Gestão de Sessões Multicast sobre Redes de Acesso Heterogéneas

Eng. Pedro Santos – INESC Porto/PT Inovação
Prof. António Pinto, Prof. Manuel Ricardo – INESC Porto
Prof. Francisco Fontes, Drª Teresa Almeida – PT Inovação

Resumo

O *multicast* IP é uma técnica de transmissão adequada ao envio de dados em tempo real para um grupo de utilizadores. Gerando apenas um fluxo de dados por grupo de utilizadores, o *multicast* IP resulta numa utilização eficiente da rede. Contudo, a adopção deste método de transmissão de dados por parte dos operadores tem sido dificultada, em parte, pela inexistência de mecanismos expeditos de controlo de acesso a sessões *multicast* (autenticação, autorização e registo de utilização).

O controlo de acesso a sessões *multicast* pode ser efectuado usando encriptação *end-to-end* dos dados *multicast* ou controlando o acesso e criação de sessões, no nó da rede mais próximo do utilizador. A primeira solução requer um sistema completo de criação e partilha de chaves criptográficas, e não impede o utilizador de receber um fluxo *multicast* não autorizado, apesar de não conseguir aceder ao conteúdo do mesmo. A segunda solução, analisada neste trabalho, implementa o controlo de acesso a sessões *multicast* no nó de acesso à rede.

A solução proposta funciona a nível IP e consiste não só na detecção de pedidos de adesão a sessões *multicast*, e na consequente autorização desses pedidos junto de um servidor de AAA (*Authentication, Authorization and Accounting*), como também permite detectar a criação de sessões *multicast* com origem na rede de acesso (utilizadores como fontes) e efectuar a autorização respectiva. Esta solução impede que um utilizador receba ou transmita um fluxo *multicast* para o qual não tem permissão, é adaptável a várias redes de acesso, fixas e móveis, incluindo xDSL, WiMAX e UMTS, e é independente dos sistemas de autenticação utilizados (neste trabalho foram usados o IEEE 802.1x e PPP).

Palavras-chave: *multicast, controlo de acesso, AAA, redes de acesso heterogéneas.*

1 Introdução

A proliferação de diferentes tecnologias de acesso capazes de suportar ligações de alto débito, aliada a um crescente número de utilizadores de banda larga, tem contribuído para o aumento de conteúdos multimédia na Internet. Os operadores, para suportar o tráfego associado a estes conteúdos, vêem-se forçados a aumentar a capacidade das ligações por si fornecidas e a adquirir *routers* capazes de lidar com o crescente número de sessões *unicast*. Tal, implica investimentos substanciais em infra-estruturas, nem sempre realizáveis (quer por razões técnicas ou financeiras).

Muitas das utilizações de conteúdos multimédia enquadram-se em comunicações em tempo-real, quer no modelo de um-para-muitos (e.g. IPTV) quer no de muitos-para-muitos (e.g. videoconferência). Em comunicação para grupos o *multicast* IP [1] surge como o método de transmissão ideal. Enquanto que em *unicast* são necessários vários fluxos, tipicamente, um fluxo de dados por utilizador, em *multicast* IP apenas se cria um fluxo por grupo de utilizadores. Os pacotes IP de um fluxo *multicast* são replicados em todos os nós da rede onde o percurso para os receptores diverge. Consequentemente, e em comparação com o *unicast*, o *multicast* IP permite, na transmissão de dados para grupos de utilizadores, uma utilização mais eficiente dos recursos de rede.

A adopção do *multicast* [2] por parte dos operadores não é uma tarefa fácil devido à sua natureza aberta. O facto de se poder receber ou transmitir dados *multicast* sem qualquer tipo de autorização ou autenticação prévia torna o *multicast* IP escalável a um grande número de utilizadores mas, ao mesmo tempo, dificulta o seu controlo por parte dos

operadores. A falta de mecanismos de controlo de sessões *multicast* torna tanto a gestão da rede, como o suporte para serviços comerciais baseados em *multicast* difíceis de implementar, já que a capacidade de AAA é essencial para a sua taxação.

Este artigo está organizado da seguinte forma: na secção 2 efectua-se um enquadramento geral sobre os temas abordados, onde se inclui o suporte para *multicast* IP nas várias tecnologias de acesso consideradas (xDSL, WiMAX e UMTS). São então especificados os requisitos do projecto e no final da secção é apresentada a solução. Na 3ª descreve-se a implementação do protótipo demonstrativo da solução apresentada, enumerando-se ainda as suas funcionalidades. Na secção 4 apresentam-se alguns exemplos de possíveis aplicações. Por fim, na secção 5, são apresentadas as conclusões.

2 Abordagem técnica

À medida que as redes de acesso convergem para o modelo IP, é de todo o interesse aproveitar as vantagens inerentes à adopção do *multicast* IP, independentemente da tecnologia de acesso utilizada [3]. A Figura 1 demonstra o cenário que serviu de base ao desenvolvimento deste trabalho. Neste cenário são consideradas 3 redes de acesso de banda larga (UMTS, xDSL e WiMAX).

