicast Routing Protocol*) [WAI88] computa sua própria tabela de roteamento, utiliza o encaminhamento unidirecional e mantém uma política de manutenção da árvore de periodicamente descartá-la e reconstruí-la. O PIM-DM<sup>7</sup> é unidirecional, mantém estado *soft* nos roteadores e baseia-se em tabelas de roteamento unidifusão. MOSPF (*Multicast Extensions to OSPF*) [MOY94] aproveita a tabela de roteamento da unidifusão, também é unidirecional, mas a política de manutenção da árvore pressupõe atividades somente em resposta a mudanças na topologia ou na associação.

Dentre os protocolos que usam árvores compartilhadas baseadas em núcleo, PIM-SM (*Protocol Independent Multicast - Sparse Mode*) [DEE98b], que utiliza encaminhamento unidirecional e estados *soft* nos roteadores, baseia-se em tabelas de roteamento unidifusão, mas necessita de pré-distribuição de informação do núcleo. A proposta CBT (*Core-Based Trees*) [BAL97], que é bidirecional, sendo atualizada periodicamente a árvore de distribuição, baseia-se em tabelas de roteamento unidifusão, mas não muda em resposta a mudanças na topologia.

Todos estes protocolos, por diferentes razões, sofrem problemas de escalabilidade: por conta da inundação, com DVMRP e PIM-DM a utilização dos enlaces é ineficiente, além do que precisarão ser mantidos estados de poda nos roteadores; o MOSPF requer que todos os roteadores conheçam onde estão todos os receptores, situação pouco escalável para um cenário de associação dinâmica; o PIM-SM exige que as informações relativas ao conjunto de núcleos sejam previamente distribuídas, só então pode fluir o tráfego difusão seletiva [HAN99]. Desta forma, estes protocolos são mais adequados para executar dentro de um domínio e não entre domínios diferentes.

A primeira solução interdomínio prática, o MSDP (*Multicast Source-Discovery Protocol*), foi desenvolvida como extensão ao protocolo interdomínio para unidifusão BGP atuando como ligação de domínios PIM-SM [FAR00]. MSDP contorna o problema da independência de domínios, mas não é escalável. Para tratar deste problema, uma proposta prática tem sido permitir o MSDP rodar sobre um protocolo de fronteira com capacidade de difusão seletiva conhecido como BGP4+ ou MBGP<sup>8</sup>. O conjunto PIM-SM/MSDP/MBGP garante uma solução completa, mas de curto termo, para difusão seletiva.

MBGP é formado por um conjunto de extensões para difusão seletiva do BGP versão 4, separando políticas de unidifusão e difusão seletiva, mas utilizando as mesmas idéias de agregação de rotas para conectar domínios autônomos. Roteadores de fronteira de domínios neste caso deverão ser capazes de manter tabelas separadas para unidifusão e difusão seletiva, e o objetivo do MBGP é comunicar mapeamentos de faixas de endereços classe D por domínios para os roteadores de fronteira. Com MBGP, roteadores necessitam conhecer apenas a topologia interna ao seu domínio e o caminho para alcançar um roteador de fronteira de domínio que rode MBGP. Na fronteira, MBGP pode portar rotas de difusão seletiva

---

<sup>7</sup> *Protocol Independent Multicast - Dense Mode* [DEE98a]. O grupo da IETF IDMR (*Inter-Domain Multicast Routing*) tem como tarefa desenvolver padrões que possam prover escalabilidade entre domínios para este tipo de tráfego.

<sup>8</sup> RFC 2283. O acrônimo MBGP, antes de ser oficial, é considerado uma terminologia aceitável, significando *Multicast Border Gateway Protocol*.

adicionando às mensagens BGP4+ o identificador de família de endereços subsequentes, especificando informação de encaminhamento, seja de unidifusão, seja de difusão seletiva.

### 3. Transição do Modelo Atual: Aperfeiçoamento ou Complicação?

A transição que se realiza no modelo de serviço atual aponta para o que parece ser a solução natural para o problema da escalabilidade em comunicação por difusão seletiva: o *roteamento hierárquico*, onde os nós são organizados em domínios. Os protocolos, operando sobre a conexão entre domínios, poderão ignorar os detalhes do interior de outros domínios. A arquitetura MASC/BGMP [KUM98][THA00] incorpora um conjunto de três protocolos<sup>9</sup> que tratam dinamicamente do esquema de endereçamento e, junto com o protocolo BGMP, representam esta transição.

MASC, atuando no nível de domínios, destina-se a resolver dois problemas básicos: encontrar um endereço de difusão seletiva globalmente único, e evitar colisões na escolha deste endereço. Cada domínio terá um servidor de alocação de endereços de difusão seletiva (MAAS) coordenando a entrega de endereços de difusão seletiva e monitorando a utilização do espaço de endereços. Haverá também um ou mais nós (tipicamente os roteadores de fronteira de domínio) rodando MASC, formando uma hierarquia que refletirá a topologia interdomínio. Nesta hierarquia haverá domínios backbone (sem domínios “pai”) que trocam entre si mensagens de utilização de rotas, alcançando acordos bilaterais, a partir dos quais estarão aptos a alocarem espaços de endereços para seus domínios “filhos”. O espaço de endereços de difusão seletiva é particionado entre regiões, e em cada região os nós MASC anunciam seus endereços. Domínios MASC “ouvem” estes anúncios e solicitam porções destes endereços, ficando à espera de possíveis colisões. Alcançado um acordo bilateral e estabelecido os endereços de um domínio, um domínio “filho” requisita endereços de um domínio “pai” em um esquema *solicita-colide*. Um domínio “pai” que tenha recém adquirido endereços MASC usa um tipo de rota em BGP chamado rota de grupo. Rotas de grupo contêm a faixa de endereços de difusão seletiva alocada e injetada no BGP pelo nó MASC. A porção da tabela de roteamento que mantém rotas de grupo é chamada G-RIBs e o BGMP usa os G-RIBs para construir uma árvore compartilhada de difusão seletiva. Para alcançar uma boa utilização, a cada faixa de endereços é associado um tempo de vida de alocação de endereços para um determinado domínio. Este esquema hierárquico favorece a escalabilidade, mas requer que as aplicações de difusão seletiva sejam escritas levando em conta estas possíveis mudanças de endereços.

