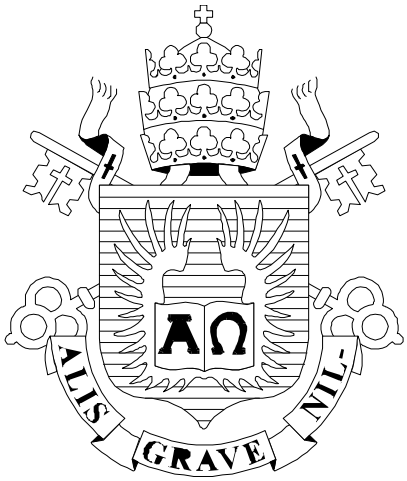


PUC

ISSN 0103-9741

Monografias em Ciência da Computação
n° 28/08

Aprimoramentos no RSVP para o *Mobile* IPv6

Anderson Oliveira da Silva
Luiz Fernando Gomes Soares
Sérgio Colcher

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO
RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22451-900
RIO DE JANEIRO - BRASIL

Monografias em Ciência da Computação, No. 28/08 ISSN: 0103-9741
Editor: Prof. Carlos José Pereira de Lucena Julho, 2008

Aprimoramentos no RSVP para o *Mobile* IPv6*

Anderson Oliveira da Silva, Luiz Fernando Gomes Soares e Sérgio Colcher

Departamento de Informática – Pontifícia Universidade Católica (PUC-Rio)

{anderson, lfgs, colcher}@inf.puc-rio.br

Abstract. Internet was originally conceived to offer only a very simple quality of service (QoS) support, known as point-to-point best-effort data delivery. As this service model does not attend requisites of real-time applications, the Integrated Services (IntServ) [1] model was specified to provide QoS support to end-to-end hosts on a network. Among its functionalities, this model incorporates the necessary mechanisms to provide resource reservation control and admission control on network elements. However, the signaling protocol specified to setup resource reservation (RSVP) [2] does not operate efficiently with mobile end-to-end hosts. This deficiency and the evolution of mobile networks determined the elaboration of innumerous proposals to enhance RSVP with new controls to provide QoS guarantees on environments with IP mobility. This monograph presents the requirements to provide a service model with QoS support to Mobile IP and analyses several proposals to enhance RSVP based on these requirements.

Keywords: RSVP, MIP, QoS, Integrated Services, Mobile IP, Quality of Service.

Resumo. A Internet foi concebida originalmente para oferecer apenas um suporte muito simplificado à qualidade de serviço (QoS), conhecido como entrega de dados por melhor esforço (best-effort) ponto-a-ponto. Como esse modelo de serviço não atende aos requisitos de aplicações de tempo-real, o modelo Integrated Services (IntServ) [1] foi especificado para prover suporte à QoS entre terminais fim-a-fim em uma rede. Dentre as suas funcionalidades, esse modelo incorpora os mecanismos necessários para prover controle de reservas de recursos e controle de admissão nos elementos de rede. No entanto, o protocolo de sinalização especificado para fazer reserva de recursos (RSVP) [2] não opera eficientemente com terminais móveis. Essa deficiência e a evolução das redes móveis determinaram a elaboração de inúmeras propostas para aprimorar o RSVP com novos controles para prover a garantia de QoS em ambientes com mobilidade IP. Essa monografia apresenta os requisitos para prover um modelo de serviço com suporte à QoS para o Mobile IP e analisa várias propostas para aprimorar o RSVP com base nesses requisitos.

Palavras-chave: RSVP, MIP, QoS, Serviços Integrados, Mobilidade IP, Qualidade de Serviço.

---

* Trabalho patrocinado pelo Ministério de Ciência e Tecnologia da Presidência da República Federativa do Brasil (e agência de fomento e o número do processo, se aplicável). (Em Inglês: This work has been sponsored by the Ministério de Ciência e Tecnologia da Presidência da República Federativa do Brasil)

Responsável por publicações

Rosane Teles Lins Castilho
Assessoria de Biblioteca, Documentação e Informação
PUC-Rio Departamento de Informática
Rua Marquês de São Vicente, 225 - Gávea
22453-900 Rio de Janeiro RJ Brasil
Tel. +55 21 3527-1516 Fax: +55 21 3527-1530
E-mail: bib-di@inf.puc-rio.br
Web site: http://bib-di.inf.puc-rio.br/techreports/

Sumário

1 Introdução

A Internet foi concebida originalmente para oferecer apenas um suporte muito simplificado à qualidade de serviço (QoS), conhecido como *entrega de dados por melhor esforço* (best-effort) ponto-a-ponto. Com apenas esse suporte, as aplicações de tempo-real não funcionavam bem através da Internet pois tipicamente ocorriam atrasos variáveis na entrega dos pacotes, associados ao enfileiramento dos mesmos, e perdas de pacotes, associadas ao congestionamento da rede.

Antes que as aplicações de tempo-real, como vídeo remoto, conferência multimídia, visualização e realidade virtual fossem amplamente difundidas, a infra-estrutura da Internet foi modificada para suportar QoS de tempo-real, provendo alguns controles para atrasos de pacotes fim-a-fim. Entre as várias formas de controle disponíveis, os equipamentos de rede foram dotados de controles para o compartilhamento de banda em enlaces particulares, entre diferentes classes de tráfego.

O modelo Integrated Services (IntServ) [1] foi especificado para prover suporte à QoS entre terminais fim-a-fim em uma rede. Dentre as suas funcionalidades, esse modelo incorpora os mecanismos necessários para prover controle de reservas de recursos e controle de admissão nos elementos de rede. No entanto, o protocolo de sinalização especificado para fazer reserva de recursos (RSVP) [2] não opera eficientemente com terminais móveis. Essa deficiência e a evolução das redes móveis determinaram a elaboração de inúmeras propostas para aprimorar o RSVP com novos controles para prover a garantia de QoS em ambientes com mobilidade IP.

Esta monografia apresenta inicialmente o modelo IntServ e o RSVP. Em seguida, são discutidos os requisitos para prover um modelo de serviço com suporte à QoS para o Mobile IP. A partir disso, são apresentadas várias propostas de aprimoramento no RSVP para o Mobile IP. Para concluir, faz-se uma análise comparativa das propostas com base nos requisitos apresentados.

2 Modelo de Serviço com Suporte à QoS

Este capítulo apresenta o modelo de serviços integrados (Integrated Services – IntServ) para suporte à QoS, destacando: (i) o controle de tráfego nos elementos de rede; e (ii) o controle de reservas de recursos.

2.1 Integrated Services – IntServ

Integrated Services (IS) é um termo utilizado para designar um modelo de serviços que acrescenta ao serviço de melhor esforço, historicamente oferecido na Internet, *categorias* de serviços com diferentes graus de comprometimento de recursos (banda passante e buffers, em particular) e, conseqüentemente, com diferentes *níveis* (ou classes) de QoS para *fluxos* de transporte distintos na rede IP.

Conforme definido em [1], fluxo corresponde a um stream distinguível de datagramas relacionados que resultam de uma única atividade do usuário e que requer a mesma QoS. Esse fluxo também foi definido para ser simplex, ou seja, para ter uma única origem, mas com N destinos.

Um modelo de implementação de referência foi definido em [1] para satisfazer o modelo IS. Esse modelo inclui quatro componentes: (i) *escalonador de pacotes*; (ii) *classificador*; (iii) *rotina de controle de admissão*; e (iv) *protocolo para efetuar reservas*.

Um roteador baseado nesse modelo deve então implementar uma QoS apropriada para cada fluxo, conforme a categoria do serviço. A função do roteador que cria diferentes qualidades de serviço é chamada de *controle de tráfego*. Por sua vez, esse controle engloba três dos componentes pevistos no modelo: (i) escalonador de pacotes; (ii) classificador; e (iii) controle de admissão.

O *escalonador de pacotes* gerencia o encaminhamento de streams de pacotes diferentes utilizando um conjunto de filas e possivelmente outros mecanismos como temporizadores. Deve ser implementado no ponto onde os pacotes são enfileirados, normalmente no nível do driver de sáida (output driver) de um sistema operacional típico, e corresponde ao protocolo da camada de enlace. Os detalhes do algoritmo de escalonamento podem ser específicos de um meio de saída particular. Por exemplo, o driver de saída precisará invocar os controles da camada de enlace apropriados quando tiver que interagir com uma tecnologia de rede que tenha um mecanisno de alocação de banda interno.

Outras funções atribuídas ao escalonador de pacotes são: (i) *policiamento ou enforcement*, que é uma operação pacote-a-pacote que ocorre na borda da rede para garantir que uma estação não viole as características de tráfego prometidas; e (ii) *estimador*, que é um componente que pode ser considerado parte do escalonador ou atuar em separado, cujo algoritmo é utilizado para medir as propriedades do stream do tráfego de saída para produzir as estatísticas que controlam o escalonamento de pacotes e o controle de admissão.

O *classificador* mapeia cada pacote recebido em alguma classe. Todos os pacotes na mesma classe recebem o mesmo tratamento do escalonador de pacotes. A escolha de uma classe pode ser baseada no conteúdo dos cabeçalhos dos pacotes existentes e/ou algum número de classificação adicional incluído em cada pacote. Uma classe poderia corresponder a uma categoria ampla de fluxos. Por exemplo, todos os fluxos de vídeo ou todos os fluxos atribuídos a uma organização. Por outro lado, a classe poderia ser associada a um fluxo único. Ou seja, a classe é uma abstração que pode ser local a um roteador particular. Por isso, o mesmo pacote pode ser classificado diferentemente por diferentes roteadores ao longo do caminho. Por exemplo, os roteadores de um backbone podem escolher mapear muitos fluxos em poucas classes agregadas, enquanto outros roteadores próximos à periferia, onde há muito menos agregação, podem utilizar uma classe separada para cada fluxo.

O *controle de admissão* é outro componente do controle de tráfego e implementa o algoritmo de decisão que um roteador ou estação utiliza para determinar se um novo fluxo pode ser garantido para a QoS requisitada sem impactar nas garantias anteriores. Deve ser invocado em cada nó para se tomar a decisão local quanto a aceitar ou rejeitar um fluxo, no momento em que uma estação requisita um serviço de tempo-real ao longo de algum caminho na rede.

O último componente fundamental definido para o modelo de implementação de referência é o *protocolo para efetuar reservas*. Esse protocolo é utilizado para criar e manter o estado específico do fluxo nas estações finais e nos roteadores ao longo do caminho. O modelo IS define a adoção do *RSVP – Resource reSerVation Protocol* para efetuar reservas. Assim, para determinar seus requisitos de recursos, uma aplicação deve especificar a QoS desejada utilizando uma lista de parâmetros chamada *flowspec*. Essa lista é

carregada pelo protocolo, passada para o controle de admissão para testar sua aceitação e utilizada para parametrizar o mecanismo de escalonamento de pacotes.

A Figura 1 ilustra o modelo de referência de implementação para roteadores [1], que é dividido em dois blocos: (i) *forwarding path* e (ii) *background code*.

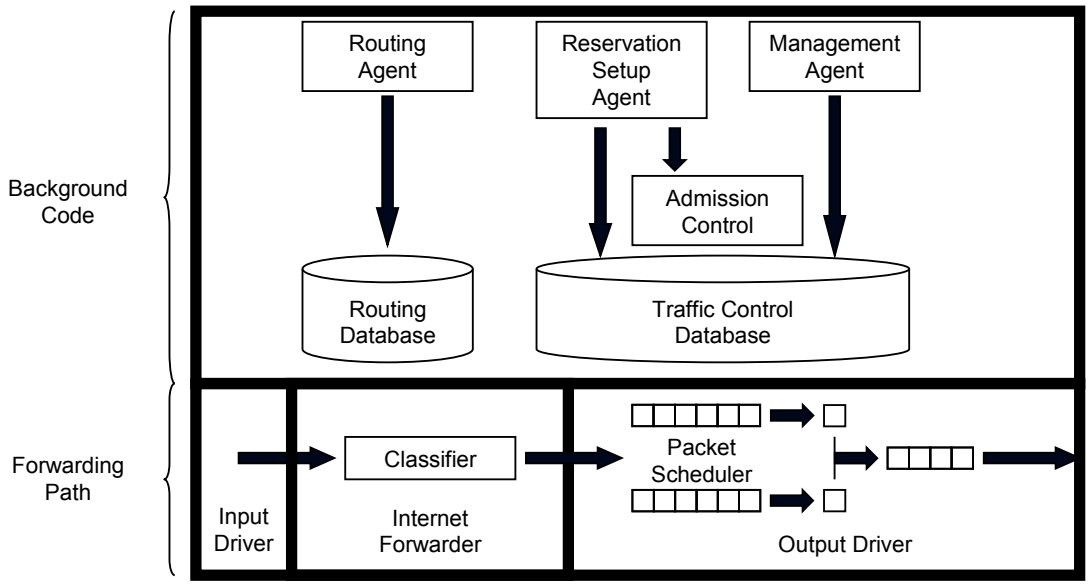


Figura 1 – Modelo de referência de implementação para roteadores [1]

O bloco *forwarding path* é executado para cada pacote e deve, então, ser altamente otimizado. Esse bloco é dividido em três seções: (i) *input driver*, (ii) *internet forwarder* e (iii) *output driver*. O input driver simplesmente recebe o pacote e o entrega ao internet forwarder que interpreta o cabeçalho do protocolo de inter-rede, executa o classificador para o pacote e então passa o pacote e sua classe para o output driver apropriado. Esse, por sua vez, enfileira o pacote com base nas informação recebidas, enquanto o escalonador seleciona o próximo pacote a ser transmitido e o estimador produz as estatísticas.

O *background code* é simplesmente carregado na memória do roteador e executado por uma CPU de propósito geral. Essas rotinas em background criam as estruturas de dados que controlam o forwarding path. É composto por três agentes: (i) o *agente de roteamento*, que implementa um protocolo de roteamento particular e monta um banco de dados de rotamento; (ii) o *agente de controle de reservas*, que implementa o protocolo utilizado para efetuar reserva de recursos e, caso o controle de admissão aceite uma nova requisição, faz as mudanças apropriadas no classificador e no banco de dados do escalonador de pacotes para implementar a QoS desejada; e (iii) o *agente de gerenciamento da rede*, que deve ser capaz de modificar o classificador e a base de dados do escalonador de pacotes para efetuar o compartilhamento de enlace controlado e aplicar as políticas de controle de admissão.