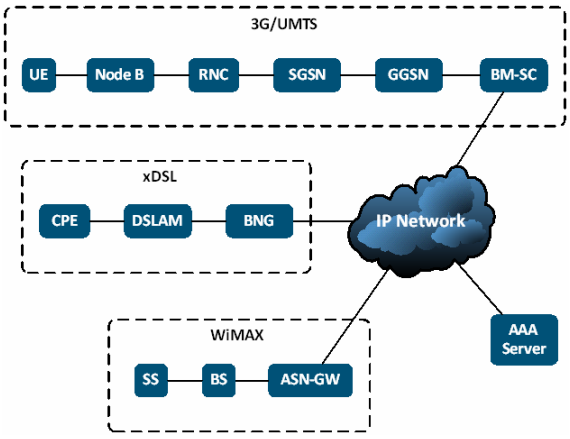

Figura 1 – Cenário de referência

O controlo de acesso aos conteúdos transmitidos por *multicast* IP pode ser conseguido de duas formas: pela cifra de dados *end-to-end*; ou controlando o acesso aos grupos *multicast* [4] .

A cifra protege o acesso não autorizado aos conteúdos transmitidos, mas não evita que utilizadores efectuem a adesão a grupos para os quais não tem permissão de acesso; obtendo assim os fluxos *multicast* correspondentes, ainda que cifrados. A cifra implica ainda a utilização de *software* específico para a distribuição e partilha de chaves criptográficas, tanto do lado do cliente como do operador.

O controlo do acesso a grupos *multicast* não garante, por si só, a confidencialidade dos dados mas permite ao operador gerir a distribuição de dados *multicast* ao nível da rede. Este método baseia-se na gestão de sessões *multicast* nos *edge routers*, já que estes equipamentos são os responsáveis por processar as mensagens IGMP dos utilizadores. É possível identificar e filtrar pedidos de adesão a grupos e transmissões *multicast* de um utilizador. Torna-se, portanto, possível discriminar que fluxos *multicast* um utilizador pode receber e para que grupos *multicast* consegue transmitir (agir como fonte).

2.1 Enquadramento

A gestão de sessões *multicast* IP implica determinar como fazer o controlo de acesso, mas também, onde efectuar este controlo. Principalmente porque a implementação do *multicast* difere de tecnologia para tecnologia, nomeadamente no que concerne: ao processo de adesões a grupos, ao mecanismo de transmissão de conteúdos; aos elementos envolvidos no processo.

Relativamente ao cenário considerado, apesar de todas as redes de acesso identificadas suportarem *multicast* IP, é importante perceber o funcionamento do *multicast* a nível 2 e de que forma é que este funcionamento poderá influenciar possíveis soluções de gestão de sessões *multicast*.

2.1.1 Multicast IP

O *multicast* IP é uma técnica de comunicação para grupos que consiste na distribuição, em tempo real, de dados (sob forma de pacotes IP) para um conjunto de utilizadores que tenha demonstrado interesse em os receber.

A Figura 2 demonstra uma típica sessão *multicast* IP. A rede é constituída por três elementos base: o grupo *multicast*, a fonte de conteúdos, e a árvore de distribuição. Conceitos estes que serão detalhados de seguida.

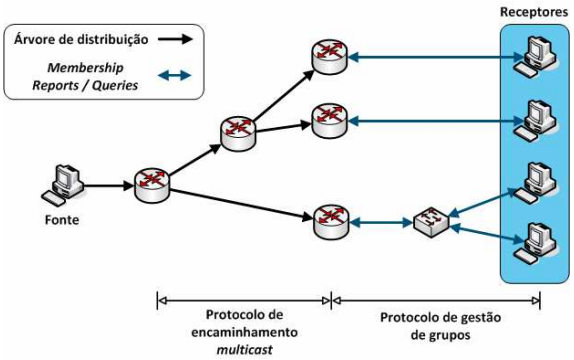

Figura 2 – Elementos de uma rede *multicast* IP

Grupo: conjunto de receptores de um fluxo de dados emitido (em tempo real) por uma ou mais fontes *multicast*. Os grupos são representados por endereços IPv4 classe D (224.0.0.0/8) [5]. Sempre que um utilizador quiser aderir a um grupo, basta enviar um pedido de adesão com o endereço IP do grupo correspondente. A gestão dos grupos em IPv4 é feita através do *Internet Group Management Protocol* (IGMP) [6]. Este protocolo permite aos receptores comunicar à rede a intenção de aderir ou de sair de um grupo *multicast*, assim como, a de manter adesões previamente efectuadas. O IGMP é um protocolo de rede local, e como tal, é apenas utilizado entre os receptores e os *routers* de acesso respectivos.

Fonte: transmite conteúdos (sob a forma de pacotes IP) para um ou mais grupos *multicast*. O envio de tráfego *multicast*, não tem qualquer requisito associado, logo, para que um elemento da rede se tornar numa fonte basta que comece a transmitir tráfego destinado a qualquer endereço *multicast*. A transmissão de dados em *multicast* IP é feita utilizando o protocolo UDP (*User Data Protocol*).