O protocolo BGMP roda em roteadores de fronteira de domínio e tem como objetivo construir árvores compartilhadas bidirecionais entre eles. À semelhança do BGP utiliza o TCP para transporte de sua sinalização. A construção da árvore depende de dois componentes: o MIGP, atuando dentro de um domínio para informar aos roteadores de fronteira sobre a associação de grupo, e o BGMP, usado para construir junto a outros roteadores de fronteira de domínio a árvore compartilhada, em um mecanismo semelhante ao PIM, só que a raiz da árvore BGMP não é um roteador específico e sim todo o domínio. A escolha de potenciais

---

<sup>9</sup> **MASC** - *Multicast Address-Set Claim*, com atuação interdomínio, **AAP** - *Address Allocation Protocol*, com atuação intradomínio, e **MADCAP** - *Multicast Address Dynamic Client Allocation Protocol*, usado pelas estações para requisitar endereços de difusão seletiva [PAT99]. **MAAA** é *Multicast Address Allocation Architecture* [HAN97][DIO00][ALM99][OOM00]. O grupo IETF BGMP WG tem o *mailing list* em <ftp://catarina.usc.edu/pub/bgmp/mail-archive/>, outubro de 1999.

núcleos da árvore leva em conta aspectos administrativos e de desempenho, significando uma grande probabilidade de escolha não ótima da raiz da árvore.

Este conjunto de protocolos se destina a oferecer uma solução de longo termo para difusão seletiva. São objetivos do projeto MASC/BGMP, além da escalabilidade resultante da redução de estados de encaminhamento, a estabilidade proveniente da redução do *overhead* do protocolo, a manutenção das premissas do modelo de serviço atual, e a habilidade para lidar com políticas em diferentes domínios. O projeto pressupõe ainda a independência do roteamento intradomínio, reduzindo qualquer impacto de modificações ou atualizações de protocolos de roteamento de um domínio no outro.

Com o completo estabelecimento desta transição, uma solução genérica mais completa de comunicação por difusão seletiva poderá envolver o conjunto formado por IGMP, para associação de estações finais, PIM-SM, para roteamento em ambientes esparsos no interior de um domínio, a arquitetura MAAA, conectando estações, domínios e servidores de endereços de difusão seletiva, e BGMP para comunicação entre domínios.

#### 4. Uma Avaliação do Modelo Atual

Uma grande força por trás do modelo de Deering está no anonimato dos participantes do grupo, reduzindo as complexidades dos mecanismos para prover distribuição multiponto. Por outro lado, uma fraqueza do modelo difusão seletiva IP é a falta de informação de endereçamento. Um endereço classe D é nada mais que um nome, nada diz sobre a localização dos membros do grupo ou a árvore à qual eles estão conectados, e isto restringe tanto a possibilidade de entrega de dados baseado no seu conteúdo, quanto a possível cooperação entre os protocolos que forneçam o serviço de difusão seletiva e as aplicações, ou mesmo cooperação entre protocolos fim a fim que utilizem o serviço [LEV99]. As diversas necessidades de difusão seletiva, nos seus diversos níveis, são cobertas por uma profusão de protocolos, ao contrário da simplicidade de unidifusão. Na Figura 1 encontra-se uma comparação entre difusão seletiva [DIO00] e unidifusão.

Unidifusão		Difusão Seletiva				
DHCP IANA	DNS	Serviços de Estação	Protocolos Difusão Seletiva Confiável	MADCAP/AAP/MASC, GLOP	Protocolos Anúncio de Sessão	Protocolos suporte de Tempo Rea
TCP			UDP			
ICMP		Interface Roteador- Estação	IGMP			
OSPF, RIP, etc		Roteamento Intra- Domínio	PIM-SM, PIM-DM	MOSPF	DVMRP	
			RIP, etc	OSPF		
BGP		Roteamento Inter- Domínio	MSDP, BGMP			
			MBGP (BGP4+)			

Figura 1: Comparação Unidifusão x Difusão Seletiva (após [DIO00])

Uma agenda mínima de requisitos demandados por aplicações de difusão seletiva exigiria rapidez e consistência na alocação de endereços, adequação à dinâmica de grupos e de rotas, caso os requisitos fossem baseados em desempenho, e deveria haver habilidade para lidar com heterogeneidade e particionamento da informação [LEV00]. Esta agenda, no entanto, não é bem suportada pelo atual modelo de difusão seletiva IP e a razão decorre dos problemas do modelo atual que passamos a analisar [BAR01].

**O Problema da Dependência de Domínios** - A existência de núcleos de árvores de roteamento IP em domínios diferentes das respectivas fontes de transmissão de pacotes levam, necessariamente, a conflitos de interesses. Não é desejável um domínio depender de outro domínio, pois:

1. O controle de congestionamento e de taxa de transmissão a partir de uma fonte num certo domínio pode se tornar incompatível com as políticas locais, quando o tráfego troca de domínio;
2. Caso um provedor de serviços Internet esteja baseado em um núcleo que se encontre em um outro domínio, certamente não poderá ter o mesmo controle sobre o serviço que seus clientes vão receber;
3. Num papel inverso, um provedor de serviço Internet não vai querer ser o núcleo de uma sessão para o qual ele não tem receptores ou emissores como clientes. Se fizessem isto, ele estaria desperdiçando recursos para terceiros, e, pior, uma vez que o atual modelo de serviço não provê nenhum mecanismo para estimar o tamanho do grupo de difusão seletiva, até a mensuração de tal desperdício fica comprometida.