O modelo de referência de implementação para estações é similar ao modelo para roteadores, com a inclusão das aplicações. Ao invés de fazer encaminhamento, os dados de uma estação se originam e terminam em uma aplicação. Uma aplicação que precise de uma QoS de tempo-real para um fluxo deve invocar um agente local para efetuar a reserva. A interface entre a aplicação e o agente não é definida em [1]. A rotina de saída do pacote IP de uma estação pode não precisar de um classificador, tendo

em vista que a associação da classe ao pacote pode ser especificada na estrutura de controle local de E/S correspondente ao fluxo.

2.1.1 Resource reSerVation Protocol (RSVP)

O RSVP [2] é um protocolo para efetuar reserva de recursos, elaborado para operar em acordo com o modelo IS [1]. Esse protocolo é utilizado por uma estação para requisitar qualidades de serviço específicas da rede para streams ou fluxos de dados particulares de uma aplicação. E também é utilizado por roteadores para entregar requisições de QoS para todos os nós ao longo do(s) caminho(s) dos fluxos e para estabelecer e manter um estado para prover o serviço requisitado. As requisições RSVP geralmente resultam na reserva de recursos em cada um dos nós ao logo do caminho dos dados.

As requisições de recursos são feitas para fluxos simplex no RSVP, ou seja, essas requisições são feitas para uma única direção. Por essa razão, o RSVP logicamente distingue o emissor (sender) do receptor (receiver), embora uma mesma aplicação possa atuar como ambos. A operação do RSVP é feita sobre IPv4 ou IPv6, equivalente a um protocolo de camada de transporte, embora não transporte dados de uma aplicação, atuando de forma semelhante a um protocolo de controle como o ICMP, o IGMP ou um protocolo de roteamento. Dessa forma, sua operação é transparente através de roteadores que não suportam o RSVP.

No RSVP, o receptor faz a requisição de uma QoS específica para um fluxo, conforme informado pelo emissor. Essa requisição de QoS da aplicação é passada para o processo RSVP local, que utiliza o protocolo RSVP para carregar a requisição para todos os nós (roteadores e estações) ao longo do(s) caminho(s) de dados reverso(s) em direção à origem dos dados. Para uma distribuição multicast, a requisição segue apenas até o roteador onde o caminho de dados do receptor se junta à árvore de distribuição. Assim sendo, o overhead associado à uma reserva RSVP é, em geral, logarítmica ao invés de ser linear em função do número de receptores.

Durante a efetivação da reserva, uma requisição de QoS via RSVP é passada para dois módulos de decisão locais: (i) o controle de admissão, que determina se o nó tem recursos disponíveis suficientes para suprir a QoS requisitada; e (ii) o controle de policiamento, que determina se o usuário tem permissão administrativa para fazer a reserva. Se ambas as verificações forem bem sucedidas, os parâmetros são acertados no classificador de pacotes e na interface da camada de enlace (por exemplo, no escalonador de pacotes) para obter a QoS desejada. Se uma das verificações falhar, o programa RSVP retorna uma notificação de erro para o processo da aplicação que originou a requisição. A Figura 2 ilustra esse processamento.

Uma requisição de reserva RSVP elementar consiste de um *flow spec* junto com um *filter spec*. Esse par é chamado *flow descriptor*. O flow spec especifica a QoS desejada. O filter spec, junto com a especificação da sessão, define o conjunto de pacotes de dados – o fluxo – à receber a QoS definida pelo flow spec. O flow spec é utilizado para aplicar parâmetros no escalonador de pacotes do nó ou em outro mecanismo da camada de enlace, enquanto o filter spec é utilizado para aplicar parâmetros no classificador de pacotes. Pacotes que são endereçados para uma sessão em particular mas que não casem com nenhum dos filter specs da sessão, são tratados como tráfego best-effort.

O flow spec em uma requisição de reserva geralmente inclui uma classe de serviço e dois conjuntos de parâmetros de números: (i) um *Rspec* (R de reserva), que define a QoS desejada; e (ii) um *Tspec* (T de tráfego), que descreve o fluxo de dados. Os forma-

tos e conteúdos do Tspec e do Rspec são determinados pelas categorias de serviços [3] e são geralmente opacos para o RSVP.

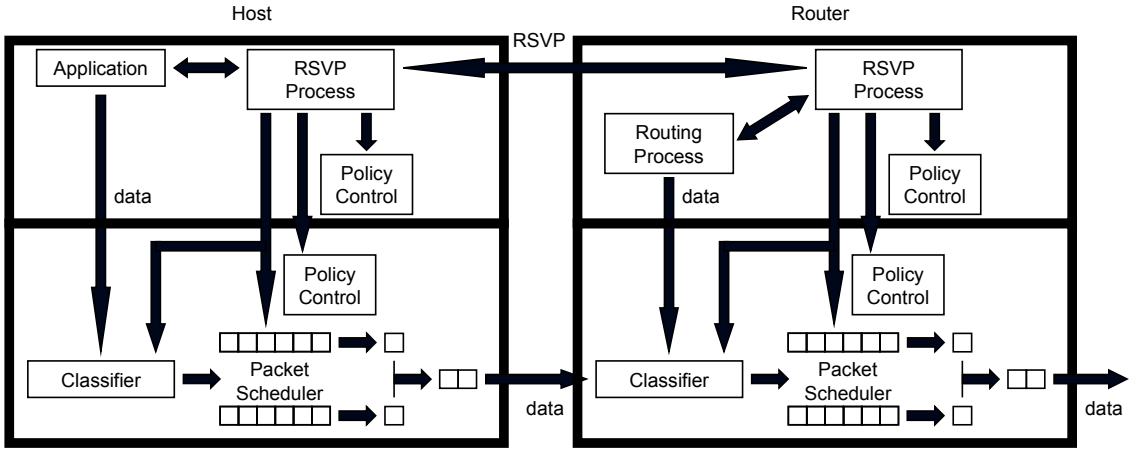


Figura 2 – Processamento de uma requisição de QoS via RSVP [2]

O RSVP é formado por duas mensagens básicas: (i) *Path*; e (ii) *Resv*.

Cada estação atuando como um emissor RSVP deve transmitir as mensagens Path no sentido *downstream* ao longo dos roteadores unicast ou multcast, indicados pelo protocolo de roteamento, seguindo o caminho dos dados. O objetivo é anunciar para os receptores as características do tráfego do emissor. A mensagem Path aloca um *path state* em cada nó ao longo do caminho. Esse path state inclui pelo menos o endereço IP unicast do nó antecessor, que será utilizado para fazer o roteamento das mensagens Resv nó-a-nó na direção inversa. A Figura 3 ilustra o encaminhamento da mensagem Path do emissor para o receptor.

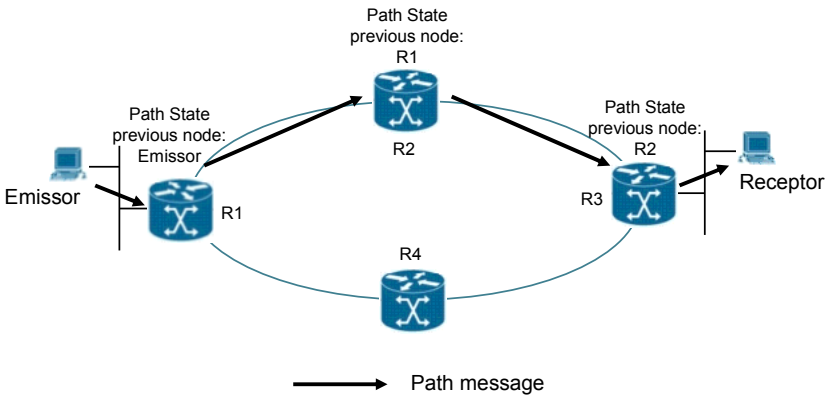


Figura 3 – Encaminhamento da mensagem Path do emissor para o receptor

Cada estação receptora deve enviar a mensagem de requisição de reserva (Resv) no sentido *upstream* na direção do emissor. A mensagem Resv deve seguir exatamente o caminho inverso que os dados vão utilizar, sentido upstream para todas as estações emissoras incluídas na seleção de emissores. Essas mensagens criam e mantém o esta-

do da reserva em cada nó ao longo do caminho. As mensagens Resv devem finalmente ser entregues às estações emissoras, de modo que as mesmas possam aplicar os parâmetros de controle de tráfego apropriados para o primeiro nó. A Figura 4 ilustra o encaminhamento da mensagem Resv do recptor para o emissor.

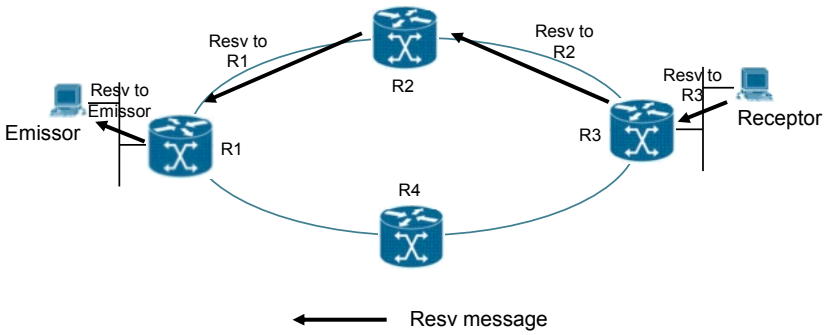


Figura 4 – Encaminhamento da mensagem Resv do recptor para o emissor

O RSVP mantém *soft states* para as reservas feitas nos roteadores e nas estações. Por essa razão, o RSVP precisa enviar mensagens Path e Resv periódicas para manter (refresh) um certo estado ao longo de um caminho reservado. Na ausência dessas mensagens, o estado de uma reserva automaticamente estrapola seu tempo limite e é removido. Os estados também podem ser explicitamente removidos através do envio de uma mensagem *tear down* (PathTear ou ResvTear).

Vários aprimoramentos e extensões foram propostos para o RSVP com o objetivo de melhorar seu desempenho e controle. Em particular, com relação ao controle de admissão (tráfego), cuja interface é apenas baseada em disponibilidade de recursos, [4] descreve um conjunto de extensões para o RSVP oferecer suporte à controle de admissão baseado em políticas, provendo melhores mecaniscos para controlar e impor políticas de acesso e uso. E, para prover sinalização RSVP em túneis IP, [5] descreve um mecanismo que permite que o RSVP faça reservas através dos túneis IP-em-IP.

Para melhorar a escalabilidade do RSVP, que é prejudicada pelo problema da grande quantidade de pequenas reservas isoladas, que exigem grande quantidade de troca de mensagens, computação e recursos de memória em cada roteador ao longo do caminho, [6] descreve um forma de reduzir esse problema a um nível mais gerenciável, utilizando a *agregação de fluxos*. Essa agregação, embora reduza o nível de isolamento entre fluxos individuais, o que permite que um fluxo possa sofrer atraso devido aos surtos de outros, não tem efeito negativo no atraso médio dos fluxos, mas, ao contrário, leva a uma redução do atraso em certas situações, conforme apresentado em [7].

Outra importante extensão do RSVP, descrita em [8], permite que uma reserva existente seja reduzida em largura de banda alocada ao invés de ser completamente descartada quando uma parte da banda reservada é necessária para outros propósitos. Isso pode ocorrer, por exemplo, em uma preempção (descarte da reserva atual em prol de outra mais prioritária) onde nem toda a banda alocada para a reserva existente é requerida. A partir da sinalização do RSVP, os pontos finais podem negociar uma nova e menor largura de banda utilizando outro protocolo. Por exemplo, para uma sessão de voz, o Session Initiation Protocol (SIP) poderia sinalizar a mudança para um codec de menor largura de banda e, assim, reter a reserva existente. No caso da agregação do

RSVP, [8] descreve um método onde apenas a mínima largura de banda requirida é tomada da reserva do agregado menos prioritário, evitando que toda reserva sofra a preempção. Com isso, apenas alguns dos micro-fluxos do agregado são afetados. Sem a extensão proposta, todos os fluxos individuais seriam afetados e o dono das reservas teria que tentar fazer a requisição de reserva novamente com uma banda reduzida.

3 Suporte à QoS no MIPv6

Esse capítulo apresenta o funcionamento do Mobile IPv6 (MIPv6) [10], suas duas principais otimizações (HMIPv6 [11] e FMIPv6 [12]), e os principais requistos para uma solução de QoS nessa plataforma.

3.1 Funcionamento do MIPv6

O Mobile IPv6 é formado pelas seguintes entidades funcionais: [10]

- ***Mobile Node (MN)*** – representa um host que altera seu ponto de acesso quando migra de uma rede ou subrede para outra. Pode mudar de localização sem modificar seu endereço IP e pode continuar a se comunicar com outros nós em qualquer localização utilizando seu endereço IP (constante), assumindo-se que uma conectividade do nível de enlace a um ponto de acesso esteja disponível.
- ***Home Agent (HA)*** – representa um roteador na *home network* (HN) de um MN que intercepta os datagramas enviados para o seu *home address* (endereço IP do MN com o prefixo da HN). Esses datagramas são tunelados para o MN quando o mesmo se encontra fora da HN. Para isso, o HA deve manter informação sobre a corrente localização do MN.
- ***Access Router (AR)*** – representa um roteador na rede visitada pelo MN, também conhecida como *foreign network* (FN), que provê serviço de roteamento ao MN enquanto está registrado. O AR entrega ao MN os datagramas recebidos através do túnel estabelecido com o HA ou enviados diretamente por outros nós. Para os datagramas enviados pelo MN, o AR atua como roteador default.
- ***Correspondent Node (CN)*** – representa o host com o qual o MN se comunica. Pode ser móvel ou estacionário. Quando suporta o armazenamento das informações sobre mobilidade do MN (*mobility binding*), as mensagens são enviadas para o MN através do roteamento pelo AR corrente do MN. Quando não suporta a manutenção dessas informações, as mensagens são enviadas para o home address do MN independente da corrente localização do mesmo, ou seja, como se o MN estivesse na HN.

Quando o MN está em algum enlace estrangeiro longe de seu home, também pode ser endereçado através do seu care-of address (CoA). O CoA é um endereço IP associado ao MN com o prefixo de subrede de um enlace estrangeiro particular. O MN pode obter seu CoA através de mecanismos IPv6 convencionais, ou seja, através de autoconfiguração com estado (ex: DHCPv6 [17]) ou sem estado [15]. Enquanto estiver nessa localização, os pacotes endereçados ao seu CoA serão roteados para o MN.

