



**Instituto Politécnico de Leiria**

**ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO**

**Departamento de Engenharia Informática**

**Projecto II**

Eng.<sup>a</sup> Informática e Comunicações

**IPv6@ESTG-Leiria**

*Vídeo-Difusão sobre Multicast IPv6*

Leiria

Fevereiro de 2006





**Instituto Politécnico de Leiria**  
**ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO**  
**Departamento de Engenharia Informática**

**Projecto II**

Eng.<sup>a</sup> Informática e Comunicações, 1º Semestre do 5º Ano

**IPv6@ESTG-Leiria**

*Vídeo-Difusão sobre Multicast IPv6*

**Realizado pelo Aluno**

Rui Manuel Ferreira Bernardo

**Orientado pelos Docentes do Departamento de Engenharia Informática**

Nuno Veiga e Paulo Cordeiro

Leiria

Fevereiro de 2006



## Resumo

No âmbito do projecto do 5º Ano do Curso de Engenharia Informática e Comunicações, IPv6@ESTG-Leiria: *Vídeo-Difusão sobre Multicast IPv6*, surgiu a possibilidade de interligar a ESTG-Leiria à rede de testes M6Bone – Multicast IPv6 Backbone. Desta forma, foram estudadas todas as possibilidades existentes, e efectuado um conjunto de contactos com vista à persecução dos objectivos. Foram também efectuados vários testes usando a plataforma disponibilizada pela FCCN (Fundação para a Computação Científica Nacional).

Ao longo deste projecto, foram estudadas as tecnologias envolvidas, partindo do estudo do endereçamento, passando pelos protocolos, conceitos e aplicações disponíveis. Após esta fase, foram implementados diversos cenários em laboratório, usando os diversos recursos disponíveis, com vista a tomar contacto directo com a tecnologia. Por conseguinte, foram implementados cenários que pretendiam simular uma rede multicast IPv6, quer usando uma topologia nativa, quer recorrendo ao uso de túneis.

## Agradecimentos

Dedico este trabalho a todas as pessoas que, de uma ou de outra forma contribuíram para o sucesso deste projecto. Em especial, para:

Os meus pais,

Maria de Lurdes Ferreira Gerardo e Pedro Silvério Bernardo,

pelo apoio sempre presente a todos os níveis, quer seja pessoal, financeiro, ...

À minha única irmã,

Ana Rita pelo apoio incondicional, motivação e, claro, pela paciência que demonstro ter ao longo dos últimos 23 anos.

Aos docentes coordenadores,

Nuno Veiga e Paulo Cordeiro, pela ajuda e pelo apoio prestado ao longo da realização do projecto.

Aos colegas e amigos da turma,

Tiago Mira Amado, Vítor Santos, Hugo Oliveira, Sérgio Morgadinho e Hugo Nogueira pela preciosa ajuda disponibilizada ao longo do decorrer do projecto.

À FCCN (Fundação para a Computação Científica Nacional).

Não posso deixar passar a oportunidade de agradecer aos técnicos na FCCN, em especial à Eng. Mónica Domingues, pelo esclarecimento de dúvidas, apoio, e pela troca de ideias aquando a realização dos testes.

E claro para terminar,

À Mónica Costa pelo apoio, motivação, ... por tudo.

A todos os outros, Muito Obrigado!

## Índice

|          |                                                                     |                  |
|----------|---------------------------------------------------------------------|------------------|
| <b>1</b> | <b><i>Introdução.....</i></b>                                       | <b><i>1</i></b>  |
| 1.1      | Objectivos .....                                                    | 1                |
| 1.2      | Projecto IPv6 @ ESTG.....                                           | 2                |
| <b>2</b> | <b><i>Multicast em redes IP.....</i></b>                            | <b><i>3</i></b>  |
| 2.2      | Redes IPv6 multicast Existentes .....                               | 4                |
| 2.3      | Características específicas das instituições.....                   | 7                |
| <b>3</b> | <b><i>Modelos de distribuição de tráfego multicast.....</i></b>     | <b><i>17</i></b> |
| 3.1      | Terminologia .....                                                  | 17               |
| 3.2      | ASM, SSM - vantagens e desvantagens.....                            | 18               |
| 3.2.1    | Problemas do ASM.....                                               | 18               |
| 3.2.2    | Vantagens do SSM .....                                              | 19               |
| 3.2.3    | Desvantagem do SSM .....                                            | 19               |
| <b>4</b> | <b><i>Endereçamento Multicast IPv6.....</i></b>                     | <b><i>21</i></b> |
| 4.1      | Básico .....                                                        | 21               |
| 4.2      | Avançado, usado em soluções Inter-domínio .....                     | 23               |
| 4.2.1    | Baseados no prefixo unicast .....                                   | 23               |
| 4.2.2    | Embedded RP .....                                                   | 25               |
| 4.3      | Endereçamento na camada 2 .....                                     | 26               |
| <b>5</b> | <b><i>Protocolos Multicast IPv6 .....</i></b>                       | <b><i>28</i></b> |
| 5.1      | Introdução aos protocolos Multicast.....                            | 28               |
| 5.2      | Protocolo de Gestão de Grupos Multicast – MLDv1 .....               | 29               |
| 5.2.1    | Descrição sucinta.....                                              | 29               |
| 5.2.2    | Formato das mensagens.....                                          | 30               |
| 5.2.3    | Funcionamento do protocolo .....                                    | 32               |
| 5.3      | Protocolo de Gestão de Grupos Multicast – MLDv2 .....               | 37               |
| 5.3.1    | Descrição sucinta.....                                              | 37               |
| 5.3.2    | Formato das mensagens.....                                          | 38               |
| 5.3.3    | Funcionamento do protocolo MLDv2 .....                              | 44               |
| 5.4      | Protocolos de encaminhamento Multicast .....                        | 47               |
| 5.4.1    | PIM.....                                                            | 47               |
| 5.4.2    | PIM – SM .....                                                      | 48               |
| 5.4.3    | PIM – SSM .....                                                     | 54               |
| 5.5      | Encaminhamento Multicast na Internet ( <i>Inter-Domínio</i> ) ..... | 56               |
| 5.5.1    | Modelo ASM e SSM .....                                              | 57               |
| 5.5.2    | Multiprotocol BGP .....                                             | 57               |
| <b>6</b> | <b><i>Implementação e Testes.....</i></b>                           | <b><i>59</i></b> |
| 6.1      | Sistemas Operativos e Aplicações utilizadas nos testes .....        | 59               |
| 6.2      | Ferramentas para verificar conectividade multicast.....             | 61               |

|                       |                                                             |            |
|-----------------------|-------------------------------------------------------------|------------|
| 6.2.1                 | SSMpingd – SSMping e ASMPing .....                          | 61         |
| 6.2.2                 | Mping.....                                                  | 66         |
| <b>6.3</b>            | <b>Teste com multicast IPv4.....</b>                        | <b>68</b>  |
| 6.3.1                 | Cenário.....                                                | 68         |
| <b>6.4</b>            | <b>Testes Multicast IPv6: PIM – SM.....</b>                 | <b>74</b>  |
| 6.4.1                 | Cenário I – Multicast Nativo.....                           | 75         |
| 6.4.2                 | Cenário II – Simular uma Ligação à FCCN por Túnel IPv6..... | 82         |
| 6.4.3                 | Cenário III – IPv6 multicast em redes IPv4.....             | 93         |
| 6.4.4                 | Cenário IV – Simular uma Ligação nativa à FCCN.....         | 96         |
| <b>6.5</b>            | <b>Testes Multicast IPv6: Embedded RP .....</b>             | <b>96</b>  |
| 6.5.1                 | Cenário I – Multicast IPv6 Nativo .....                     | 97         |
| 6.5.2                 | Cenário II – Multicast IPv6 sobre um túnel IPv6.....        | 105        |
| <b>6.6</b>            | <b>Testes Multicast IPv6: PIM-SSM .....</b>                 | <b>111</b> |
| 6.6.1                 | Cenário – Multicast IPv6 sobre um túnel IPv6 .....          | 111        |
| <b>7</b>              | <b>Túnel com a FCCN .....</b>                               | <b>118</b> |
| 7.1                   | Cenário dos testes.....                                     | 118        |
| 7.2                   | Fase I - Encaminhamento Unicast .....                       | 120        |
| 7.2.1                 | Encaminhamento do túnel.....                                | 121        |
| 7.3                   | Fase II – Encaminhamento Multicast .....                    | 122        |
| 7.4                   | Fase III – Teste de conectividade - SSM .....               | 124        |
| 7.5                   | Fase IV – Configurações ASM – Ligação à M6Bone .....        | 126        |
| 7.6                   | Fase V – Teste de conectividade - ASM .....                 | 126        |
| 7.7                   | Como aceder aos conteúdos da rede M6Bone .....              | 127        |
| <b>8</b>              | <b>Conclusão .....</b>                                      | <b>130</b> |
| <b>9</b>              | <b>Referências .....</b>                                    | <b>132</b> |
| <b>Apêndice .....</b> |                                                             | <b>135</b> |
| <b>9.1</b>            | <b>O essencial do IOS da Cisco .....</b>                    | <b>135</b> |
| 9.1.2                 | Escolha das funcionalidades – Cisco IOS Packaging .....     | 137        |
| <b>9.2</b>            | <b>Aplicações H.264/x264 .....</b>                          | <b>138</b> |
| 9.2.1                 | Tecnologia H.264.....                                       | 139        |
| 9.2.2                 | x264 – O codificador H.264 Open-Source.....                 | 139        |
| 9.2.3                 | Projectos que usam o x264 .....                             | 140        |
| <b>9.3</b>            | <b>Configurações efectuadas nos Testes.....</b>             | <b>146</b> |
| 9.3.1                 | IPv4 – PIM-SM (nativo) .....                                | 146        |
| 9.3.2                 | IPv6 – PIM-SM (nativo) .....                                | 147        |
| 9.3.3                 | IPv6 – Embedded RP (nativo) .....                           | 149        |
| 9.3.4                 | IPv6 – PIM-SM (túnel).....                                  | 151        |
| 9.3.5                 | IPv6 – Embedded RP (túnel) .....                            | 153        |
| 9.3.6                 | IPv6 – PIM-SSM (túnel).....                                 | 155        |
| <b>10</b>             | <b>Anexos .....</b>                                         | <b>157</b> |
| <b>10.1</b>           | <b>IEFT – Grupos de Trabalho.....</b>                       | <b>157</b> |
| 10.1.1                | IPv6.....                                                   | 157        |
| 10.1.2                | Multicast & Anycast .....                                   | 158        |
| 10.1.3                | Protocol Independent Multicast .....                        | 158        |
| 10.1.4                | Source-Specific Multicast .....                             | 159        |
| 10.1.5                | Audio/Video Transport .....                                 | 159        |
| 10.1.6                | Reliable Multicast Transport.....                           | 160        |



|             |                                                              |            |
|-------------|--------------------------------------------------------------|------------|
| <b>10.2</b> | <b>RFCs.....</b>                                             | <b>160</b> |
| 10.2.1      | IPv6.....                                                    | 160        |
| 10.2.2      | Vídeo .....                                                  | 175        |
| <b>10.3</b> | <b>FCCN - Projecto Estúdios.....</b>                         | <b>184</b> |
| <b>10.4</b> | <b>FCCN – Formulário de inscrição nos Testbeds IPv6.....</b> | <b>186</b> |
| <b>10.5</b> | <b>Conceitos relacionados com o Vídeo .....</b>              | <b>188</b> |

## Lista de Siglas e Acrónimos

API – Application Programming Interface

ARP – Address Resolution Protocol

ASM – Any Source Multicast

BGP – Border Gateway Protocol

BSR – Bootstrap Router

DoS – Denial of Service

CODEC – Coder/Decoder

DR – Designated Router

DTI – Department of Telematic Engineering

DVMRP – Distance Vector Multicast Routing Protocol

DVTS – Digital Video Transport System

ICMP – Internet Control Message Protocol

IETF – Internet Engineering TaskForce

IGMP – Internet Group Management Protocol

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

LAN – Local Area Network

MIB – Management Information Base

MBGP – Multicast Extensions to Border Gateway Protocol

M-ISIS – Multi Topology in IS-IS

MLD – Multicast Listener Discovery

MRIB – Multicast Routing Information Base

MSDP – Multicast Source Discovery Protocol

MOSPF – Multiprotocol Extensions for Open Shortest Path First

NDP – Neighbour Discovery Protocol

NTE – Network Text Editor

PIM – Protocol Independent Multicast

PIM-DM – Protocol Independent Multicast - Dense Mode

PIM-SM – Protocol Independent Multicast - Sparse Mode

PSNC – Poznan Supercomputing and Networking Center

OSPF – Open Shortest Path First

RCTS – Rede de Ciência, Tecnologia e Sociedade

RP – Rendezvous Point

RPF – Reverse Path Forwarding

SDP – Source Discovery Protocol

SDR – Session Directory

SM – Sparse Mode

SSM – Source Specific Multicast

SSMSDP – Source Specific Multicast Source Discovery Protocol

VLC – VideoLan Client

VLS – VideoLan Server

## Lista de Figuras

|                                                                                                              |           |
|--------------------------------------------------------------------------------------------------------------|-----------|
| <i>Figura 2.1 - Transmissão em unicast.....</i>                                                              | <i>3</i>  |
| <i>Figura 2.2 - Transmissão em multicast.....</i>                                                            | <i>4</i>  |
| <i>Figura 2.3 - Topologia lógica da rede Abilene.....</i>                                                    | <i>5</i>  |
| <i>Figura 2.4 - Topologia lógica da rede M6Bone.....</i>                                                     | <i>5</i>  |
| <i>Figura 2.5 - Esquema que representa a topologia das redes IPv4 e IPv6 da ESTG.....</i>                    | <i>7</i>  |
| <i>Figura 2.6 - Backbone da rede, OC-192c (9.952 Gbps) .....</i>                                             | <i>8</i>  |
| <i>Figura 2.7 - Topologia lógica da rede Abilene .....</i>                                                   | <i>9</i>  |
| <i>Figura 2.8 - Estado da rede Abilene ao nível do IPv6.....</i>                                             | <i>9</i>  |
| <i>Figura 2.9 - Início do projecto M6Bone - 2001 .....</i>                                                   | <i>10</i> |
| <i>Figura 2.10 - Backbone do 6NET - multicast enabled.....</i>                                               | <i>10</i> |
| <i>Figura 2.11 - Equipamentos não suportam rotas multicast.....</i>                                          | <i>11</i> |
| <i>Figura 2.12 - Equipamentos com suporte para rotas multicast.....</i>                                      | <i>12</i> |
| <i>Figura 2.13 - Estado da rede M6Bone em Novembro de 2004 .....</i>                                         | <i>13</i> |
| <i>Figura 2.14 - Estado actual da rede M6Bone (2006) .....</i>                                               | <i>13</i> |
| <i>Figura 2.15 - Escola Superior de Tecnologia e Gestão de Leiria – Instituto Politécnico de Leiria.....</i> | <i>14</i> |
| <i>Figura 2.16 - Topologia actual da rede IPv6 Multicast da ESTG – Leiria (ligação por túnel) .....</i>      | <i>15</i> |
| <i>Figura 2.17 - Topologia futura da rede IPv6 Multicast da ESTG – Leiria (ligação nativa) .....</i>         | <i>15</i> |
| <i>Figura 3.1 - Exemplo de utilização do modelo ASM.....</i>                                                 | <i>17</i> |
| <i>Figura 3.2 - Exemplo de utilização do modelo SSM .....</i>                                                | <i>18</i> |
| <i>Figura 3.3 - Exemplo retirado da RFC 3180 - endereçamento global unicast em IPv4.....</i>                 | <i>18</i> |
| <i>Figura 3.4 - Servidores ligados à rede M6Bone, ASM e SSM .....</i>                                        | <i>20</i> |
| <i>Figura 4.1 - Formato dos endereços multicast IPv6 .....</i>                                               | <i>21</i> |
| <i>Figura 4.2 - Descrição das flags definidas na RFC 3513 .....</i>                                          | <i>21</i> |
| <i>Figura 4.3 - Endereços Unicast-Based Multicast Address.....</i>                                           | <i>23</i> |
| <i>Figura 4.4 - Extracção do endereço RP de um endereço multicast.....</i>                                   | <i>26</i> |
| <i>Figura 4.5 - Esquema com o mapeamento de um endereço da camada três para a camada dois.....</i>           | <i>27</i> |
| <i>Figura 4.6 - Mapeamento de um endereço da camada três para a camada dois .....</i>                        | <i>27</i> |
| <i>Figura 5.1 - Protocolos necessários em multicast IPv6.....</i>                                            | <i>29</i> |

|                                                                                                                  |           |
|------------------------------------------------------------------------------------------------------------------|-----------|
| <i>Figura 5.2 - Formato das mensagens MLD .....</i>                                                              | <i>30</i> |
| <i>Figura 5.3 - Formato dos pacotes MLDv1 .....</i>                                                              | <i>31</i> |
| <i>Figura 5.4 - Processo de Join no MLD .....</i>                                                                | <i>33</i> |
| <i>Figura 5.5 - Eleição do Router Querier.....</i>                                                               | <i>33</i> |
| <i>Figura 5.6 - Eleição do router responsavel (Querier Router) .....</i>                                         | <i>34</i> |
| <i>Figura 5.7 - Querier Router responsavel.....</i>                                                              | <i>34</i> |
| <i>Figura 5.8 - Mensagem MLQ – “General Query” .....</i>                                                         | <i>34</i> |
| <i>Figura 5.9 - Mensagem “Multicast Listener Done” .....</i>                                                     | <i>35</i> |
| <i>Figura 5.10 - Funcionamento do processo MLD Leave – fase inicial.....</i>                                     | <i>36</i> |
| <i>Figura 5.11 - Mensagem MLDv2 – grupos Include e Exclude .....</i>                                             | <i>37</i> |
| <i>Figura 5.12 - Mensagem MLDv2 – Multicast Listener Query’ .....</i>                                            | <i>39</i> |
| <i>Figura 5.13 - Envio de pacotes MLDv2 ‘Join’ para o endereço IP que representa todos os routers MLDv2.....</i> | <i>44</i> |
| <i>Figura 5.14 - Envio de um pacote MLDv2 ‘Join’ após pedido da aplicação.....</i>                               | <i>44</i> |
| <i>Figura 5.15 - MLDv2 “Query Process”.....</i>                                                                  | <i>45</i> |
| <i>Figura 5.16 - Core Based Tree.....</i>                                                                        | <i>48</i> |
| <i>Figura 5.17 - Formulas existentes para distribuição de tráfego .....</i>                                      | <i>49</i> |
| <i>Figura 5.18 - Cenário implementado para verificar o funcionamento do PIM-SM .....</i>                         | <i>50</i> |
| <i>Figura 5.19 - Associação do cliente ao grupo multicast [FF16::6] .....</i>                                    | <i>51</i> |
| <i>Figura 5.20 - Mensagem PIM-Register.....</i>                                                                  | <i>51</i> |
| <i>Figura 5.21 - Mensagem PIM-Join.....</i>                                                                      | <i>52</i> |
| <i>Figura 5.22 - Mensagem Register-Stop.....</i>                                                                 | <i>53</i> |
| <i>Figura 5.23 - Inscrição do cliente no grupo G1 do servidor Multicast IPv6 (S) .....</i>                       | <i>54</i> |
| <i>Figura 5.24 - Servidor a difundir para o grupo 1 do servidor Multicast IPv6 (S).....</i>                      | <i>55</i> |
| <i>Figura 5.25 - Cenário real PIM – SSM configurado na ESTG – Leira .....</i>                                    | <i>56</i> |
| <i>Figura 5.26 - Comando colocado no router R4 que permite ver os pares (S,G).....</i>                           | <i>56</i> |
| <i>Figura 5.27 - Topologia actual, a nível global da rede M6Bone.....</i>                                        | <i>58</i> |
| <i>Figura 6.1 - Funcionamento do SSMping .....</i>                                                               | <i>62</i> |
| <i>Figura 6.2 - Criador do SSMping – Stig Venaas .....</i>                                                       | <i>64</i> |
| <i>Figura 6.3 - Topologia utilizada nos testes do SSMping .....</i>                                              | <i>64</i> |
| <i>Figura 6.4 - Exemplo do funcionamento do SSMping .....</i>                                                    | <i>65</i> |
| <i>Figura 6.5 - VLC a transmitir para o IP 239.1.1.239 .....</i>                                                 | <i>66</i> |
| <i>Figura 6.6 - Exemplo do funcionamento do Mping.....</i>                                                       | <i>66</i> |
| <i>Figura 6.7 - Cenário utilizado nos testes multicast IPv4 .....</i>                                            | <i>68</i> |
| <i>Figura 6.8 - Passos de configuração do servidor - VLC.....</i>                                                | <i>69</i> |

|                                                                                                                     |           |
|---------------------------------------------------------------------------------------------------------------------|-----------|
| <i>Figura 6.9 - Endereço IPv4 usado para difundir vídeo - VLC .....</i>                                             | <i>70</i> |
| <i>Figura 6.10 - Configurar o VLC para receber vídeo.....</i>                                                       | <i>70</i> |
| <i>Figura 6.11 - Endereço IPv4 usado para difundir vídeo - VLC.....</i>                                             | <i>71</i> |
| <i>Figura 6.12 - Grupos multicast associados à máquina cliente .....</i>                                            | <i>71</i> |
| <i>Figura 6.13 - Ethereal colocado entre o PC cliente e o Router 3 .....</i>                                        | <i>72</i> |
| <i>Figura 6.14 - Envio da Mensagem IGMP Membership Report para o grupo multicast .....</i>                          | <i>72</i> |
| <i>Figura 6.15 - Problemas com o campo TTL dos pacotes enviados pelo VLC .....</i>                                  | <i>73</i> |
| <i>Figura 6.16 - Forma de resolver o problema do campo TTL do VLC.....</i>                                          | <i>74</i> |
| <i>Figura 6.17 - Visualização do Stream de vídeo no cliente .....</i>                                               | <i>74</i> |
| <i>Figura 6.18 - Cenário multicast IPv6 nativo usando o paradigma PIM-SM.....</i>                                   | <i>75</i> |
| <i>Figura 6.19 - Colocar o VLC a emitir para uma endereço multicast IPv6 usando os protocolos UDP e RTP.....</i>    | <i>77</i> |
| <i>Figura 6.20 - Endereçamento multicast IPv6 utilizado neste cenário.....</i>                                      | <i>77</i> |
| <i>Figura 6.21 - Configurar o VLC para receber vídeo.....</i>                                                       | <i>78</i> |
| <i>Figura 6.22 - Limpar as configurações temporárias de IPv6 na máquina .....</i>                                   | <i>79</i> |
| <i>Figura 6.23 - Visualização do Stream de vídeo no cliente .....</i>                                               | <i>79</i> |
| <i>Figura 6.24 - Ethereal colocado entre o PC cliente e o Router 3 .....</i>                                        | <i>80</i> |
| <i>Figura 6.25 - Configurar o Ethereal para decodificar pacotes RTP.....</i>                                        | <i>81</i> |
| <i>Figura 6.26 - Obtenção de estatísticas sobre o tráfego RTP usando o Ethereal.....</i>                            | <i>81</i> |
| <i>Figura 6.27 - Parâmetros de QoS medidos pelo Ethereal .....</i>                                                  | <i>82</i> |
| <i>Figura 6.28 - Cenário baseado num esquema presente na M6Bone.....</i>                                            | <i>83</i> |
| <i>Figura 6.29 - Configurações efectuadas no R1 (FCCN).....</i>                                                     | <i>86</i> |
| <i>Figura 6.30 - Configuração das aplicações .....</i>                                                              | <i>88</i> |
| <i>Figura 6.31 - E-Mail enviado para a Mail-List da M6Bone.....</i>                                                 | <i>89</i> |
| <i>Figura 6.32 - Visualização do Stream de vídeo no cliente .....</i>                                               | <i>90</i> |
| <i>Figura 6.33 - Ethereal colocado entre o router R2 e o router R3.....</i>                                         | <i>91</i> |
| <i>Figura 6.34 - Pacotes enviados no túnel.....</i>                                                                 | <i>91</i> |
| <i>Figura 6.35 - Configurações do túnel efectuadas no R1.....</i>                                                   | <i>92</i> |
| <i>Figura 6.36 - Encapsulamento de pacotes multicast IPv6 no cabeçalho GRE .....</i>                                | <i>92</i> |
| <i>Figura 6.37 - Pacote multicast IPv6.....</i>                                                                     | <i>92</i> |
| <i>Figura 6.38 - IPv6 multicast em redes IPv4.....</i>                                                              | <i>93</i> |
| <i>Figura 6.39 - Simular uma ligação nativa multicast IPv6.....</i>                                                 | <i>96</i> |
| <i>Figura 6.40 - Cenário multicast IPv6 nativo usando o paradigma Embedded RP .....</i>                             | <i>97</i> |
| <i>Figura 6.41 - Configurações efectuadas no Router 1 .....</i>                                                     | <i>98</i> |
| <i>Figura 6.42 - Embedded RP, cenário nativo - Principais configurações efectuadas no Router 2 e Router 3 .....</i> | <i>99</i> |