Árvore de distribuição: caminho pelo qual o tráfego multicast associado a um grupo é encaminhado. As árvores de distribuição são construídas pelos *routers* da rede utilizando para o efeito protocolos de encaminhamento *multicast* (e.g. PIM-SM). As árvores de distribuição podem ser subdivididas em 2 tipos: árvores centradas na fonte (raiz da árvore na fonte *multicast*) e árvores partilhadas (raiz da árvore num nó algures na rede).

Em *multicast* IP existem 2 modelos de serviço: o *Any-Source Multicast* (ASM) e o mais recente *Source-Specific Multicast* (SSM) [7]. Em ASM, o modelo de comunicação adoptado é o de M-N (M fontes, N receptores) sendo que cada grupo é representado unicamente pelo endereço IP *multicast* (IPv4 classe D). Em SSM, o modelo de comunicação adoptado é o de 1-N, onde cada grupo é identificado, não só pelo endereço IP *multicast,* mas também pelo endereço IP da fonte correspondente.

A utilização do SSM apresenta várias vantagens em relação ao ASM [8]. Ffacilita, por exemplo, a construção da árvore de distribuição, pois o endereço da fonte é imediatamente conhecido pelo *router* de acesso no momento de adesão.

Para limitar a replicação de pacotes nos elementos de rede de nível 2, que por omissão replicam os pacotes multicast por todas as portas, é utilizado o IGMP *snooping* [9]. O IGMP *snooping* pode ser efectuado em modo transparente ou em modo *proxy*. No modo transparente, os equipamentos de nível 2 inspeccionam os pacotes IGMP (sem os alterar) com a finalidade de replicar os pacotes *multicast* recebidos apenas por portas onde existam membros a montante. Em modo *proxy* o elemento de nível 2 age, simultaneamente, como um *router* (na interacção com receptores) e cliente IGMP (na interacção com *routers multicast*).

2.1.1 UMTS

O elemento funcional que permite a comunicação *multicast* IP em redes UMTS é o GGSN. Este assue o papel de *router multicast* [10]. Processa as mensagens IGMP provenientes dos utilizadores e implementa os protocolos de encaminhamento *multicast* IP (ver Figura 3). Contudo, o transporte do tráfego *multicast* na rede UMTS é efectuado sobre ligações ponto-a-ponto. O GGSN replica os pacotes *multicast*, enviando uma cópia para cada um dos receptores. Perde-se portanto alguns dos benefícios inerentes ao uso do *multicast* IP.

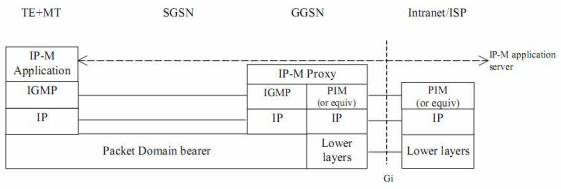

Figura 3 – Plano de controlo para *multicast* IP em UMTS

O suporte nativo para comunicações *multicast* (ponto-a-multiponto) em UMTS é conseguido através do *Multimedia Broadcast/Multicast Service* (MBMS) [11], que implementa de raiz um sistema de AAA para as sessões *multicast*.

Para tal o MBMS adiciona às redes 3GPP o BM-SC (ver Figura 4), um novo elemento funcional, responsável pela gestão *multicast* dentro da rede UMTS, incluindo o anúncio de sessões *multicast*; a

autorização e autenticação de utilizadores; o transporte de dados; e a respectiva sinalização. O MBMS também impõe alterações nos restantes elementos da rede UMTS tendo em vista o suporte das novas funcionalidades.

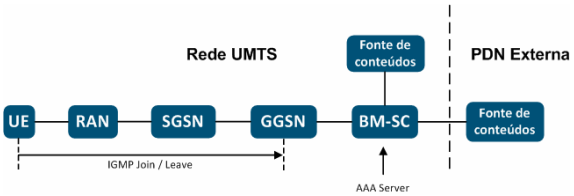

Figura 4 – Arquitectura MBMS

Tal como no *multicast* IP, recorrem-se às mensagens IGMP, para aderir e sair de grupos *multicast*, assim como, a endereços IPv4 classe D para representar os grupos. O MBMS é, portanto, inter-operável com o *multicast* IP. No entanto, presentemente a interface entre o BM-SC e as redes de pacotes IP externas não se encontra definida [11]. Assim, apenas são presentemente suportados conteúdos *multicast* criados especificamente para utilizadores da rede UMTS. Além disso, o MBMS, não considera a possibilidade de existência de utilizadores como fontes *multicast*. A distribuição de dados por *multicast* é efectuada apenas no sentido descendente, do GGSN para os utilizadores e no modelo de um-para-muitos.

2.1.2 xDSL

Na Figura 5 encontra-se representada a mais recente arquitectura xDSL disponibilizada pelo DSL *Forum* [12]. Identifica ainda os pontos susceptíveis de optimização *multicast* ao nível do transporte de pacotes. O BNG (BRAS) assume funções de *router multicast*, processando todas as mensagens IGMP provenientes da rede de acesso.