Sempre que o MN muda de enlace estrangeiro, precisa registrar seu novo CoA no HA. A mensagem de registro enviada pelo MN para o HA é a mensagem de *Binding Update*, enquanto que a mensagem de confirmação do registro enviada pelo HA para o MN é a mensagem de *Binding Acknowledgement*.

Existem dois modos possíveis para comunicação entre o MN e o CN: (i) tunelamento bidirecional (*bidirecional tunneling*) e (ii) otimização de roteamento (*route optimization*). A Figura 5 ilustra os dois modos de comunicação do MIPv6.

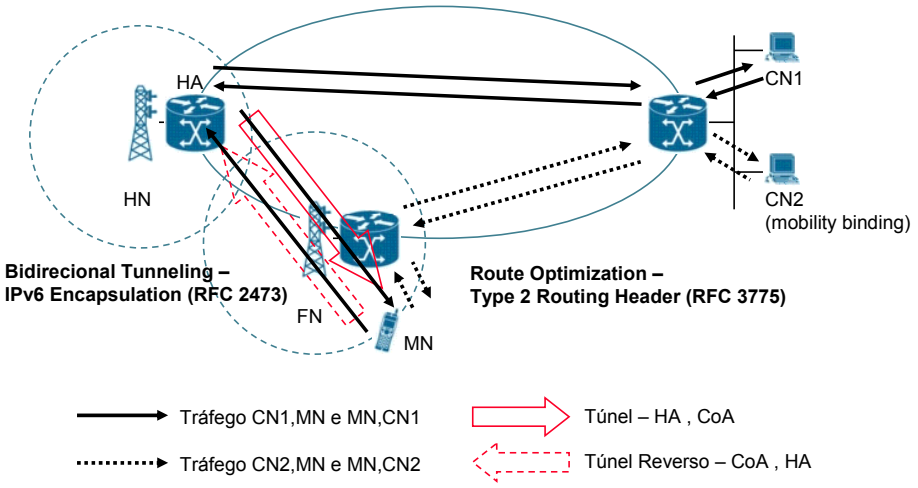


Figura 5 – Modos de comunicação do MIPv6

O *tunelamento bidirecional* não requer o suporte à MIPv6 no CN e está disponível mesmo se o MN não fizer o registro do seu binding atual no CN. Os pacotes do CN são roteados para o HA e então tunelados para o MN. Os pacotes para o CN são tunelados do MN para o HA através de *tunelamento reverso* e então roteados normalmente da home network para o CN. Nesse modo, o HA utiliza o esquema de *proxy Neighbor Discovery* para interceptar qualquer pacote IPv6 endereçado ao home address do MN no enlace home. Cada pacote interceptado é tunelado para o primary CoA do MN. O tunelamento é feito com encapsulamento IPv6 [16].

A *otimização de rotamento* requer que o MN registre seu binding atual no CN. Para isso, é necessário que o CN suporte mobility binding e que o MN execute o procedimento de *registro no correspondente*. Como parte desse procedimento, o teste chamado *return routability*, que é descrito em [10], deve ser executado para autorizar o estabelecimento do binding. Esse teste fornece ao MN as informações de segurança necessárias para construir a mensagem de *Binding Update* que deve ser enviada para o CN atualizar o binding do MN.

No modo de otimização de roteamento, os pacotes do CN podem ser roteados diretamente para o CoA do MN. Quando pacotes são enviados para qualquer destino IPv6, o CN busca uma entrada em sua cache de bindings para o endereço de destino do pacote. Se for encontrada uma entrada, o nó utiliza um novo tipo de cabeçalho de roteamento IPv6, chamado *Type 2 Routing Header* [10], para rotear o pacote para o MN através do CoA indicado no binding. Para o correto roteamento, o CN preenche o endereço de destino no cabeçalho IPv6 com o CoA do MN e o novo tipo de cabeçalho com o home address do MN. Esse roteamento encurta o caminho de comunicação a ser utilizado e também elimina congestionamento no HA do MN e no enlace home. Ainda como conseqüência, o impacto de possíveis falhas associadas ao HA ou às redes no caminho entre o MN e o HA é reduzido.

De forma semelhante, os pacotes do MN podem ser roteados diretamente para os CNs. Para isso, o MN preenche o endereço de origem do cabeçalho IPv6 do pacote com

seu CoA e o endereço de destino com o endereço do CN. Em seguida, o MN adiciona uma nova opção, chamada *IPv6 Home Address Destination* [10], para carregar seu home address. A inclusão do home address nesses pacotes torna o uso do CoA transparente para as camadas de rede superiores (ex: na camada de transporte).

Existem otimizações propostas para o MIPv6, como o HMIPv6 [11] e o FMIPv6 [12], que podem contribuir com a implantação das soluções de QoS. O principal objetivo dessas propostas é minimizar a latência do handoff e reduzir o atraso e a perda de datagramas durante essa operação. De modo geral, as propostas visam soluções para: (i) minimizar o tempo de registro do CoA; (ii) minimizar o tempo de mudança do ponto de acesso; e (iii) evitar o atraso e a perda dos datagramas. Um estudo comparativo sobre essas otimizações pode ser encontrada em [18]. As duas seções seguintes fazem uma breve apresentação dessas duas otimizações.

3.2 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)

Um dos problemas que afetam a comunicação no MIPv6 é a latência referente à efetivação do registro do novo CoA. Essa operação é lenta pois envolve a troca de mensagens de sinalização com componentes fora da nova rede, em particular, com o HA e com os CNs que suportam otimização de roteamento.

Para minimizar essa latência, o esquema de handoff hierárquico divide a mobilidade em duas categorias: (i) *micromobilidade* (geralmente intra-domínio) e (ii) *macromobilidade* (geralmente inter-domínio). O elemento central desse esquema é a entidade conceitual chamada de *Mobility Anchor Point* (MAP) [11], que define um domínio MAP formado por uma ou mais redes. A movimentação de um MN entre redes de um mesmo domínio MAP determina uma micromobilidade, e a movimentação do MN entre redes de domínios MAP diferentes determina uma macromobilidade.

Cada uma das redes de um domínio MAP possui um Access Router (AR) que corresponde ao roteador default dos MNs em sua região de alcance. A presença do MAP do domínio ao qual o AR pertence é anunciada na mensagem de Router Advertisement. Assim, a mudança de um domínio MAP é percebida pelo MN quando um novo anúncio com a informação de um novo MAP é recebida pelo MN.

Conforme especificado em [11], quando em um novo domínio MAP, o MN faz o binding do seu CoA obtido na rede local, conhecido como *Local CoA* (LCoA), com um endereço na subrede do MAP, conhecido como *Regional CoA* (RCoA) e que, normalmente, é o endereço do próprio MAP. Agindo como um local HA, o MAP intercepta todos os pacotes destinados ao MN e os encapsula e encaminha diretamente para o LCoA. Se o MN mudar para outra rede do mesmo domínio MAP, apenas o registro do novo LCoA é feito junto ao MAP com uma mensagem de Binding Update. E então, apenas o RCoA precisa ser registrado, através de outra mensagem de Binding Update, no HA e nos CNs com os quais o MN se comunica. Esse RCoA não se modifica se a movimentação do MN for ao longo de um mesmo domínio MAP. Isso torna a micromobilidade do MN transparente com relação ao HA e aos CNs. A Figura 6 ilustra o esquema do MIPv6 hierárquico.

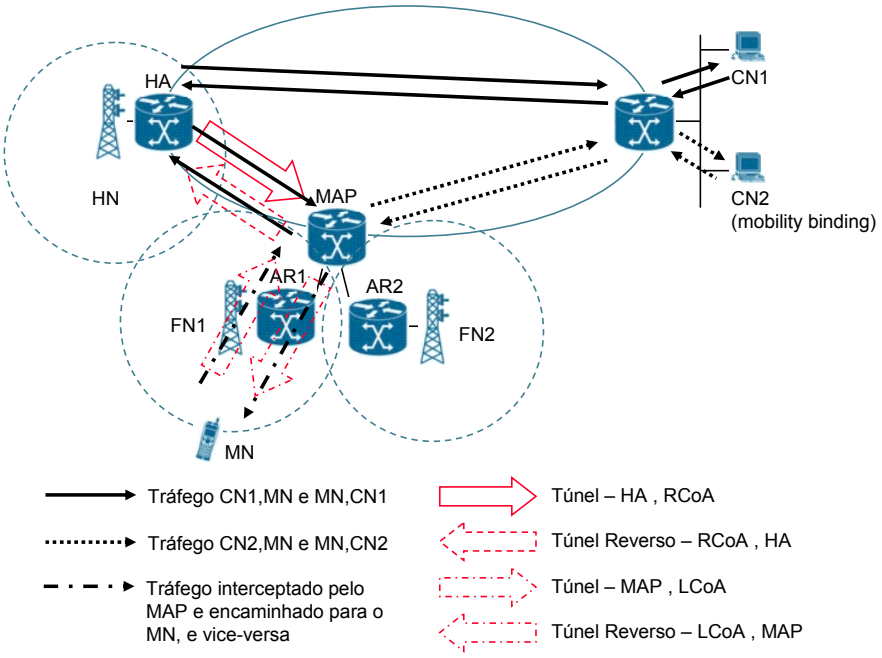


Figura 6 – Esquema do MIPv6 hierárquico

Com o objetivo de acelerar o handoff entre MAPs e reduzir a perda de pacotes, o MN deve enviar uma mensagem de Binding Update para seu MAP anterior, especificando seu novo LCoA. Os pacotes que estiverem em trânsito para o MAP anterior serão então encaminhados para o novo LCoA. Também é permitido que MNs enviem mensagens de Binding Updates contendo o LCoA (ao invés do RCoA) para CNs que estão presentes na mesma rede visitada. Dessa forma, os pacotes serão roteados diretamente sem atravessarem o MAP.

3.3 Fast Handovers for Mobile IPv6 (FMIPv6)

Conforme descrito em [12], a habilidade de imediatamente enviar pacotes a partir de um novo enlace de subrede depende da latência da conectividade IP, que por sua vez, depende da latência da detecção de movimento e da latência de configuração do novo CoA. Uma vez restaurada a capacidade IP do MN, a mensagem de Binding Update pode ser enviada ao seu HA e a todos os seus CNs. A partir do processamento bem sucedido do Binding Update pelos seus CNs, o que tipicamente envolve a execução do procedimento de return routability [10], o MN pode receber pacotes no novo CoA. Sendo assim, a habilidade de receber pacotes a partir de CNs diretamente para seu novo CoA depende da latência do Binding Update e da latência da conectividade IP.

O protocolo definido em [12] possibilita que o MN rapidamente detecte sua movimentação para uma nova rede pois provê informação sobre o novo ponto de acesso (Access Point – AP) e sobre o prefixo de subrede associado enquanto o MN ainda se encontra conectado à sua subrede atual, cujo roteador default passa a ser chamado de *roteador de acesso anterior* (Previous Access Router – PAR). Por exemplo, um MN pode descobrir os APs disponíveis utilizando mecanismos do nível de enlace (ex: operação *scan* na WLAN) e então requisitar informações da subrede correspondente a um ou mais dos APs descobertos. Essa requisição é feita com o envio da mensagem de *Router Solicitation for Proxy Advertisement* (RtSolPr) para o seu roteador de acesso. O MN pode

executar essa operação depois do procedimento de router discovery ou a qualquer momento quando se encontrar conectado ao seu rotedor corrente.

O resultado da resolução do identificador associado a um AP é a tupla [AP-ID, AR-Info], onde AP-ID é o identificador do AP e AR-Info é composto pelo endereço L2 do roteador, endereço IP do roteador e um prefixo válido na subrede a qual o AP está conectado. Essa resposta é enviada pelo AR para o MN na mensagem de *Proxy Router Advertisement* (PrRtAdv).

Com as informações obtidas, o MN formula um novo CoA (NCoA) em potencial e envia uma mensagem de *Fast Binding Update* (FBU) quando ocorre um evento de handoff específico de enlace. Essa mensagem tem o propósito de autorizar o PAR a fazer o binding do PCoA (Previous CoA) para o NCoA, de modo que os pacotes que cheguarem possam ser tunelados para a nova localização do MN. Sempre que possível, o FBU deve ser enviado a partir do enlace do PAR. Quando não for, o FBU é enviado a partir do novo enlace. Com a execução desse procedimento, a latência referente à descoberta do novo prefixo subsequente ao handoff é eliminado.

Como confirmação de recebimento do FBU, o PAR deve enviar a mensagem de *Fast Binding Acknowledgment* (FBack). Dependendo se a mensagem FBack é recebida ou não ainda no enlace anterior, dois modos de operação são definidos:

1) O MN recebe a mensagem FBack no enlace anterior. Isso significa que o tunelamento de pacotes já se encontrará em progresso no momento em que o MN fizer o handoff para o NAR. Logo, o MN deve enviar a mensagem de *Fast Neighbor Advertisement* (FNA) imediatamente após se conectar ao NAR, de modo que os pacotes que estejam chegando e os que foram armazenados sejam encaminhados para o MN.

Antes do envio de uma mensagem FBack para um MN, o PAR pode determinar um NCoA aceitável pelo NAR através da troca das mensagens *Handover Initiate* (HI) e *Handover Acknowledge* (HAck). Quando o modo *assigned addressing* é utilizado, o NCoA proposto pelo MN na mensagem FBU é carregado na mensagem HI que é enviada pelo PAR para o NAR, que pode associar o NCoA ao MN. Esse NCoA deve então ser retornado na mensagem HAck enviada pelo NAR para o PAR, que por sua vez, deve informar o NCoA atribuído na mensagem FBack. Se existir um NCoA retornado na mensagem FBack, o MN deve utilizá-lo, ao invés do NCoA proposto, quando se conectar ao NAR.

2) O MN não recebe a mensagem FBack no enlace anterior pois o mesmo não enviou a mensagem FBU ou deixou o enlace após enviar a mensagem FBU (que pode ter sido perdida), mas sem receber a mensagem FBack. Sem ter recebido a mensagem FBack no último caso, o MN não tem como se certificar quanto ao processamento bem sucedido da mensagem FBU enviada para o PAR. Por essa razão, o MN re-envia uma mensagem FBU assim que se conecta ao NAR. Para permitir que o NAR encaminhe os pacotes imediatamente (no caso em que a mensagem FBU foi processada pelo PAR) e verifique se o NCoA é aceitável, o MN deve encapsular a mensagem FBU na mensagem FNA. Se for detectado que o NCoA está em uso quando a mensagem FNA for processada, o NAR deve descartar o pacote interno com a mensagem FBU e enviar uma mensagem de Router Advertisement com a opção *Neighbor Advertisement Acknowledge* (NAACK) na qual o NAR pode incluir um endereço IP alternativo para o MN utilizar.