|                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------|------------|
| <i>Figura 6.43 - Embedded RP, cenário nativo - Configurar o VLC para emitir vídeo .....</i>                 | <i>100</i> |
| <i>Figura 6.44 - Embedded RP, cenário nativo - Endereço do grupo multicast configurado no servidor.....</i> | <i>100</i> |
| <i>Figura 6.45 - Embedded RP, cenário nativo - Configurar o VLC para receber vídeo.....</i>                 | <i>101</i> |
| <i>Figura 6.46 - Cenário incorrecto: o RP não está colocado no sítio certo.....</i>                         | <i>102</i> |
| <i>Figura 6.47 - Cenário incorrecto: não existe um RP definido .....</i>                                    | <i>103</i> |
| <i>Figura 6.48 - Embedded RP, cenário nativo - Visualização do Stream de vídeo no cliente .....</i>         | <i>103</i> |
| <i>Figura 6.49 - Embedded RP, cenário nativo - Ethereal colocado entre o PC cliente e o Router 3.....</i>   | <i>104</i> |
| <i>Figura 6.50 - Parâmetros de QoS medidos pelo Ethereal.....</i>                                           | <i>105</i> |
| <i>Figura 6.51 - Cenário baseado num esquema presente na M6Bone .....</i>                                   | <i>105</i> |
| <i>Figura 6.52 - Configurações efectuadas no Router ‘RSouce‘.....</i>                                       | <i>106</i> |
| <i>Figura 6.53 - Configurações do túnel efectuadas no R1 .....</i>                                          | <i>109</i> |
| <i>Figura 6.54 - Encapsulamento de pacotes multicast IPv6 no cabeçalho GRE .....</i>                        | <i>109</i> |
| <i>Figura 6.55 - Pacote multicast IPv6 .....</i>                                                            | <i>110</i> |
| <i>Figura 6.56 - Parâmetros de QoS medidos pelo Ethereal.....</i>                                           | <i>110</i> |
| <i>Figura 6.57 - Configurações efectuadas no router ‘RSouce‘ e no router ‘R4’ .....</i>                     | <i>112</i> |
| <i>Figura 6.58 - PIM-SSM, cenário com túneis - configuração da aplicação no servidor ....</i>               | <i>114</i> |
| <i>Figura 6.59 - PIM-SSM, cenário com túneis - configuração da aplicação no cliente.....</i>                | <i>114</i> |
| <i>Figura 6.60 - Pacotes enviados no túnel .....</i>                                                        | <i>115</i> |
| <i>Figura 6.61 - Esquema com as configurações dos servidores e do cliente .....</i>                         | <i>116</i> |
| <i>Figura 6.62 - Configurações efectuadas na máquina cliente – Linux.....</i>                               | <i>116</i> |
| <i>Figura 6.63 - Ambos os servidores estão a emitir para o mesmo grupo multicast [FF36::6] .....</i>        | <i>117</i> |
| <i>Figura 6.64 - Visionamento, no cliente, de dois filmes enviados por diferentes servidores .....</i>      | <i>117</i> |
| <i>Figura 7.1 - Topologia inicial da ligação .....</i>                                                      | <i>119</i> |
| <i>Figura 7.2 - Servidores ligados na rede M6Bone.....</i>                                                  | <i>128</i> |
| <i>Figura 7.3 - Forma de configurar o VLC para receber conteúdos da M6Bone.....</i>                         | <i>129</i> |
| <i>Figura 8.1 - Topologia existente da ESTG –Leiria, ligação à M6Bone.....</i>                              | <i>131</i> |
| <i>Figura 9.1 - Nomenclatura usada para representar as versões dos IOS .....</i>                            | <i>135</i> |
| <i>Figura 9.2 - Evolução da versão 12.3 .....</i>                                                           | <i>136</i> |
| <i>Figura 9.3 - Evolução da versão T e M dos IOSs .....</i>                                                 | <i>137</i> |
| <i>Figura 9.4 - Hierarquia de serviços oferecidos na versão 12.3 .....</i>                                  | <i>138</i> |

## Lista de Tabelas

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
| <i>Tabela 4.1 - Exemplo de endereços reais multicast IPv6.....</i>                         | <i>22</i>  |
| <i>Tabela 4.2 - Abrangências dos endereços multicast IPv6.....</i>                         | <i>22</i>  |
| <i>Tabela 4.3 - Comparação entre as abrangências do IPv4 e IPv6.....</i>                   | <i>22</i>  |
| <i>Tabela 4.4 - Endereços utilizados nos testes.....</i>                                   | <i>23</i>  |
| <i>Tabela 4.5 - formatos das mensagens e descrição de cada uma delas 3306.....</i>         | <i>24</i>  |
| <i>Tabela 4.6 - formatos das mensagens e descrição de cada uma delas 3956.....</i>         | <i>26</i>  |
| <i>Tabela 5.1 - Formado e descrição das mensagens MLDv1 .....</i>                          | <i>32</i>  |
| <i>Tabela 5.2 - Mensagens MLDv1 .....</i>                                                  | <i>41</i>  |
| <i>Tabela 6.1 - Servidores SSMping públicos .....</i>                                      | <i>63</i>  |
| <i>Tabela 6.2 - Principais configurações efectuadas no Router 1 .....</i>                  | <i>76</i>  |
| <i>Tabela 6.3 - Abrangências actualmente definidas para os endereços multicast.....</i>    | <i>78</i>  |
| <i>Tabela 6.4 - Suporte multicast e unicast dos equipamntos .....</i>                      | <i>83</i>  |
| <i>Tabela 6.5 - Configurações efectuadas no RSource .....</i>                              | <i>84</i>  |
| <i>Tabela 6.6 - Configurações efectuadas R4 (LCA).....</i>                                 | <i>87</i>  |
| <i>Tabela 6.7 - Problemas no cenário Embedded RP .....</i>                                 | <i>102</i> |
| <i>Tabela 6.8 - Equipamentos configurados como Multicast e Unicast .....</i>               | <i>112</i> |
| <i>Tabela 6.9 - configurações efectuadas no router R1.....</i>                             | <i>113</i> |
| <i>Tabela 9.1 - Descrição dos pacotes existentes na versão 12.3 do Cisco IOS.....</i>      | <i>138</i> |
| <i>Tabela 10.1 - Grupos de trabalho do IETF que trabalham na área deste projecto .....</i> | <i>157</i> |



# 1 Introdução

O projecto que se pretende levar a cabo na cadeira de Projecto Informático II, *Vídeo-Difusão sobre Multicast IPv6*, pertence à área das redes, não sendo desta forma, um projecto tradicional de engenharia, mas sim um projecto de Investigação. Neste projecto propriamente dito, não se pretende criar uma aplicação, mas sim, fazer um estudo do *state-of-art* da tecnologia, elabora enúmeros cenários práticos e realizar diversos testes sobre os mesmos com vista, de uma forma genérica, a descobrir qual a melhor tecnologia para difusão de Vídeo. Por conseguinte, foi necessário elaborar um relatório com partes teóricas, partes que correspondem ao estudo das tecnologias, e com partes práticas contendo os cenários, resultados e conclusões obtidas através da realização dos testes efectuados. Deste modo, um projecto da Área de Redes e Serviços de Comunicação é essencialmente um projecto de investigação.

Em concreto, espera-se que no final deste projecto estejam presentes os seguintes elementos:

Produzir um relatório pragmático que sirva de base para consulta futura

Elaboração de uma apresentação no final do semestre, em PowerPoint, que resuma todo o trabalho realizado, bem como os todos os resultados e conclusões obtidas

Elaboração de um poster em formato A2 e escrita de um artigo final

Em anexo, está presente um excelente documento com todos os conceitos relacionadas com o vídeo. Este foi efectuado no âmbito da disciplina de Projecto I por alunos do curso de EIC – Engenharia Informática e Comunicações.

## 1.1 Objectivos

O objectivo deste projecto é o estudo e experimentação de uma solução de Vídeo-Difusão sobre Multicast IPv6, envolvendo a investigação e estudo das tecnologias envolvidas, a definição de cenários e a realização de testes. Mais concretamente, o objectivo deste trabalho, passa pela

experimentação de uma solução de multicast em IPv6 e posterior elaboração de um documento técnico que apresente as conclusões, os resultados, os cenários e as tecnologias envolvidas. O documento deverá apresentar também o estado da arte actual da tecnologia e clarificar as diferenças da tecnologia multicast em IPv6 face à existente em IPv4. Deverão ainda ser realizados diversos testes de vídeo, com medições ao nível da qualidade subjectiva e efectiva, com o intuito de escolher qual a melhor tecnologia para a difusão do vídeo.

Numa segunda fase, serão efectuados testes entre a ESTG e a FCCN, com vista a dar credibilidade ao trabalho desenvolvido ao longo deste projecto.

### **1.2 Projecto IPv6 @ ESTG**

O projecto IPv6@ESTG, desenvolvido por dois alunos de EIC no decorrer do ano de 2005, tinha como objectivo a implementação de uma rede piloto IPv6 no Departamento de Engenharia Informática (DEI) da Escola Superior de Tecnologia e Gestão de Leiria (ESTG-Leiria). A rede a implementar deveria ser heterogénea, constituída por terminais com sistemas operativos distintos: Microsoft Windows XP Professional SP2, Linux Fedora Core 3, Open BSD, Apple Mac OS X e Cisco IOS.

O projecto, concluído com bastante sucesso, dividiu-se em três partes: estudo abrangente da tecnologia IPv6; implementação da rede IPv6 e elaboração de relatório técnico de serviria de base para trabalhos futuros.

Tendo por base o trabalho desenvolvido, dois docentes do Departamento de Engenharia Informática da ESTG - Leiria, resolveram lançar um projecto que permite-se acrescentar valor e possibilitasse o estudo de tecnologias cada vez mais emergentes na Internet – a vídeo-difusão e o multicast IPv6. Ao projecto lançado foi dado o nome de **IPv6@ESTG-Leiria: Vídeo-Difusão sobre Multicast IPv6** e pretende-se que este contribua para aumentar o conhecimento de IPv6, Multicast e Vídeo-Difusão na Escola Superior de Tecnologia e Gestão de Leiria, bem como outras que manifestem interesse em usar o referido projecto.

## 2 Multicast em redes IP

*“Do you know multicast over IP ? quite an old story...but not so old compared to the time needed to Arpanet to become the wild wild web. This is "Group communication over IP", or "Hosts groups" defined by Steve Deering during his Phd thesis”* [1].

A tecnologia multicast fornece um mecanismo de transmissão de dados de forma extremamente eficiente, quer para aplicações com baixos débitos, quer essencialmente para aplicações que requerem elevada largura de banda. *Video-on-demand*, videoconferência e televisão de alta definição, são alguns exemplos de aplicações que, com a utilização da tecnologia multicast, irão estar disponíveis nos próximos anos em qualquer computador pessoal, PDA ou outro equipamento que esteja ligado à Internet.

Em comunicações tradicionais envolvendo vários sites simultaneamente, para cada pacote do host de origem é efectuada uma replicação para o número de host destino e cada pacote é enviado para o seu destino separadamente. Este modelo impõe uma limitação no número de computadores que podem estar envolvidos na comunicação, pois o tráfego na rede e as necessidades computacionais do host de origem aumentam linearmente consoante o número de hosts destino envolvidos [2] [3].

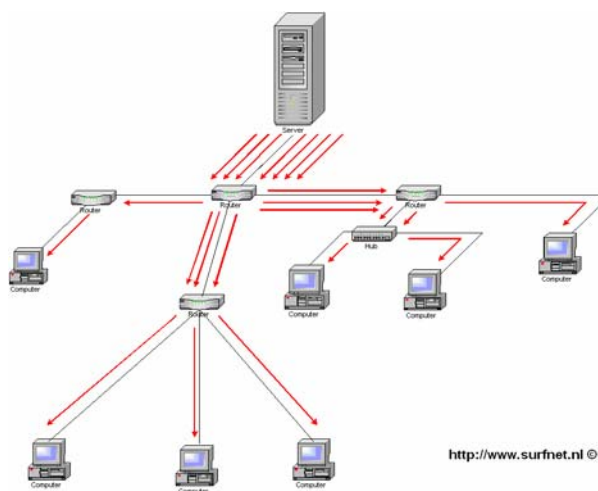


Figura 2.1 - Transmissão em unicast

Existem porém tecnologias que tratam estas limitações, sendo denominadas por soluções escalares de rede. O uso do IP multicast é uma destas soluções. Utilizando multicast, apenas uma cópia de cada pacote é enviada em cada segmento de rede, sendo esta replicada apenas quando se justifique.

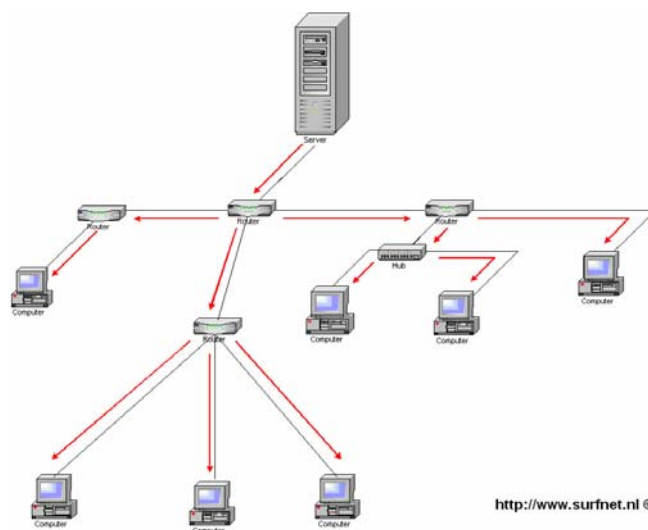


Figura 2.2 - Transmissão em multicast

## 2.2 Redes IPv6 multicast Existentes

A rede **Abilene** (backbone de alta performance que suporta a Internet2), actualmente implementada na América e a rede **M6Bone** são exemplos das principais implementações da tecnologia Multicast. Existem cada vez mais instituições a aderir à tecnologia, sendo a ESTG – Leiria um exemplo.



**Abilene**, acrónimo de *Advanced Networking for Leading-edge Research and Education*, é a rede actualmente mais avançada do Estados Unidos, que existe sobre IP, tendo sido criada para possibilitar o desenvolvimento de novas e inovadoras aplicações bem como de serviços avançados (**multicast**, **IPv6**, qualidade de serviço, segurança, ...) para a Internet do futuro, a nova Internet2 [4]. Esta rede interliga vários laboratórios e diferentes universidades, cerca de 220 membros na América do Norte, sobre um backbone de alta velocidade que, actualmente atinge débitos na ordem dos 10Gbit/s (OC-192c). Usa a tecnologia óptica para transportar os dados, bem como equipamentos de alto desempenho com tecnologia de ponta.

A rede Abilene é uma sociedade da Internet2, Qwest Communications, Nortel Networks, Juniper Networks, e universidade do Indiana.

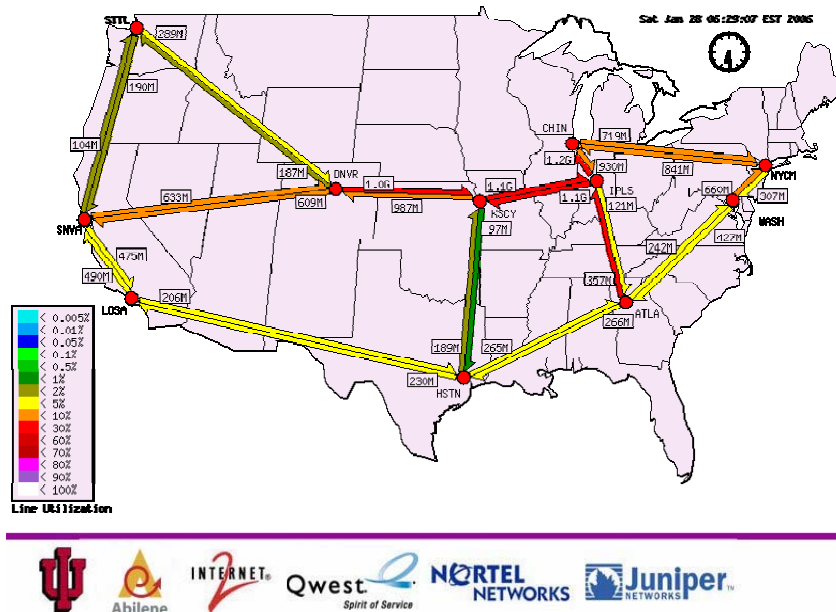


Figura 2.3 - Topologia lógica da rede Abilene

#### M6Bone - IPv6 multicast network

Site Map  
Summary  
Private area

**M6Bone** é uma rede de testes IPv6 multicast que iniciou em 2001 a sua actividade. Um dos grandes objectivos do projecto passa por desenvolver tecnologias e oferecer serviços multicast a todos os sites interessados bem como desenvolver serviços avançados com vista a promover o novo protocolo – IPv6 [5] [6] [7] [8] [9].

A rede é usada para testar equipamentos, software e implementações relacionadas com a tecnologia. Periodicamente, esta é também usada para transmitir eventos ou difundir conteúdos multimédia.

A figura seguinte esquematiza a topologia lógica, a nível mundial da rede M6Bone.

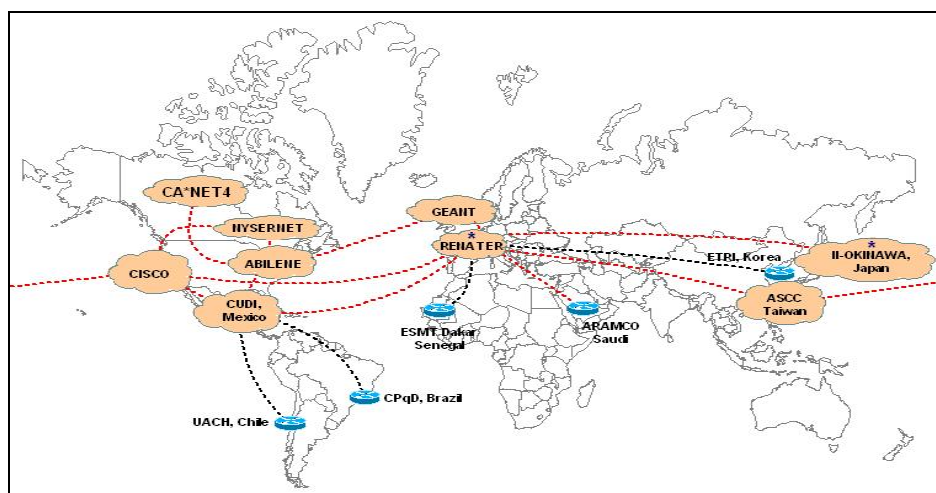


Figura 2.4 - Topologia lógica da rede M6Bone

A rede M6Bone conta com o apoio do RENATER (*Le Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche*), que fornece a infra-estrutura IPv6 nativa, com o suporte logístico da entidade francesa que divulga as novas tecnologias (*Aristote association*) e do grupo de testes IPv6 Francês G6.

A M6Bone estabeleceu parcerias com diversas organizações europeias, destacam-se a 6NET e a Euro6IX. Graças ao backbone europeu criado para sustentar o projecto 6NET, é possível a qualquer momento modificar a topologia em estrela que existe actualmente, e migrar para a topologia em malha [9]. A 30 de Junho de 2005, o projecto 6NET teve o seu termino e actualmente o transito de tráfego multicast IPv6 é feito pela rede Europeia de educação e investigação – **GÉANT**<sup>1</sup> [10].



A ESTG - Escola Superior de Tecnologia e Gestão de Leiria, a maior escola do Instituto Politécnico de Leiria, embora sendo uma escola recente, tem procurado estar sempre na vanguarda da tecnologia. Desta forma, esta tem lançado vários projectos ao longos dos anos que tem acompanhado as mais recentes inovações e tecnologias desenvolvidas nas principais escolas europeias ou mesmo mundiais.

Actualmente a ESTG de Leiria já dispõem de uma rede interna multicast IPv6 e aguarda apenas que o seu fornecedor de acesso de Internet, a FCCN, disponibilize uma ligação com multicast nativa. Segundo se conseguiu apurar com os responsáveis da FCCN, com a Eng. Mónica Domingues em particular, a ligação nativa irá ser disponibilizada em breve, e a ESTG – Leiria irá mais uma vez ser pioneira.

Toda a rede IPv6 da ESTG já possui suporte para multicast, incluído o ‘Router de Acesso’, trocado propositadamente para esse efeito no âmbito do referido projecto. Assim, quando a FCCN disponibilizar a conectividade multicast, a ESTG irá ser das primeiras escolas a obter conectividade. A imagem seguinte apresenta a topologia actual multicast IPv6.

---

<sup>1</sup> GÉANT is the multi-gigabit pan-European research network. Through connectivity with Europe's NRENs, GÉANT provides pan-European high-speed data communications connectivity to more than 3500 research and education institutions around Europe.

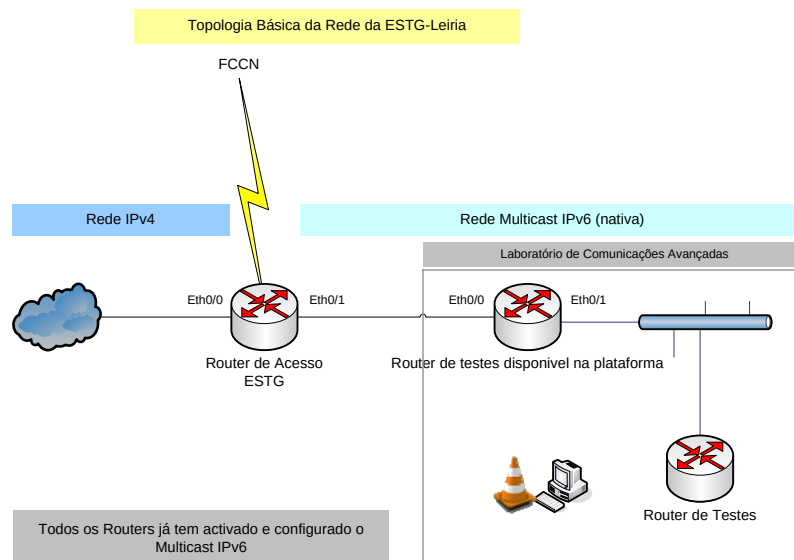


Figura 2.5 - Esquema que representa a topologia das redes IPv4 e IPv6 da ESTG

## 2.3 Características específicas das instituições

Nesta secção, para cada uma das redes multicast mencionadas anteriormente, é apresentado um enquadramento histórico, sendo de seguida apresentadas algumas características específicas da rede em particular.