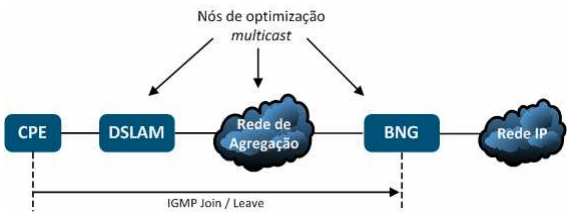

Figura 5 – Arquitectura xDSL

Em xDSL a ligação de dados é feita por PPPoE entre o CPE e o BNG. Tal implica que a replicação *multicast* seja efectuada no BNG. Um fluxo *multicast* proveniente da rede IP, ao chegar ao BNG é replicado e transmitido por ligações ponto-a-ponto (PPPoE) até ao CPEs membros do grupo ao qual o fluxo se destina. Desta forma poderá existir duplicação de tráfego em determinados segmentos de rede, isto é, tráfego de um grupo, enviado sobre a mesma ligação física, mas por ligações PPPoE diferentes. As ligações PPPoE impossibilitam, portanto, uma utilização eficaz do *multicast* IP na rede de acesso.

A optimização da rede de acesso xDSL para aplicações como o IPTV, onde a distribuição dos conteúdos é efectuada por *multicast*, implica que os elementos da rede, entre o CPE e o BNG, participem na replicação *multicast*. Para tal, é necessário que a ligação do CPE à rede seja por IPoE e que os equipamentos de nível 2 executem IGMP *snooping*.

Por enquanto, a ligação PPPoE é indispensável já que é esta que possibilita a autenticação/autorização dos utilizadores [13]. Assim, para que seja possível a optimização do transporte de tráfego *multicast* IP são necessárias 2 ligações entre o CPE e o BNG: uma ligação PPPoE para dados; e outra ligação IPoE para tráfego *multicast*.

As mensagens IGMP podem ser enviadas pelas duas ligações (PPPoE e IPoE) ou apenas pela ligação IPoE. Assumindo o primeiro caso, o BNG é capaz de controlar individualmente os membros de cada grupo correlacionado as mensagens IGMP recebidas com a ligação PPPoE em que as recebeu (a cada ligação corresponde um utilizador). Já no segundo caso, onde os pacotes IGMP são enviados apenas pela ligação IPoE, o BNG poderá ou não controlar os membros individuais dependendo de coo são tratads os pacotes IGMP no DSLAM. Se for efectuado o IGMP *snooping* transparente, o BNG consegue identificar membros individuais a partir do endereço MAC dos pacotes IGMP. Se, por outro lado, for efectuado IGMP *proxy*, o BNG perde a capacidade de distinguir os membros de cada grupo (apenas tem conhecimento dos grupos que possuem membros).

2.1.3 WiMAX

A arquitectura da rede WiMAX (802.16d) [14][15] encontra-se representada na Figura 6. A nível MAC são estabelecidas ligações ponto-a-ponto entre a ASN-GW e as SSs. Cada uma das ligações é identificada pelo CID (*Connection Identifier*) de 16bit. Apesar de os equipamentos possuírem um endereço MAC de 48 bit, este apenas é utilizado no estabelecimento inicial da ligação.

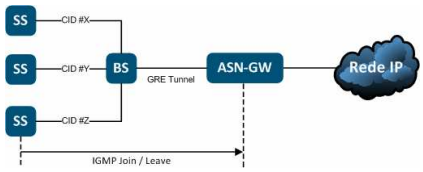

Figura 6 – Arquitectura WiMAX (802.16d)

As ligações ascendentes (SS → ASN-GW) são exclusivamente *unicast*. É, no entanto, possível utilizar mCIDs (*multicast* CIDs) no sentido descendente (ASN-GW → SS) para identificar uma ligação partilhada por várias SSs. A gestão destes mCIDs ainda não está definida pelo WiMAX *Forum*. Além disto, existem alguns problemas da utilização de mCIDs [16], nomeadamente, fraca eficiência na transmissão de dados para grupos *multicast* de pequena dimensão, inexistência de mCID para ligações ascendentes, maior consumo de energia das SSs, entre outros.

Assim sendo, e de acordo com o modelo mais recente proposto no IETF [16], o ASN-GW deve processar as mensagens IGMP provenientes dos utilizadores e efectuar a replicação final dos pacotes *multicast*.

2.2 Requisitos

Os objectivos deste trabalho aqui apresentado consistiu na análise da problemática associada ao controlo de sessões *multicast* em ambientes heterogéneos de forma a propor uma solução capaz de satisfazer os seguintes requisitos:

- Difusão de conteúdos multimédia em *multicast* IP sobre redes de acesso heterogéneas (xDSL, WiMAX, UMTS);
- Gestão do endereçamento *multicast* ao nível IP (L3) e ao nível MAC (L2);
- Identificação dos nós da rede onde se pode exercer controlo de acesso, autorização e gestão de recursos para comunicações *multicast*;
- Suporte para grupos *multicast* com fontes no core da rede;
- Suporte para grupos *multicast* com fontes na rede de acesso;
- Autenticação, autorização e registo de pedidos de acesso a grupos *multicast*;
- Autenticação, autorização e registo de pedidos de criação de grupos *multicast*;

O projecto visou ainda o desenvolvimento de um protótipo capaz de efectuar a gestão de sessões *multicast*, nomeadamente:

- Identificação de utilizadores que tentam aceder ou criar uma sessão *multicast*
- Identificação das sessões *multicast*
- Autorização/Registo das sessões *multicast*

2.3 Solução proposta

A solução proposta funciona a nível do IP e consiste na detecção por parte do nó de acesso de: 1) pedidos de adesão a grupos *multicast*; 2) inicio de transmissão de dados *multicast* com origem na rede de acesso (utilizadores como fontes). E, após a sua detecção, validar a sua autorização junto de um servidor de AAA [17].