O cenário no qual o MN envia uma mensagem FBU e recebe uma mensagem FBack no enlace do PAR é chamado de *operação em modo pré-indicado ou antecipado* (*predictive*), e é ilustrado na Figura 7.

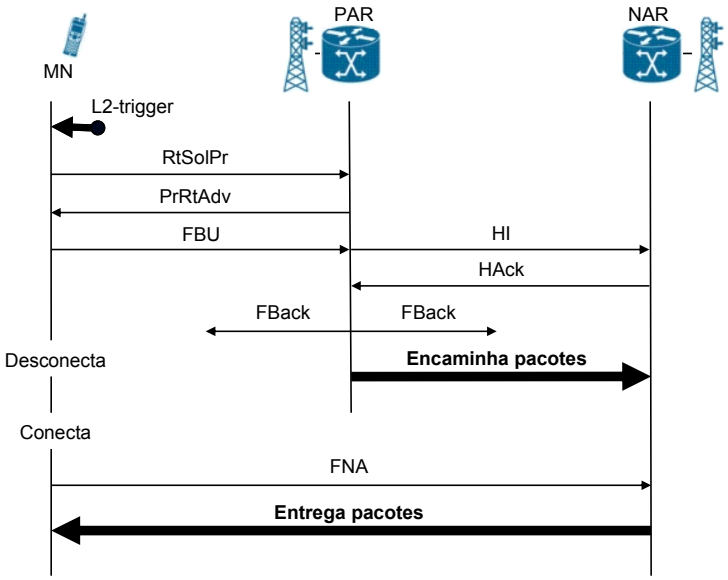


Figura 7– Fast Handover: operação em modo pré-indicado ou antecipado

O cenário no qual o MN envia a mensagem FBU a partir do enlace do NAR é chamado de *operação em modo reativo*, e é ilustrado na Figura 8. Esse modo também atende o caso no qual a mensagem FBU é enviada a partir do enlace do PAR, mas uma mensagem FBack ainda não foi recebida.

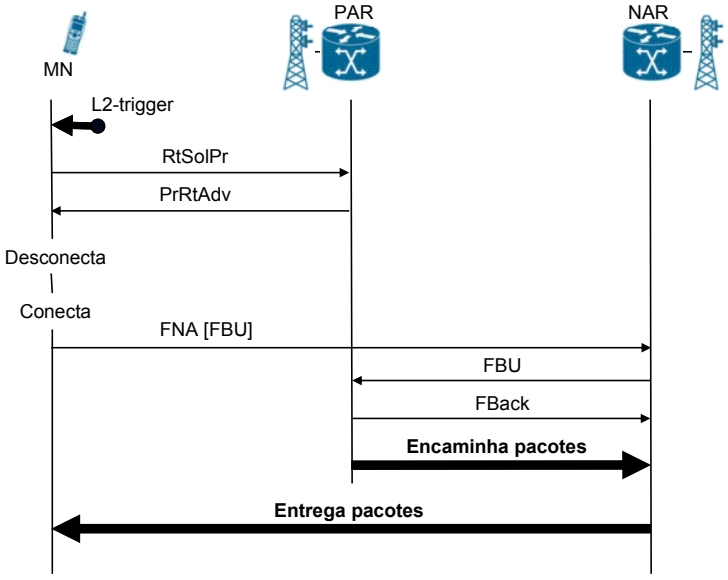


Figura 8– Fast Handover: operação em modo reativo

Por fim, a mensagem PrRtAdv pode ser enviada de forma não solicitada, ou seja, sem o envio anterior da mensagem RtSolPr. Essa operação possibilita que o MN se mantenha informado sobre redes geograficamente adjacentes, reduzindo, assim, a quantidade de tráfego necessária para obter o mapa de topologia da vizinhança de enlaces e subredes.

Já, as mensagens HI e HAck podem ainda ser utilizadas para transferência de informações referentes ao contexto de rede, como controle de acesso, QoS e compressão de cabeçalho, em conjunto com o handoff.

3.4 Requisitos de uma solução de QoS para o MIPv6

Após a movimentação do MN entre redes (handoff) enquanto atua como um dos pontos terminais de um fluxo de dados (emissor ou receptor), as informações associadas à sua localização são alteradas, o que geralmente implica em mudança do caminho do fluxo. Essa mudança requer o restabelecimento das reservas feitas para o fluxo em andamento com referência ao novo caminho estabelecido entre os pontos terminais. A complexidade desse problema aumenta se ambos os pontos terminais forem móveis.

Tendo em vista a necessidade de se prover soluções de QoS adequadas para o MIP, [9] apresenta três requisitos básicos para a busca dessas soluções: (i) requisitos de desempenho; (ii) requisitos de interoperabilidade; e (iii) requisitos gerais.

Com relação aos requisitos de desempenho, três pontos devem ser observados: (i) minimizar a interrupção da QoS no momento do handoff, que se refere ao rápido encaminhamento dos requisitos de QoS para a nova localização para evitar perda na garantia de QoS provida na antiga localização, (ii) localizar os pontos afetados pelo handoff que requerem o restabelecimento da QoS, que se refere à identificação dos pontos afetados pela mudança de localização, normalmente próximos da extremidade, visando evitar a replicação de reservas de recursos; e (iii) liberar os recursos alocados no antigo caminho do fluxo após o handoff, que se refere à necessidade de rápida liberação das reservas associadas ao antigo caminho do fluxo, o que nem sempre é simples pois há perda de conectividade do MN no enlace da antiga localização.

Os requisitos de interoperabilidade dizem respeito a dois requisitos básicos: (i) interoperabilidade com protocolos de mobilidade, que implica em ter mecanismos que tirem proveito das otimizações propostas para os protocolos de mobilidade quando as mesmas estiverem disponíveis; e (ii) interoperabilidade com caminhos de fluxos heterogêneos com respeito à paradigmas de QoS, que implica em se ajustar às mudanças dos modelos de suporte à QoS implantados nas redes atravessadas pelo MN após um handoff.

Quanto aos requisitos gerais, dois pontos são destacados: (i) suporte à QoS ao longo de múltiplos caminhos possíveis, que se refere à possibilidade de ter suporte à QoS nos diversos caminhos possíveis entre o emissor e o receptor, como por exemplo, ao longo do túnel bidirecional entre o MN e o HA, ou no caminho direto entre o MN e o CN através da otimização de roteamento; e (ii) interações com o suporte à QoS da camada de enlace sem fio, que visa prover mecanismos para tirar proveito dos recursos de QoS oferecidos pela camada de enlace.

Com base nesses requisitos vários aprimoramentos foram propostos para o RSVP com o objetivo de adequá-lo ao Mobile IP. Esses aprimoramentos são apresentados no capítulo seguinte.

4 Aprimoramentos no RSVP para o MIPv6

Este capítulo apresenta alguns dos principais aprimoramentos propostos no RSVP para otimizar a garantia de QoS no MIPv6. De modo geral, essas propostas visam soluções para: (i) prever a futura localização do nó móvel; (ii) antecipar reservas de recursos nas

redes vizinhas; (iii) minimizar o tempo para restabelecimento das reservas correntes; e (iv) evitar demasiadas alterações na estrutura do RSVP.

4.1 Mobile Extension to RSVP

A extensão proposta em [19] define, primeiramente, a distinção entre três classes de reservas no RSVP: (i) *committed*, (ii) *quiescent* e (iii) *transient*. A reserva *commited* se refere a forma tradicional de reserva e alocação de recursos do RSVP, ou seja, com reserva exclusiva de recursos para um certo fluxo. Na reserva *quiescent*, os recursos são reservados, mas não são alocados. A vantagem é que, nesse estado, um recurso pode ser temporariamente alocado para algum cliente que solicite uma reserva *transient*, mudando, então, de estado. Um recurso no estado transient sofre preempção quando a reserva é ativada pelo cliente que originalmente fez a reserva quiescent do mesmo.

O trabalho também propõe a criação de uma entidade chamada *virtual receiver* nas estações base ou access points das células. Sua tarefa é atuar como um procurador (proxy) para nós móveis viabilizando a criação de reservas quiescent nas células para onde esses nós pretendem migrar. O virtual receiver é responsável por executar as operações de refresh requeridas pelo RSVP em nome dos nós móveis para os quais foram feitas reservas quiescent.

Por fim, [19] também menciona a necessidade de procedimentos para predição de mobilidade com o objetivo de estimar a mais provável futura localização dos nós móveis, determinando, assim, onde as reservas quiescent devem ser feitas.

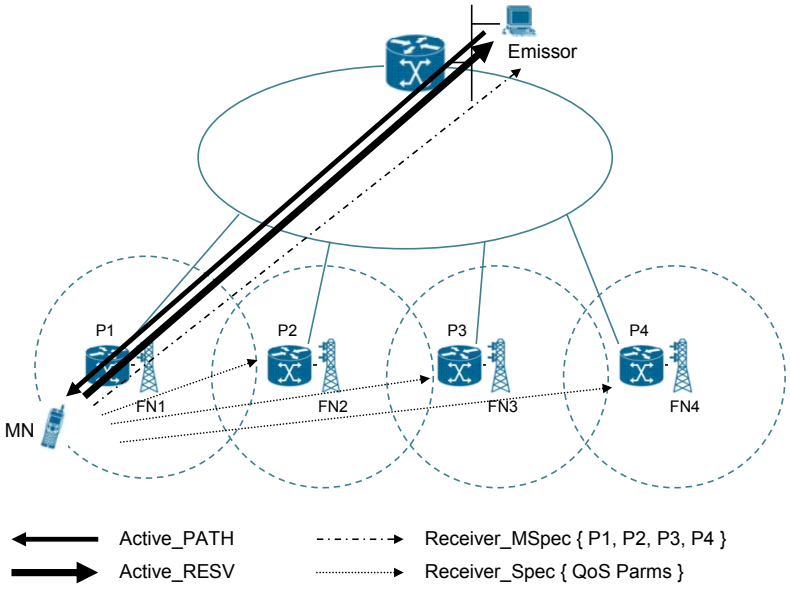
4.2 Mobile Resource ReSerVation Protocol (MRSVP)

A proposta de protocolo de reserva feita por [20], baseia-se na antecipação de reservas em todas as células que serão visitadas pelo nó móvel durante sua participação em um fluxo. Essa definição de percurso é chamada Mobility Specification (MSPEC) e, de acordo com [20], poderia ser determinada através de vários mecanismos citados no trabalho ou pelo próprio nó móvel. Em particular, [20] assume que cada localização no MSPEC do nó móvel é representada pelo endereço de rede da subrede que cobre a localização.

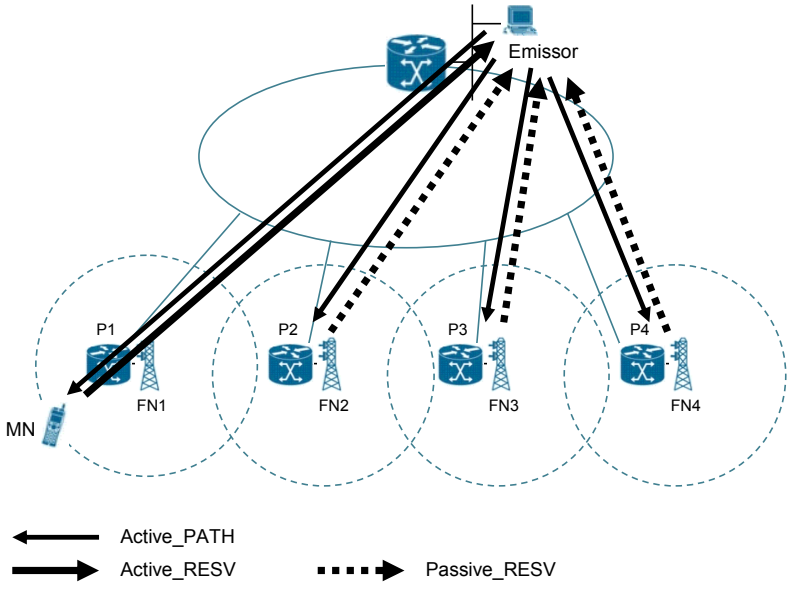
O modelo proposto suporta dois tipos de reservas: (i) *ativas* e (ii) *passivas*. Um emissor móvel faz uma reserva ativa a partir de sua localização corrente e faz reservas passivas a partir das outras localizações indicadas no seu MSPEC. De modo semelhante, um receptor móvel faz uma reserva ativa para sua localização corrente e faz reservas passivas para as outras localizações no seu MSPEC. Em um mesmo enlace, reservas ativas e passivas são mescladas, embora possam ser removidas de forma independente. Para melhorar a utilização dos enlaces, a largura de banda da reserva passiva de um fluxo pode ser utilizada por outros fluxos que requerem menor garantia de QoS ou serviço de melhor esforço. No entanto, quando uma reserva passiva se torna ativa, esses fluxos podem ser afetados.

O MRSVP requer *proxy agents* para fazerem as reservas ao longo dos caminhos a partir das localizações indicadas no MSPEC do emissor para as localizações indicadas no MSPEC do receptor. Na localização corrente esse proxy é chamado de *local proxy agent*, e nas outras localizações indicadas no MSPEC é chamado de *remote proxy agent*. Os remote proxy agents fazem reservas passivas em nome do nó móvel, enquanto o local proxy agent atua como um roteador normal, onde a reserva ativa é solicitada pelo nó móvel. Tendo em vista que os endereços de rede das localizações são conhecidos, a

descoberta dos endereços IP dos proxy agents é feita através do *proxy discovery protocol*, conforme descrito em [20].



(a)



(b)

Figura 9 – Antecipação de reservas no MRSVP com Emissor fixo e Receptor móvel

Conforme ilustrado na Figura 9a, após a descoberta dos remote proxy agents referentes às redes que serão atravessadas pelo MN durante a manutenção de um fluxo, o MN envia a mensagem Receiver_MSPEC para o Emissor informando sobre esses remote proxy agents, no caso, P2, P3 e P4. Simultaneamente, o MN envia a mensagem Receiver_Spec para cada um dos remote proxy agents para informar sobre os parâmetros de QoS utilizados pelo fluxo corrente. Em seguida, conforme ilustrado na Figura 9b, o Emissor, que é fixo, envia mensagens Active_PATH para cada um dos remote proxy agents indicados no MSPEC do MN. Por fim, cada um dos remote proxy agents envia a mensagem Passive_RESV para o Emissor.