### Abilene

Como já foi mencionado previamente, a rede **Abilene** é actualmente a mais avançada e a mais evoluída rede dos Estados Unidos. Criada para suportar o desenvolvimento de novas aplicações e novos serviços, (Multicast, IPv6, Qualidade de Serviço, Segurança, Medições de parâmetros de rede, entre outros) para a Internet do futuro, a Internet2.

### Objectivos

A rede Abilene, foi criada para possibilitar o desenvolvimento de aplicações inovadoras, com novas técnicas, que requerem a existência de redes de alta performance que não estão disponíveis actualmente em redes comerciais. De seguida são apresentados mais alguns dos objectivos:

- Desenvolvimento e testes de serviços de redes avançados, nos quais se incluem o **multicast**, o **IPv6**, qualidade de serviço e segurança.

- Conectividade com outras redes de investigação e educação através de peerings internacionais com outras redes, possibilitando desta forma uma investigação a nível mundial de diversas formas.

- Acesso dos investigadores a uma rede com valiosos recursos, com alto débito suportando novas e inovadoras aplicações.

## Historial

Em 14 de Abril de 1998, o vice-presidente dos Estados Unidos Al Gore, anunciou durante uma cerimónia na Casa Branca, a criação da rede Abilene. Este entrou efectivamente em funcionamento em Fevereiro do ano seguinte, com um débito inicial no backbone de 2.5 Gigabits/s. Em 2003 ficou completa mais uma fase da rede, com um upgrade para 10Gbtis/s e com o suporte nativo para IPv6.



Figura 2.6 - Backbone da rede, OC-192c (9.952 Gbps)

## Topologia e Serviços da rede Abilene

Nas imagens seguintes são apresentadas imagens da topologia actual da rede e os serviços disponibilizados.





## M6Bone

**M6Bone** é um acrónimo de Multicast IPv6 Backbone. Trata-se de uma rede mundial para testes de IPv6 multicast que foi criada inicialmente 2001 nos laboratórios da RENETER, (Centro Nacional Francês de investigação e Telecomunicações).



Figura 2.9 - Início do projecto M6Bone - 2001

O projecto aquando a sua criação, tinha um grande objectivo inicial: ter o multicast IPv6 activo na rede 6NET [10].

Foram estabelecidas diversas parcerias com os engenheiros da Cisco, e à medida que as implementações foram surgindo, foram sendo configuradas no core da 6NET [9]. Em Março de 2003, foram iniciados os primeiros testes e em Setembro do mesmo ano, estava concluído o primeiro grande objectivo da rede M6Bone – tecnologia multicast IPv6 nativa no core da 6NET. Grande parte das Redes dos Centros Nacionais de Investigação e Desenvolvimento (NRENs – *Nation Research and Education Networks*) já possuíam configurado a tecnologia, alguns apenas em testbeds, outros já em ambientes de produção.

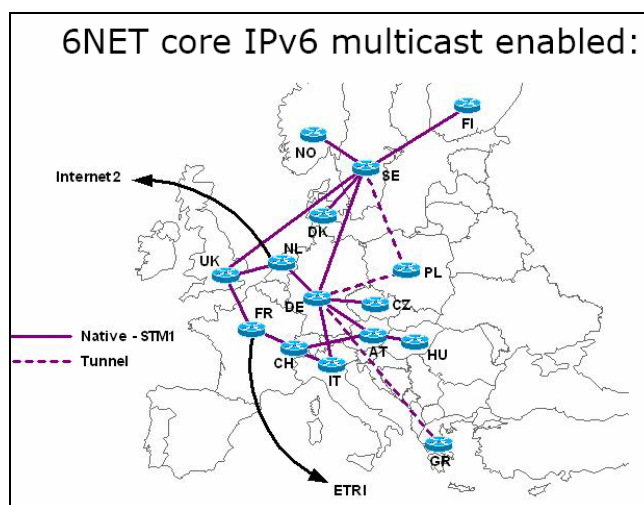


Figura 2.10 - Backbone do 6NET - *multicast enabled*

No início de 2005, a rede 6NET teve o seu termo e todos os NREN passaram a estar interligados à rede GÉANT.

## Objectivos

Um dos grandes objectivos do projecto passou por desenvolver tecnologias e oferecer serviços multicast a todos os sites interessados bem como desenvolver serviços avançados com vista a promover o novo protocolo – IPv6. Pretende ter um papel preponderante na criação e normalização das tecnologias multicast, em especial no inter-domínio.

O projecto aquando a sua criação, tinha um grande objectivo inicial: ter o multicast IPv6 activo na rede 6NET.

## Historial

No início do projecto, Junho de 2001, eram raros os equipamentos que dispunham de encaminhamento multicast IPv6. Existiam vários com suporte para tráfego unicast, mas para multicast, existiam muito poucos. Aliada a esta limitação, existia uma outra, o facto dos poucos equipamentos com capacidades para processar tráfego multicast, nenhum destes possuía tabelas de encaminhamento separadas para tráfego multicast e unicast.. A figura seguinte ilustra a topologia inicial da rede.

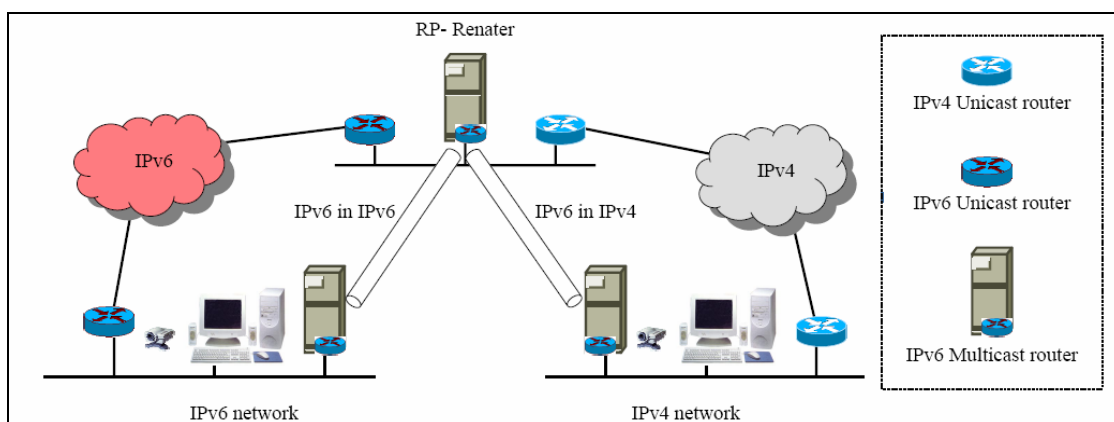


Figura 2.11 - Equipamentos não suportam rotas multicast

Como facilmente se compreende, a limitação encontrada requeria o uso de dois equipamentos, um dedicado exclusivamente ao tráfego unicast e um outro a tráfego multicast. Desta forma, passavam a existir caminhos distintos para cada tipo de tráfego. Assim, a solução encontrada para resolver o primeiro dilema encontrado na rede M6Bone foi usar diferentes routers configurando num deles, o router multicast, um túnel directo ao servidor da Renater. Este último foi configurado com endereçamento global para que fosse visível a todos os sites espalhados pelo mundo.

Os túneis multicast poderiam ser dos seguintes tipos:

- IPv6 multicast sobre IPv6 unicast
- IPv6 multicast sobre IPv4 unicast
- IPv6 multicast sobre Generic Routing Encapsulation (GRE)

À medida que o tempo foi avançando, e consecutivamente a investigação e implementação, foram surgindo os primeiros equipamentos com suporte para tabelas de encaminhamento multicast, distintas das de unicast. Desta forma, passou a ser possível, ao invés de usar dois, usar apenas um equipamento com capacidade para lidar com diferentes topologias.

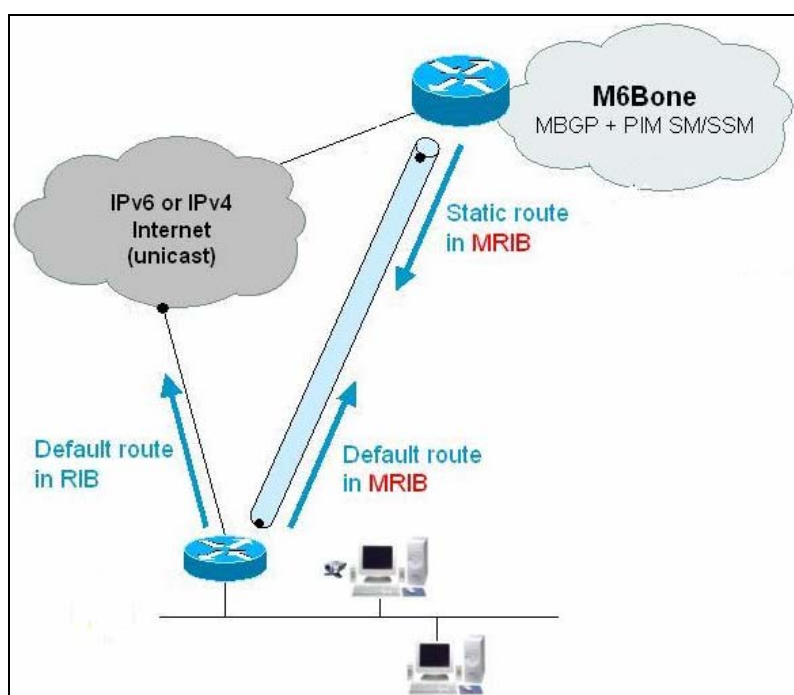


Figura 2.12 - Equipamentos com suporte para rotas multicast

Nestes equipamentos é possível configurar rotas estáticas multicast e rotas estáticas unicast. Assim é possível usar apenas um equipamento para lidar com diferentes topologias. Mais concretamente, vai existir uma topologia para os pacotes unicast e uma outra, distinta para multicast. A necessidade de usar topologias distintas para os diferentes tipos de tráfego, deve-se ao facto de não existir conectividade multicast ipv6 nativa.

Os primeiros equipamentos a suportarem esta funcionalidade foram os Cisco, Juniper e 6WIND.



## Topologia

Actualmente a rede conta com mais de 30 redes e 50 sites interligados entre si.

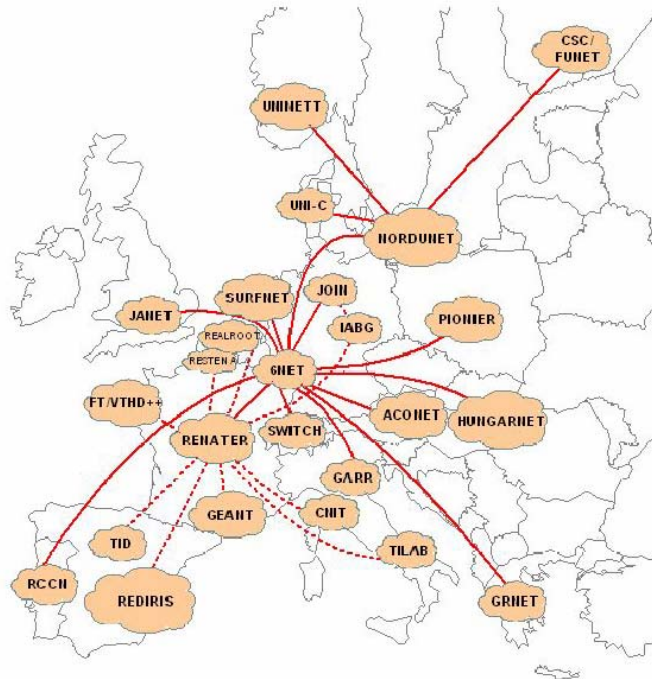


Figura 2.13 - Estado da rede M6Bone em Novembro de 2004

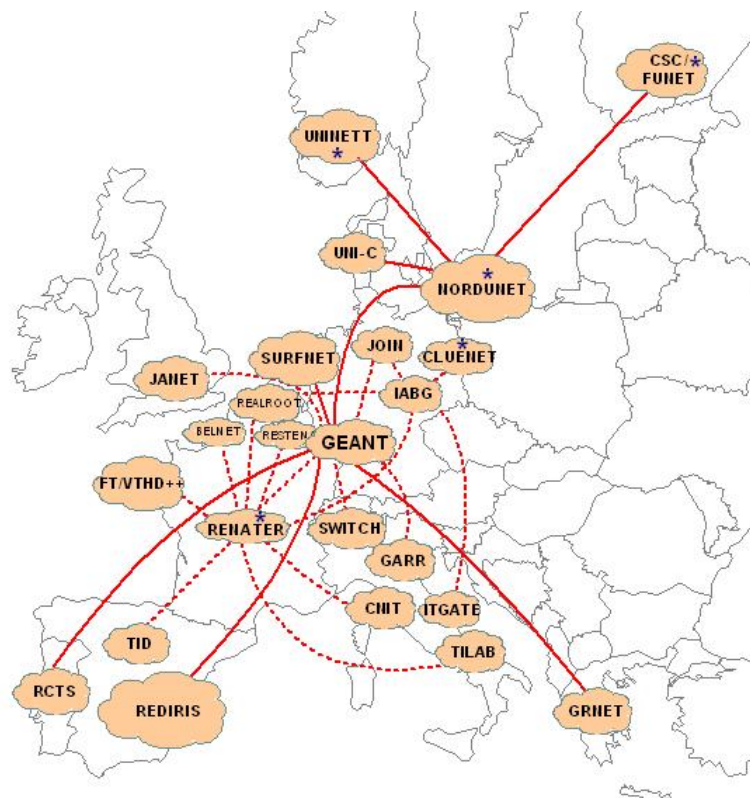


Figura 2.14 - Estado actual da rede M6Bone (2006)

## **ESTG – Leiria**

A celebrar no ano lectivo, 2004/2005, o 15º aniversário, a ESTG-Leiria, uma das cinco escolas integradas no Instituto Politécnico de Leiria, é actualmente o maior estabelecimento de ensino superior do distrito de Leiria e, entre os seus congéneres, um dos maiores a nível nacional. A ESTG – Leiria tem como missão formar, prestar serviços, e impulsionar a investigação científica e tecnológica. Destas actividades resultam projectos que contribuem para manter/ aumentar o bom nome da instituição e a qualidade dos seus formandos.



Figura 2.15 - Escola Superior de Tecnologia e Gestão de Leiria – Instituto Politécnico de Leiria

## **Objectivos**

No âmbito da disciplina de Projecto II do 5º ano do curso de Engenharia Informática e Comunicações, surgiu a possibilidade de interligar a escola com a rede europeia de Multicast IPv6 (M6Bone). Foram efectuados vários contactos com a M6Bone e FCCN com vista à concretização dos objectivos, tendo-se chegado à conclusão que a melhor solução seria ligar a ESTG à FCCN, em detrimento da ligação directa da ESTG à rede europeia. De acordo com a Eng. Mónica Domingues da FCCN, não existe vantagem em ligar a ESTG de Leiria directamente à França. Dado que a FCCN já possui uma ligação nativa com a rede M6Bone, e a ESTG está ligada directamente à FCCN.

## **Historial**

Em meados de 2005, foi lançado o projecto de Vídeo-difusão sobre multicast IPv6. Embora não estivesse previsto no início a ligação da ESTG à rede europeia, constatou-se no decorrer do referido projecto que existia essa possibilidade. Como tal, foram realizados todos os esforços para alcançar os objectivos.

Em Janeiro de 2006, foi efectivamente efectuada a ligação da ESTG à rede europeia.

### Topologia

Visto que actualmente a FCCN ainda não disponibiliza conectividade aos seus parceiros, foi necessário configurar um túnel IPv6 multicast sobre IPv6. Numa fase posterior, e atendendo às configurações existentes nos equipamentos da ESTG, é possível o acesso nativo à rede europeia. Para isso acontecer, basta que a FCCN disponibilize o serviço uma vez que, da parte da ESTG, já está tudo preparado. Todos os equipamentos, incluindo o router de acesso, já se encontram configurados, basta apenas que a entidade fornecedora do serviço Internet disponibilize a referida conectividade IPv6 Multicast nativa.

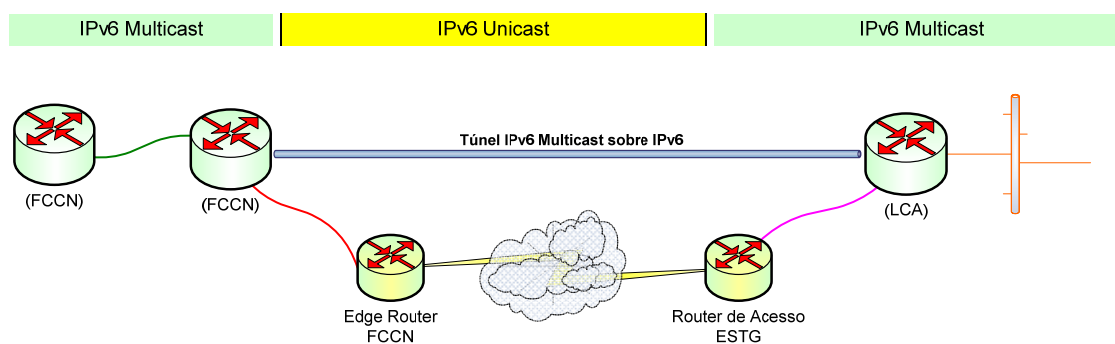


Figura 2.16 - Topologia actual da rede IPv6 Multicast da ESTG – Leiria (ligação por túnel)

Como já foi mencionado, depois da FCCN disponibilizar conectividade multicast IPv6 à ESTG, a ligação à rede M6Bone passa a ser nativa, não sendo por isso necessário o uso de túneis. A figura seguinte, ilustra a topologia que irá existir num futuro muito breve.

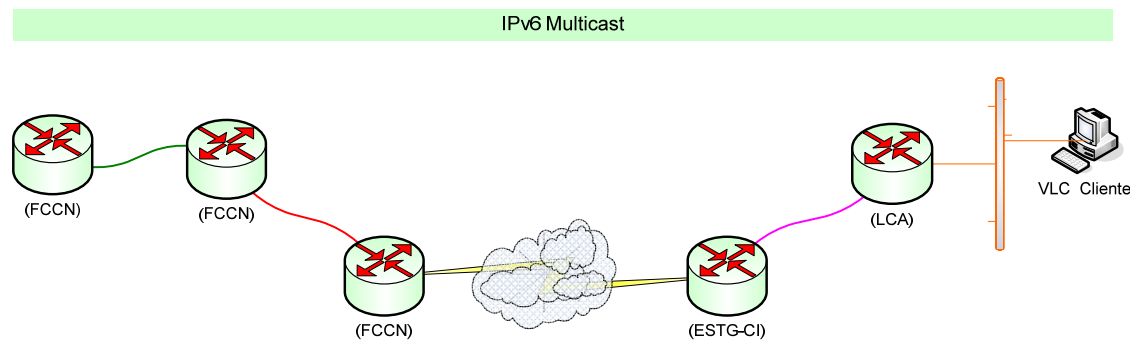


Figura 2.17 - Topologia futura da rede IPv6 Multicast da ESTG – Leiria (ligação nativa)





### 3 Modelos de distribuição de tráfego multicast

Nesta secção são apresentados os dois modelos de distribuição de tráfego multicast que estão definidos actualmente. Para cada um destes, irá ser apresentada uma descrição sucinta, numa primeira fase, sendo posteriormente apresentados os seus detalhes. Numa fase posterior, são apresentadas as vantagens e desvantagens de cada um destes modelos.

#### 3.1 Terminologia

Actualmente existem dois modelos de distribuição de tráfego multicast, sendo o primeiro datado do ano 1989 e o outro, mais recente, foi publicado em Julho de 2003.

**ASM – Any-Source Multicast;** Modelo multicast tradicional, definido na RFC 1112. Neste, os pacotes são transmitidos para um endereço IP que corresponde ao endereço do grupo. A figura seguinte apresenta o modelo ASM, onde os clientes necessitam de definir apenas o grupo de que desejam receber pacotes multicast [11]. Como é visível, no exemplo seguinte, o cliente deseja receber dados do grupo [FF16::6]

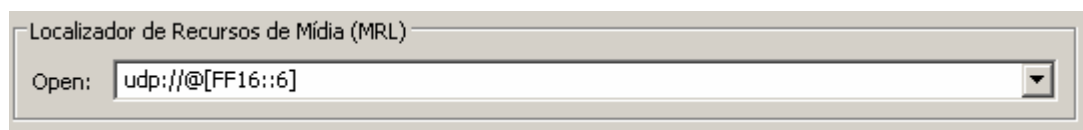


Figura 3.1 - Exemplo de utilização do modelo ASM

A título meramente indicativo, o modelo ASM foi criado por Steve Deering aquando da sua tese de Doutoramento (Phd thesis) [1]. Este é co-autor de diversas RFCs relacionadas com endereçamento e multicast IPv6.

**SSM – Source-Specific Multicast:** Modelo multicast definido na RFC 3569, onde um pacote IP é transmitido por um servidor (S) para um endereço destino SSM (G). Desta forma os clientes podem receber os pacotes subscrevendo o canal (S,G). Cada canal possui apenas uma fonte e a ele podem estar associados vários clientes.

A figura seguinte apresenta o modelo SSM, onde os clientes necessitam de definir o grupo a que se desejam associar, necessitando também de especificar o endereço do servidor. Como é visível, no exemplo em particular, o cliente deseja receber dados do grupo [FF36::6] oriundos do servidor [2001:D::2].

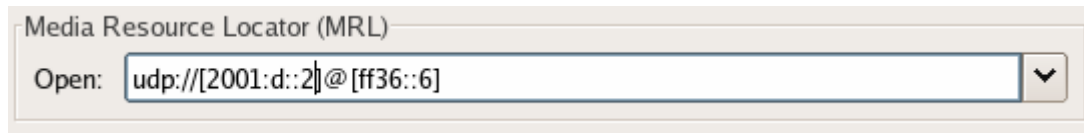


Figura 3.2 - Exemplo de utilização do modelo SSM

## 3.2 ASM, SSM - vantagens e desvantagens

Nesta secção são apresentadas as vantagens e desvantagens do modelo SSM face ao predecessor ASM.

### 3.2.1 Problemas do ASM

O modelo ASM, devido à sua simplicidade, possui vários problemas associados. Assim, nesta secção, cada um deles está apresentado em detalhe.

**Alocação de endereços:** A arquitectura actual não fornece uma solução para a colisão de endereços entre múltiplos domínios. No IPv4 o problema do endereçamento global unicast foi parcialmente resolvido pela RFC 3180 (IPv4 GLOP), onde um *provider* embutia o seu número do sistema autónomo no endereço 233/8. Desta forma, apenas restavam 256 endereços para grupos multicast [13].