Em todas as redes de acesso consideradas, o estabelecimento de uma ligação à rede implica a autorização e autenticação do utilizador (ver Figura 7). Uma vez efectuada a ligação, são registados alguns parâmetros (i.e. *Accounting*), como por exemplo, o endereço IP atribuído, o momento de início da ligação, entre outros.

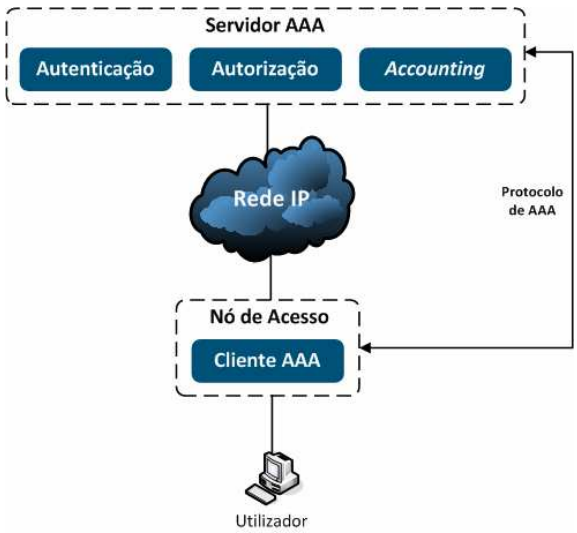

Figura 7 – Arquitectura de AAA

A solução proposta utiliza alguns desses parâmetros para identificar inequivocamente o utilizador (o endereço IP e a porta do DSLAM no caso do xDSL) e, tendo por base a informação contida nos pacotes *multicast* IP provenientes da rede de acesso, efectuar o respectivo pedido de autorização (da sessão *multicast*).

2.3.1 Arquitectura

A solução é composta por dois elementos: o controlador *multicast* e o servidor de AAA.

Controlador *multicast*: situado no nó de acesso à rede e cujas funcionalidades incluem um cliente de AAA e o processamento de mensagens IGMP. O controlador é responsável por detectar e intersectar pedidos de acesso a grupos e transmissões de dados *multicast* (utilizadores como fontes), antes que o nó de acesso os processe. Validando de seguida a sua autorização junto do servidor de AAA. O controlador *multicast*, de acordo com a resposta obtida pelo servidor de AAA, processa ou descarta o pedido de acesso recebido, ou, no caso de o utilizador ser uma fonte *multicast*, encaminha ou não do fluxo de tráfego respectivo.

Servidor de AAA: este elemento pode se situar num qualquer ponto da rede do operador, desde que acessível ao controlador *multicast*. O servidor de AAA contém informação de autenticação, autorização e de registo relativa à ligação do utilizador à rede, bem assim como um perfil *multicast* por utilizador. No perfil *multicast* de cada utilizador estão definidos os direitos de acesso e de criação de sessões *multicast*. A informação de AAA deve ser tal que permita ao controlador *multicast*, munido apenas dos dados contidos nos pacotes *multicast* e da informação de ligação à rede de acesso do utilizador, identificá-lo inequivocamente junto do servidor de AAA.

Tipo de pacote recebido	Identificadores da sessão *multicast* [1]
IGMPv1	SA, GDA
IGMPv2	SA, GDA
IGMPv3	SA, GDA, GSA
UDP *multicast*	SA, DA

Tabela 1 – Parâmetros identificadores das sessões *multicast*

O controlo de adesões é efectuado através da detecção de mensagens IGMP *Join* e da consequente autorização da sessão junto do servidor de AAA (ver Figura 8). O controlador *multicast* irá então aceitar o pedido de adesão ou descartá-lo por completo, em conformidade com a resposta do servidor de AAA. Caso o pedido de adesão seja aceite, o pacote IGMP é processado normalmente pelo nó de acesso e o fluxo *multicast* associado é encaminhado na direcção do utilizador. Caso contrário, o nó de acesso nunca chega a receber o pedido.

O controlo de fontes *multicast* é efectuado de forma análoga, só que neste caso, é a detecção de pacotes UDP com endereço *multicast* IPv4 de destino, e não pacotes IGMP, que despoleta o processo de autorização e consequente filtragem do tráfego *multicast* (ver Figura 8).