A proposta MSDP resolve o problema da independência de domínios, porém, às custas da escalabilidade e da adequação à dinâmica de grupo [ALM99]. Grupos dinâmicos apresentam freqüente processo de associação-retirada ou então apresentam fontes transmitindo em rajadas. Com o MSDP, a informação de existência de fontes emissoras deve ser conhecida antes que o estado de roteamento seja criado, situação que fica difícil ser gerenciada no cenário apontado. Desta forma, MSDP foi veiculado intencionalmente como uma solução de curto termo à espera de uma outra proposta mais abrangente que resolva definitivamente o problema. Tal proposta efetivamente surgiu, representada pelo projeto BGMP/MASC, porém deve ser reconhecida sua complexidade, particularmente se pensamos em termos da viabilidade de montar uma estrutura global e do estímulo dos provedores de serviços da Internet em assumir tal complexidade.

**O Problema da Funcionalidade Não Resolvida** - A elegância do modelo de difusão seletiva paga um preço pela sua simplicidade, oferecendo poucas opções para serviços de entrega de dados em grupo. Aplicações de larga escala vão precisar bem mais da camada de rede do que entrega anônima de pacotes. Em aplicações de larga escala, o cenário mais provável é que nem todos os usuários vão querer todos os dados de todas as fontes. Com tal perfil de demanda, poderá haver ao longo da rede algum processamento desnecessário, entupimento de filas em roteadores e em “*buffers*” de chegada em estações finais. Este cenário negativo poderia ainda ser piorado com protocolos confiáveis tentando retransmitir pacotes perdidos que poderiam não ser de interesse de alguns usuários. Uma solução mais natural seria a existência de formas de endereçabilidade dentro do grupo, com a organização de grupos por interesse em dados, reduzindo o problema ainda na camada rede, e, conseqüentemente, reduzindo tráfego desnecessário. Não é difícil imaginarmos outros exemplos similares para ensino à distância, conferências, simulação interativa e assim por diante.

Uma arquitetura de difusão seletiva deveria também pressupor uma gerência de grupo, seja para fins de tarifação por uso, seja para descoberta de endereços, ou ainda, para funções

de controle de acesso. O modelo atual deixa em aberto estas funcionalidades, permitindo desta forma que uma sessão de difusão seletiva fique vulnerável a diversos perigos, tais como: ataques por negação de serviço (inundação), colisões de sessões, recepção não autorizada e interferência clandestina em fontes autênticas.

Para fins específicos de controle de acesso, deveria existir um mecanismo que controlasse autorizações (para recepção e para transmissão) e criação de grupos. Uma solução natural que preveniria aqueles perigos apontados seria haver uma adesão explícita para uma lista de fontes transmissoras conhecidas durante a existência de uma sessão de grupo. Evidentemente esta linha de ação conflita com o atual paradigma, onde a identidade de receptores não é de conhecimento da fonte nem mesmo esta precisa ser do grupo.

**Custo de Protocolo, Latência de Grupo e Escalabilidade** - Quaisquer das soluções até agora apontadas incorrem em custos de processamento, tempo e de sinalização. O custo de latência de associação, por exemplo, é particularmente alto no MSDP. Mensagens de confirmação de associação no domínio são enviadas periodicamente e pode haver um significativo retardo entre o momento que o novo candidato a receptor pede associação e o momento que ele é de fato confirmado. Minimizar este problema no MSDP pode ser feito ao preço de aumentar estados.

Da mesma forma outros protocolos de roteamento difusão seletiva propagam periodicamente informação por inundação na rede: MOSPF propagam informação de associação de grupo para roteadores para que eles possam construir árvores de distribuição; DVMRP e PIM-DM também periodicamente inundam pacotes de dados na rede; mesmo CBT e PIM-SM, que escalam melhor, propagam por inundação para todos roteadores candidatos a núcleo as informações de mapeamento do grupo.

Os protocolos de roteamento, sejam eles baseados em fonte, sejam baseados em árvore compartilhada, incorrem em novos problemas de escalabilidade causados por:

1. *Manutenção do estado de conexão* – todos roteadores que venham a participar de uma árvore de difusão seletiva mantêm tabelas de encaminhamento que podem significar grande consumo de recursos, tanto de memória quanto de processamento. Enquanto árvores compartilhadas incorrem em custo de manutenção do grupo, árvores baseadas nas fontes emissoras incorrem em custos associados à manutenção do grupo e da fonte.
2. *Mecanismo de anúncio de fonte emissora* – membros de um grupo de difusão seletiva se tornam conectadas a fontes emissoras sem que precisem ter conhecimento delas. Em protocolos modo esparsa, como CBT e PIM-SM, isto acontece porque apenas o nó núcleo precisa ter completo conhecimento e controle de todo o domínio. Em protocolos do modo denso, como DVMRP e PIM-DM, mecanismos de inundação e poda garantem aquela conexão sem que também se tenha ciência das fontes emissoras. Num caso ou noutro, surgem problemas de escalabilidade, seja por fazer crescer as informações de estado a serem mantidas, seja pelo crescimento das mensagens periódicas de atualização.