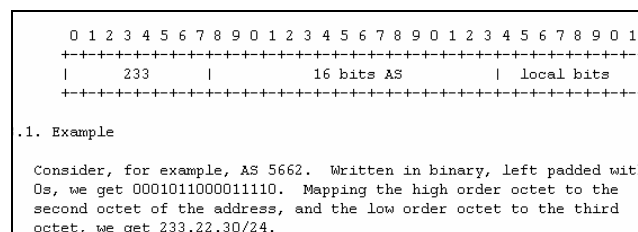


Figura 3.3 - Exemplo retirado da RFC 3180 - endereçamento global unicast em IPv4

**Falta de controlo no acesso:** No modelo ASM, um cliente não consegue especificar de que servidor deseja receber os dados. Além disso, quando uma fonte está a transmitir para um endereço multicast, não possui mecanismos que lhe garantam que outras fontes não irão usar o mesmo grupo [12].

**Uso ineficiente dos recursos quando se conhece o endereço do servidor:** Nos casos em que os clientes conhecem o endereço do servidor, é preferível usar árvores originadas na fonte, SBF (*source-based forwarding*) ao invés de se usarem árvores partilhadas, onde é necessário a existência do RP (*Rendezvous Point*) [12]. O conceito de árvores de distribuição é apresentado, com detalhe, na secção 5.2.

### 3.2.2 Vantagens do SSM

Como foi mencionado anteriormente, no modelo SSM define-se um canal identificado pelo par Servidor,Grupo (S,G). Por este motivo, é apenas necessário o uso de árvores *source-based forwarding*. Este conceito é descrito com detalhe na secção 5.2.

**Alocação de endereços:** os canais SSM estão associados às fontes, ou seja, o canal (S1,G) é diferente do canal (S2,G), onde S1 e S2 são endereços de servidores e G é um grupo específico utilizado pelas duas fontes. Usando este mecanismo, o problema da alocação de endereços multicast globais fica resolvido.

**Controlo de acesso:** SSM fornece uma solução bastante eficaz para controlar o problema de acesso. Quando um cliente se associa a um canal (S,G) este recebe os dados, garantidamente, do servidor especificado. De forma oposta, no ASM, qualquer host pode responder a um pedido de multicast para o grupo G.

No que se refere aos servidores, quando um servidor transmite para um canal (S,G), fica automaticamente assegurado que mais nenhum servidor vai enviar dados para esse canal (excepto nos casos em que exista um ataque malicioso de *spoofing* (troca) de endereços).

**Uso ineficiente dos recursos quando se conhece o endereço do servidor:** Dado que, usando o modelo SSM os clientes conhecem o endereço do servidor, então deixa de ser necessário o uso de pontos centrais na rede (RP - *Rendezvous Point*), dado que os *routers* possuem encaminhamento unicast para o servidor (S) e podem usar o caminho com a distância administrativa mais baixa.

### 3.2.3 Desvantagem do SSM

De facto, nem tudo são vantagens no modelo SSM. É de salientar que a inexistência de um mecanismo que permita anunciar os grupos onde existem servidores activos é uma lacuna bastante grande do SSM. No entanto, esta falha pode ser ultrapassada recorrendo a páginas na Internet com essa informação [14].

A figura seguinte contém os servidores ligados à rede M6Bone e apresenta também o estado destes.

The screenshot shows a web browser window with the address bar displaying `http://dbeacon.innerghost.net/contents`. The page title is "dbeacon Wiki" and the page content is titled "contents". The page text explains that it lists available permanent contents on the M6bone network and that the status is checked every 10 minutes. Below the text is a table with the following data:

| Name                          | Address                                                 | Description                                                                   | Status |
|-------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------------|--------|
| Frequence3 Radio              | <code>vlc udp://@[ff1e::8888]:8888</code>               | This is a well known <a href="#">French Internet radio</a> , 270kb/s required | ✓      |
| Frequence 3 Radio             | <code>udp://@[ff0e::2:ffdd]:1234</code>                 | "                                                                             | ✗      |
| Frequence 3 Radio             | <code>vlc udp://[gluon.q2s.ntnu.no]@[ff3e::8888]</code> | SSM transported version of the radio                                          | ✓      |
| University of Bergen Kamera 1 | <code>vlc udp://[gluon.q2s.ntnu.no]@[ff3e::8886]</code> | A nice high resolution view from the university of bergen                     | ✓      |

Figura 3.4 - Servidores ligados à rede M6Bone, ASM e SSM

No futuro, o modelo SSM irá tornar-se bastante importante, particularmente para aplicações onde os servidores de origem permaneçam inalteráveis [14]. Ou seja, este modelo é particularmente ideal para Vídeo-Difusão.

## 4 Endereçamento Multicast IPv6

De uma forma breve, no multicast IPv6 todos os endereços começam por [FF::

### 4.1 Básico

O endereçamento básico do multicast IPv6 é definido na RFC 3513. Esta define que um endereço é composto por 8 bits iniciais a “1”, seguidos de 4 bits para flags, outros 4 para o *scope*, e por fim, os restantes 112 bits contêm o endereço do grupo multicast propriamente dito. A figura seguinte, retirada da RFC, esquematiza o formato dos endereços multicast IPv6.

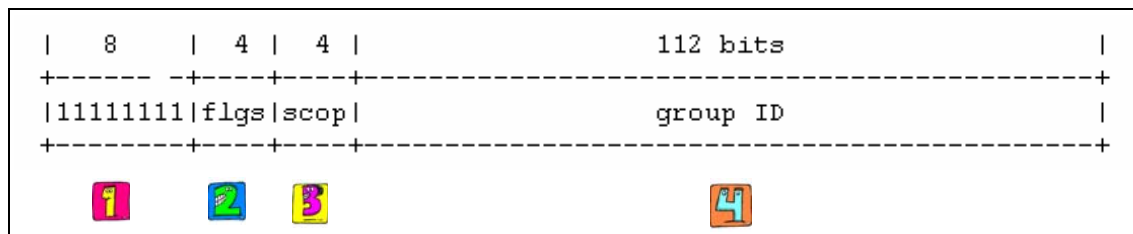


Figura 4.1 - Formato dos endereços multicast IPv6

No segundo campo (ícone 2), campo **flags**, composto por 4 bits, a RFC 3513 apenas especifica a utilização do último bit, sendo que os restantes 3 bits estão reservados e não são utilizados. A figura seguinte demonstra em pormenor as flags definidas para o segundo campo.

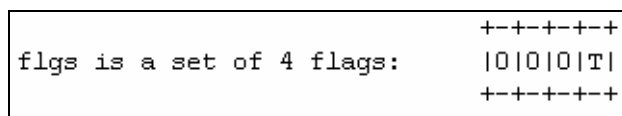


Figura 4.2 - Descrição das flags definidas na RFC 3513

O bit T define se estamos perante um endereço especial ("well-known") (valor 0), que necessita de ser atribuído pela autoridade que regista e controla os endereços IPs – IANA, ou se o endereço pode ser usado livremente, ou seja, se se trata de um endereço provisório ("transient") (valor 1).

Efectivamente, os endereços permanentes ("*well-known*") estão constantemente a ser actualizados e estão disponíveis no site do IANA [15]. De modo a facilitar a compreensão da atribuição de endereços, é apresentada a seguinte tabela com exemplos reais, utilizados neste projecto.

| Endereços Registados (IANA)               | Endereços Temporários                    |
|-------------------------------------------|------------------------------------------|
| FF01::1 – todos os <i>nodes</i> do link   | FF1e::1:2                                |
| FF01::2 – todos os <i>routers</i> do link | (endereço usado nos testes com a FCCN)   |
| FF02::9 – todos os <i>routers</i> RIP     | FF1e::8888                               |
| FF02::D – todos os <i>routers</i> PIM     | (endereço de um servidor da rede M6Bone) |

Tabela 4.1 - Exemplo de endereços reais multicast IPv6

Relativamente ao terceiro campo () **scope**, este é usado para definir a abrangência de um endereço multicast. Uma vez que este campo possui 4 bits, é possível ter 16 tipos de abrangência distintos, no entanto actualmente, apenas estão definidos 5 deles. Os restantes, ou estão reservados, ou não estão a ser usados presentemente.

A tabela seguinte expõe as abrangências actualmente definidas e realça as mais utilizadas.

| Abrangências actualmente definidas para os endereços multicast |
|----------------------------------------------------------------|
| 1 – interface-local scope                                      |
| 2 – link-local scope                                           |
| 4 – admin-local scope                                          |
| 5 – site-local scope                                           |
| 8 – organization-local scope                                   |
| E – global scope                                               |

Tabela 4.2 - Abrangências dos endereços multicast IPv6

De grosso modo, este campo é equivalente às zonas definidas em IPv4. No entanto, no IPv6 este conceito foi bastante melhorado. A tabela seguinte, retirada da RFC 2365 (Administratively Scoped IP Multicast) e de [3] permite analisar, de forma breve as semelhanças entre o endereçamento multicast dos dois protocolos.

| IPv4                        | IPv6                         |
|-----------------------------|------------------------------|
| 224.0.0.0/24                | 2 – link-local scope         |
| 239.255.0.0/16              | 3 – não atribuído            |
| 239.0.0.0 a 239.255.255.255 | 8 – organization-local scope |
| 233.0.0.0 a 233.255.255.255 | E – global scope             |
| 224.0.1.0 a 238.255.255.255 |                              |

Tabela 4.3 - Comparação entre as abrangências do IPv4 e IPv6

O último campo () **group ID**, contém 112 bits e identifica o endereço do grupo multicast propriamente dito. Assim, tomando como referência a tabela seguinte, consegue-se concluir que, nos

testes efectuados com a FCCN foi utilizado o grupo multicast “transient”, de “scope” global [1:2], e com a rede M6Bone foi utilizado o [8888].

#### Endereços utilizados nos Testes

FF1e::1:2

(endereço usado nos testes com a FCCN)

FF1e::8888

(endereço de um servidor da rede M6Bone)

Tabela 4.4 - Endereços utilizados nos testes

## 4.2 Avançado, usado em soluções Inter-domínio

Nesta secção são apresentados dois tipos de endereços, criados para poderem ser usados na Internet (Inter-Dominios) sem recorrer a protocolos adicionais.

### 4.2.1 Baseados no prefixo unicast

A RFC 3306, conhecida como *Unicast-Based Multicast Address*, define uma extensão ao endereçamento multicast IPv6 definido na RFC 3513. Resumidamente, esta permite que o prefixo unicast do site seja embutido dentro do endereço multicast.

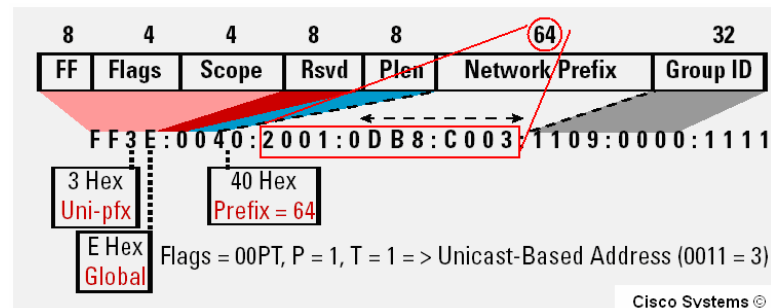


Figura 4.3 - Endereços Unicast-Based Multicast Address

Desta forma, ao adicionar-se o endereço unicast com o multicast, os gestores de redes conseguem identificar sempre o seu endereço multicast sem ser necessário recorrer a protocolos adicionais [13].

Resumidamente, a RFC 3306 introduz informação *encoded* no endereço multicast por forma a permitir troca dinâmica de endereços multicast e endereços IPv6 *Source-Specific Multicast Address* (ver secção PIM- SSM).

Na tabela seguinte são apresentados os formatos das mensagens e descrito em pormenor cada um deles. Convém referir que a gama para este tipo de endereços é iniciada sempre com o prefixo [FF30::/12]

|                                                                       |                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Flags</b></p> <pre> +---+---+   0   0   P   T   +---+---+</pre> | <p>A RFC 3306 redefiniu o campo Flags, acrescentando-lhe mais um bit.</p> <p>Caso o valor da flag P seja 0, então o endereço contido na mensagem é definido na RFC3513 (endereço base).</p> <p>Caso o valor da flag P seja um, obrigatoriamente a flag T também tem de ser um. Indica que se está perante um endereço <i>Unicast-Based</i>.</p> |
| <p><b>Scope</b></p>                                                   | <p>Igual à versão anterior</p>                                                                                                                                                                                                                                                                                                                  |
| <p><b>Reserved</b></p>                                                |                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>Plen</b></p>                                                    |                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>Network Prefix</b></p>                                          |                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>Group IP</b></p>                                                | <p>Campo de 32 bits que contém o endereço do grupo multicast.</p> <p>Para definir correctamente o grupo multicast devem-se usar as linhas de orientação definidas na RFC 3307.</p>                                                                                                                                                              |

Tabela 4.5 - formatos das mensagens e descrição de cada uma delas 3306



#### 4.2.2 Embedded RP

*“The 'Embedded RP' technique allows for easier and simpler deployment of IP multicast, and complements the IPv6 multicast architecture, especially when Source-Specific Multicast (SSM) is unavailable or unsuitable”* - Pekka Savola, co-autor da técnica *Embedded RP*.

A técnica *Embedded RP* (RFC 3956) estende a RFC 3306, especificando um método para codificar num endereço multicast, endereço do RP (*Rendezvous Point*) (ver secção PIM-SM) . Esta está.

Na tabela seguinte são apresentados os formatos das mensagens e descrito em pormenor cada um deles. Convém referir que a gama para este tipo de endereços é iniciada sempre com o prefixo [FF70::/12]

|                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Flags</b><br><pre> +--+--+--+--+   0   R   P   T   +--+--+--+--+ </pre> | <p>A RFC 3306 redefiniu o campo Flags, acrescentando-lhe mais um bit.</p> <p>Caso o valor da flag R e P seja 0, então o endereço contido na mensagem é definido na RFC3513 (endereço base).</p> <p>Caso o valor da flag R seja um, obrigatoriamente a flag R e T tem de ser um também. Indica que se está perante um endereço <i>Embedded RP</i>.</p>                                                                                                 |
| <b>Scope</b>                                                               | <p>Igual à versão anterior</p> <p>Todos os bits a zero</p> <p>Também conhecido como Rpad, segundo a nomenclatura da Cisco. Contém o endereço do RP do PIM-SM RP.</p> <p>Define em hexadecimal o número de bits úteis no campo '<i>network prefix</i>'.</p> <p>O exemplo permite compreender o funcionamento. Imagine-se um site com um prefixo /48 (3FFE:FFFF:1:: /48). Este campo irá ter o valor de 30, que corresponde ao valor 48 em decimal.</p> |
| <b>Reserved</b>                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>RIID</b>                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Plen</b>                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Network Prefix</b>                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|          |                                                                                                                                                                                                                                                                                      |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>ser colocados a zero.</p> <p>Convém referir que, na secção 2.5.1 da RFC 2373, o prefixo associado a uma rede IPv6 está limitado a 64 bits, sendo os restantes usados para identificar a interface. Desta forma, se depreende o motivo deste campo estar limitado com 64 bits.</p> |
| Group IP | <p>Campo de 32 bits que contém o endereço do grupo multicast.</p>                                                                                                                                                                                                                    |

Tabela 4.6 - formatos das mensagens e descrição de cada uma delas 3956

Observando a figura seguinte é possível compreender de que forma é que o endereço IP do RP é retirado do endereço multicast.

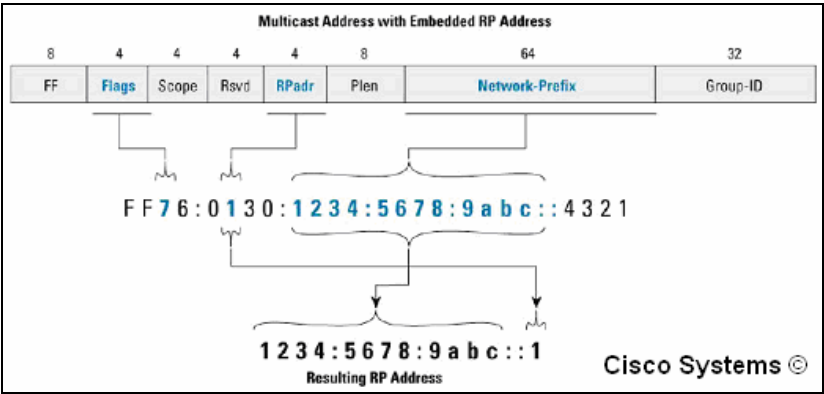


Figura 4.4 - Extracção do endereço RP de um endereço multicast

Desta forma, para um endereço multicast *Embedded RP* [FF76:0130:1234:5678:9ABC::4321], o RP embutido é [1234:5678:9ABC::1].

### 4.3 Endereçamento na camada 2

O mapeamento dos endereços IPv6 multicast para endereços MAC Ethernet é especificado na RFC 2464. A figura seguinte mostra o mapeamento dos 128bits do endereço multicast da camada 3, para os 48 bits do endereço MAC. É visível que apenas os 32 bits menos significativos são preservados, sendo os restantes perdidos no processo.

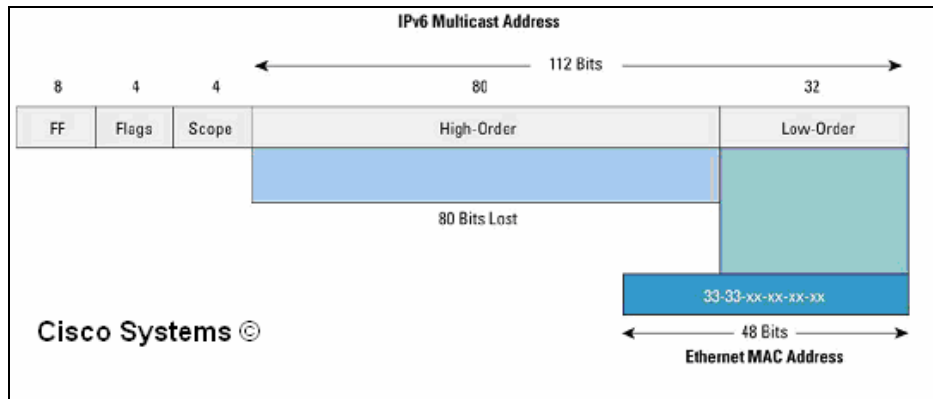


Figura 4.5 - Esquema com o mapeamento de um endereço da camada três para a camada dois

Observando um outro exemplo, este realizado em laboratório, é possível verificar que o endereço IP [FF1E::4321] foi adaptado para a camada dois como [33:33:00:00:43:21]

| No. -      | Time      | Source     | Destination | Protocol |
|------------|-----------|------------|-------------|----------|
| 1043 18.79 | 2001:a::2 | ff1e::4321 | UDP         |          |
| 1044 18.81 | 2001:a::2 | ff1e::4321 | UDP         |          |
| 1045 18.82 | 2001:a::2 | ff1e::4321 | UDP         |          |
| 1046 18.86 | 2001:a::2 | ff1e::4321 | UDP         |          |
| 1047 18.88 | 2001:a::2 | ff1e::4321 | UDP         |          |
| 1048 18.92 | 2001:a::2 | ff1e::4321 | UDP         |          |

+ Frame 1045 (1378 bytes on wire, 1378 bytes captured)

Ethernet II, Src: Intel 58:f1:c0 (00:11:11:58:f1:c0), Dst: IPv6-Neighbor-Discovery\_00:00:43:21 (33:33:00:00:43:21)

Source: Intel\_58:f1:c0 (00:11:11:58:f1:c0)

Type: IPv6 (0x86dd)

Internet Protocol Version 6

Version: 6

Traffic class: 0x00

Flowlabel: 0x00000

Payload length: 1324

Next header: UDP (0x11)

Hop limit: 128

Source address: 2001:a::2

Destination address: ff1e::4321

+ User Datagram Protocol, Src Port: 1026 (1026), Dst Port: 1234 (1234)

Data (1316 bytes)

Figura 4.6 - Mapeamento de um endereço da camada três para a camada dois

## 5 Protocolos Multicast IPv6

Existem vários tipos de protocolos associados ao multicast. Desta forma, nesta secção são apresentados os principais protocolos e os mais utilizados actualmente. Numa primeira fase é efectuada uma distinção entre os dois grandes grupos de protocolos multicast, sendo posteriormente apresentados os detalhes de funcionamento para protocolos usados no IPv6.

### 5.1 Introdução aos protocolos Multicast

Quando se fala de *multicast*, é necessário distinguir dois cenários, LAN e WAN. Numa rede local é necessária a existência de um protocolo de controle, a entrada e saída dos *Hosts* nos grupos multicast, ao passo que, em redes WAN é necessário existir um protocolo de encaminhamento multicast que permita transportar os pedidos, através de vários equipamentos, desde a origem até aos destinatários.

O protocolo responsável pela gestão de grupos numa LAN no IPv4, é o IGMP (*Internet Group Management Protocol*), sendo que para IPv6 existe um outro, o MLD (*Multicast Listener Discovery*).

No que diz respeito a protocolos de encaminhamento multicast, em IPv4 existem vários, *Distance Vector Multicast Routing Protocol* (DVMRP), *Protocol Independent Multicast Dense Mode* (PIM-DM) e *Sparse-Mode* (PIM-SM). Ao passo que, no IPv6, actualmente apenas existe o PIM versão 6. Este é semelhante ao usado em IPv4, mas contém as devidas modificações para poder ser usado com o protocolo IPv6 [16].

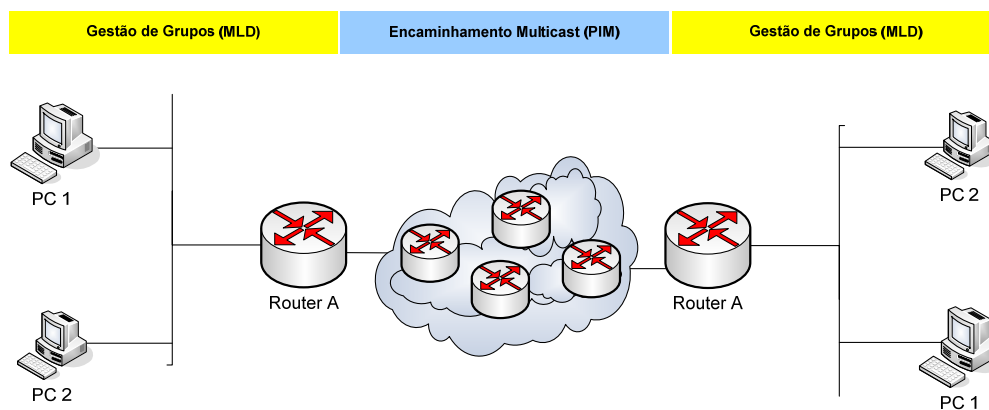


Figura 5.1 - Protocolos necessários em *multicast* IPv6

Desta forma, caso se pretenda implementar multicast numa rede, é necessário que o(s) router(s) suporte(m) protocolos de encaminhamento multicast. Caso a transmissão *multicast* ocorra entre máquinas dispersas pela Intranet, é necessário que todos os equipamentos, layer 2 e 3, suportem multicast. Caso isso não seja possível, é necessário usar mecanismos adicionais por forma a garantir a entrega dos pacotes em diferentes domínios.

## 5.2 Protocolo de Gestão de Grupos Multicast – MLDv1

Nesta secção, numa primeira fase, é apresentada uma descrição sumária do protocolo de gestão de grupos multicast de IPv6, MLD - *Multicast Listener Discovery*, sendo posteriormente descrito o formato dos pacotes e o funcionamento do protocolo.

### 5.2.1 Descrição sucinta

O protocolo MLD permite aos hosts comunicarem o **seu interesse em receberem tráfego** de uma fonte multicast específica – grupo multicast. Este protocolo é usado ao nível das sub-redes, e permite aos hosts trocarem informações com o router mais próximo. A informação enviada pelos hosts é usada pelos routers para que estes saibam, entre outras coisas, quais dos hosts vizinhos pretendem receber tráfego multicast.