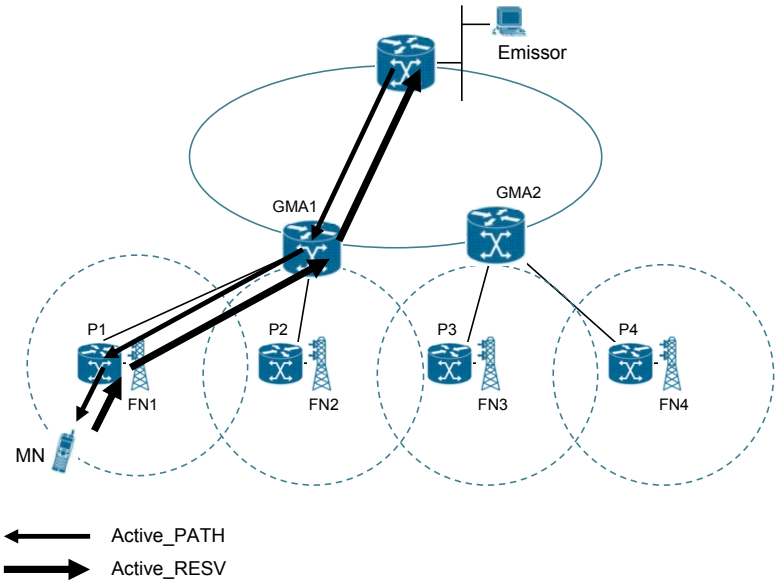
A arquitetura proposta causa uma grande sobrecarga na rede devido à grande quantidade de mensagens geradas pela execução do proxy discovery protocol e pela manutenção das reservas antecipadas em todas as localizações indicadas no MSPEC. A análise de escalabilidade feita em [20] admite que uma abordagem hierárquica poderia reduzir a sobrecarga.

Uma modificação no MRSVP é proposta por [21], assumindo uma arquitetura de rede microcelular, onde um nó móvel conhece o endereço de sua estação base e facilmente obtém os seis endereços das estações bases vizinhas, onde residem os proxy agents. Essa modificação também introduz o parâmetro de QoS chamado *rate reduction factor* para lidar com as reservas passivas solicitadas. Como uma estação base tem que fazer reservas passivas antecipadas com as vizinhas, existe a possibilidade que alguma dessas reservas não seja feita devido à ausência de recursos disponíveis. Por isso, esse parâmetro indica um fator pelo qual a requisição original do recurso pode ser reduzida caso não seja viável. Esse mecanismo garante que pelo menos algum recurso será reservado.

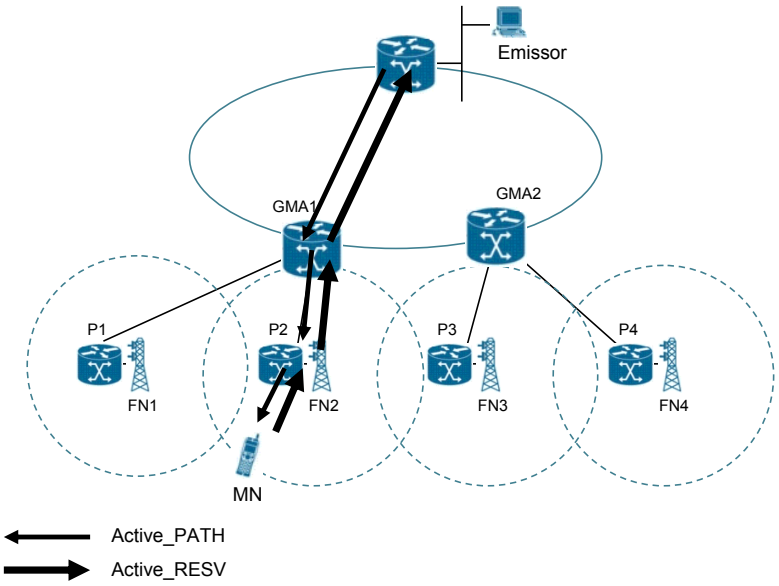
4.3 Hierarchical Mobile RSVP (HMRSVP)

O HMRSVP [22] visa aprimorar o MRSVP aproveitando a característica hierárquica do Mobile IP Regional Registration [14], que foi a base da idealização do HMIPv6 [11]. O modelo hierárquico especificado em [14] divide a mobilidade em duas categorias: (i) *intra-domínio* (micromobilidade) e (ii) *inter-domínio* (macromobilidade). Esse modelo possui um elemento central chamado *Gateway Mobility Agent* (GMA), conhecido como MAP no HMIPv6, que define um domínio formado por uma ou mais redes.

A Figura 10a apresenta o MN no domínio do GMA1, formado por duas redes, FN1 e FN2, cada uma com seu proxy agent, respectivamente P1 e P2. A linha escura apresenta o caminho das reservas ativas entre o Emissor (CN) e o MN. Supondo que o MN se move em direção à rede FN2, a movimentação será intra-domínio. Conforme ilustrado na Figura 10b, quando o MN passar para a rede FN2, o processo de *regional registration* do seu novo CoA nessa rede será iniciado pelo mesmo e interceptado pelo GMA1, que, então, cancelará o caminho das reservas ativas entre o GMA1 e o P1 e estabecerá o caminho das reservas ativas entre o GMA1 e o P2, de forma transparente para o Emissor.



(a)



(b)

Figura 10 – Movimento intra-domínio no HMRSVP

Com relação à movimentação inter-domínio, [22] assume que o MN é capaz de detectar que o mesmo se encontra em uma região de sobreposição entre duas redes. A Figura 11 ilustra essa movimentação, onde o MN se desloca da rede FN2 para a rede FN3. Nessa situação, o MN executa o procedimento *Multiple Simultaneous Registration* para obter seu novo CoA, fornecido pelo P3. Essa mensagem de registro é então enviada pelo P3 ao GMA2, que a encaminha para o HA do MN. Com isso, o HA adiciona o GMA2 na lista de CoAs do MN, retornando a mensagem Registration Reply para o GMA2. Ao receber essa mensagem, o GMA2 a encaminha para o MN através do P3. Dessa forma, o MN obtém o endereço do GMA2 embutido na mensagem Registration Reply recebida.

Após o processo de registro, conforme ilustrado na Figura 11a, o MN envia a mensagem Receiver_MSpec { GMA1, GMA2 } para o Emissor informando que ele se encontra em uma área de sobreposição entre as redes servidas por GMA1 e GMA2. Ao mesmo tempo, o MN envia a mensagem Receiver_Spec ao P3 para informá-lo sobre os parâmetros de QoS do fluxo corrente. Em seguida, conforme ilustrado na Figura 11b, o Emissor inicia a reserva de recursos (mensagem Active_PATH) ao longo do caminho até o P3, passando pelo GMA2. Por sua vez, o P3 faz as reservas passivas enviando a mensagem Passive_RESV para o Emissor, seguindo o caminho no sentido inverso.

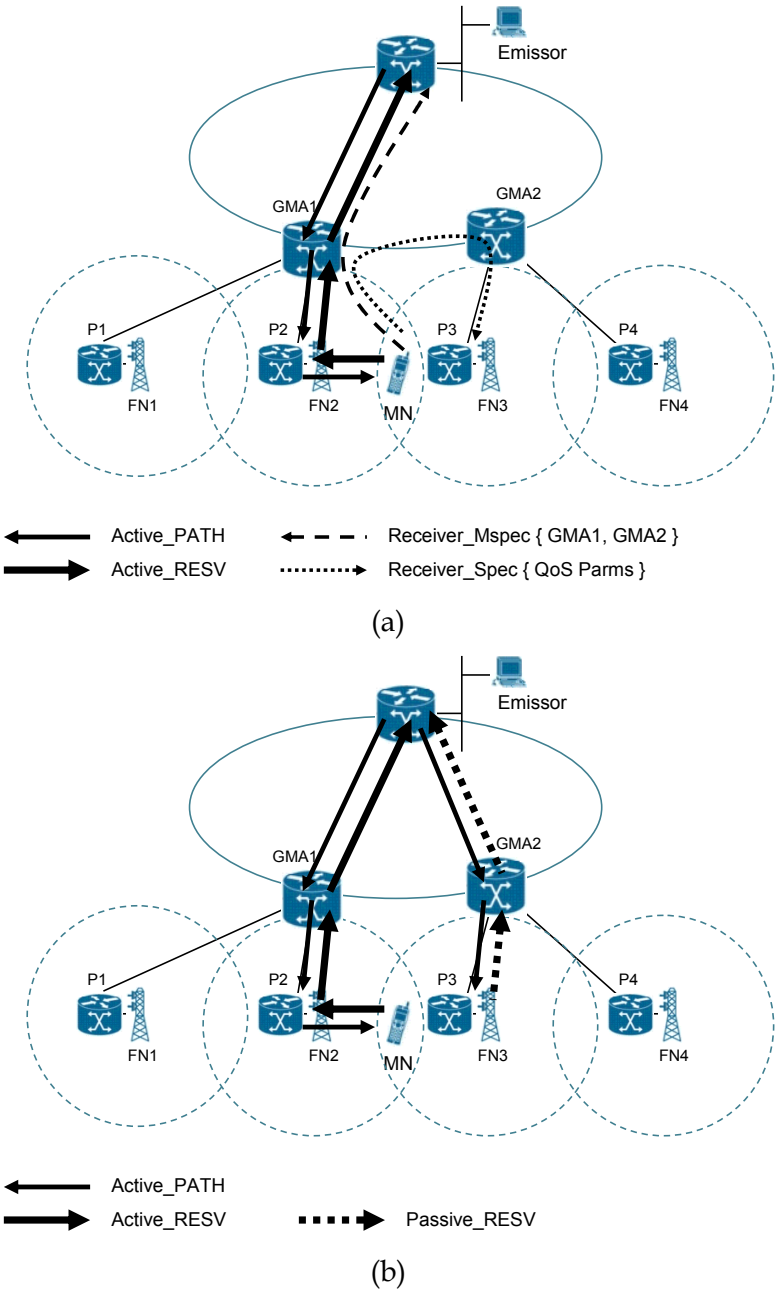
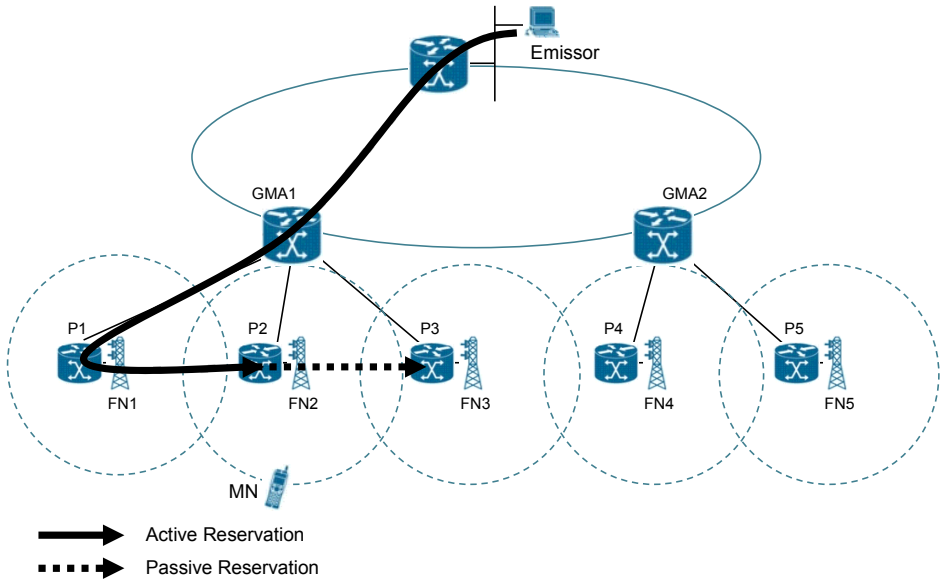


Figura 11 – Movimento inter-domínio no HMRSVP

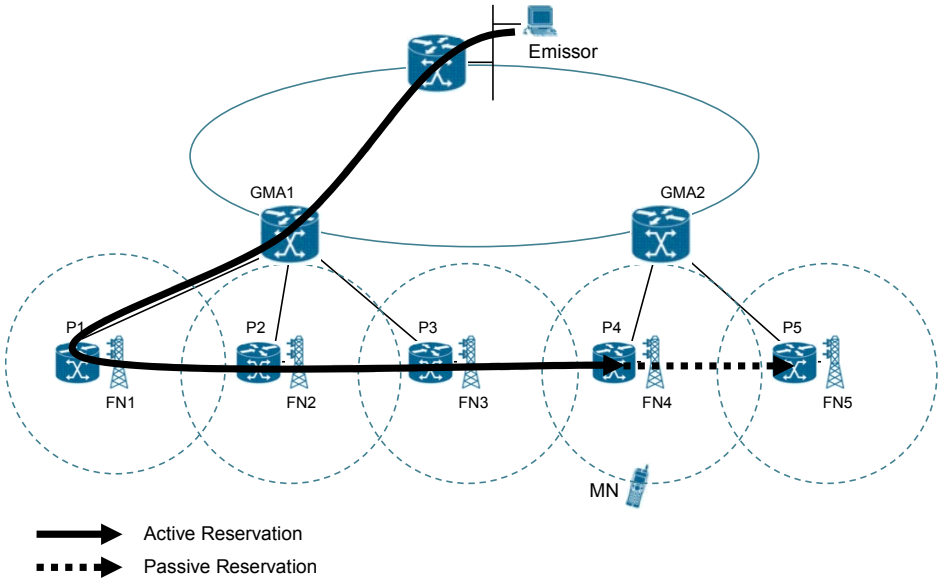
Conforme apresentado, diferentemente do MRSVP, que faz reservas passivas em todas as redes vizinhas, o HMRSVP antecipa a reserva passiva de recursos para um MN apenas quando o mesmo se encontra na área de sobreposição de duas redes vizinhas.

4.4 HMRSVP with Pointer Forwarding

[23] introduz um esquema de otimização no HMRSVP chamado *Pointer Forwarding*. Nesse esquema, assume-se que a probabilidade da micromobilidade ocorrer é bem maior que da macromobilidade, e que o MN percorre um sentido único. A Figura 12 ilustra esse esquema para a: (a) movimentação intra-domínio; e (b) movimentação inter-domínio.