**Espaço de Endereço** - A alocação de endereços para difusão seletiva IP ainda está desregulamentada. As implementações derivadas do modelo de Deering revelam os custos:

1. *Alocação de endereço de difusão seletiva* – o criador de um grupo de difusão seletiva deve alocar um endereço globalmente único. Como não é definido no modelo de serviço atual e não existe nenhum padrão reconhecido para isto, a IETF tem experimentado fazer alocação estática de blocos de endereços de difusão seletiva, porém com prazo marcado para ser substituído pelo conjunto de protocolos MAAA. Se por um lado a proposta MAAA padronizará a alocação de endereços, pelo outro se teme pela sua complexidade. Mais especificamente, o MASC, projetado para resolver as alocações de endereços interdomínio, apresenta dois pontos

controvertidos. No primeiro, fica clara a solução de compromisso entre agregação e a demanda antecipada por grupos de endereços. No outro, a alocação de prefixos de grupo não são fixos a domínios, e sim, digamos, “arrendados”. Por seu lado, aplicações precisam saber o endereço de grupo e isto seria facilitado caso estes fossem fixados.

2. *Desconhecimento de destinatários* – quando um pacote de difusão seletiva chega a um roteador, ele determina em quais interfaces de saída vai encaminhá-lo, mas ele não sabe quais e quantos destinatários irão recebê-lo. Esta inconsciência, olhada do ponto de vista de portadores e de provedores de serviço de Internet, impacta demandas de segurança, de contabilidade e de políticas.
3. *Colisão de endereços* – com o crescimento da Internet, aumenta na mesma medida a possibilidade de mais de um iniciador de grupo escolher o mesmo endereço. Evidentemente isto impõe alguma forma hierárquica de alocação de endereços, coisa que não existe hoje nem está previsto no modelo de Deering.

**A Inconsciência das Questões Qualidade de Serviço e Preferências** – Pela própria natureza do modelo de Deering, qualquer membro de um grupo receberá todos pacotes de dados transmitidos para aquele grupo ao qual ele está associado. Por outro lado, a tendência moderna é personalizar dados para consumidores. Existirão aplicações que poderão permitir uma seleção de dados por conteúdo. Deveria ser permitido à infra-estrutura não deixar como única opção o descarte do pacote na estação destino, pois, assim fazendo, tais aplicações estariam lidando com tráfego gerado inutilmente na rede, desperdiçando recursos da rede e das estações finais.

Para este cenário também não existe nenhum suporte no modelo de serviço atual, e, pior ainda, o modelo de serviço impede o tratamento de dados baseado em conteúdo por um grupo. Personalização está na contra-mão de difusão seletiva segundo seu modelo atual, feito para um cenário de rede que oferece serviço de melhor esforço. Evidentemente o problema poderia ser contornado grosseiramente com a criação de um maior número de endereços de grupo por sessão, ou, senão, com um tratamento de roteamento sensível à QoS, oferecendo rotas alternativas segundo alguma métrica. Mas não é assim que acontece. Quando um novo membro propõe associação, QoS não é considerada na seleção das rotas. CBT, PIM-SM e mesmo BGMP são exemplos desta inconsciência [WAN00a][CRA98]. Todos eles constroem árvores baseadas em núcleo que simplificam o roteamento, mas introduzem problemas de seleção de núcleo e de particionamento de endereços, afetando o desempenho do protocolo.

## 5. Novos Paradigmas para Difusão Seletiva

Um primeiro movimento na direção de mudanças no modelo atual, como vimos, atacou as limitações quanto à dependência de domínios, certos aspectos da escalabilidade, como a redução de estados em roteadores, e um esquema global mais eficiente de alocação de endereços e de controle de acesso. A solução representada por MASC/BGMP é complexa, enquanto as implementações práticas baseiam-se em alocação e designação estáticas de endereços, e são consideradas insatisfatórias. A única proposta que resolve quase todos os requisitos de endereços é a mudança anunciada para IPv6, que, sabemos, não se dará de forma suficientemente rápida, por conta das mudanças necessárias em toda infraestrutura da Internet. Outro movimento, mais radical, propõe mudanças no âmago do modelo, defendendo a tese que a utilização de endereçamento anônimo de difusão seletiva combinada com a falta de

apoio da rede<sup>11</sup> não permitirão uma solução real de longo termo que atenda satisfatoriamente usuários finais e fornecedores de serviços. Nesta vertente, existem os que propõem mudanças simplificadoras do paradigma de difusão seletiva com as propostas SM (*Simple Multicast*) [PER99] e EXPRESS [HOL99]. Mais uma proposta simplificadora, CLM (*ConnectionLess Multicast*) [OOM00], traduz a tentativa de complementar o modelo atual, desvincilhando-se de estados no roteador, mesmo às custas da restrição no tamanho do grupo. Uma outra classe de propostas representada por AIM (*Addressable Internet Multicast*) [LEV99] enfoca um dos principais argumentos contra o modelo atual, a sua incapacidade de endereçamento intragrupo, com um serviço que permita subgrupos receberem seletivamente dados baseado no seu conteúdo e não apenas no seu endereço de difusão seletiva. Um outro movimento de mudanças, mas que foge ao escopo deste trabalho, lança mão de técnicas que levam em conta QoS nas alternativas de rotas para difusão seletiva.

## 5.1 AIM e *Anycasting*

AIM generaliza a arquitetura de difusão seletiva IP introduzindo informação de endereçamento dentro das árvores de roteamento de difusão seletiva. Com isso, procura prover uma infra-estrutura de roteamento que suporte simultaneamente baixa latência na alocação de endereços, pequeno *overhead* na criação de grupos, um mecanismo de *anycasting*<sup>12</sup> flexível e um esquema de nomeação de dados. AIM se insere na arquitetura alternativa ALF<sup>13</sup>, dedicada a aumentar a expressividade das necessidades das aplicações para as camadas de mais baixo nível e requer uma árvore de roteamento de qualquer tipo, seja baseada em fonte, seja compartilhada, estendendo a difusão seletiva IP com o estabelecimento de três tipos de rótulos que deverão ser associados a roteadores, cada um representando um tipo de serviço.