O protocolo MLD é derivado da versão 2 do protocolo IGMP (*Internet Group Management Protocol*) existente no IPv4. Ou seja, com a chegada do protocolo IPv6, o IGMP deu lugar a um novo protocolo MLD, que possui algumas semelhanças e é derivado das versões 1 e 2 do seu antecessor IGMP [17][18].

Resumidamente, a finalidade do MLD é permitir a um router IPv6, descobrir a presença de ouvintes multicast (isto é, hosts que desejam receber pacotes multicast) nas interfaces directamente ligadas e descobrir especificamente quais os endereços multicast de que os vizinhos desejam receber tráfego. De seguida, esta informação é fornecida aos protocolos de encaminhamento multicast configurados no router, por forma a garantir que os pacotes são entregues em todas as interfaces onde existam hosts interessados. [18].

As principais diferenças entre o MLD e o IGMP encontram-se no formato das mensagens e no formato do endereçamento. O MLD utiliza mensagens ICMPv6 (*Internet Control Management Protocol version 6*), ao contrário do IGMP, que possui mensagens independentes do protocolo ICMP [14].

### 5.2.2 Formato das mensagens

O MLD é um sub-protocolo do ICMPv6, isto é, as mensagens MLD estão contidas dentro das mensagens ICMPv6, e são identificadas no cabeçalho IPv6 com o valor do Next\_Header de 0x3a. (ver figura seguinte). Além disso, todas as mensagens MLD são enviadas usando o endereço IPv6 de origem Link-Local.

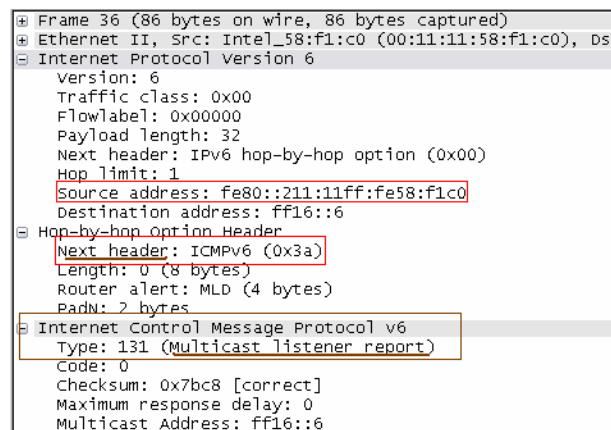


Figura 5.2 - Formato das mensagens MLD

O Hop-limit contém o valor 1, garantindo desta forma que o pacote nunca irá sair da sub-rede local, além disso, usa no cabeçalho Hop-by-Hop, a opção router alert. Desta forma, esta opção obriga os routers a examinar mensagens para endereços multicast que não lhes interesse.

A figura seguinte apresenta o formato das mensagens MLD e, posteriormente, é efectuada a respectiva explicação de cada um dos campos.

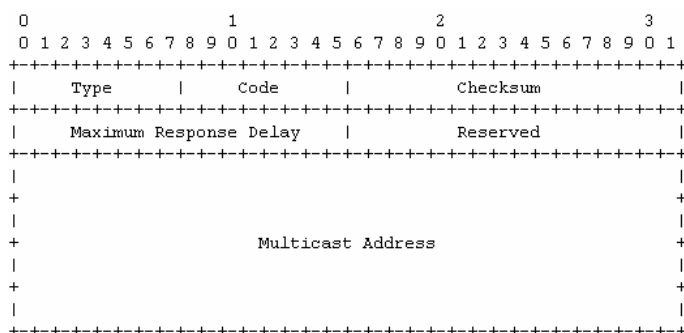


Figura 5.3 - Formato dos pacotes MLDv1

### Descrição das mensagens do protocolo MLD

| Type                                                                                                                                                                                             | Existem três tipos de mensagens MLD, as quais são apresentadas nas tabelas seguintes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                           |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                  | O primeiro tipo, <b>Multicast Listener Query (x130)</b> , subdivide-se em três, tal como se verifica de seguida. Convém referir que uma mensagem deste tipo é sempre enviada pelos routers.                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                           |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
|                                                                                                                                                                                                  | <table><thead><tr><th>Tipo</th><th>SubTipo</th><th>Descrição</th></tr></thead><tbody><tr><td rowspan="2"><b>Multicast Listener Query (x130)</b></td><td><i>General Query</i></td><td>Enviadas, em intervalos regulares, para descobrir quais os hosts e quais os grupos a que estes pertencem.</td></tr><tr><td><i>Multicast-Address-Specific Query</i></td><td>Enviadas como resposta a uma mensagem <b>MLD - Multicast Listener Done</b>. Usada com o objectivo de aprender se um determinado grupo ainda tem membros associados num segmento de rede.</td></tr></tbody></table> |                                                                                                                                                                                           |           | Tipo | SubTipo   | Descrição                               | <b>Multicast Listener Query (x130)</b>                                                                                                                                                       | <i>General Query</i> | Enviadas, em intervalos regulares, para descobrir quais os hosts e quais os grupos a que estes pertencem. | <i>Multicast-Address-Specific Query</i> | Enviadas como resposta a uma mensagem <b>MLD - Multicast Listener Done</b> . Usada com o objectivo de aprender se um determinado grupo ainda tem membros associados num segmento de rede. |
|                                                                                                                                                                                                  | Tipo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | SubTipo                                                                                                                                                                                   | Descrição |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
| <b>Multicast Listener Query (x130)</b>                                                                                                                                                           | <i>General Query</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Enviadas, em intervalos regulares, para descobrir quais os hosts e quais os grupos a que estes pertencem.                                                                                 |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
|                                                                                                                                                                                                  | <i>Multicast-Address-Specific Query</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Enviadas como resposta a uma mensagem <b>MLD - Multicast Listener Done</b> . Usada com o objectivo de aprender se um determinado grupo ainda tem membros associados num segmento de rede. |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
| <p>- Como é visível, ambas as mensagens anteriores possuem o mesmo valor hexadecimal (x130). Desta forma, as mensagens são diferenciadas pelo valor que contêm no campo “Multicast Address”.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                           |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
|                                                                                                                                                                                                  | <table><thead><tr><th>Tipo</th><th>Descrição</th></tr></thead><tbody><tr><td><b>Multicast Listener Report (x131)</b></td><td>Usada pelos <b>hosts multicast</b> para indicarem o seu interesse em receber tráfego <i>multicast</i> de um endereço específico, ou para responderem a uma <i>query</i> enviada pelo router.</td></tr></tbody></table>                                                                                                                                                                                                                                |                                                                                                                                                                                           |           | Tipo | Descrição | <b>Multicast Listener Report (x131)</b> | Usada pelos <b>hosts multicast</b> para indicarem o seu interesse em receber tráfego <i>multicast</i> de um endereço específico, ou para responderem a uma <i>query</i> enviada pelo router. |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
| Tipo                                                                                                                                                                                             | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                           |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |
| <b>Multicast Listener Report (x131)</b>                                                                                                                                                          | Usada pelos <b>hosts multicast</b> para indicarem o seu interesse em receber tráfego <i>multicast</i> de um endereço específico, ou para responderem a uma <i>query</i> enviada pelo router.                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                           |           |      |           |                                         |                                                                                                                                                                                              |                      |                                                                                                           |                                         |                                                                                                                                                                                           |

|                               | Tipo                                                                                                                                                                                                                                                                              | Descrição                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|                               | <b>Multicast Listener Done (x132)</b>                                                                                                                                                                                                                                             | Usada pelos <b>hosts</b> que pretendem deixar de receber tráfego de certo endereço <i>multicast</i> . |
| <b>Code</b>                   | Sempre '0'                                                                                                                                                                                                                                                                        |                                                                                                       |
| <b>Checksum</b>               | 16 bits reservados para correcção de erros. Estes bits fazem a validação de todo o pacote, isto é, validam o pacote MLD.                                                                                                                                                          |                                                                                                       |
| <b>Maximum Response Delay</b> | <p>O campo <b>Maximum Response Delay</b> contém um valor que especifica o tempo máximo permitido que um host pode esperar antes de enviar uma resposta (report).</p> <p>Com excepção das mensagens <b>Query</b>, este campo contém o valor "0" e é ignorado pelos receptores.</p> |                                                                                                       |

Tabela 5.1 - Formado e descrição das mensagens MLDv1

### 5.2.3 Funcionamento do protocolo

Nesta secção, é apresentado, de forma detalhada, o funcionamento do protocolo MLD

#### MLD “Join”

Quando um *host* pretende receber uma *stream* multicast, este envia uma mensagem “**Multicast Listener Report (x131)**” para o grupo multicast a que se deseja associar. Coloca no campo Hop-Limit o valor 1, o que implica que estes pacotes não vão ultrapassar o router local.

Na figura seguinte é ilustrado o processo de “MLD join”. É visível que o host com o IP [FE80::211:11FF:FE58:F1C0] se deseja associar a um grupo multicast. Mais concretamente, esta figura foi retirada após ter configurado o VLC para se associar ao grupo [FF16::6].

|                                                                                                                                                                                                                                                                                                                                                                                                        |       |                          |             |          |                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------------|-------------|----------|---------------------------|
| Filter: icmpv6                                                                                                                                                                                                                                                                                                                                                                                         |       |                          |             |          |                           |
| No. ↓                                                                                                                                                                                                                                                                                                                                                                                                  | Time  | Source                   | Destination | Protocol | Info                      |
| 29                                                                                                                                                                                                                                                                                                                                                                                                     | 13.38 | fe80::211:11ff:fe58:f1c0 | ff16::6     | ICMPv6   | Multicast listener report |
| 50                                                                                                                                                                                                                                                                                                                                                                                                     | 18.88 | fe80::211:11ff:fe58:f1c0 | ff16::6     | ICMPv6   | Multicast listener report |
| 72                                                                                                                                                                                                                                                                                                                                                                                                     | 26.88 | fe80::211:11ff:fe58:f1c0 | ff02::2     | ICMPv6   | Multicast listener done   |
| Frame 29 (86 bytes on wire, 86 bytes captured)<br>Ethernet II, Src: Intel_58:f1:c0 (00:11:11:58:f1:c0), Dst: IPv6-Neighbor-Discovery_00:00:00:00:00:00<br>Internet Protocol Version 6<br>Hop-by-hop Option Header<br>Internet Control Message Protocol v6<br>Type: 131 (Multicast listener report)<br>Code: 0<br>Checksum: 0x7bc8 [correct]<br>Maximum response delay: 0<br>Multicast Address: ff16::6 |       |                          |             |          |                           |



Figura 5.4 - Processo de Join no MLD

Visto que esta mensagem é enviada, ao nível do IP, para o grupo multicast desejado, todos os hosts que já pertençam a esse grupo vão escutar essa mensagem.

### MLD “Query”

Quando num segmento de rede existem dois routers, é necessária a existência de um método que permita a selecção de apenas um deles como sendo o responsável pelo dito segmento. Ou seja, quando existem dois routers é necessário eleger o *Querier Router*, ou seja, o router que vai receber os pedidos dos hosts directamente ligados àquele segmento de rede.

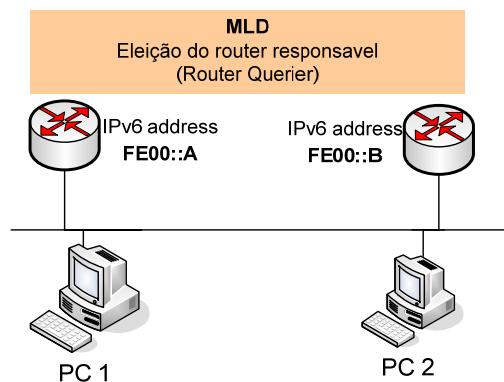


Figura 5.5 - Eleição do Router Querier

Efectivamente, quando se configura um router com o MLD, este auto intitula-se o *Querier Router* e começa a enviar mensagens “**Multicast Listener Query**” para a rede e todos os equipamentos, inclusive outros routers, vão “escutar” a mensagem.

Quando um router detecta uma **Querie** enviada por outro router **com o endereço IP inferior ao dele**, deixa de actuar como *Querie Router* e entra em modo *Nonquerier*. Mantém-se neste modo até que deixe de escutar mensagens “**Queries**” enviadas pelo router responsável, mensagens essas que são enviadas em intervalos regulares. Ou seja, caso este não detecte mensagens deste tipo, ele volta a assumir a posição de chefia, tornando-se novamente o “*Querie Router*”.

Nas figuras seguintes são visíveis dois routers “MLD enable” na mesma subrede.

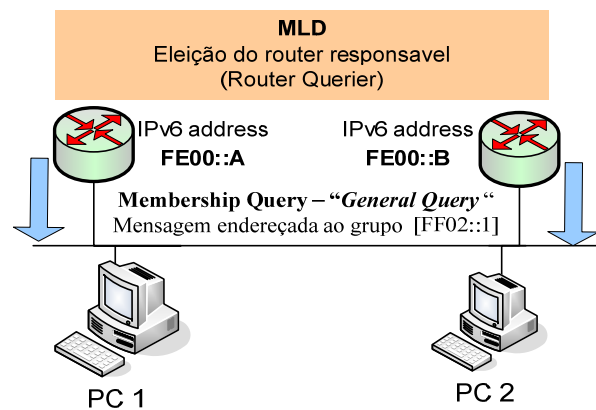


Figura 5.6 - Eleição do router responsavel (Querier Router)

Como foi referido anteriormente, o MLD especifica que apenas pode existir um router “Querier” por interface de rede e, sempre que existir mais do que um, é necessário proceder a uma eleição que tem como mecanismo de desempate o endereço IP.

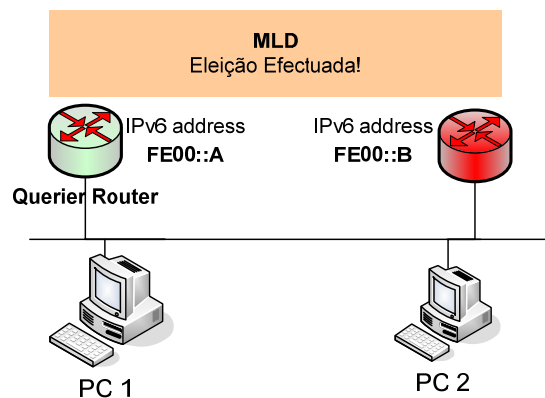


Figura 5.7 - Querier Router responsavel

Com o protocolo MLD, tal como na versão 2 do IGMP, é necessário os routers informarem os hosts de quanto tempo eles têm para responder a uma query. Esta funcionalidade é conhecida como **Maximum Response Delay** e é usada para otimizar o protocolo.

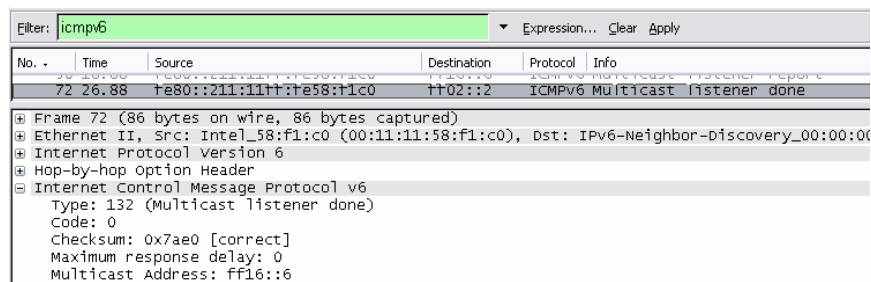
| Filter: icmpv6.type == 130                                                                                                                                                                                                                                                                                                                                                                                          |        |                          |             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------------------|-------------|
| No.                                                                                                                                                                                                                                                                                                                                                                                                                 | Time   | Source                   | Destination |
| 149                                                                                                                                                                                                                                                                                                                                                                                                                 | 49.46  | fe80::213:19ff:fe59:f1e0 | ff02::1     |
| 605                                                                                                                                                                                                                                                                                                                                                                                                                 | 174.46 | fe80::213:19ff:fe59:f1e0 | ff02::1     |
| 620                                                                                                                                                                                                                                                                                                                                                                                                                 | 217.79 | fe80::213:19ff:fe59:f1e0 | ff02::1     |
| Frame 149 (90 bytes on wire, 90 bytes captured)<br>Ethernet II, Src: Cisco_59:f1:e0 (00:13:19:59:f1:e0), Dst: ff02::1<br>Internet Protocol Version 6<br>Hop-by-hop Option Header<br>Internet Control Message Protocol v6<br>Type: 130 (Multicast listener query)<br>Code: 0<br>Checksum: 0x4a4a [correct]<br>Maximum response delay[ms]: 10000<br>Multicast Address: ::<br>S Flag: OFF<br>Robustness: 2<br>QQI: 125 |        |                          |             |

Figura 5.8 - Mensagem MLQ – “General Query”

Como é visível na imagem anterior, as mensagens Multicast Listener Query - “General Query”, são enviadas para o endereço de todos os hosts de uma subrede – [FF02::1] e contêm, no campo Multicast Address, o endereço nulo (::).

### MLD “Leave”

Usando o MLD é possível um *Host* informar explicitamente o router que quer abandonar um grupo multicast especificamente. Desta forma, um host que não deseje receber tráfego de um grupo multicast, envia ao router (Querie Router) uma mensagem do tipo “**Multicast Listener Done**” para o endereço [FF02::2]. Este endereço representa todos os routers multicast, ou seja, todos os routers necessitam de estar associados a este grupo.



The image shows a Wireshark packet capture window. The filter is set to 'icmpv6'. The packet list shows a packet at time 26.88 from source fe80::211:11ff:fe58:1c0 to destination ff02::2. The packet details pane shows the following structure:

| No. | Time  | Source                  | Destination | Protocol | Info                    |
|-----|-------|-------------------------|-------------|----------|-------------------------|
| 72  | 26.88 | fe80::211:11ff:fe58:1c0 | ff02::2     | ICMPv6   | Multicast Listener Done |

Packet details (Frame 72):

- Frame 72 (86 bytes on wire, 86 bytes captured)
- Ethernet II, Src: Intel\_58:f1:c0 (00:11:11:58:f1:c0), Dst: IPv6-Neighbor-Discovery\_00:00:00:00:00:00
- Internet Protocol Version 6
- Hop-by-hop Option Header
- Internet Control Message Protocol v6
  - Type: 132 (Multicast listener done)
  - Code: 0
  - Checksum: 0x7ae0 [correct]
  - Maximum response delay: 0
  - Multicast Address: ff16::6

Figura 5.9 - Mensagem “Multicast Listener Done”

O router, depois de receber a mensagem anterior, executa um pequeno algoritmo com o intuito de saber se existem mais hosts interessados em receber tráfego do grupo específico. Ou seja, o router depois de receber uma mensagem com o pedido de abandono, MLD Leave, necessita de saber se existem mais hosts, naquela subrede, interessados em receber pacotes do grupo [FF16::6]. Se não existirem, este pode efectivamente deixar de enviar tráfego multicast para a interface de onde recebeu os pedidos.

Desta forma, o router depois de receber uma mensagem MDL Leave, envia uma mensagem **Membership Query** – “*Group Specific Query*” para o grupo em questão (No exemplo anterior, o router envia para o grupo [FF16::6]). Esta mensagem contém um time-out associado, enviado no campo **Maximum Response Delay**, que especifica o tempo máximo permitido que um host pode esperar, antes de enviar uma resposta para dizer que deseja receber tráfego do grupo em questão.

Desta forma, se ainda existirem mais interessados, estes devem responder dentro do tempo definido pelo router, para que este continue a enviar pacotes para esse grupo. Se passado esse tempo nenhum host responder, o router volta a enviar um pacote igual ao anterior. Se mesmo assim, não existir resposta, ele deixa de enviar pacotes multicast para o grupo específico.

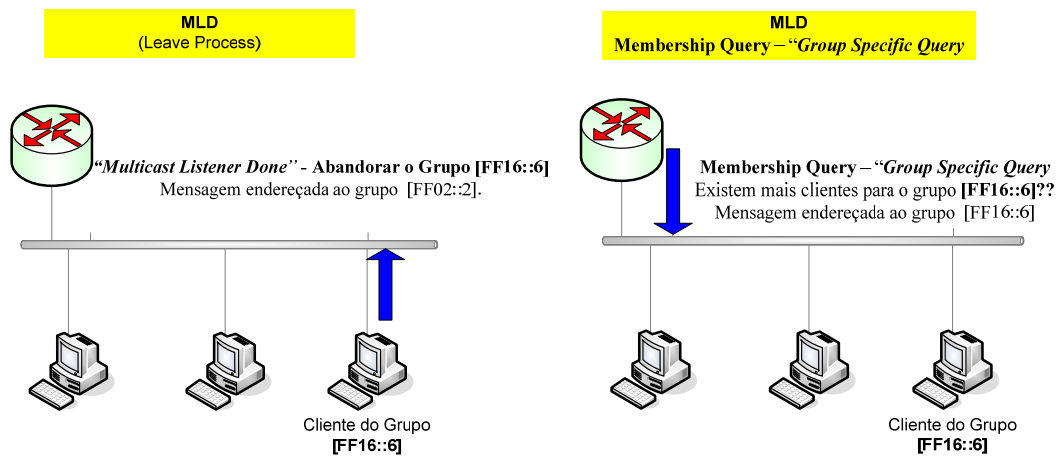
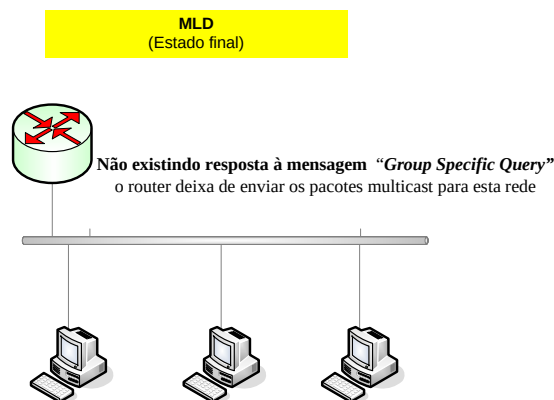


Figura 5.10 - Funcionamento do processo MLD Leave – fase inicial

As figuras anteriores ilustram o funcionamento que foi detalhado em cima. Na primeira, é visível um host a informar o router que não deseja receber dados de um grupo específico [FF16::6]. Ao passo que na segunda, é visível o envio, por parte do router, de uma mensagem **Membership Query – “Group Specific Query**, como resposta à mensagem enviada pelo host. Este processo é repetido duas vezes por omissão antes do router deixar definitivamente de enviar tráfego.

Na figura seguinte está representado o caso em que nenhum host respondeu às mensagens enviadas pelo router e onde foi removida a associação da interface ao grupo [FF16::6].



Funcionamento do processo MLD Leave – fase final

## 5.3 Protocolo de Gestão de Grupos Multicast – MLDv2

Nesta secção é apresentada uma descrição sumária da versão 2 do protocolo de gestão de grupos multicast de IPv6, MLDv2 - *Multicast Listener Discovery*, numa primeira fase, sendo posteriormente descrito o formato dos pacotes e o funcionamento deste.

### 5.3.1 Descrição sucinta

O MLDv2 é uma tradução do protocolo IGMPv3 [RFC3376] para a semântica do IPv6. Este, quando comparado com o MLDv1, adiciona suporte para filtragem da fonte, ou seja, possibilita a um host obter conteúdos de apenas uma fonte específica, tal como é requerido pelo modelo SSM – Source-Specific Multicast, ou obter conteúdos de todas as fontes menos uma fonte em particular. Desta forma, existe também um melhoramento na segurança.