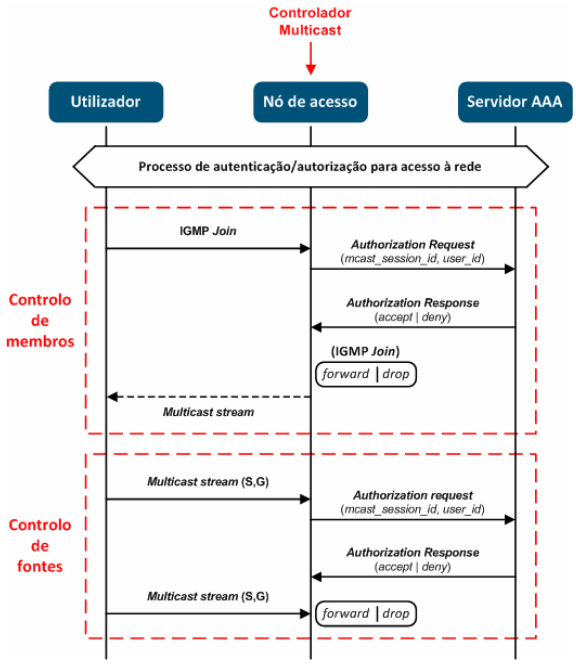

Figura 8 – Controlo do acesso a grupos e de fontes *multicast*

É importante salientar que apesar de esta solução implicar que o controlo de acesso seja efectuado no local onde são processadas as mensagens IGMP, tal controlo terá também de ser efectuado no último ponto de replicação *multicast*. Este último ponto poderá, ou não, coincidir com o nó de acesso. Caso contrário, um fluxo *multicast* autorizado para um utilizador pelo controlador *multicast*, poderá ser encaminhado para outro utilizador sem permissão para o receber. Esta situação ocorre quando, por exemplo, um *switch* da rede de acesso com IGMP *snooping*, recebe um pedido de adesão IGMP para um grupo não autorizado do qual já se encontra a receber o fluxo previamente estabelecido resultante de uma adesão autorizada. Neste caso, o controlador *multicast* irá rejeitar o pedido de acesso mas o *switch* poderá na mesma efectuar a replicação do fluxo para esse utilizador. Para prevenir esta situação, poderão

[1] SA – *Source Address*, GSA – *Group Source Address*, GDA – *Group Destination Address*.

ser adoptadas duas soluções: 1) implementar o controlador *multicast* no último ponto de replicação; 2) permitir ao controlador *multicast* gerir as tabelas de encaminhamento *multicast* do último ponto de replicação.

2.3.2 UMTS

Em UMTS o MBMS já oferece controlo de acesso a grupos *multicast* com a particularidade de apenas serem permitidas, por enquanto, fontes de conteúdos exclusivas para a rede UMTS. O controlo de fontes com origem nos utilizadores pode ser conseguido implementando a detecção de pacotes *multicast* no GGSN, acrescentando uma nova mensagem de autorização para fontes e modificando o BM-SC para permitir a autenticação e registo automático das sessões MBMS iniciadas pelos utilizadores.

2.3.3 xDSL

Em xDSL, o BNG é o responsável por processar as mensagens IGMP, daí ser este elemento onde deve ser implementado o controlador *multicast*. Uma vez que o BNG já possui funcionalidades de cliente de AAA apenas é necessário adicionar a capacidade de solicitar autorização para sessões *multicast*.

Normalmente o DSLAM bloqueia a replicações de pacotes *multicast* entre portas pertencentes a utilizadores, logo, todo o tráfego *multicast* proveniente da rede de acesso irá sempre até ao BNG. No entanto, como o último ponto de replicação de pacotes pode ser o DSLAM, este também poderá necessitar de implementar controlo de acesso para grupos *multicast*. Isto pode ser conseguido implementando um controlador *multicast* no próprio DSLAM, ou utilizando um controlador no BNG para configurar remotamente as tabelas de encaminhamento *multicast* do DSLAM [18].

2.3.4 WiMAX

Em WiMAX o local adequado à implementação do controlador *multicast* é o ASN-GW. Isto porque que este elemento não só faz o processamento das mensagens IGMP, como também é o último ponto de replicação *multicast*. Além do mais, como o ASN-GW também funciona como cliente de AAA (tal como o BNG em xDSL) seria apenas necessário acrescentar a capacidade de solicitar autorização para sessões *multicast*.

3 Resultados

O protótipo desenvolvido abrange apenas às funcionalidades da solução proposta consideradas essenciais, sendo estas:

- Autenticação de utilizadores com recurso a um servidor de AAA no momento de ligação à rede.
- Implementação do controlador *multicast*
  - Detectar de pedidos de adesão;
  - Detectar de fontes na rede de acesso;
  - Efectuar pedidos de autorização com base na informação disponível;
  - Filtragem do tráfego *multicast* não autorizado.

3.1.1 Protótipo

O sistema de teste está representado na Figura 9. Por uma questão de simplicidade, O servidor de AAA foi instalado na mesma máquina que o controlador *multicast* (*router* de acesso), no entanto, tal não é obrigatório.