**Rótulo Posicional do Roteador** - especifica sua localização relativa a um ponto fixo da árvore, usado como raiz de endereçamento, e não necessariamente o mesmo que a fonte ou núcleo da árvore de difusão seletiva subjacente. Com *rótulos posicionais*, os roteadores têm um endereço dentro da árvore de difusão seletiva e, com este endereço, passa a ser possível selecionar a recepção em um subconjunto de um grupo. O algoritmo de rotulagem posicional de roteadores atribui ao nó raiz da árvore o rótulo “1” e cada outro nó têm um prefixo correspondente ao rótulo do nó pai e um sufixo único dentre os filhos daquele pai. Um novo prefixo de um roteador deve ser sempre passado para seus filhos e assim sucessivamente até o final da árvore. Com os roteadores na árvore assim rotulados, o roteamento é implícito, não necessitando manter para este fim qualquer estado nos roteadores. Uma simples comparação do rótulo posicional do destinatário com o rótulo do roteador define se o destinatário é um antecessor ou um descendente na árvore e o encaminhamento é feito de acordo.

---

<sup>11</sup> Na concepção de rede predominante, o núcleo é “burro” e veloz, nas pontas da rede o processamento é mais complexo. Surgem, no entanto, nos últimos tempos idéias que advogam um maior apoio da rede.

<sup>12</sup> Um serviço *anycasting* consiste na entrega de um pacote para qualquer um (mas apenas um) receptor dentro de um conjunto de destinatários [WON00]. Vamos manter esta nomenclatura neste trabalho.

<sup>13</sup> *Application Level Framing*. A idéia central é que semânticas de aplicações devam estar refletidas no projeto de seu protocolo de rede, otimizando seu desempenho no meio da rede e nos sistemas finais. A arquitetura ALF integra o nível de transporte na aplicação, propondo que a aplicação gerencie o empacotamento dos dados de aplicação, e estes, se tornem a única unidade de processamento, controle e transmissão através de todos os níveis da rede. Isto requer um novo processo de nomear dados, colocando entidades de aplicações e fluxos de dados em estruturas baseadas em suas relações no contexto das aplicações [LEV00][McC99].

Para uma fonte saber a quem enviar os pacotes, deve conhecer os respectivos rótulos ou atribuir uma máscara correspondente, caso os recipientes ocupem uma sub-árvore completa. Quando os receptores são esparsos, somente o maior prefixo comum (GCP – *Greatest Common Prefix*) da lista é processado pelo roteador correspondente e a lista dos outros receptores é mantida em extensões de cabeçalho do IPv6 (o que, de passagem, implica uma certa restrição ao AIM). Quando o pacote em questão chega ao roteador GCP, este determina, indicado por um *flag* (#), o próximo GCP e assim sucessivamente.

Com rótulos posicionais, é possível que fontes emissoras enderecem uma porção selecionada do grupo de difusão seletiva, baseadas em informações colocadas dentro do pacote, sem que isto signifique tráfego adicional.

**Rótulo de Distância** - é associado a cada interface que pertença à árvore de difusão seletiva, e especifica a distância (segundo alguma métrica) na árvore para o próximo roteador qualificado no mesmo grupo. Também este tipo de rótulo permite roteadores endereçarem um subgrupo específico dentro do grupo de difusão seletiva. O *rótulo de distância* deve especificar um tipo pré-definido. O tipo 1 determina o *hop count* entre roteador e estação-membro mais próxima. Outros tipos podem ser usados para representar recursos disponíveis ou a carga média em uma estação. Uma estação que executa certa aplicação informa a seu roteador imediatamente ligado qual o tipo de rótulo de distância desejado. O roteador que recebe uma atualização de rótulo de distância de uma das “suas” estações (ou de um roteador vizinho) incrementa o rótulo recebido e associa este rótulo à interface por onde chegou a atualização. A seguir, o roteador anuncia aos seus roteadores vizinhos na árvore o seu menor rótulo de distância, resultando numa árvore rotulada. Este esquema possibilita um serviço *anycasting*. Para executá-lo, pacotes são encaminhados por um certo roteador apenas através da sua interface que tenha rótulo de distância mínima. Havendo duas ou mais interfaces que tenham a mesma distância, o roteador seleciona uma delas usando algum critério consistente. As rotas tomadas quando de um roteamento *anycast* não são as mesmas que as do roteamento de difusão seletiva subjacente. Por exemplo, em PIM-SM, todos pacotes são primeiramente encaminhados ao núcleo, depois disseminados, coisa que não ocorre com *anycasting*.

**Rótulo “Stream”<sup>14</sup>** - especifica a associação de um ou vários receptores para um tráfego gerado por um subconjunto de fontes no grupo de difusão seletiva. Este tipo de rótulo permite que receptores identifiquem um subconjunto de fontes e rapidamente formem um novo grupo, dentro do grupo principal, sem a necessidade de novas árvores de roteamento. Com rótulos *stream*, aplicações (ou protocolos de mais alto nível) podem definir iguais contextos e significados para diferentes pacotes individuais rotulando-os com uma mesma identificação, de modo que grupos de difusão seletiva possam ser agregados explicitamente na camada de rede.

O gerenciamento de *streams* pelo AIM é feito com cada roteador mantendo uma tabela local de *streams*, tendo um registro indicando sua identificação e outro indicando o estado de encaminhamento em cada uma das interfaces do roteador. A cada *stream* existe um roteador associado, funcionando como *núcleo de stream*, responsável por anunciar o *stream* para os outros roteadores atualizarem sua respectiva tabela local.