Conceptualmente, o MLDv2 é composto por um conjunto de registos, havendo para cada um deles, um filtro e um conjunto de endereços dos servidores fonte. O filtro poderá ser: INCLUDE ou EXCLUDE. O modo INCLUDE, indica que o host vai aceitar tráfego oriundo da lista de fontes que tem configurada. No modo Exclude, a recepção de pacotes continua activa, pode receber conteúdos de todas as fontes, com excepção da lista de fontes que tem configurada.

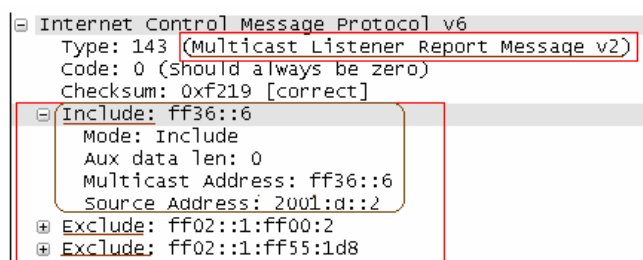


Figura 5.11 - Mensagem MLDv2 – grupos Include e Exclude

A figura anterior, captada com o Ethereal, contém uma mensagem MLDv2. Através desta, é possível observar os dois modos apresentados, o modo Include e o modo Exclude. Se se observar o rectângulo em volta do grupo Include, é visível, por exemplo, que o Host vai , para o endereço multicast [FF36::6] apenas aceitar tráfego oriundo do servidor com o endereço [2001:d::2]. Observando a figura, é visível que uma interface pode conter mais do que um registo/endereço.

As mensagens enviadas pelos hosts contêm sempre o mesmo endereço multicast de destino, possuindo o valor [FF02::16]. Este endereço foi definido especificamente para o MLDv2 e significa, todos os

routers com suporte para o protocolo MLDv2 (ALL-MLDv2-CAPABLE-ROUTES) [google: multicast ipv6 address].

### **5.3.2 Formato das mensagens**

O MLDv2, como foi mencionado, é uma actualização ao protocolo MLDv1, como tal, este continua a ser um sub-protocolo do ICMPv6, estando as mensagens MLDv2 contidas nas mensagens ICMPv6.

Essencialmente existem dois tipos de mensagens utilizadas no MLDv2

Multicast Listener Query (130)

Multicast Listener Report Version 2 (143)

De modo a garantir a interoperabilidade entre hosts que apenas suportem a versão 1 do MLD, foi necessário criar os dois tipos de mensagens seguintes:

Multicast Listener Report Version 1 (131)

Multicast Listener Done Version 1 (132)

#### **Mensagem ‘Multicast Listener Query’**

As mensagens Multicast Listener Query são enviadas pelos routers multicast para questionar os Hosts ligados sobre o interesse destes em receber tráfego multicast. As mensagens deste tipo possuem o seguinte cabeçalho (retirado da RFC 3810)

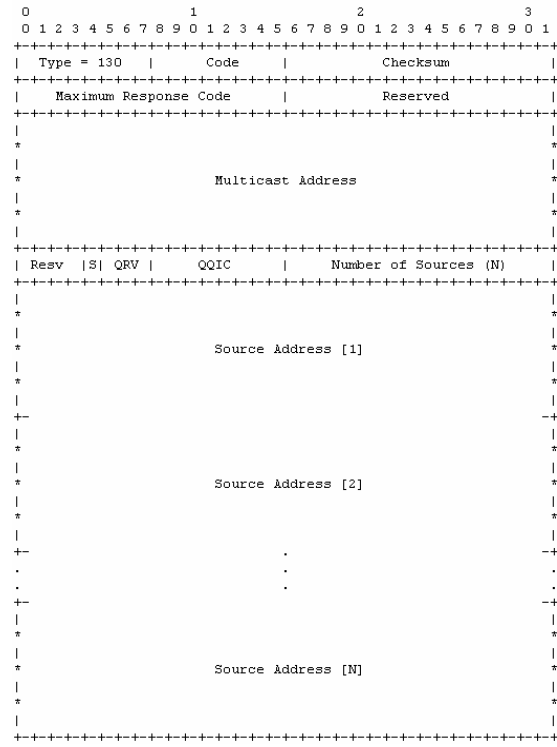


Figura 5.12 - Mensagem MLDv2 – Multicast Listener Query’

No MLDv2 existem três tipos de mensagens “Query”, ao passo que no MLDv1 apenas existiam duas:

*General Queries*

*Multicast Address Specific Queries*

*Multicast Address and Source Specific Queries*

|      |                                                                                            |               |                                                                                                                                                                                                                                                                                                                           |
|------|--------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type | Uma mensagem do tipo <b>Multicast Listener Query</b> é sempre enviada pelos <b>routers</b> |               |                                                                                                                                                                                                                                                                                                                           |
|      | Tipo                                                                                       | SubTipo       | Descrição                                                                                                                                                                                                                                                                                                                 |
|      | Multicast Listener Query (x130)                                                            | General Query | Enviadas, em intervalos regulares, para descobrir quais os hosts e quais os grupos a que estes pertencem.<br><br>Numa mensagem deste tipo, os campos <b>Multicast Address</b> e <b>Number of Sources (N)</b> são colocados a zero, e a mensagem é enviada para o endereço que identifica todos os <i>Hosts</i> [FF02::1]. |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <div data-bbox="785 145 1225 468" data-label="Code-Block"> <pre> Internet Protocol Version 6 Version: 6 Traffic class: 0xe0 Flowlabel: 0x00000 Payload length: 36 Next header: IPv6 hop-by-hop option (0x00) Hop limit: 1 Source address: fe80::213:19ff:fe59:ef80 Destination address: ff02::1 Hop-by-hop Option Header Internet Control Message Protocol v6 Type: 130 (Multicast listener query) Code: 0 Checksum: 0x4caa [correct] Maximum response delay[ms]: 10000 Multicast Address: :: S Flag: OFF Robustness: 2 QQI: 125 </pre> </div> <p><b>Multicast-Address-Specific Query</b></p> <p>Enviadas como resposta a uma mensagem <b>MLD - Multicast Listener Done</b>. Usada com o objectivo de aprender se um determinado grupo ainda tem membros associados num segmento de rede.</p> <p><b>Multicast Address and Source Specific Query</b></p> <p>Enviada com o objectivo de descobrir se existem Hosts interessados em receber dados de um servidor específico.</p> <p>Numa mensagem deste tipo, o campo <b>Multicast Address</b> contém o grupo multicast do grupo e o <b>Source Address[I]</b> contém o(s) endereço(s) do servidor de origem.</p> <p>As mensagens <b>Multicast Address Specific</b> e <b>Multicast Address and Source Specific Queries</b> contêm o IP destino igual ao grupo multicast de interesse.</p> <div data-bbox="802 1310 1249 1684" data-label="Code-Block"> <pre> Internet Protocol Version 6 Version: 6 Traffic class: 0xe0 Flowlabel: 0x00000 Payload length: 52 Next header: IPv6 hop-by-hop option (0x00) Hop limit: 1 Source address: fe80::213:19ff:fe59:ef80 Destination address: ff36::6 Hop-by-hop Option Header Internet Control Message Protocol v6 Type: 130 (Multicast listener query) Code: 0 Checksum: 0x503b [correct] Maximum response delay[ms]: 1000 Multicast Address: ff36::6 S Flag: OFF Robustness: 2 QQI: 125 Source Address: 2001:d::2 (2001:d::2) </pre> </div> |
| <b>Code</b>     | Obrigatório ser '0'                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Checksum</b> | 16bits reservados para correcção de erros. Estes bits fazem a validação de todo o pacote, isto é, validam os 8bytes do pacote IGMP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



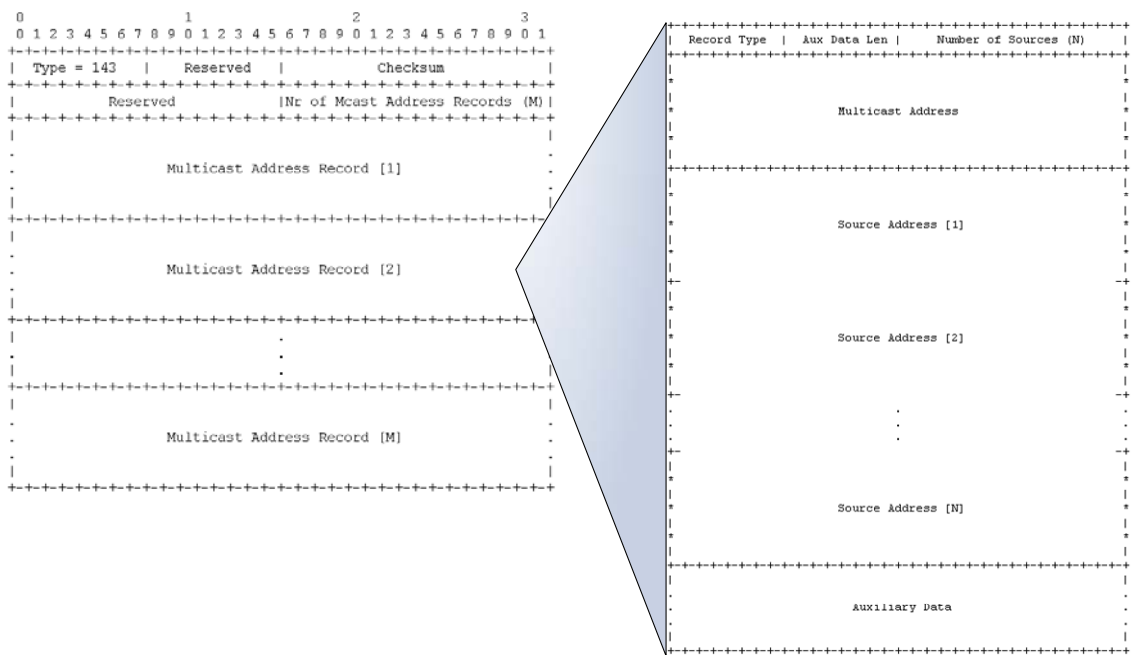
|                               |                                                                                                                                                                                                                                                                                                            |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum Response Delay</b> | <p>O campo <b>Maximum Response Delay</b> contém um valor que especifica o tempo máximo permitido que um host pode esperar antes de enviar uma resposta (report).</p> <p>Com excepção das mensagens <b>Query</b>, este campo contém o valor "0" e é ignorado pelos hosts receptores</p>                     |
| <b>Multicast Address</b>      | <p>Para uma mensagem <b>Multicast General Query</b> este campo é preenchido com zeros.</p> <p>Para mensagens <b>Multicast Address Specific Queries</b> e <b>Multicast Address and Source Specific Queries</b>, é constituído pelo endereço multicast do grupo ao qual o pacote pertence (ver secção X)</p> |
| <b>Number of Sources (N)</b>  | <p>Especifica o número de endereços de servidores que estão presentes na mensagem. Este valor é zero para mensagens <b>General Query</b> e <b>Multicast Address Specific Query</b>, e contém um valor diferente de zero para o outro tipo de mensagens Query.</p>                                          |
| <b>Source Address</b>         | <p>Endereço, ou lista de endereços unicast de servidores associados ao grupo multicast.</p>                                                                                                                                                                                                                |

Tabela 5.2 - Mensagens MLDv1

### Mensagem ‘Multicast Listener Report Version 2’

As mensagens **Multicast Listener Report Version 2** são utilizadas pelos **hosts multicast** para indicarem o seu interesse em receber, ou não, tráfego *multicast* de um endereço específico. São também usadas como resposta a uma *Query Message* enviada pelo Router.

As mensagens deste tipo possuem o seguinte cabeçalho (retirado da RFC 3810)



Mensagem MLDv2 – ‘Multicast Listener Report Version 2’

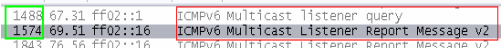
Descrição dos campos presentes numa mensagem ‘Multicast Listener Report Version 2’ [RFC 3810].

| Type                           | Caso este valor seja 143, então o pacote é do tipo ‘Multicast Listerner Report Version 2’.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                          |            |           |             |                      |                                                                                                          |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|------------|-----------|-------------|----------------------|----------------------------------------------------------------------------------------------------------|
| Chechsum                       | 16 bits reservados para correcção de erros. Estes bits fazem a validação de todo o pacote, isto é, validam o pacote MLD.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                          |            |           |             |                      |                                                                                                          |
| Nr of Mcast Address Records(M) | Especifica o número de campos ‘Multicast Address Record’ que o pacote MLD possui.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                          |            |           |             |                      |                                                                                                          |
| Multicast Address Record [n]   | <div>Contém vários sub-campos com informação de vários tipos (ver imagem anterior).</div> <table><tr><th>Tipos</th><th>Sub-Campos</th><th>Descrição</th></tr><tr><td>Record Type</td><td>Current State Record</td><td>Contém a lista de endereços multicast aos quais um Host deseja pertencer, ou deseja deixar de pertencer.</td></tr></table> <div><div>1574 69.51 fe80::206:5b55:1d8 ff02::16</div><div>1843 76.56 fe80::213:19ff:fe59:ef80 ff02::16</div><div>2249 86.93 fe80::206:5b55:1d8 ff02::16</div><div>Frame 1574 (146 bytes on wire, 146 bytes captured)</div><div>Ethernet II, Src: DellComp_55:01:d8 (00:06:5b:55:01:d8)</div><div>Internet Protocol Version 6</div><div>Hop-by-hop Option Header</div><div>Internet Control Message Protocol v6</div><div>Type: 143 (Multicast Listener Report Message v2)</div><div>Code: 0 (Should always be zero)</div><div>Checksum: 0xf219 [correct]</div><div>Include: ff36::6</div><div>Exclude: ff02::1:ff00:2</div><div>Exclude: ff02::1:ff55:1d8</div></div> | Tipos                                                                                                    | Sub-Campos | Descrição | Record Type | Current State Record | Contém a lista de endereços multicast aos quais um Host deseja pertencer, ou deseja deixar de pertencer. |
| Tipos                          | Sub-Campos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Descrição                                                                                                |            |           |             |                      |                                                                                                          |
| Record Type                    | Current State Record                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Contém a lista de endereços multicast aos quais um Host deseja pertencer, ou deseja deixar de pertencer. |            |           |             |                      |                                                                                                          |

Na imagem anterior, é visível um pacote,

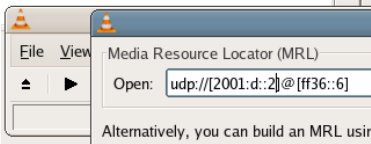
Na imagem anterior, é visível um pacote,

1574, a ser enviado para o endereço de todos os routers MLDv2.

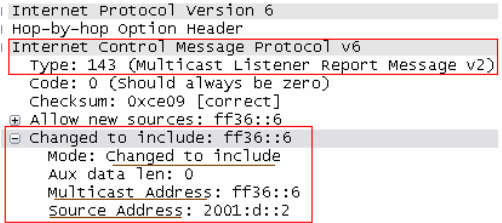


Uma mensagem deste tipo, é sempre enviada em resposta a uma mensagem ‘Query’.

**Filter** **Mode** Enviada pelos Hosts sempre que existe um  
**Change** pedido duma aplicação em receber multicast  
**Record** de um servidor-grupo específico.

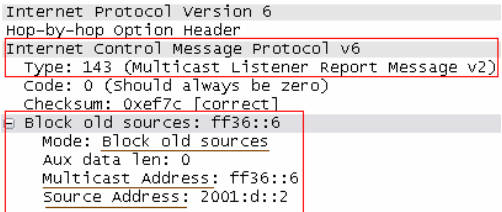


Depois de se ter configurado a aplicação, foi gerada a seguinte mensagem.



**Source** **List** Enviada pelos Hosts quando estes desejam  
**Change** deixar de receber tráfego de um grupo  
**Record** específico. Recorrendo ao exemplo utilizado,

depois de se ter terminado a aplicação, foi enviada uma mensagem deste tipo



**Aux Data Len**

Contém o tamanho do campo ‘Auxiliary Data’. Pode conter o valor zero (0), indicando desta forma que não existem dados auxiliares.

**Number** **of**  
**Sources (N)**

Especifica o número de endereços ‘Source Address’ que estão presentes no pacote.

**Multicast**

Contém o endereço multicast do **Multicast Address Record**, ao qual este pertence.

**Address**

**Source Address**

**[i]**

Lista de endereços unicast

**Auxiliary Data**

Actualmente este campo não tem nenhuma função. Este é reservado para futuras versões.

### 5.3.3 Funcionamento do protocolo MLDv2

Nesta secção, é apresentado de forma detalhada, o funcionamento do protocolo MLDv2.

#### MLDv2 “Join”

A versão 2 do MLD é significativamente diferente da versão anterior. A primeira grande diferença é que as mensagens MLDv2 são enviadas *out of band*, isto é, ao invés de enviar as mensagens para o grupo específico, os hosts enviam as mensagens para um endereço específico, [FF16::6].

| No.  | Time  | Destination | Protocol | Info                                 |
|------|-------|-------------|----------|--------------------------------------|
| 1574 | 69.51 | ff02::16    | ICMPv6   | Multicast Listener Report Message v2 |
| 1843 | 76.56 | ff02::16    | ICMPv6   | Multicast Listener Report Message v2 |
| 2249 | 86.93 | ff02::16    | ICMPv6   | Multicast Listener Report Message v2 |

Figura 5.13 - Envio de pacotes MLDv2 ‘Join’ para o endereço IP que representa todos os routers MLDv2

Visto que os pacotes são enviados desta forma, o router vai ficar a conhecer o interesse de todos os hosts no que se refere à associação com os grupos.

O processo de ‘Join’ foi extremamente melhorado, visto que uma mensagem deste tipo passa a conter o endereço do servidor e o grupo que se deseja inscrever.

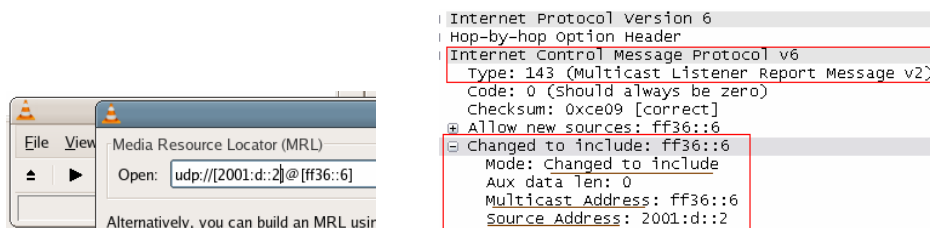


Figura 5.14 - Envio de um pacote MLDv2 ‘Join’ após pedido da aplicação

Na figura anterior é visível o envio de uma mensagem ‘Join’ (*Membership Listener Report*). Nesse exemplo, o Host pretende-se associar ao grupo [FF36::6], mas apenas deseja receber os pacotes de uma fonte específica [2001:d::2]. Isto significa que se existirem dois servidores associados ao mesmo grupo, ele apenas tem interesse em receber dados de um deles.

#### MLDv2 ‘Query Process’

Dado que a versão 2 do MLD possui um mecanismo de controlo de canal *out of band*, o processo de ‘Query’ difere das restantes versões [17]. Na versão anterior, apenas um host por grupo necessitava de responder a uma ‘General Query’. O objectivo era reduzir o tráfego MLD, mas um router não sabia

para quem estava a enviar o tráfego – *Protocolo Stateless*, apenas sabia que existia pelo menos um receptor por grupo multicast.

As ‘*Query*s’ do MLDv2 continuam a ser enviadas num intervalo específico, tal como acontece com a versão anterior, continuam a ser enviadas para o endereço que representa todos os hosts [FF02::1]. A grande diferença consiste no facto de, na versão 2, todos os hosts responderem a essa Query. Os hosts respondem para o endereço [FF02::16] e colocam no pacote de resposta os grupos em que estão interessados.

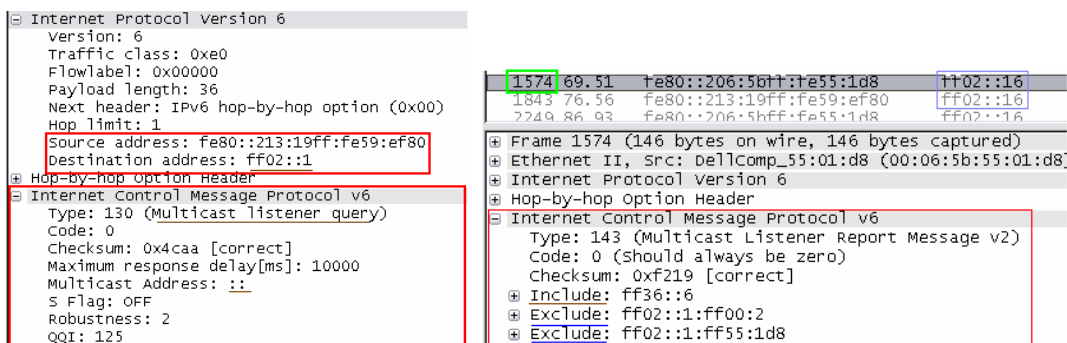


Figura 5.15 - MLDv2 “Query Process”

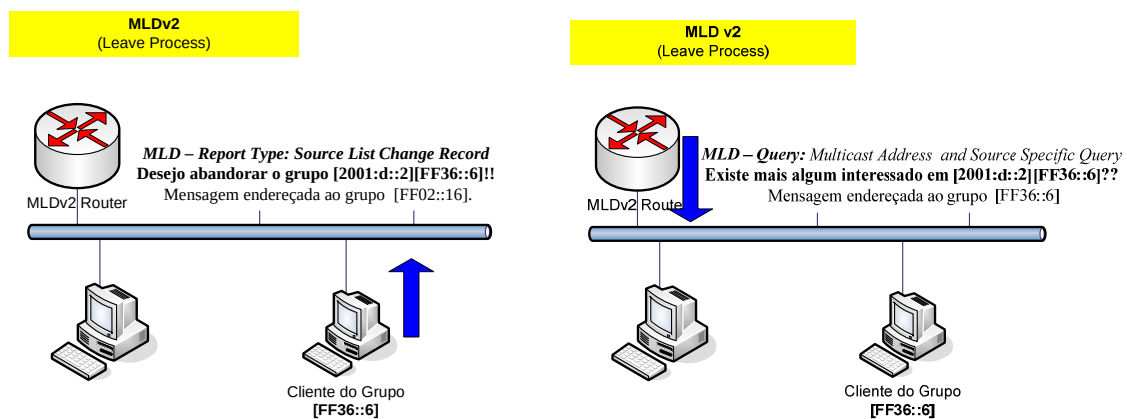
Na figura anterior, à esquerda, é visível uma mensagem MLDv2 ‘*Query*’. Na figura à direita é visível a resposta de um host informando quais os grupos a que este deseja continuar associado, ou quais os grupos a que este deseja deixar de pertencer.

### MLDv2 ‘Leave Process’

Na versão 2, o processo de desassociação pode ocorrer de duas formas distintas. A primeira é idêntica à versão 1, à excepção do endereço para o qual a mensagem de ‘*Leave*’ é enviada [FF02::16 na versão 2; FF02:2 na versão 1].

Por conseguinte, um router vai enviar mensagens “*Multicast-Address-Specific Query*” como resposta a mensagens “*Leave*” apenas para confirmar que não existem mais membros que desejam receber tráfego desse grupo.