(a) movimentação intra-domínio



(b) movimentação inter-domínio

Figura 12 – HMRSVP with Pointer Forwarding

Outra contribuição de [23] é a análise comparativa do custo da reserva de recursos entre três esquemas: (i) reservas passivas em todos os proxy agents de um domínio; (ii) reservas passivas apenas nos dois proxy agents vizinhos ao proxy agent do MN; e (iii) reserva passiva apenas no proxy agent seguinte da corrente formada pelo pointer forwarding. Como resultado, verificou-se que o custo do primeiro esquema é significativamente maior que o segundo e o terceiro, e o esquema com pointer forwarding é melhor que o segundo esquema quando a movimentação é curta, ou seja, quando a quantidade de elos na corrente é pequena. A análise indicou a necessidade de se determinar um ponto de reinicialização (*resetting point*) da corrente quando a movimentação for longa, garantindo assim, melhor desempenho que o segundo esquema.

Essa necessidade também é verificada por [24], que apresenta uma proposta modificada do HMRSVP with Pointer Forwarding, na qual a corrente deve ser restabelecida

durante uma movimentação intra-domínio. Outro ponto importante observado por [24] é a possibilidade da corrente formar um loop após um período de movimentação do MN. Esse loop deve ser identificado e quebrado para evitar perda de desempenho, e tal função deve ser executada pelo proxy agent que é adicionado como um novo elo da corrente.

O trabalho apresentado em [25] foca na movimentação intra-domínio. A proposta apresentada é baseada em uma arquitetura bastante similar ao HMRSVP with Pointer Forwarding, aprimorada com um mecanismo chamado *paging* para grupar subredes de um mesmo domínio em *paging areas* (PAs), conforme ilustrado na Figura 13. Para evitar uma longa corrente de encaminhamento, são adotados dois esquemas de reinicialização: (i) baseado em região; e (ii) baseado em movimento. No primeiro, a reinicialização da corrente ocorre quando o MN se move entre paging areas. No segundo, ocorre quando o número de movimentos do MN entre as subredes do domínio excede um valor limite. Conforme verificado em [25], a reinicialização da corrente com base em movimento tem melhor desempenho na maioria dos casos analisados.

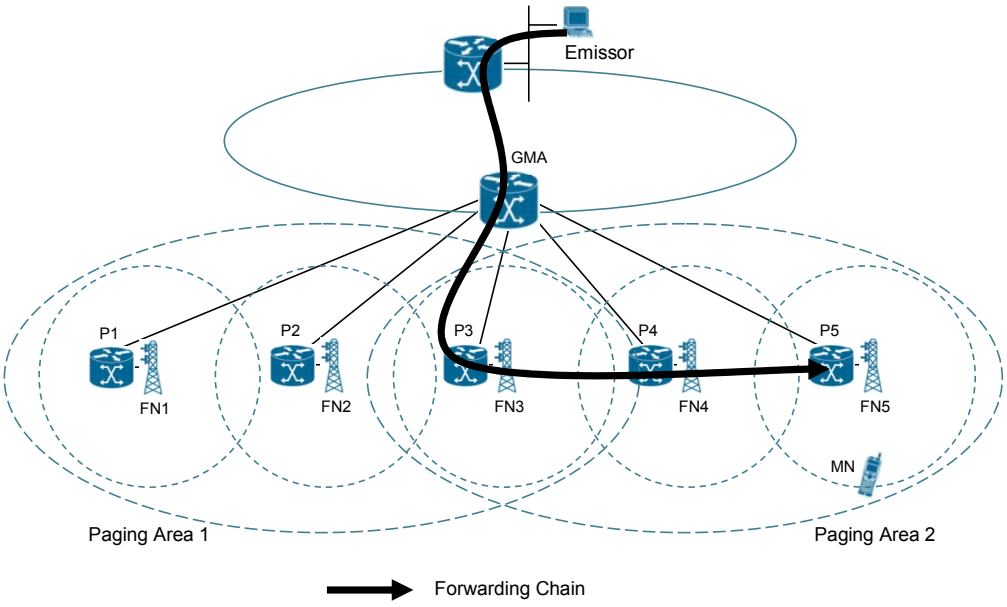


Figura 13 – HMRSVP with Pointer Forwarding and Paging Areas

4.5 RSVP Mobility Proxy (RSVP-MP)

A proposta apresentada em [26] também visa aprimorar o funcionamento do RSVP na arquitetura hierárquica do MIPv6 [11]. Em particular, essa proposta aproveita a distinção feita entre os dois care-of addresses associados ao MN quando dentro de um domínio hierárquico: (i) o *Regional CoA* (RCoA), também conhecido como CoA do domínio; e (ii) o *Local CoA* (LCoA), também conhecido como CoA da rede local interna ao domínio. Na proposta feita, a entidade funcional conhecida como RSVP Mobility Proxy é responsável pela manipulação das mensagens RSVP que atravessam a borda da rede sem fio. Sua funcionalidade básica se resume em interceptar as mensagens PATH e RESV entre o MN e o CN substituindo o RCoA pelo LCoA no sentido externo-interno, e vice-versa. Assim, as reservas feitas para o fluxo entre o MN e o CN nos elementos de rede externos ao domínio ficam associadas ao par <RCoA, CN>, enquanto as reservas nos elementos de rede internos do domínio ficam associadas ao par <LCoA, CN>. Dessa forma, após um movimento intra-domínio do MN, as reservas <RCoA, CN> existen-

tes permanecem inalteradas, enquanto apenas as reservas <LCoA, CN> são restabelecidas pelo RSVP-MP em nome do MN e do CN. A Figura 14 ilustra a topologia de rede com o RSVP-MP.

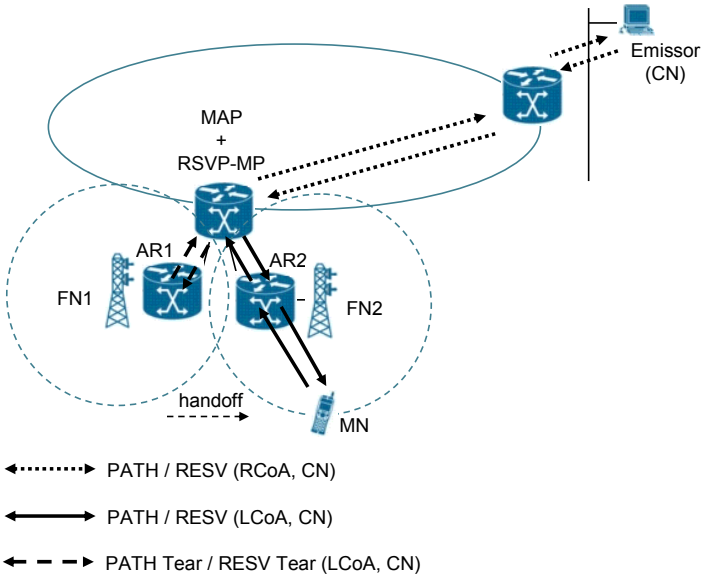


Figura 14 – Topologia de rede com o RSVP-MP

O detelhamento da troca de mensagens para uma reserva de QoS bidirecional entre o MN e o CN utilizando o RSVP-MP é apresentada na Figura 15. Em particular, pode-se observar que as reservas externas ao domínio ficam associadas ao RCoA do MN, enquanto as reservas internas ficam associadas ao LCoA do MN. Isso simplifica o restabelecimento das reservas na nova localização do MN após o handoff e restringe as trocas de mensagens vitais do RSVP ao domínio corrente do MN. Durante esse processo, o *Mobility Anchor Point* (MAP) definido na arquitetura hierárquica do MIP atua em conjunto com o RSVP-MP no mapeamento entre o RCoA e o LCoA dos pacotes.

A Figura 16 ilustra o diagrama de mensagens para restabelecimento das reservas existentes no domínio. Enquanto as novas reservas são feitas para a nova localidade do MN, as antigas reservas são canceladas para a antiga localidade com as mensagens PATH Tear e RESV Tear. As mensagens PATH e RESV enviadas para fora do domínio funcinam como mensagens de refresh para as reservas feitas nos elementos de rede externos no caminho até o CN.

Como o restabelecimento das reservas ocorre apenas no domínio do RSVP-MP, a probabilidade de rejeição de novas reservas para fluxos em andamento após o handoff é bastante reduzida, podendo ocorrer apenas durante uma macromobilidade, onde há mudança de domínio, ou na falta de recursos nos elementos de rede do domínio, durante uma micromobilidade.

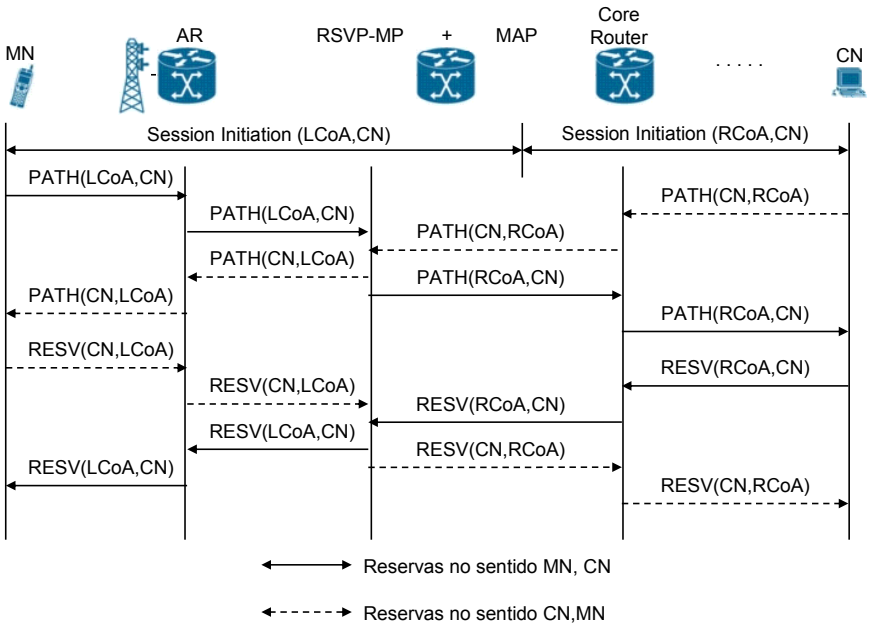


Figura 15 – Diagrama de mensagens para reserva de QoS bidirecional no RSVP-MP

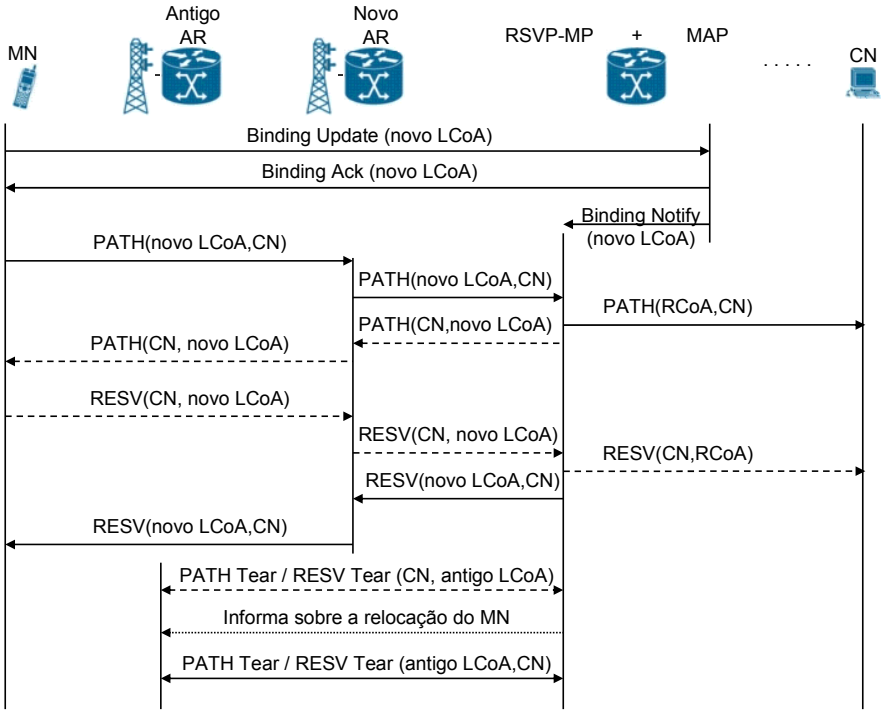


Figura 16 – Restabelecimento das reservas após o handoff no RSVP-MP

4.6 Hierarchical Proxy Mobile RSVP (HPMRSVP)

A proposta do HPMRSVP [27] aproveita as vantagens da arquitetura do F-HMIPv6 [13], que, basicamente, conjuga as otimizações do handoff introduzidas pelo HMIPv6 [11] e pelo FMIPv6 [12]. Assim como no RSVP-MP [26], descrito na seção 4.5 , o HPMRSVP aproveita a distinção feita entre os dois care-of addresses (RCoA e LCoA)

associados ao MN quando dentro de um domínio hierárquico. No HPMRSVP, o próprio MAP atua como RSVP Mobility Proxy e intercepta as mensagens PATH e RESV entre o MN e o CN, substituindo o RCoA pelo LCoA no sentido externo-interno, e vice-versa. A principal diferença entre o RSVP-MP e o HPMRSVP é a utilização do FMIPv6 para minimizar o atraso e a perda dos pacotes no processo de handoff, durante o tempo de ausência de conexão na camada de enlace. Esse procedimento faz com que o MAP encaminhe os pacotes destinados ao MN para o NAR, que, por sua vez, armazena esses pacotes até o registro do MN em sua rede. A Figura 17 ilustra o diagrama de mensagens do HPMRSVP durante o handoff.