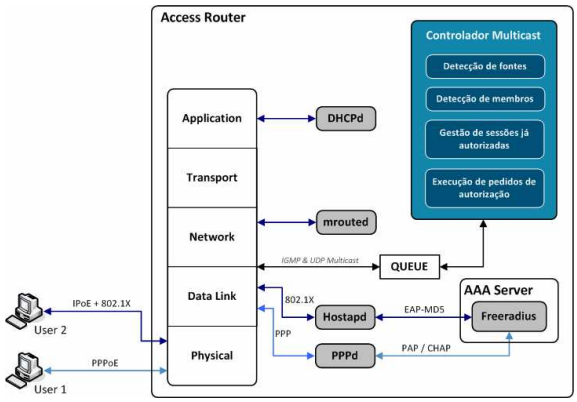

Figura 9 – Protótipo implementado

O utilizador efectua a ligação à rede, autenticando-se com o seu par *username*/*password*. No *router* de acesso, compete aos *daemons*, hostapd e pppd, efectuarem a autenticação dos utilizadores junto do servidor RADIUS (FreeRADIUS). Todo tráfego *multicast* (IGMP e UDP) é capturado pelo *iptables*/*netfilter* para uma fila de espera (QUEUE).

A captura é efectuada antes mesmo de os pacotes serem processados pelo sistema operativo. Uma vez na QUEUE, o controlador *multicast* processa os pacotes um a um com o intuito de, uma vez feita a distinção entre receptor e fonte, verificar se a sessão deve ou não ser autorizada.

3.1.2 Detecção de fontes

Se o pacote capturado for um pacote UDP, então trata-se de uma transmissão *multicast* proveniente da rede de acesso. São imediatamente obtidos, do cabeçalho IP, os parâmetros que identificam a sessão *multicast e* inicia-se o processo de verificação da autorização de transmissão do utilizador em questão. O utilizador neste caso é identificado pelo seu endereço IP.

3.1.3 Detecção de membros

Se o pacote capturado for um pacote IGMP, então estamos na presença de um receptor na rede de acesso. Os parâmetros caracterizadores da sessão *multicast* são obtidos do pacote IGMP, assim que se determine o seu tipo (*join*, *leave*, ou *membership report*) e versão (v1, v2 ou v3).

3.1.4 Execução de pedidos de autorização

O controlador *multicast* utiliza o endereço IP de origem do pacote como identificador do utilizador. O endereçamento IP só se torna suficiente como identificador se existir um registo com associações entre *usernames* e endereços IP. É necessário que exista ainda um registo dos perfis *multicast* dos utilizadores. Idealmente, tal informação residiria num servidor de AAA ou numa base de dados centralizada, no entanto, a solução AAA utilizada no protótipo não dispunha de nenhuma forma de armazenar tal informação. Em especial, enquanto que em ligações PPPoE, o servidor RADIUS armazena o endereço IP atribuído ao utilizador, tal já não acontece em IPoE com 802.1X. Neste último, a autenticação e obtenção de IP são dois processos distintos. O *hostapd* apenas autentica, compete ao utilizador obter a sua configuração IP por DHCP. O servidor RADIUS desconhece portanto o endereço do utilizador com ligação por IPoE.

Tendo em vista a resolução deste problema, monitorizaram-se os registos do FreeRADIUS e do DHCP (ver Figura 10) com o intuito de relacionar o endereço IP com um *username* autenticado.

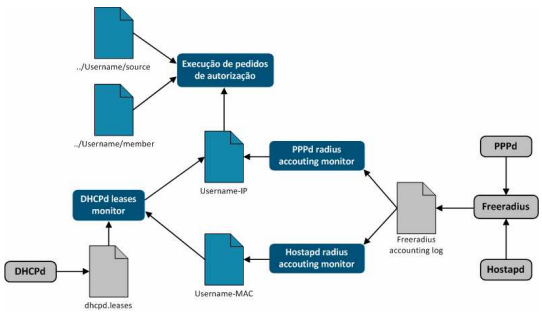

Figura 10 – Associação *Username-IP*

O registo do FreeRADIUS fornece o endereço IP e o *username* associado às ligações PPPoE, bem assim como, o endereço MAC e o *username* associado às ligações IPoE com 802.1X. Sabendo o MAC e os endereços IP correspondentes, e recorrendo aos registos das atribuições do DHCP, é então possível estabelecer a relação entre o *username* e o endereço IP atribuído nas ligações IPoE. Uma vez conseguida a associação, o controlador *multicast* consulta os ficheiros contendo os perfis *multicast* dos utilizadores para determinar se deve ou não autorizar as sessões *multicast*.

3.1.5 Gestão de sessões já autorizadas

Tendo em vista a optimização do sistema o controlador *multicast* recorre a duas listas temporárias a fim de evitar a constante revalidação de autorizações (uma para fontes e outra para membros). Estas listas contêm as sessões recentemente autorizadas e são consultadas, sempre que é processado um pacote da QUEUE, para determinar rapidamente se trata de uma sessão já autorizada. Como os protocolos IGMPv1 e IGMPv2 não possuem mensagens de adesão explícitas, ou seja, o *memberhip report* inicial representa um IGMP *Join,* é necessário manter informação de estado no que concerne a membros activos. Tal permite diferenciar *membership reports* normais de *memberhip report* iniciais (i.e. adesões) .

Todas as listas são refrescadas regularmente, sendo efectuado um novo pedido de autorização para cada sessão existente. Caso surjam sessões não autorizadas, estas são retiradas da lista.