Além disso, é possível a um receptor abandonar uma fonte específica (S) de um grupo. Neste caso, o router vai enviar uma “*Multicast Address and Source Specific Query*” para garantir que não existem mais receptores para o par Fonte(S)-Grupo(G).



Na figura anterior é apresentado um host que informa a rede que não deseja receber tráfego de uma fonte específica. Uma vez que o router recebeu a mensagem, este enviou uma mensagem “*Multicast Address and Source Specific Query*”.

## 5.4 Protocolos de encaminhamento Multicast

De modo a permitir a distribuição de conteúdos multicast num domínio alargado, constituído por vários equipamentos, é necessário o uso de protocolos específicos, com capacidades para lidar com os pacotes multicast. Existem vários protocolos deste tipo disponíveis para IPv4, mas no entanto, para IPv6 actualmente apenas existe um protocolo, conhecido como PIM (*Protocol Independent Multicast*).

Desta forma, nesta secção é apresentado de forma sucinta o protocolo PIM, numa fase inicial, sendo posteriormente detalhados os modos de funcionamento e as principais mensagens trocadas.

### 5.4.1 PIM

O protocolo PIM (*Protocol Independent Multicast*) pertence à família de protocolos de encaminhamento multicast e é usado para distribuir o tráfego pela Internet [20]. Este não possui nenhum método próprio para a descoberta da topologia da rede, usando a informação disponibilizada pelos protocolos de encaminhamento unicast. Desta forma, este protocolo usa as rotas apreendidas pelos protocolos unicast e é, devido a isso que é conhecido como '*Protocol Independent*'.

Actualmente existem quatro variantes do PIM [20],

PIM – SM (*Sparce Mode*), definido na RFC 2362

PIM – DM (*Dense Mode*), revisto em Janeiro de 2005 e publicado na RFC 3973

PIM – Bi-direccional, publicado no *draft-ietf-pim-bidir-08*

PIM – SSM (*Source Specific Multicast*), publicado na RFC 3569.

Embora existam as quatro variantes apresentadas, actualmente apenas dois deles têm divulgação. Convém também referir que, o PIM – DM não foi actualizado para IPv6 podendo apenas ser implementado em rede IPv4 [21].

Importa referir que dos quatro apresentados o mais utilizado actualmente é o PIM-SM [20]. Segundo [14] futuramente o PIM-SSM irá ter uma expansão em larga escala. Por conseguinte, neste relatório optou-se por descrever em pormenor, não apenas o PIM-SM, mas também o PIM-SSM.

### 5.4.2 PIM – SM

O protocolo PIM-SM foi inicialmente definido na RFC 2117. No entanto, esta encontra-se actualmente obsoleta, tendo sido substituída pela RFC 2362.

Segundo [3], o protocolo PIM – SM, tal como o nome indica, foi desenvolvido para encaminhar grupos multicast espalhados numa área dispersa. É ideal para grupos com reduzida percentagem de clientes finais, conhecidos na nomenclatura como *nodes*.

O PIM-SM requer um mecanismo onde é necessária a existência de um ponto central responsável por receber e tratar os pedidos de tráfego multicast enviados, quer pelos *nodes*, quer pelos servidores. Este mecanismo requer a existência de um caminho partilhado por todos os equipamentos envolvidos na comunicação, sendo este conhecido como *Core Based ou Shared Based Tree*.

De uma forma sucinta, para se usar o PIM-SM é necessária a existência de um ponto central responsável por controlar a distribuição de tráfego multicast na rede. Este ponto central é tecnicamente conhecido como RP (*Rendezvous Point*).

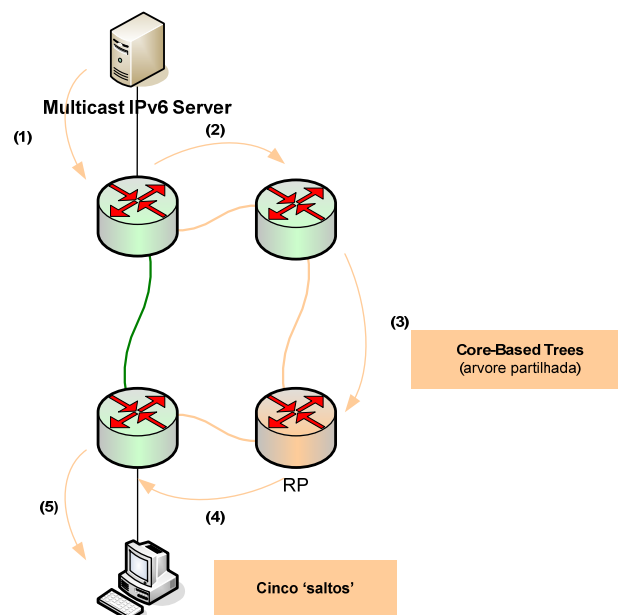


Figura 5.16 - Core Based Tree

A figura anterior ilustra o funcionamento básico do protocolo PIM-SM. Como é visível, existe um router central que necessita de conhecer todo o tráfego multicast que é enviado dentro do domínio PIM. Efectivamente, o router RP da figura é responsável por aceitar os pedidos oriundos dos clientes e por ‘controlar’ a difusão de pacotes multicast oriundos dos servidores.



Como se pode constatar pela figura, sempre que o servidor pretenda enviar pacotes multicast, este necessita de consultar o ponto central da rede e o mesmo acontece com os clientes. É também visível que, com o uso do PIM –SM nem sempre se usa o melhor caminho, caminho mais curto, para alcançar os destinatários. Efectivamente, no exemplo anterior, é necessário que os pacotes “passem” por quatro routers, o que implica que os pacotes multicast necessitem de dar cinco saltos para alcançar o cliente final.

O método de distribuição de tráfego utilizado no exemplo anterior é usado pelo PIM e é tecnicamente conhecido como *Core Based ou Shared Based Tree*.

O funcionamento apresentado na figura anterior representa o funcionamento do PIM –SM. No entanto, com a versão 2 do mesmo protocolo foi definido, para além do método já existente, um outro mais eficiente, onde os servidores podem comunicar directamente com os clientes depois de terem “permissão” para fazer parte do equipamento central da rede, o RP[14][20].

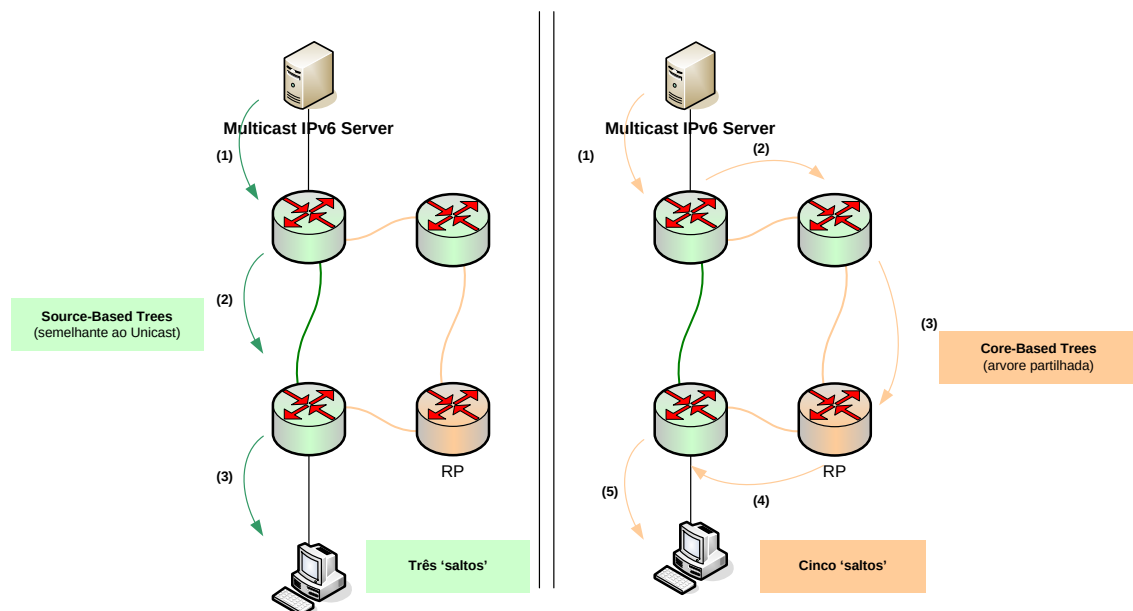


Figura 5.17 - Formulas existentes para distribuição de tráfego

A figura anterior demonstra as duas formas possíveis de distribuição de pacotes numa rede multicast. Como é visível na secção da esquerda, os pacotes enviados pelo servidor apenas necessitam de dar três saltos para alcançar os clientes, ao passo que na secção da direita, necessitam de cinco.

### Funcionamento do protocolo

Nesta secção é descrito o funcionamento do protocolo PIM-SM. É apresentado um cenário prático configurado e posteriormente apresentadas e documentadas as principais mensagens.

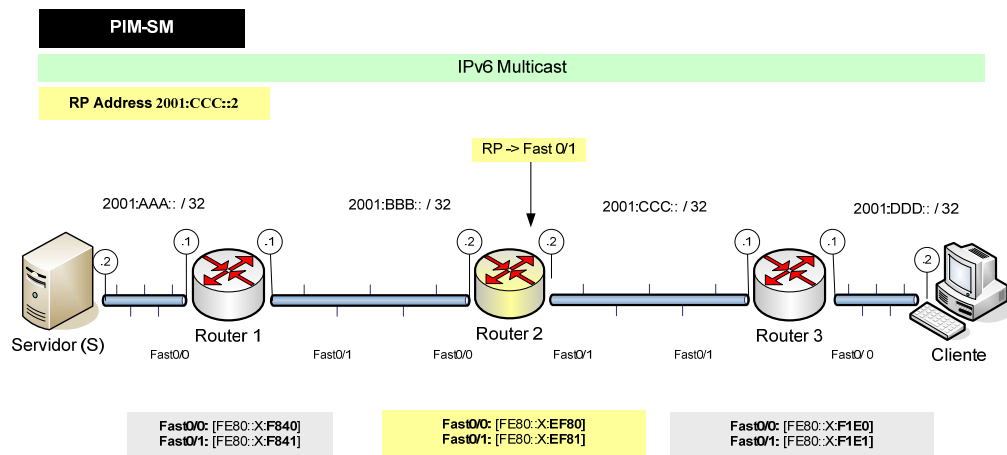


Figura 5.18 - Cenário implementado para verificar o funcionamento do PIM-SM

O cenário esquematizado na figura anterior foi implementado em laboratório com vista à compreensão do funcionamento do protocolo PIM-SM. O endereçamento usado foi [2001:AAA::/32], [2001:BBB::/32], [2001:CCC::/32] respectivamente, para o router 'Router1', 'Router2' e 'Router3'.

Na figura são também apresentados os endereços *Link-local* associados a cada equipamento, uma vez que assim, é possível saber efectivamente quais as mensagens trocadas pelos equipamentos.

Convém referir que as mensagens multicast PIM são sempre enviadas para o mesmo endereço. Esse endereço identifica todos os routers PIM e é definido pela IANA como sendo o IP [FF02::D]. Analisando as imagens seguintes, é possível comprovar o que acaba de ser descrito.

De uma forma sucinta, o PIM-SM possui os seguintes modos de operação:

Pedidos de Clientes

Registo no RP

RP Joining/pruning

### Pedidos de Clientes – Mensagens *Join*

Como é sabido, os clientes (*nodes*) que desejam receber tráfego multicast necessitam de informar o router mais próximo de qual o grupo a que estes se desejam associar. Por conseguinte, o router vai informar o RP do interesse dos clientes a ele directamente ligados.

Os routers locais, conhecidos como *Designated Router* (DR), quando recebem um pedido de um cliente, enviam uma mensagem *PIM-Join* com o grupo a que os clientes se desejam associar.

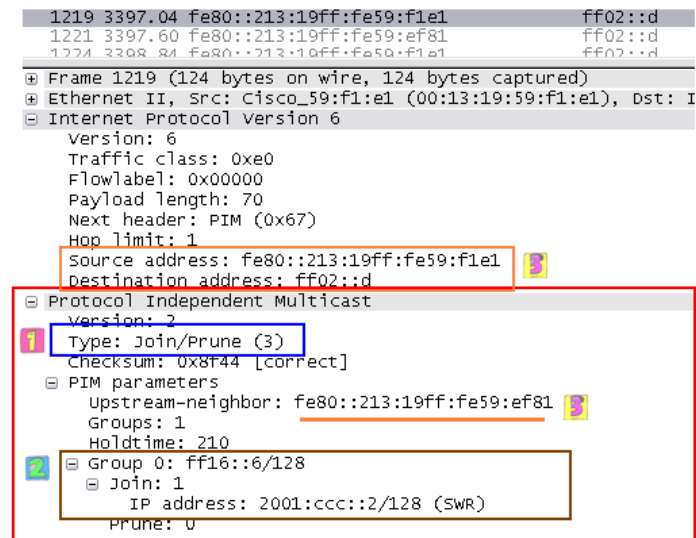


Figura 5.19 - Associação do cliente ao grupo multicast [FF16::6]

Na figura anterior é apresentado o funcionamento do protocolo PIM, ao nível da associação de clientes a grupos multicast. Mais concretamente, a figura anterior captada pelo Ethereal contém a mensagem *Join*, criada logo após o cliente se ter associado ao grupo [FF16::6].

Como é visível em , trata-se de uma mensagem PIM do tipo *Join/Prune*, enviada pelo PC cliente  e referente ao grupo multicast [FF16::6] .

### Registo no RP – Mensagens *Register*

Quando uma origem, por exemplo o **servidor (S)** da figura anterior, inicia uma difusão de pacotes multicast para um determinado grupo, o router mais próximo (Router 1) vai encapsular os pacotes em mensagens *Register* unicast e enviá-los para o RP associado ao grupo.

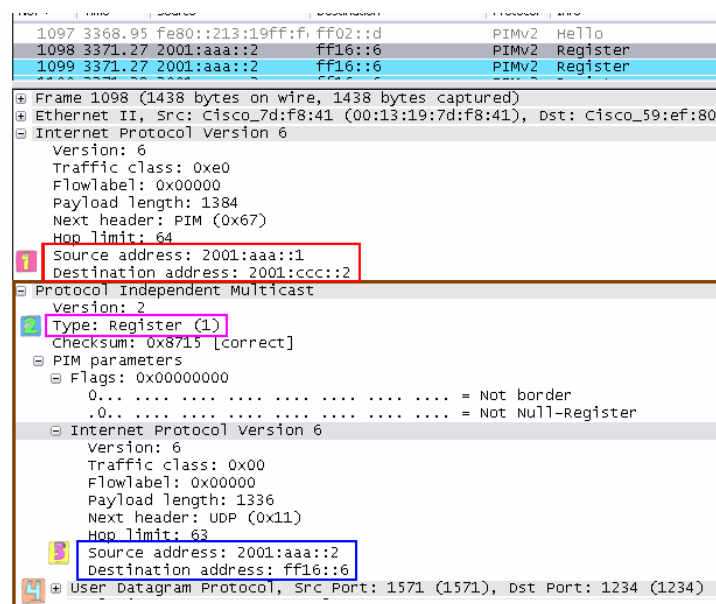


Figura 5.20 - Mensagem PIM-Register

A figura anterior foi captada após se ter colocado o servidor (S), com o IP 2001:AAA::2 a difundir pacotes multicast para o grupo [FF16::6] .

Como é visível em , as mensagens estão a ser enviadas para o endereço unicast [2001:CCC::2], endereço esse que corresponde ao RP configurado no router 2.

Observando , verifica-se que a mensagem é do tipo *Register* e contém encapsulada a mensagem original criada pelo servidor (S)  .

### RP Joining/pruning – Mensagens *Join*

Depois de receber a mensagem anterior, *PIM-Register*, o RP envia uma mensagem *Join* para o router mais próximo da fonte, o router 1 [2001:AAA::1]. Enquanto todos os routers intermédios, desde o RP até ao router da fonte, não receberem e processarem a mensagem *Join*, todas as mensagens multicast são encapsuladas em mensagens unicast. Nesta fase, o RP é responsável pela entrega destas mensagens para os membros do grupo.

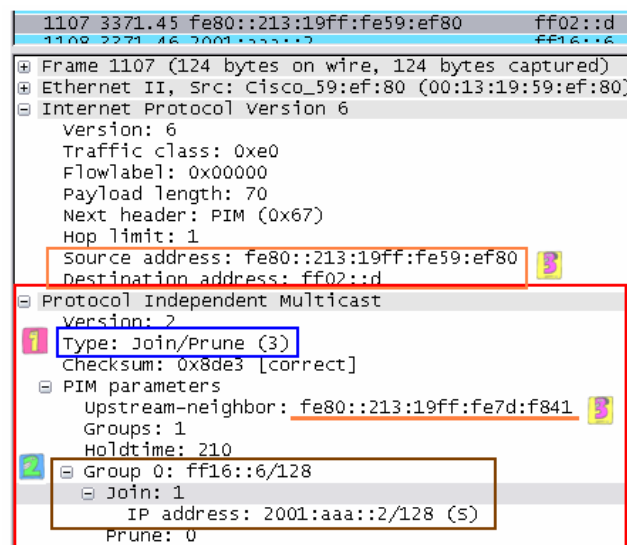


Figura 5.21 - Mensagem PIM-Join

No esquema anterior é visível uma mensagem PIM *Join*. . Se se observar , verifica-se que a mensagem é enviada do endereço do router 2 ([FE80::x:EF80]), para o endereço link-local do router 1 ([FE80::x::EF80]).

### Registo no RP – Mensagens *Register-Stop*

Quando o RP detecta que os pacotes multicast estão a ser entregues em multicast [Pim-SM], o RP envia uma mensagem *Register-Stop* ao router mais próximo da fonte. Desta forma, após a recepção de uma mensagem deste tipo o DR vai deixar de encapsular o tráfego multicast em unicast, passando assim a enviar apenas mensagens multicast.

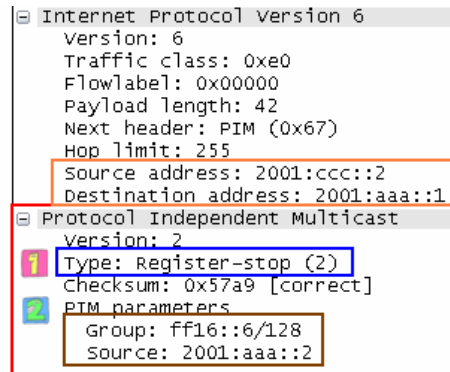


Figura 5.22 - Mensagem Register-Stop

O uso de uma árvore partilhada geralmente não é a melhor opção. Desta forma, na versão 2 do PIM, passou a ser possível o uso de árvores *Source-Based*. No entanto, usando o cenário anterior, não foi possível testar/analisar as mensagens trocadas.

### Descoberta do RP

O protocolo PIM-SM requer que todos os equipamentos tenham conhecimento do IP do RP, ou seja, este necessita de saber para onde enviar, por exemplo as mensagens *PIM- Register*. Deste modo, existem actualmente alguns métodos possíveis para efectuar essa “descoberta”, sendo os mais utilizados apresentados de seguida:

#### Configuração estática

#### Uso de endereços *Embedded-RP*

O primeiro método, configuração estática, é semelhante à configuração estática de rotas unicast. Este método tem como desvantagem o facto de ser necessário configurar, em todos os equipamentos, o IP do RP manualmente. Desta forma, se por exemplo, o RP (*Rendezvous Point*) estiver inacessível, não é possível existir comunicação de tráfego multicast.

O segundo método, *Embedded-RP*, foi projectado especificamente para o IPv6 e permite que o endereço do RP seja embutido dentro do endereço do grupo multicast. Segundo [14], com “Embedded RP”, o problema da descoberta dos rendezvous points (RPs) fica resolvido, e dado que os equipamentos não necessitam de configurações adicionais, é extremamente acessível comutar tráfego

entre sistemas – autónomos distintos. Uma desvantagem do uso deste método é o facto do endereço do RP se tornar globalmente visível, o que poderá torná-lo num possível alvo de ataques de DoS (*Denial of Service*).

Pekka Savola, co-autor do mecanismo Embedded RP, disse:

*The 'Embedded RP' technique allows for easier and simpler deployment of IP multicast, and complements the IPv6 multicast architecture, especially when Source-Specific Multicast (SSM) is unavailable or unsuitable.*

### 5.4.3 PIM – SSM

O protocolo PIM-SSM (*Source Specific Multicast*) utiliza funcionalidades do PIM-SM mas sem necessidade de recorrer a árvores partilhadas (*Shared Trees*) [14]. Ou seja, a descoberta do caminho entre o cliente e o servidor é efectuada automaticamente, sem ser necessário um router central, conhecido como RP.

Como já foi referido na secção 3, o modelo SSM apresenta diversas vantagens em relação ao modelo ASM utilizado pelo PIM-SM. Como tal, o PIM-SSM é uma adaptação do protocolo PIM de modo a que este suporte árvores de distribuição de tráfego partilhadas (modelo SSM). Segundo [RFC-3569], apenas uma parte das funcionalidades existentes no protocolo PIM-SM são necessárias para o modelo SSM. Convém no entanto recordar que, para usar o modelo SSM é necessário utilizar endereços específicos ([FF3x::]).

Uma outra vantagem do modelo SSM é a facilidade de configuração nos equipamentos, dado que, apenas é necessário activar o protocolo PIM e o MLDv2. Deixando assim de ser necessário configurar em todos os equipamentos, o endereço IP do RP.

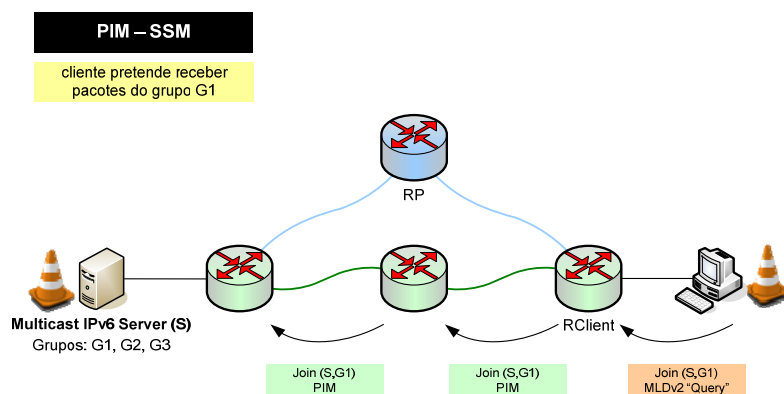


Figura 5.23 - Inscrição do cliente no grupo G1 do servidor Multicast IPv6 (S)

A figura anterior esquematiza o processo de associação de um cliente a um grupo existente no servidor. Mais concretamente, esta representa o caso em que o cliente deseja receber pacotes do grupo

G1, e além disso, especifica a fonte, ou seja, qual o servidor a que este se deseja associar - o servidor Multicast IPv6, identificado pelo endereço IPv6 genérico (S).

É também visível que apesar de estar um RP configurado na rede, este não é utilizado, dado que o router RClient sabe qual a interface para onde deve enviar o pedido Join (S,G1)  
PIM. Esta funcionalidade é possível porque o cliente especificou o endereço do servidor ao qual este se deseja associar. Desta forma, o router RClient analisa a sua tabela de encaminhamento e descobre qual o caminho mais curto para chegar ao destinatário (S).

Convém também mencionar que o pacote Join (S,G1)  
MLDv2 "Query" só pode ser enviado se os clientes suportarem a versão 2 do MLD.