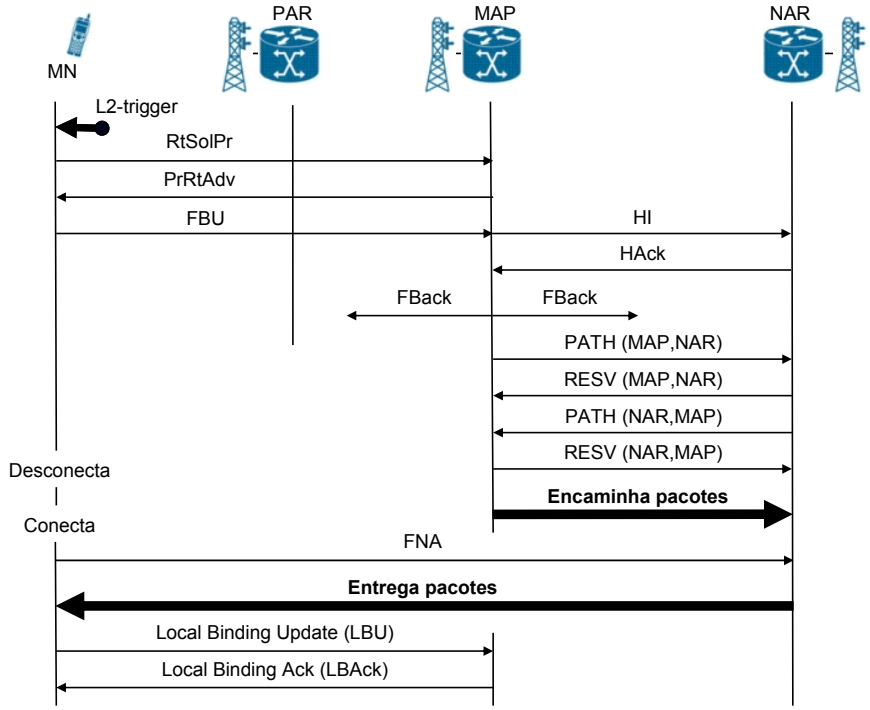


Figura 17 – Diagrama de mensagens do HPMRSVP durante o handoff

Ao receber uma indicação da camada de enlace com a identificação de um AP para o qual vai migrar, o MN inicia o procedimento do FMIPv6 com a diferença de trocar mensagens com o MAP e não com o seu AR atual, identificado como PAR (Previous Access Router) na Figura 17. Resumidamente, o MN envia a mensagem *Router Solicitation for Proxy Advertisement* (RtSolPr) para requisitar informações sobre a subrede correspondente ao AP descoberto, cuja resposta é enviada pelo MAP para o MN na mensagem *Proxy Router Advertisement* (PrRtAdv), exatamente como definido no FMIPv6.

Com as informações obtidas, o MN formula um novo CoA (NCoA) e envia uma mensagem de *Fast Binding Update* (FBU). Essa mensagem tem o propósito de autorizar o MAP a fazer o binding do PCoA (Previous CoA) para o NCoA, de modo que os pacotes passem a ser tunelados para a nova localização do MN. Em seguida, o NCoA proposto pelo MN na mensagem FBU é carregado na mensagem *Handover Initiate* (HI) que é enviada pelo MAP para o NAR, que deve fazer o binding do NCoA com o MN. Se o binding for possível, esse NCoA deve ser retornado na mensagem *Handover Acknowledge* (HAck). Como confirmação de recebimento do FBU, o MAP deve enviar a mensagem de *Fast Binding Acknowledgment* (FBack) confirmando a validade do NCoA.

No passo seguinte, o MAP, ao invés de restabelecer as reservas referentes aos fluxos no sentido downstream com o NCoA do MN, faz isso com o NAR. Da mesma forma, o

NAR, e não o NCoA, restabelece as reservas no sentido upstream com o MAP. Essa característica do HPMRSVP, embora descaracterize o RSVP, que é um protocolo para reservas fim-a-fim, é apresentada em [27] como uma vantagem, pois argumenta-se que esse procedimento diminui o overhead de sinalização na rede sem fio. Por essa razão, o NAR mantém as reservas (refresh) dos fluxos correntes do MN no sentido upstream em benefício do mesmo.

Após essa etapa, o MAP inicia o encaminhamento de todos os pacotes destinados ao RCoA para o NAR, que, por sua vez, os armazena até o registro do MN em sua rede. Dessa forma, após o restabelecimento de sua conectividade de enlace, o MN envia o quanto antes a mensagem *Fast Neighbor Advertisement* (FNA) para que o NAR inicie o encaminhamento de todos os pacotes que estão chegando e que foram armazenados para o MN.

Para finalizar, o MN envia a mensagem *Local Binding Update* (LBU) para informar ao MAP sobre sua disponibilidade na nova localização. Após a recepção da mensagem *Local Binding Acknowledgment* (LBAck), o MN e o MAP voltam a operar como no HMIPv6 tradicional.

Com o objetivo de minimizar os problemas causados pelo efeito *ping-pong* da camada de enlace, onde o MN migra para uma nova rede, mas, imediatamente em seguida, retorna para a rede a antiga, [27] propõe utilizar *bicasting*, onde o MAP duplica o encaminhamento dos pacotes destinados ao RCoA, repassando-os simultaneamente para o PAR e para o NAR. Isso ocorre até a recepção da mensagem LBU, quando o bicasting deve ser interrompido.

4.7 Localized RSVP

A proposta apresentada em [28] visa possibilitar a reserva de recursos ao longo do caminho parcial entre duas entidades terminais quando uma das partes não suporta o RSVP. Para isso, [28] faz a distinção entre reservas na rede local e reservas fim-a-fim, onde o primeiro caso é aplicado quando apenas uma das partes suporta RSVP e o segundo, quando ambos suportam essa sinalização.

No esquema adotado pelo Localized RSVP (LRSVP), o terminal local deve suportar o RSVP, e o serviço *Localized RSVP Proxy* (LRSVP Proxy) deve ser instalado em algum lugar na rede, preferencialmente no roteador de borda. Para se distinguir entre reservas locais e reservas fim-a-fim, o LRSVP define a utilização de um dos bits não usados do campo Flags do RSVP Session Object, sendo chamado *Local Indication* (LI) bit (0x8). Quando esse bit está marcado, a mensagem RSVP é considerada parte da sinalização de reserva local e, assim, o roteador RSVP com o serviço LRSVP Proxy não a encaminha para o nó seguinte, entregando-a ao serviço LRSVP. No caso contrário, sem a marcação do bit LI, a mensagem indica uma sinalização padrão fim-a-fim, onde o LRSVP Proxy não atua.

A Figura 18 ilustra a situação onde o terminal local deseja fazer uma reserva no sentido *upsteam* e o terminal remoto não suporta RSVP. Nessa situação, a operação de reserva é bastante similar ao padrão. O terminal local apenas envia uma mensagem PATH tradicional com a flag LI marcada. Assim, a mensagem PATH é encaminhada por todos os roteadores até chegar ao roteador com o serviço LRSVP Proxy. Quando a mensagem é entregue a esse serviço, a mensagem RESV correspondente é enviada para o terminal local, confirmando as reservas em cada roteador ao longo do caminho.

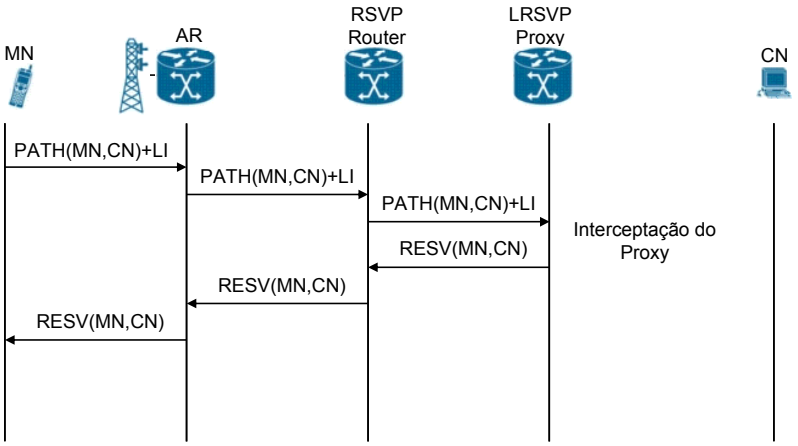


Figura 18 – Reserva no sentido upstream no LRSVP

Para o terminal local fazer uma reserva no sentido *downstream* para receber dados de um terminal remoto que não suporta RSVP, o LRSVP define uma nova mensagem chamada PATH Request. Essa mensagem é similar à mensagem PATH tradicional, com a diferença de ter a flag LI marcada e não fazer reservas ao longo do caminho até o roteador com o serviço LRSVP Proxy. Nela são carregadas informações sobre o receptor (no caso, o próprio terminal remoto), o emissor esperado e o Traffic Specification (Tspec), que pode ser baseado na especificação do usuário do terminal local ou em uma sinalização de sessão do nível de aplicação anterior à transferência.

Conforme ilustrado na Figura 19, a reserva no sentido downstream se inicia com o envio da mensagem PATH Request pelo terminal local. Essa mensagem é interceptada pelo serviço LRSVP Proxy que, então, envia uma mensagem PATH, marcada com a flag LI, em benefício do terninal remoto para o terminal local. Esse último responde com a mensagem RESV, marcando a flag LI, que força o roteador com o serviço LRSVP Proxy a não encaminhá-la adiante.

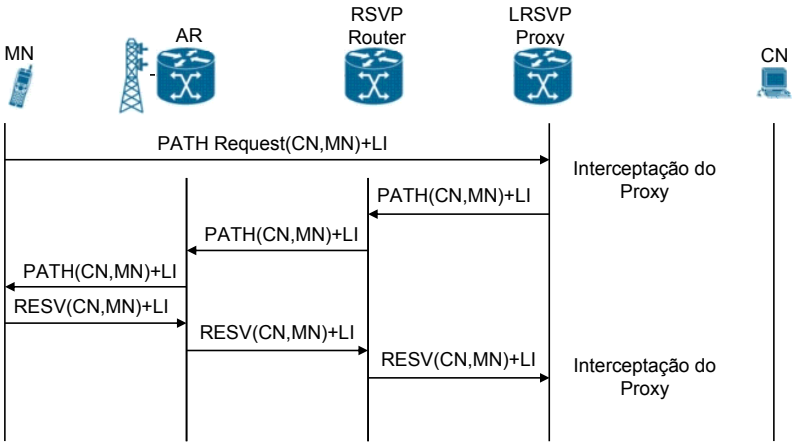


Figura 19 - Reserva no sentido downstream no LRSVP

As reservas no sentido downstream são finalizadas com a mensagem *PATH Request Tear*, também definida em [28]. Sua operação é similar à PATH Request, ou seja, essa mensagem não muda estados ao longo do caminho mas força o LRSVP Proxy a enviar a mensagem PATH Tear na direção do terminal local, para a sessão especificada.

Nas situações de mobilidade do terminal local móvel onde o handoff ocorre, as reservas correntes precisam ser restabelecidas. Para o restabelecimento das reservas no sentido upstream, o terminal local móvel deve enviar uma mensagem PATH, com a flag LI marcada, relacionada a cada uma das reservas correntes. Essas mensagens são interceptadas pelo LRSVP Proxy, que, então, envia as respectivas mensagens RESV, com a flag LI marcada, na direção do terminal local móvel, na nova localização.

Com relação ao sentido downstream, conforme o padrão do RSVP, o terminal local móvel deve aguardar a recepção da mensagem PATH, enviada pelo emissor, para, então, enviar a mensagem RESV para refazer as reservas ao longo do novo caminho.

Para agilizar o processo de restabelecimento de reservas no sentido downstream, o LRSVP define um segundo bit, chamado *Expedited Refresh* (ER) bit (0x4), para viabilizar o *Fast Downstream Reservation*. Na mensagem PATH Request, esse bit sinaliza a necessidade de refresh em algum caminho, sendo encaminhada imediatamente para o LRSVP Proxy. Essa indicação força o envio da mensagem PATH, com as flags LI e ER marcadas, a partir do LRSVP Proxy, em benefício do CN, na direção do terminal local móvel, na nova localização. Ao receber essa mensagem, o terminal local móvel envia a mensagem RESV, com a flag LI marcada, ao longo do caminho percorrido pela mensagem PATH, na direção do LRSVP Proxy. Durante seu percurso, a mensagem RESV pode ser interceptada por um *roteador crossover* a partir do qual a rota do fluxo corrente não foi alterada. A Figura 20 ilustra o procedimento descrito.

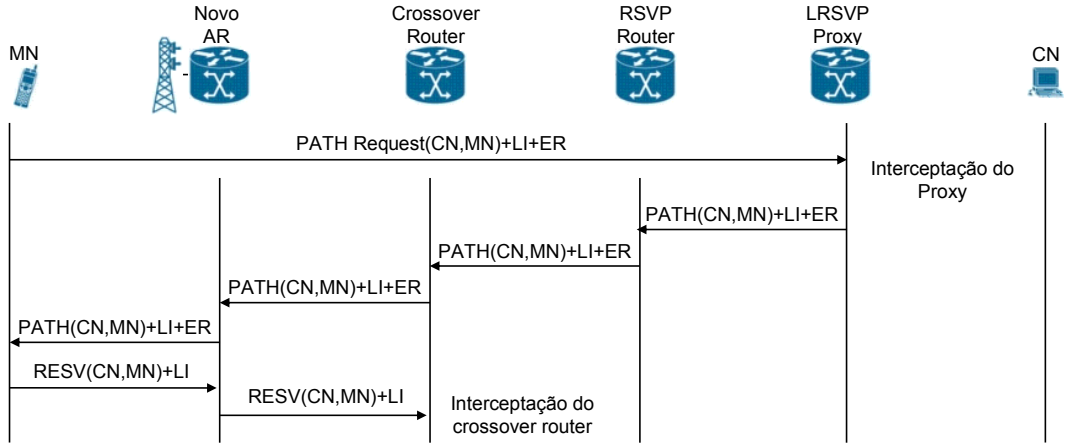


Figura 20 – Fast Downstream Reservation no LRSVP

5 Análise Comparativa dos Aprimoramentos no RSVP para o MIPv6

Esse capítulo faz uma análise comparativa das propostas apresentadas no capítulo 4 com relação aos requisitos discutidos na seção 3.4 com respeito à soluções de QoS para o MIP.

A técnica de antecipação das reservas nas redes que serão vizitadas é utilizada pela maioria das propostas para minimizar a interrupção da QoS no momento do handoff. A forma de implantação dessa solução depende diretamente do grau de informação conhecido sobre a movimentação do MN através das redes sem fio, que pode variar desde a especificação do percurso completo (Mobility Specification - MSpec), como feito pelo MRSVP, até a simples identificação das redes vizinhas de forma antecipada ou

quando na área de sobreposição entre as mesmas, conforme feito nas propostas baseadas no HMRSVP.

Enquanto o MRSVP faz reservas passivas antecipadas em todas as redes indicadas no MSpec do MN, a maioria das propostas baseadas no HMIPv6 opta por reservas passivas apenas durante a micromobilidade. Em particular, o HMRSVP opta por fazer reservas ativas durante a micromobilidade e utilizar o MSpec e as reservas passivas apenas durante a macromobilidade.