---

<sup>14</sup> Neste contexto, “*stream*” significa o grupamento lógico de pacotes dentro de um grupo de difusão seletiva. O uso destes grupamentos pela aplicação é recursivo dentro da árvore de difusão seletiva principal. É o caso de grupamento de dados de áudio e vídeo transmitidos por uma fonte para um grupo de difusão seletiva. Tomamos o termo na sua forma original.

## 5.2 Propostas RAMA

As propostas deste modelo<sup>15</sup> abrem mão de aspectos do modelo atual em nome de simplificações no roteamento. Neste modelo, um canal é endereçado univocamente através da tupla (N - endereço de núcleo ou fonte, G - endereço de grupo). No caso do EXPRESS [HOL99], duas fontes (F1 e F2) transmitindo dados para o mesmo grupo (G) só serão recebidos por receptores associados a ambas fontes, e, portanto, a grupos diferentes. Da mesma forma, no SM, o anúncio de um núcleo (N) de uma árvore compartilhada estará associado a um endereço específico (G) de grupo.

SM e EXPRESS, no entanto, têm diferenças. Enquanto EXPRESS impõe uma árvore unidirecional por fonte emissora, SM constrói uma árvore compartilhada e bidirecional para vários emissores. SM requer modificação no formato dos pacotes, EXPRESS não.

Para nossos propósitos, o SM é mais representativo do modelo RAMA pela sua capacidade de dar uma solução ao roteamento interdomínio [PER99][BAL99]. O projeto SM parte do princípio que a noção de sessão deve ser resolvida no nível de uma única árvore compartilhada (EXPRESS vincula a noção de sessão à camada de aplicação), dado que um grande número de aplicações usa múltiplos emissores. Desta forma, o modelo de serviço apresentado aqui é do tipo multi-parceiro, com a árvore bidirecional compartilhada, centrada em um núcleo. Igual ao EXPRESS e diferente do modelo tradicional, este protocolo desassocia a descoberta de grupo e do núcleo das questões de roteamento. Os parâmetros de endereço do grupo (N, G) podem ser descobertos por algum mecanismo “fora-de-banda” no nível da aplicação (WWW, e-mail, DNS, SAP, etc.), livrando-se de complexidades e unificando roteamento intra- e interdomínio, eliminando a necessidade de alocação global de endereço de difusão seletiva.

Se uma fonte de dados já é membro do grupo, seu pacote de dados SM deve portar um cabeçalho encapsulado por IP, contendo o identificador de grupo (N, G) e no campo de endereço de destino do IP deve ser colocado o código correspondente a ALL-SM-NODES, assegurando com isto que nós não preparados para SM irão ignorar o pacote. Um roteador SM que receba o pacote verifica (N, G) em sua tabela de encaminhamento para decidir encaminhá-lo ou descartá-lo. Se a porta de saída é um túnel, o roteador SM substitui o campo de endereço de destino do IP pelo endereço do destino do túnel, e, chegando neste, certamente também um roteador SM, aquele campo volta a ser substituído por ALL-SM-NODES.

Mensagens de controle do SM, também encapsuladas pelo IP, são emitidas em direção do núcleo. Uma mensagem “*join*” contém a opção do IP *Router Alert* [KAT97], que acarretará a inspeção e processamento deste pacote por todos roteadores colocados no caminho para o núcleo, com cada roteador que processe SM inserindo no campo próprio do cabeçalho sua identificação ou tunelando pacotes entre roteadores SM não adjacentes. Chegando ao núcleo e aceito o pedido de “*join*”, o reconhecimento segue pelo caminho inverso, confirmando as informações de estado de roteamento até o emissor original do “*join*”. A manutenção da árvore é feita de modo similar ao CBT, com os roteadores pais monitorando os filhos e vice-versa, emitindo e monitorando mensagens de “vida” e “pulsção”.

---

<sup>15</sup> SM e EXPRESS. Esta classe de propostas tem sido chamada de RAMA (*Root Addressed Multicast Architecture*) [ALM99].

### 5.3 CLM: Difusão Seletiva para Pequenos Grupos

Têm surgido dentro e fora [BOI00] da IETF propostas que procuram tirar partido das características reais da demanda de aplicações de difusão seletiva sem abdicar das facilidades de unidifusão, reconhecendo que aplicações práticas se encaixam melhor no modelo *poucos-para-poucos*. As diversas filosofias voltadas para resolver a difusão de pacotes idênticos incorrem em um dentre os três custos, ortogonais entre si, que descreveremos e se encontram ilustrados na Figura 2. A solução unidifusão pura ( $n$  transmissões unidifusão) corresponde ao ponto (1) no gráfico. A solução tradicional, à moda *Deering*, (uma única transmissão para um endereço de difusão seletiva) corresponde ao ponto (2). A proposta representada por CLM (a informação é enviada uma única vez, porém, contém em seu interior uma lista de  $n$  destinatários) corresponde ao ponto (3). As soluções propostas dentro do modelo de serviço atual permitem algum trânsito entre os pontos (1) e (2) no gráfico, podendo-se, portanto, trocar custo de banda por custo de manutenção de estado e sinalização nos roteadores. As técnicas propostas em CLM (e mencionadas na figura) permitem trocar custo de processamento no roteador de borda por banda ou trocar processamento no roteador de borda por estado e sinalização.