No caso das fontes, a necessidade de optimização é ainda mais crítica já que a afluência de pacotes é muito superior. A fim de evitar que todos os pacotes UDP *multicast* sejam processados pelo controlador *multicast* sempre que uma sessão é autorizada, é inserida uma nova regra no *iptables* para que o tráfego associado à sessão não seja enviado para a QUEUE. Todas as regras presentes nas *iptables*

associadas a fontes que venham a ser desautorizadas são removidas. Outra optimização possível seria a de introduzir regras no *iptables* para bloquear pacotes associados a sessões não autorizadas.

3.1.6 Testes e Validação

A validação funcional do protótipo consistiu na execução de vários testes de transmissão e recepção de vídeos transmitidos em *multicast* IP entre os dois utilizadores. Um assumindo o papel de fonte, outro assumindo o papel de receptor (ver Figura 9). Os procedimentos testados com sucesso incluem: 1) a adesão a um grupo autorizado e não autorizado; 2) a transmissão autorizada e não autorizada de conteúdos; 3) a desautorização de um membro ou de uma fonte previamente autorizados. Todos os testes foram bem sucedidos.

4 Impacto para a PT

A solução apresentada pode ser utilizada para gerir o acesso a qualquer serviço que faça uso do *multicast* IP. Emissão e recepção de vídeo por parte dos utilizadores, distribuição de informação financeira em tempo real, rádio por IP, jogos online, são alguns exemplos. Basicamente, qualquer aplicação que envolva distribuição de dados em tempo real para um grupo de utilizadores.

Por outro lado, uma vez que a gestão da sessão *multicast* é feita no nó de acesso, os utilizadores são impedidos de receber fluxos não autorizados prevenindo-se desta maneira potenciais riscos de segurança (como ataques de DoS).

5 Conclusões

Neste artigo foi apresentada uma solução capaz de gerir sessões *multicast* sobre redes de acesso heterogéneas. A solução permite controlar e monitorizar pedidos de adesão a grupos e a criação de novos grupos na rede de acesso, de acordo com os perfis *multicast* dos utilizadores.

A solução apresentada funciona a nível IP, pelo que é adaptável as várias tecnologias de acesso suportem IP. Contudo, o funcionamento do *multicast* a nível 2 dessas redes deve sempre ser considerado. Nos casos onde o último ponto de replicação *multicast* não coincida com o nó de acesso onde se implementado o controlador *multicast*, torna-se necessário controlar a replicação a nível 2. Mesmo aqui, o controlo *multicast* pode ser adaptado para operar a nível MAC no último ponto de replicação.

O sistema apresentado é transparente para o utilizador, aplicações, protocolos e equipamentos de rede. Excepção feita ao equipamento que implemente o controlador *multicast*.

6 Bibliografia

[1] Deering, S., "RFC 1112 Host Extensions for IP Multicasting," Aug. 1989; http://tools.ietf.org/html/rfc1112.

[2] C. Diot et al., "Deployment issues for the IP multicast service and architecture," Network, IEEE, vol. 14, 2000, pp. 78-88.

[3] L. Heden et al., "Broadcast and multicast - a vision on their role in future broadband access networks (BMC Vision)," Jan. 2005.

[4] P. Judge and M. Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Aurvey," Network, IEEE, vol. 17, 2003, pp. 30-36.

[5] IANA (Internet Assigned Numbers Authority), "Internet Multicast Addresses," Jan. 2008; http://www.iana.org/assignments/multicast-addresses.

[6] B. Cain et al., "RFC 3376 Internet Group Management Protocol, Version 3," Oct. 2002; http://tools.ietf.org/html/rfc3376.

[7] H. Holbrook and B. Cain, "RFC 4607 Source-Specific Multicast for IP," Aug. 2006; http://tools.ietf.org/html/rfc4607.

[8] S. Bhattacharyya, "RFC 3569 An Overview of Source-Specific Multicast (SSM)," Jul. 2003; http://tools.ietf.org/html/rfc3569.

[9] M. Christensen, K. Kimball, and F. Solensky, "RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast

Listener Discovery (MLD) Snooping Switches," May. 2006; http://tools.ietf.org/html/rfc4541.

[10] 3rd Generation Partnership Project (3GPP), "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (Release 7)," Jun. 2007.

[11] 3rd Generation Partnership Project (3GPP), "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 7)," Jun. 2007.

[12] DSL Forum, "Migration to Ethernet-Based DSL Aggregation," Apr. 2006.

[13] M. Bernstein, "Understanding PPPoE and DHCP," May. 2006.

[14] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.

[15] "WiMAX Forum Network Architecture Stage 2 - 3. Release 1, Version 1.1," Jul. 2007.

[16] H. Jeon, M. Riegel, and S. Jeong, "Transmission of IP over Ethernet over IEEE 802.16 Networks draft-ietf-16ng-ip-over-ethernet-over-802.16-04," Dec. 2007; http://tools.ietf.org/html/draft-ietf-16ng-ip-over-ethernet-over-802.16-04.

[17] C. Metz, "AAA protocols: authentication, authorization, and accounting for the Internet," IEEE Internet Computing, vol. 3, 1999, pp. 75-79.

[18] S. Ooghe et al., "Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks (draft-ietf-ancp-framework-04)," Nov. 2007; http://tools.ietf.org/html/draft-ietf-ancp-framework-04.