O requisito referente à localização dos pontos que requerem o restabelecimento do QoS após o handoff é o ponto chave da otimização nas propostas hierárquicas. O grande facilitador é a própria organização hierárquica, que possibilita a distinção entre a micromobilidade e a macromobilidade. Na primeira, a mudança do roteamento até o MN é transparente para o CN e para todos os elementos de rede externos ao domínio. Ou seja, o flow descriptor não muda para esses integrantes do caminho das reservas entre o MN e o CN, logo não há necessidade de restabelecimento de reservas nessa parte externa ao domínio.

Na micromobilidade, as formas adotadas para o restabelecimento das reservas ao longo dos elementos de rede do domínio varia entre as propostas hierárquicas. O HMRSVP with Pointer Forwarding e sua variante com Paging Areas optam por formar uma corrente de reservas para manutenção dos fluxos em andamento, antecipando reservas passivas com o próximo vizinho, elo da corrente. A reinicialização da corrente pode ocorrer de duas formas: (i) em função de um número máximo de elos; e (ii) em função da mudança de paging area. Ao contrário dessas duas propostas, o HMRSVP, o RSVP-MP, HPMRSVP e o Localized RSVP optam pelo restabelecimento de reservas ativas apenas nos trechos do domínio afetados pela micromobilidade.

A liberação dos recursos alocados no antigo caminho do fluxo após o handoff, pode ser feita por expiração das reservas ou pela desalocação explícita. Todas as propostas hierárquicas oferecem formas para a desalocação explícita, otimizando assim a liberação desses recursos para futuras reservas.

Com respeito à interoperabilidade, as propostas hierárquicas adotam o HMIPv6 e apenas o HPMRSVP integra o FMIPv6 e o HMIPv6 em sua solução. Com isso, o HPMRSVP minimiza a perda de pacotes durante o processo de handoff. Quanto ao tratamento de fluxos heterogêneos com respeito à paradigmas de QoS, todas as propostas apresentadas visam aprimoramentos exclusivamente focados no RSVP, atrelando as soluções ao modelo de serviços integrados, sem buscar qualquer interoperabilidade com outros modelos de serviços ou protocolos.

Embora a especificação do MIPv6 ofereça dois caminhos entre o MN e o CN, o túnel bidirecional (comunicação triangular) é pouco explorado pelas propostas devido à grande otimização oferecida pelo caminho direto (comunicação com otimização de roteamento) entre o MN e o CN. No entanto, o caminho direto só é viável se o CN suporta o controle de mobilidade (mobility binding) do MN, e assim, as propostas que optam por esse caminho também ficam dependentes da disponibilidade desse controle.

Quanto às possíveis interações com o suporte à QoS da camada de enlace sem fio, o modelo IntServ recomenda que se tal suporte existe, o mesmo deve ser aproveitado. No entanto, o HPMRSVP segue essa recomendação apenas no enlace sem fio onde o fluxo foi iniciado. Após um handoff, as reservas dos fluxos em andamento são apenas restabelecidas entre o MAP e o NAR da rede para diminuir o overhead de sinalização no enlace sem fio. Essa estratégia não é adequada para a situação onde um fluxo de dados prioritário é transferido para uma novo enlace sem fio congestionado, onde tal

fluxo será prejudicado por fluxos menos relevantes apenas por falta da reserva no enlace sem fio.

A Tabela 1 apresenta um resumo da análise comparativa apresentada nesta seção.

Tabela 1 – Resumo da análise comparativa com base nos requisitos do RFC 3583

Resumo da análise comparativa com base nos requisitos do RFC 3583

Requisitos		Mobile Extension to RSVP	MRSVP	HMRSVP	HMRSVP with Pointer Forwarding	HMRSVP with Pointer Forwarding and Paging	RSVP Mobility Proxy	HPMRSVP	Localized RSVP
desempenho	minimizar a interrupção da QoS no momento do handoff	Sim, com antecipação de reservas em todas as redes do percurso.	Sim, com antecipação de reservas em todas as redes do percurso.	Sim, com antecipação de reservas apenas na rede vizinha, quando na área de sobreposição.	Sim, com antecipação de reservas apenas na rede vizinha, quando na área de sobreposição.	Sim, com antecipação de reservas apenas na rede vizinha, quando na área de sobreposição.	Sim, apenas na micromobilidade, pois otimiza o restabelecimento das reservas no domínio.	Sim, apenas na micromobilidade, pois otimiza o restabelecimento das reservas no domínio.	Sim, restringe o restabelecimento das reservas ao domínio durante uma micromobilidade.
	localizar os pontos afetados pelo handoff que requerem o restabelecimento da QoS	Não, reservas antecipadas são feitas ao longo do caminho completo.	Não, reservas antecipadas são feitas ao longo do caminho completo.	Não, reservas antecipadas são feitas ao longo do caminho completo.	Sim, as novas reservas são feitas apenas no novo elo da corrente.	Sim, as novas reservas são feitas com o novo elo da corrente na mesma paging area.	Sim, as novas reservas são feitas apenas no caminho até o RSVP-MP.	Sim, as novas reservas são feitas apenas no caminho até o MAP.	Sim, as novas reservas são feitas apenas no caminho até o LRSVP Proxy.
	liberar os recursos alocados no antigo caminho do fluxo após o handoff	Não, recursos liberados por timeout.	Não, recursos liberados por timeout.	Sim, solicitação de liberação feita pelo GMA do domínio.	Sim, solicitação de liberação feita pelo GMA do domínio.	Sim, solicitação de liberação feita pelo GMA do domínio.	Sim, solicitação de liberação feita pelo RSVP-MP.	Sim, solicitação de liberação feita pelo MAP.	Sim, solicitação de liberação feita pelo LSRVP Proxy.
interoperabilidade	interoperabilidade com protocolos de mobilidade	Não aproveita otimizações do MIPv6.	Não aproveita otimizações do MIPv6.	Sim, aproveita a otimização HMIPv6.	Sim, aproveita a otimização HMIPv6.	Sim, aproveita a otimização HMIPv6.	Sim, aproveita a otimização HMIPv6.	Sim, aproveita a otimização HMIPv6 e FMIPv6.	Não aproveita otimizações do MIPv6.
	interoperabilidade com caminhos de fluxos heterogêneos com respeito à paradigmas de QoS	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.	Não suporta. Foco no modelo IntServ.
gerais	suporte à QoS ao longo de múltiplos caminhos possíveis	Não definido.	Sim, pelo túnel bidirecional e pelo caminho direto.	Não, utiliza apenas o caminho direto.	Não, utiliza apenas o caminho direto.	Não, utiliza apenas o caminho direto.	Não, utiliza apenas o caminho direto.	Não, utiliza apenas o caminho direto.	Não, restrito ao caminho até o LRSVP Proxy.
	interações com o suporte à QoS da camada de enlace sem fio	Sim, requisito do IntServ.	Sim, requisito do IntServ.	Sim, requisito do IntServ.	Sim, requisito do IntServ.	Sim, requisito do IntServ.	Sim, requisito do IntServ.	Sim, mas apenas no enlace onde o fluxo foi iniciado.	Sim, requisito do IntServ.

6 Conclusão

O modelo de serviços integrados (IntServ) oferece suporte à QoS através de dois serviços: (i) serviço garantido, para aplicações sensíveis ao retardo, como serviços conversacionais; e (ii) serviço de carga controlada, para aplicações menos sensíveis ao retardo, como streaming de audio e vídeo. Esses serviços são mantidos com base em dois controles: (i) controle de tráfego, composto por um escalonador de pacotes, um classificador e pelo controle de admissão; e (ii) controle de reserva de recursos, que utiliza o RSVP para efetuar reservas.

Nesse modelo, uma QoS exigida por um fluxo de dados é garantida de forma fim-a-fim entre os terminais, notoriamente estáticos, através da reserva de recursos em cada um dos elementos de rede presentes ao longo do caminho do fluxo. O advento da mobilidade dos terminais adicionou uma grande complexidade ao modelo devido à mudança que ocorre no caminho do fluxo após um handoff. Essa mudança exige o restabelecimento das reservas para o fluxo, o que compromete a garantia da QoS.

Várias propostas foram apresentadas para aprimorar o RSVP com o objetivo de manter a garantia da QoS para os fluxos em andamento após o handoff do terminal móvel. A técnica de antecipação das reservas nas redes que serão vizitadas é utilizada pela maioria das propostas. No entanto, essa técnica exige o conhecimento prévio dessas redes, o que nem sempre é possível. Numa abordagem mais simplificada, as reservas são antecipadas apenas quando o terminal móvel se encontra na área de sobreposição de duas redes vizinhas.

As propostas baseadas no HMIPv6 oferecem a vantagem da diferenciação entre a micromobilidade e a macromobilidade. Conforme observado na análise comparativa, na micromobilidade, a mudança do roteamento até o terminal móvel é transparente para o terminal correspondente (CN) e para todos os elementos de rede externos ao domínio, e, assim, não há necessidade de restabelecimento de reservas nessa parte externa ao domínio. Por essa razão, algumas propostas hierárquicas adotam reservas ativas para micromobilidade e reservas passivas apenas para macromobilidade.

Integrando o FMIPv6 com o HMIPv6, o HPMRSVP minimiza a perda de pacotes durante o handoff. A partir desse ganho, o HPMRSVP dispensa o restabelecimento de recursos no enlace sem fio da nova rede para minimizar o overhead de sinalização. Essa estratégia não é adequada para a situação onde um fluxo de dados prioritário é transferido para um novo enlace sem fio congestionado, onde tal fluxo será prejudicado por fluxos menos relevantes apenas por falta da reserva no enlace sem fio.

O Localized RSVP se apresenta como uma solução interessante para o caso onde um dos terminais não suporta a sinalização do RSVP. Nesse caso, o terminal que suporta RSVP é capaz de fazer a reserva de recursos até o LRSVP Proxy de sua rede, tanto no sentido upstream quanto no sentido downstream (em benefício do terminal que não suporta o RSVP). Essas reservas locais podem fazer diferença para muitas aplicações que requerem um mínimo de QoS.

Todas as propostas apresentadas como aprimoramentos ao RSVP contribuem de alguma forma com a manutenção da QoS após o handoff, sendo fundamentais para soluções de QoS para o Mobile IP. Nesse sentido, como meta futura, pode-se estudar a contribuição das técnicas e estratégias utilizadas nessas propostas para garantir a QoS na mobilidade de terminais em ambientes que adotam o Host Identity Protocol (HIP) [29][30].

Referências

[1] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC 1633, June 1994.

[2] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", RFC 2205, September 1997.

[3] J. Wroclawski, "The Use of RSVP with IETF Integrated Services", RFC 2210, September 1997.

[4] S. Herzog, "RSVP Extensions for Policy Control", RFC 2750, January 2000.

[5] A. Terzis, J. Krawczyk, J. Wroclawski, L. Zhang, "RSVP Operation Over IP Tunnels", RFC 2746, January 2000.

[6] F. Baker, C. Iturralde, F. Le Faucheur, B. Davie, "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175, September 2001.

[7] Clark, D., S. Shenker, and L. Zhang, "Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism", in Proc. SIGCOMM'92, September 1992.

[8] J. Polk, S. Dhesikan, "A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow", RFC 4495, May 2006.

[9] H. Chaskar, Ed., "Requirements of a Quality of Service (QoS) Solution for Mobile IP", RFC 3583, September 2003.

[10] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[11] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

[12] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[13] H. Jung et al., "Fast Handover for Hierarchical MIPv6 (F-HMIPv6)", draft-jung-mobileip-fastho-hmipv6-04, Internet draft, June 2004.

[14] E. Fogelstroem, A. Jonsson, C. Perkins, "Mobile IPv4 Regional Registration", draft-ietf-mip4-reg-tunnel-04, Internet Draft, October 2006.

[15] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[16] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[17] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[18] A. O. da Silva, S. Colcher, "Evolução da Otimização do Handoff no Mobile IP", Monografia, Pontifícia Universidade Católica, Departamento de Informática, November 2007.

[19] D. O. Awduche and E. Agu, "Mobile Extensions to RSVP", Proc. 6th Int'l. Conf. Comp. Commun. And Nets., Sept. 1997, pp. 132–36.

[20] A. K. Talukdar, B. R. Badrination, and A. Acharya, "MRSVP: A Resource Reservation Protocol for an Integrated Services Network with Mobile Hosts", Wireless Nets., vol. 7, no. 1, 2001, pp. 5–19.

[21] I. Mahadevan and Krishna M. Sivalingam, "An Experimental Architecture for Providing QoS Guarantees in Mobile Networks Using RSVP", Proc 9th IEEE Int'l. Symp. Pers., Indoor Mobile Radio Commun., vol. 1, Sept. 1998, pp. 50-54.

[22] C.-C. Tseng et al., "HMRSVP: A Hierarchical Mobile RSVP Protocol", Proc. Int'l. Conf. Distrib. Comp. Sys. Wksp., Apr. 2002, pp. 467–72.

[23] G.-C. Lee, T.-P. Wang, and C.-C. Tseng, "Resource Reservation with Pointer Forwarding Schemes for the Mobile RSVP", IEEE Commun. Lett., vol. 5, no.7, July 2001, pp. 298–300.

[24] Y. Min-hua et al., "A Modified HMRSVP Scheme", Proc. 57th Semiannual VTC, vol. 4, Apr. 2003, pp. 2779–82.

[25] Shou-Chih Lo, Guanling Lee, Wen-Tsuen Chen, Jen-Chi Liu, "Architecture for Mobility and QoS Support in All-IP Wireless Networks", IEEE Journal on Selected Areas in Communications, Vol. 22, No. 4, May 2004.

[26] S. Paskalis, A. Kaloxylos, and E. E. Zevas, "An Efficient QoS Scheme for Mobile Hosts", Proc. 26th Annual IEEE Conf. Local Comp. Nets., Nov. 2001, pp. 630–37.

[27] C. A. Abondo, S. Pierre, "Hierarchical Proxy Mobile Resource Reservation Protocol for Mobile IP Networks", IEEE, 2005.

[28] J. Manner, T. Suihko, M. Kojo, M. Liljeberg, K. Raatikainen, "Localized RSVP", draft-manner-lrsvp-04, Internet Draft, September 2004.

[29] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, “Host Identity Protocol”, draft-ietf-hip-base-10, Internet Draft, October 2007.

[30] T. Henderson, “End-Host Mobility and Multihoming with the Host Identity Protocol”, draft-ietf-hip-mm-05, Internet Draft, March 2007.