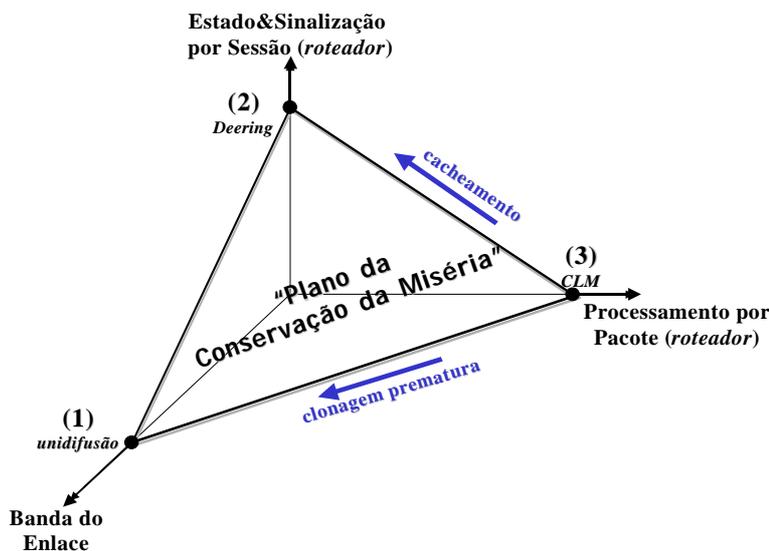


Figura 2: “Plano de Conservação de Miséria”

Ooms em [OOM00] afirma um perfil hiperbólico do custo por membro do grupo em função do número de membros. Este perfil evidencia que o atual modelo de serviço torna-se caro para seus membros se o grupo é pequeno e se são muitos destes grupos, como é o caso de videoconferência, jogos interativos e aplicações colaborativas. São a estas aplicações que CLM se destina.

A filosofia CLM é simples. Usar unidifusão corresponde a um maior custo do consumo de banda, recurso escasso no acesso à rede, além de evidentes prejuízos de desempenho. Usar difusão seletiva à moda *Deering* incide no custo de manutenção de estado e sinalização, exigindo recursos que se tornam escassos (memória e CPU) no backbone pela imensa concorrência. A proposta CLM volta a transferir o foco dos custos para os roteadores das bordas, só que não mais em termos de custo de banda, mas agora em termos de processamento por pacote. A implementação desta filosofia se assemelha ao Mbone, construindo-se uma rede virtual por sobre a Internet, com roteadores e estações CLM,



1. *Escalabilidade* - implementa alocação trivial de endereços para difusão seletiva, uma vez que, para cada núcleo, abre-se todo o leque de endereços classe D. Uma estação final pode participar do grupo, quer esteja ela adjacente ou não a um roteador que processe SM.
2. Apoio ao *controle de acesso* no grupo - realizado no núcleo onde é mantida uma lista de autorizados/incluídos e desautorizados/excluídos. As regras de acesso determinadas pelo núcleo são propagadas para os outros roteadores em mensagens de “pulsção”, incluindo uma lista de controle de acesso para roteadores de fronteira.
3. *Escopo de Difusão Seletiva* – diferentemente do modelo atual, SM pode utilizar para difusão seletiva os limites de escopo definidos para o roteamento unidifusão (sub-rede, área, sistema autônomo e confederação de sistemas autônomos), desde que os roteadores de fronteira processem pacotes SM sem qualquer protocolo especial para tratar da questão. Também um identificador de grupo (N, G) pode ser usado em múltiplos escopos.
4. *Independência de domínios* – quando SM é usado intra e interdomínio, é necessário assegurar que “joins” de diferentes receptores internos a um domínio confluem a um ponto comum dentro do outro domínio.
5. *Adaptabilidade à dinâmica de difusão seletiva* – podem ser estabelecidos vários grupos por sessão tirando proveito da fatura de pares (N, G), com isto, alcançando maior presteza na entrega ou balanceamento de carga na rede.

Persistem com a proposta SM várias questões controvertidas ou em aberto:

1. *Filtragem na camada de enlace* - como numa sub-rede o mapeamento para o endereço MAC é feito a partir da porção baixa (endereço classe D) do endereço SM do grupo de difusão seletiva, pode ser que estações em diferentes grupos SM, mas com o mesmo endereço classe D, recebam pacotes desnecessariamente.
2. *Questões de desempenho* – encaminhar um pacote SM envolve pesquisar uma tabela baseada no conteúdo do cabeçalho SM, encaminhando para a(s) respectiva(s) interface(s) uma cópia do pacote. Roteadores não preparados para SM perderão em desempenho, por manipularem por *software* pacotes SM, por outro lado é comum que mecanismos de encaminhamento sejam implementados diretamente por *hardware*.
3. *Agregação de estado de grupo* - não existe nenhuma sugestão específica na proposta SM quanto à agregação de informação de roteamento de grupo.

A última alternativa que analisamos, CLM, abre mão explicitamente da escalabilidade admitindo o cenário simplificado de aplicações *poucos-para-poucos*. A estratégia de abrir mão de alocação de endereços classe D, codificando a lista dos membros do grupo no pacote de dados, contorna os problemas de manutenção de estados nos roteadores, facilita a adaptabilidade a mudanças topológicas e o conhecimento da identidade dos associados, que implica no total controle de gerencia de sessão. Com CLM não se fazem necessários acordos complexos para emparceiramento entre domínios, podendo assim ser usado como protocolo interdomínio em parceria com protocolos como SM e PIM-SM. Estes benefícios são obtidos ao custo de *overhead* do pacote e maior processamento do cabeçalho, sendo adequado para pequenos grupos esparsos.

Ao lado destas, outras questões que não abordamos neste trabalho, dentro ou fora do escopo do modelo de difusão seletiva IP, como roteamento restringido, difusão seletiva confiável e segura, deverão contribuir oferecendo soluções mais simples, gerais e adequadas para que difusão seletiva alcance sua completa maturação.

## Referências

- [ALM99] "The Evolution of Multicast: From the Mbone to Inter-Domain Multicast to Internet2 Deployment", K. C. Almeroth, IEEE Network, setembro/1999
- [BAL97] "Core Based Trees (CBT) Multicasting Routing Architecture", A. Ballardie, RFC 2201, 1997

- [BAL99] “*Simple Scalable Internet Multicast*”, T. Ballardie, R. Perlman, C. Lee, J. Crowcroft, tech. rep., University College London, abril/1999
- [BAR01] “*Difusão Seletiva: Confiabilidade, Escalabilidade e Qualidade de Serviço*”, F. A. R. Barros, Dissertação de Mestrado, Instituto de Computação, Universidade Federal Fluminense - UFF, 2001
- [BOI00] “*Small Groups Multicast*”, R. Boivie, N. Feldman, ietf draft, draft-boivie-sgm-01.txt, work in progress, 2000
- [COM95] “*Internetworking with TCP/IP*”, vol 1, 3a. ed., D. E. Comer, Prentice-Hall, 1995
- [CRA98] “*A Framework for QoS-based Routing in the Internet*”, E. Crawley, R. Nair. B. Rajagopalan, H. Sandick, RFC 2386, agosto/1998
- [DEE89] “*Host Extensions for IP Multicasting*”, S. Deering, RFC1112, 1989
- [DEE91] “*Multicast Routing in a Datagram Internetwork*”, S. Deering, Tese PhD, Stanford University, dezembro/1991
- [DEE98a] “*Protocol Independent Multicast vs.2 Dense Mode Specification*”, S. Deering et al., draft-ietf-pim-v2-dm-\*.txt, work in progress, 1998
- [DEE98b] “*Protocol Independent Multicast Sparse-Mode (PIM-SM): Protocol Specification*”, S. Deering et al., RFC 2362, 1998
- [DIO00] “*Deployment Issues for the IP Multicast Service and Architecture*”, C. Diot et al., IEEE Network, janeiro/2000
- [FAR00] “*Multicast Source Discovery Protocol*”, D. Farinacci et al., draft-ietf-msdp-spec-06.txt, work in progress, 2000
- [HAN97] “*The Internet Multicast Address Allocation Architecture*”, M. Handley, D. Thaler, D. Estrin, draft-handley-malloc-arch-\*.ps, 1997
- [HAN99] “*Internet Multicast Today*” M. Handley, J. Crowcroft, The Internet Protocol Journal, Vol 2, No. 4, dezembro/1999
- [HOL99] “*IP Multicast Channels: EXPRESS Support for Large-Scale Single-source Applications*”, H. W. Holbrook, D. R. Cheriton, ACM SIGCOMM’99, setembro/1999
- [KAT97] “*IP Router Alert Option*”, D. Katz, RFC 2113, fevereiro/1997
- [KUM98] “*The MASC/BGMP Architecture for Inter-Domain Multicast Routing Protocol*”, S. Kumar et al, ACM Sigcomm, 1998
- [LEV00] “*Consideration of Receiver Interest for IP Multicast Delivery*”, B. N. Levine, J. Crowcroft, C. Diot, J. J. Garcia-Luna-Aceves, J. F. Kurose, IEEE INFOCOM 2000
- [LEV99] “*Network Support for Group Communication*”, Tese PhD, University of California, B. N. Levine, junho/1999
- [McC99] “*Scalable Multimedia Communication Using IP Multicast and Lightweight Sessions*”, S. McCanne, IEEE Internet Computing, 1999
- [MIL98] “*Reliable Multicast Protocols and Applications*” C. K. Miller, The Internet Protocol Journal, Vol 1, No. 2, setembro/1998
- [MOY94] “*Multicast Extensions to OSPF*”, J. Moy, RFC 1584, 1994
- [OOM00] “*Connectionless Multicast*”, D. Ooms, W. Livens, ietf-draft, draft-ooms-cl-multicast-02.txt, work in progress, 2000
- [PAT99] “*Multicast Address Dynamic Client Allocation Protocol*” B. Patel, M. Shah, S. Hanna, ietf draft, draft-ietf-malloc-madcap-\*.txt, work in progress, fevereiro/1999
- [PER99] “*SIMPLE Multicast: A Design for Simple, Low-Overhead Multicast*”, R. Perlman et al, ietf draft, draft-perlman-simple-multicast-03.txt, work in progress, 1999
- [QUI99] “*IP Multicast Applications: Challenges and Solutions*”, B. Quinn, K. Almeroth, Internet Draft, Mboned Working Group IETF, Junho/1999
- [SAH00] “*Multicast Routing Algorithms and Protocols: A Tutorial*”, L. Sahasrabudde, B. Mukherjee, IEEE Network janeiro/2000
- [THA00] “*BGMP Protocol Specification*” D. Thaler, D. Estrin, D. Meyer, Internet Draft, draft-ietf-bgmp-spec-01.txt, work in progress, 2000
- [WAI88] “*Distance Vector Multicast Routing Protocol*”, D. Waitzman, C. Partridge, S. Deering, RFC 1075, 1988
- [WAN00a] “*Multicast Routing and Its QoS Extensions*”, B. Wang, J. C. Wou, IEEE Network, janeiro/2000
- [WAN00b] “*QoS-Based MCast Routing for Distributing Layered Video to Heterogeneous Receivers in Rate-based Networks*”, B. Wang, J. Hou, IEEE INFOCOM 2000
- [WON00] “*An Evaluation of Preference Clustering in Large-Scale Multicast Applications*”, T. Wong, R. Katz, S. McCanne, INFOCOM, 2000