A mensagem Join (S,G1)  
PIM vai ser enviada ao longo dos routers, desde o cliente até ao último router, e por cada router que passa, este armazena a seguinte informação: existe um cliente interessado em receber tráfego da fonte (S) e do grupo (G1). Além disso, este regista ainda as interfaces por onde recebeu e por onde enviou o pacote. Desta forma, quando o servidor começar a difundir os pacotes pela rede, este necessita de saber qual a interface a utilizar para enviar os pacotes direccionados ao cliente. Este funcionamento é conhecido como *Source Tree*.

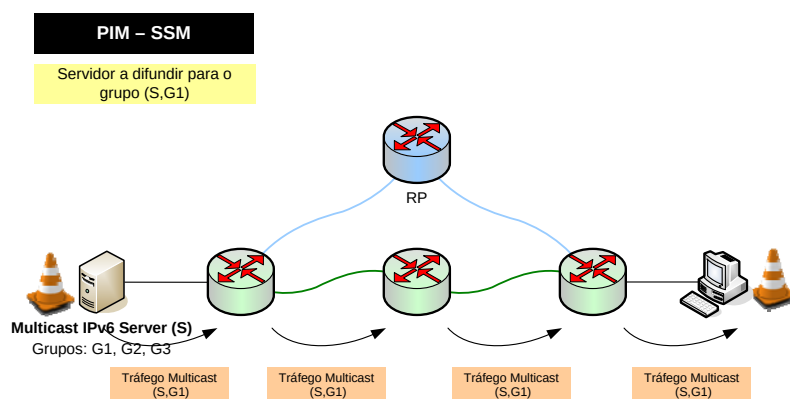


Figura 5.24 - Servidor a difundir para o grupo 1 do servidor Multicast IPv6 (S)

Uma vez completo o processo anterior, os equipamentos ficam aptos a encaminhar os pacotes multicast do canal (S,G1). A figura seguinte demonstra o servidor a difundir para o grupo (S,G1).

### Exemplo real

Como forma de verificar o que acaba de ser descrito, é apresentado de seguida um esquema que contém um cenário prático configurado nos laboratórios da ESTG – Leiria. Mais concretamente, com este cenário, pretendia-se verificar o funcionamento do PIM-SSM

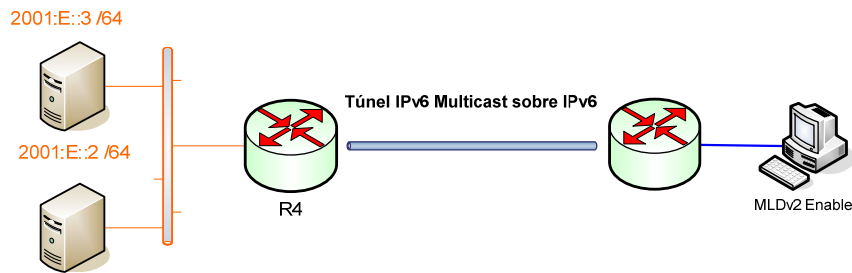


Figura 5.25 - Cenário real PIM – SSM configurado na ESTG – Leira

O teste consistiu no seguinte, implementar um cenário PIM – SSM usando um cliente Linux (MLDv2 enable) e um servidor Windows. As aplicações usadas para transmitir e receber foram configuradas para usar o endereço [FF36::6]. Convém referir novamente que para se usar o modelo SSM é necessário recorrer a endereços da gama [FF3x::].

A figura seguinte contém o resultado de um comando introduzido no router R4. Através desta é possível verificar que existe um par , constituído por {2001:E::2, FF36::6}, sendo [2001:E::2] o endereço do servidor que está a difundir os pacotes multicast e [FF36::6] o grupo multicast SSM configurado em ambas as aplicações.

Observando , verifica-se que o tráfego é oriundo da interface FastEthernet0/0 e encaminhado pelo túnel 11. Todo este processo é efectuado sem ser necessário recorrer a árvores partilhadas (*Shared Trees*) e sem o recurso a mensagens *PIM-Register* unicast.

```
R4#show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal
              AR - Activity Required, K - Keepal
Forwarding Counts: Pkt Count/Pkts per second/Av
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - N
                  IC - Internal Copy, NP - Not platf
                  SP - Signal Present
1 Interface Counts: FS Pkt Count/PS Pkt Count
{2001:E::2, FF36::6} Flags:
Forwarding: 3231/39/1364/420, Other: 0/0/0
FastEthernet0/0 Flags: A 
Tunnel11 Flags: F NS
Pkts: 0/3231
```

Figura 5.26 - Comando colocado no router R4 que permite ver os pares (S,G)

## 5.5 Encaminhamento Multicast na Internet (*Inter-Domínio*)



Nesta secção são apresentadas as soluções existentes para encaminhar pacotes multicast entre sistemas autónomos distintos. É apresentado o protocolo BGP e as mudanças necessárias para o suporte de pacotes multicast.

### 5.5.1 Modelo ASM e SSM

Usando o modelo ASM, existe um problema na distribuição de tráfego multicast entre domínios autónomos distintos, dado que, os RPs não têm maneira de comunicar com outros domínios, nem têm maneira de saber quais as fontes (servidores) que estão activas [RFC 3569].

No IPv4 essa tarefa era efectuada pelo MSDP (*Multicast Service Discovery Protocol*), no entanto, esse protocolo não foi actualizado para o IPv6 [<http://www.6net.org/publications/standards/draft-ietf-mboned-ipv6-multicast-issues-02.txt>]. O funcionamento do MSDP é problemático, dado que, a quantidade de tráfego aumenta linearmente com o número de origens activas na Internet, não sendo portanto, um protocolo escalável [14].

Efectivamente, o modelo ASM (*Any Source Multicast*), não pode ser usado para soluções Inter-domínio, ou seja, não pode ser usado na Internet. O modelo SSM (*Source-Specific Multicast*) [12] resolve os problemas anteriores mas não é uma solução completa porque requer que os clientes possuam capacidades para efectuar os pedidos (MLDv2).

### 5.5.2 Multiprotocol BGP

Para que o BGP podesse encaminhar tráfego multicast, através da Internet, foi necessário adicionar novas funcionalidades que ficaram conhecidas como MBGP – Multiprotocol MGP (RFC 2858) [22]. De uma outra forma, o BGP passou a transportar dois tipos de rotas, uma para encaminhamento unicast e outra para encaminhamento multicast. As rotas multicast são depois usadas pelo protocolo PIM para distribuir o tráfego pela rede.

O protocolo MBGP envia mensagens *Join* e *Prune* para os peers de outros domínios, com os quais ele está ligado [14].

A imagem seguinte contém um cenário completo, onde é usado o protocolo MLD, PIM e MBGP. Mais concretamente, a figura representa a ligação da ESTG – Leiria à rede M6Bone e os protocolos usados sempre que se pretende efectuar uma comunicação usando o modelo ASM.

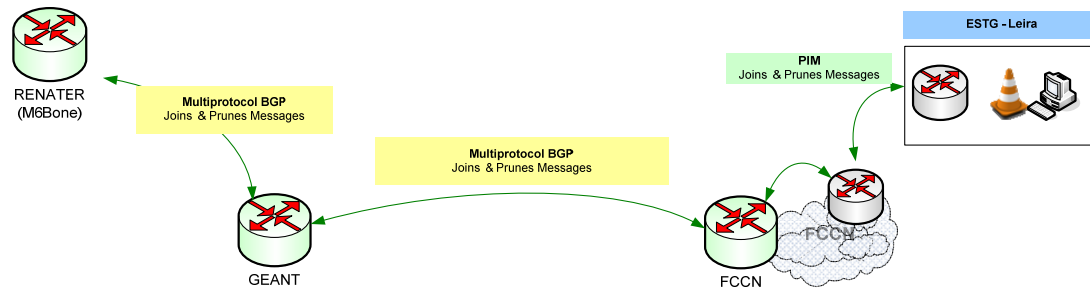


Figura 5.27 - Topologia actual, a nível global da rede M6Bone

Actualmente, e como se demonstra na figura anterior, a rede M6Bone é constituída por um único domínio PIM, sendo o MBGP usado para transportar as mensagens de *Join/Prune*.

## 6 Implementação e Testes

O capítulo seguinte possui uma elevada importância neste relatório porque nele são efectuados múltiplos testes em diferentes cenários, com o objectivo de obter conclusões referentes aos temas apresentados nos capítulos anteriores.

São apresentados vários testes em diferentes cenários, aumentando gradualmente o nível de complexidade. Deste modo, no início são efectuados testes básicos de IPv6 e IPv6 Multicast em máquinas com o sistema operativo Windows, passando-se depois para testes mais elaborados com equipamentos de encaminhamento (tipicamente conhecidos como Routers ou Gateways) e de comutação (switchs).

### 6.1 Sistemas Operativos e Aplicações utilizadas nos testes

Nesta secção são apresentadas as aplicações usadas no decorrer deste projecto, sendo para cada uma delas, efectuado um pequeno enquadramento. É também apresentado o motivo que justificou a sua escolha.

#### **Fedora Core 4**



De uma forma geral, pode ver-se a distribuição Fedora Core 4 como correspondente à distribuição *Red Hat* 13. No entanto esta difere da *Red Hat* devido ao facto de ser um projecto aberto à comunidade, onde qualquer pessoa pode participar no desenvolvimento, bastando para tal mostrar-se disponível. Além disso, um outro factor que as distingue tem a ver com o período limitado de 6 meses que existe entre novas distribuições.

Neste projecto escolheu-se a distribuição Fedora Core 4 porque é a que o aluno melhor conhece e porque esta já foi utilizada em outras cadeiras do curso. O uso de uma distribuição Linux no decorrer deste projecto deve-se ao facto de não ser possível testar todos os cenários usando o sistema operativo Windows XP, pois, como já foi mencionado noutras secções deste projecto, o Windows apenas suporta MLDv1, não sendo possível testar cenários com SSM.

## Microsoft Windows XP



O **Windows XP** é um sistema operativo da Microsoft, criado para ser usado em computadores pessoais ou de escritório. Este é sobejamente conhecido e utilizado em vários países.

O Windows XP foi utilizado no decorrer deste projecto para efectuar testes com multicast ASM, visto que o SSM ainda não está disponível.

## YUM



O **Yum**, acrónimo de Yellow Dog Updater é uma ferramenta para instalar, remover e actualizar pacotes RPM em sistemas Linux. É uma ferramenta que facilita substancialmente a instalação de software em máquinas Linux, pelo facto de deixar de ser necessário instalar todas as dependências manualmente. Ou seja, o **Yum** automaticamente descobre, verifica e instala todas as dependências necessárias para instalar um determinado pacote de software – RPM.

No decorrer deste projecto foi usado o sistema operativo Linux e foi necessário instalar diversas aplicações neste. Como tal, usou-se o Yum para facilitar a instalação.

## VLC media player



O **VLC** é um player multimédia *open-source*, possuindo suporte para vários formatos de vídeo, tais como o MPEG-1, MPEG-2, MPEG-4, DivX, DVD, VCDs, etc. Além disso, tem suporte a vários protocolos de streaming, podendo ser usado tanto como cliente, como servidor. Possui suporte para transmissão de pacotes em unicast ou multicast e além disso, opera em redes IPv4 e IPv6. O VLC tem versões para vários sistemas operativos, tais como Windows, Mac OS, FreeBSD, Linux, BeOS. Possui também suporte para protocolos de rede, destacando-se o UDP, HTTP, RTP e RTSP.

O VLC é um dos melhores softwares usados para transmissão e reprodução de vídeos, devido à gama de plataformas suportadas, formatos de arquivos suportados, de entre outras funcionalidades que vêm sendo agregadas ao VLC constantemente. Mais informações sobre as características do VLC podem ser obtidas através da página oficial: <http://www.videolan.org/vlc/>

No decorrer deste projecto foram usadas versões do VLC para o sistema operativo Windows e Linux. Embora o VLC suporte vários protocolos, a versão utilizada no Linux apenas suportava Codecs standards, isto é, apenas conseguimos usar o VLC com ficheiros codificados com H.263.

## Ethereal



O Ethereal é um popular analisador de protocolos usado para efectuar *troubleshooting* e análises às redes. É usado por profissionais e distribuído de forma open source a toda a comunidade. Ele funciona em diversas plataformas, incluindo o Unix, Linux e Windows [23].

Esta aplicação foi intensivamente usada ao longo deste projecto, e mostrou-se extremamente útil para a resolução de um grande número de problemas.

## 6.2 Ferramentas para verificar conectividade multicast

Nesta secção são apresentadas ferramentas (SSMpingd – SSMping, ASMPing e Mping) que permitem verificar a conectividade multicast de determinado site. Mping apenas possui suporte para multicast IPv4 ao passo que as restantes, possuem suporte para multicast IPv4 e IPv6, sendo estas, actualmente as ferramentas aconselhadas pela M6Bone para testar a conectividade multicast.

### 6.2.1 SSMpingd – SSMping e ASMPing

A aplicação SSMping, disponível através do site <http://www.venaas.no/multicast/ssmping/>, é uma ferramenta que permite testar se determinado site está apto a receber tráfego multicast. A ferramenta tem um comportamento semelhante a um **ping** normal, no entanto requer no servidor uma aplicação SSMpingd para responder aos pedidos efectuados pelos clientes. Ou seja, no servidor é necessário que o *daemon* SSMpingd esteja a funcionar.

A figura seguinte ajuda a compreender o funcionamento da ferramenta SSMping.

## How it works

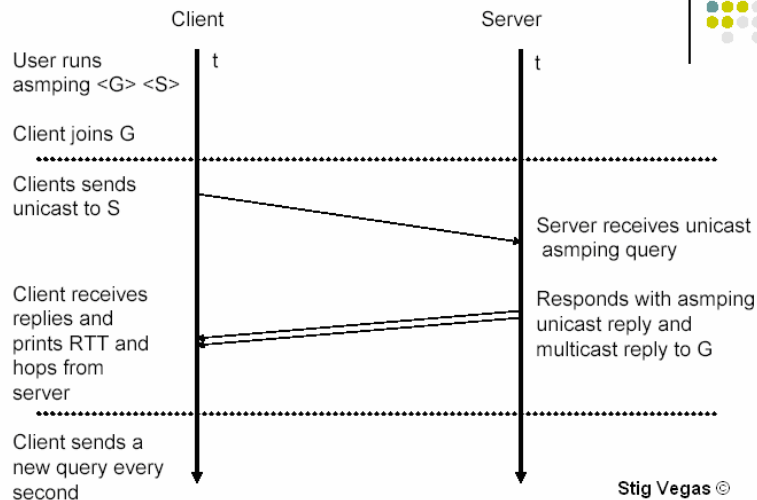


Figura 6.1 - Funcionamento do SSMping

Embora em versões iniciais, a aplicação apenas permitisse testar SSM, segundo informação retirada do site oficial<sup>2</sup>, em Outubro de 2005, a aplicação passou a suportar também ASM.

Apesar de ambas as versões terem sido inicialmente implementadas no Linux, actualmente estas já estão disponíveis para sistemas operativos Windows. Convém no entanto não esquecer que o Windows XP apenas suporta ASM e assim, a versão SSMping disponível para Windows apenas pode ser testada usando Windows Vista.

### Funcionamento da aplicação

A aplicação servidora, *ssmpingd* esta à escuta no porto UDP 4321, quer para IPv4 como para IPv6.

**Ferramenta SSMping:** Descrição do funcionamento

```
[root@localhost bin]# ssm ping -6 -I eth0 2001:690:1FFF:1610::2
```

Depois de se introduzir o comando anterior, a aplicação *ssmping* vai o join ao grupo (S,G), onde S é o endereço do servidor introduzido no comando - 2001:690:1FFF:1610::2, e onde G é o grupo multicast propriamente dito ao qual a aplicação se pretende associar. Segundo [24], por forma a evitar possíveis ataques, o último octeto do grupo multicast tem de terminar obrigatoriamente em [234], para IPv4 ou [::4321:1234], para IPv6.

<sup>2</sup> <http://www.venaas.no/multicast/ssmping/>

Resumindo, o comando anterior vai fazer o Join ao grupo (S,G), onde S é o endereço do servidor e onde G é o endereço multicast configurado no servidor mais o ultimo octeto obrigatório (**4321:1234**). O exemplo seguinte permite esclarecer todas as dúvidas.

```
[root@localhost bin]# ssmpling -6 -I eth0 2001:690:1FFF:1610::2
ssmpling joined (S,G) = (2001:690:1fff:1610::2, ff3e::4321:1234)
pinging S from 2001:690:1fff:16
multicast from 2001:690:1fff:1610::2, seq=17 dist=2 time=8.771 ms
unicast from 2001:690:1fff:1610::2, seq=18 dist=2 time=12.539 ms
```

### Ferramenta ASMPing:

A aplicação *asmping* opera de forma semelhante à anterior, com a excepção que, o grupo multicast usado necessita de ser especificado na linha de comandos. Ou seja, é necessário, para iniciar a aplicação, descrever o IP do grupo (1) e o IP do servidor (2).

```
asmping FF1e:: 2001:690:1FFF:1610::2
1 2
```

### Servidores SSMping públicos

Para fins de testes, o site da aplicação disponibiliza um conjunto de endereços de servidores que possuem o SSMpingd (*daemon*) a correr e, sobre os quais é possível a qualquer cliente se ligar para testar a conectividade do seu site.

| Endereço do Servidor     | IPv6 | IPv4 | ASM |
|--------------------------|------|------|-----|
| ssmpling.uninett.no      | x    | x    | x   |
| ssmpling.net.switch.ch   | x    | x    | x   |
| ssmpling.erg.abdn.ac.uk  | x    | x    | x   |
| ssmpling.beacon.ja.net   |      | x    | x   |
| ssmpling.nysernet.org    | x    |      |     |
| ssmpling.ecs.soton.ac.uk | x    |      |     |
| flo.nrc.ca               |      | x    |     |
| canet.u-strasbg.fr       | x    |      |     |

**Tabela 6.1** - Servidores SSMping públicos

A aplicação foi desenvolvida por Stig Venaas, cientista veterano da rede de investigação Norueguesa - **UNINETT**. Este tem estado envolvido em diversas actividades relacionadas com o IPv6, tendo trabalhado no projecto 6NET, focalizado principalmente no multicast.



Figura 6.2 - Criador do SSMping – Stig Venaas

### Exemplo de utilização – Testbeds FCCN

Nos testes efectuados com a FCCN foi utilizada a aplicação SSMping para testar a conectividade multicast extremo-a-extremo na rede. Através desta, conseguiu-se verificar que a ESTG –Leiria possuía conectividade multicast IPv6, quer ASM quer SSM, com a rede M6Bone. Convém referir que, para testar ASM, foi necessário configurar no router de Leiria, o endereço IP do RP central da rede M6Bone, localizado na França. Deste modo, o comando seguinte, configurado no equipamento de Leiria, faz com que o equipamento envie os pedidos de ASM ao router central da rede M6Bone.

```
ipv6 pim rp-address 2001:660:3007:300:1::
```

De seguida é apresentado o cenário onde a aplicação foi testada, sendo posteriormente apresentado as configurações introduzidas nos equipamentos.

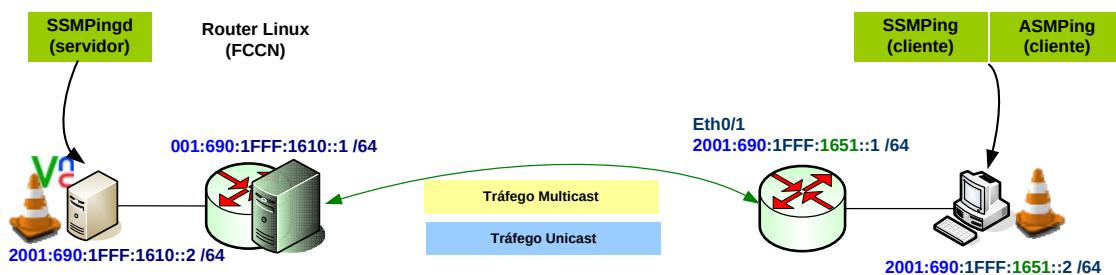


Figura 6.3 - Topologia utilizada nos testes do SSMping

No **servidor** foi colocado o SSMpingd a funcionar:

```
root@localhost bin]#ssmpingd
```

No **cliente**, em Leiria foram introduzidos dois comandos, um para testar a conectividade multicast ASM e um outro para testar o SSM.



## Teste de multicast IPv6 SSM

```
[root@localhost bin]# ssm ping -6 -I eth0 2001:690:1FFF:1610::2
ssm ping joined (S,G) = (2001:690:1fff:1610::2, ff3e::4321:1234)
pinging S from 2001:690:1fff:16
multicast from 2001:690:1fff:1610::2, seq=17 dist=2 time=8.771 ms
  unicast from 2001:690:1fff:1610::2, seq=18 dist=2 time=12.539 ms
multicast from 2001:690:1fff:1610::2, seq=18 dist=2 time=12.813 ms
  unicast from 2001:690:1fff:1610::2, seq=19 dist=2 time=9.980 ms
multicast from 2001:690:1fff:1610::2, seq=19 dist=2 time=11.968 ms
  unicast from 2001:690:1fff:1610::2, seq=20 dist=2 time=14.841 ms
multicast from 2001:690:1fff:1610::2, seq=20 dist=2 time=15.116 ms
  unicast from 2001:690:1fff:1610::2, seq=21 dist=2 time=20.145 ms
multicast from 2001:690:1fff:1610::2, seq=21 dist=2 time=20.600 ms
....
--- 2001:690:1fff:1610::2 ssm ping statistics ---
21 packets transmitted, time 20782 ms
unicast:
  21 packets received, 0% packet loss
  rtt min/avg/max/std-dev = 8.498/18.395/79.747/15.357 ms
multicast:
  20 packets received, 0% packet loss since first mc packet (seq 2) recvd
  rtt min/avg/max/std-dev = 8.771/20.625/79.958/17.029 ms
[root@localhost bin]#
```

Figura 6.4 - Exemplo do funcionamento do SSMping

## Teste de multicast IPv6 ASM

```
[root@localhost bin]# asmping FF1e:: 2001:690:1FFF:1610::2
ssm ping joined (S,G) = (2001:690:1fff:1610::2, ff1e::4321:1234)
pinging S from 2001:690:1fff:1651::2
  unicast from 2001:690:1fff:1610::2, seq=1 dist=2 time=22.377 ms
  unicast from 2001:690:1fff:1610::2, seq=2 dist=2 time=20.249 ms
multicast from 2001:690:1fff:1610::2, seq=2 dist=2 time=21.659 ms
  unicast from 2001:690:1fff:1610::2, seq=3 dist=2 time=18.257 ms
multicast from 2001:690:1fff:1610::2, seq=3 dist=2 time=19.480 ms
recv failed: Connection refused
errno=111
....
--- 2001:690:1fff:1610::2 ssm ping statistics ---
231 packets transmitted, time 230749 ms
unicast:
```

```
200 packets received, 0% packet loss
rtt min/avg/max/std-dev = 8.165/33.320/188.618/38.705 ms
multicast:
199 packets received, 0% packet loss since first mc packet (seq 2) recvd
rtt min/avg/max/std-dev = 8.658/34.348/191.721/38.951 ms
[root@localhost bin]#
```

Exemplo do funcionamento do ASMPing

### 6.2.2 Mping

A ferramenta Mping é uma pequena aplicação desenvolvida por [Jim Gemmell](#) (investigador da Microsoft Research) que permite enviar e receber pacotes multicast para um determinado grupo. Desta forma, a aplicação consegue também receber pacotes gerados por outras aplicações.

A ferramenta Mping apenas possui suporte para IPv4 e está acessível através do seguinte endereço: <http://research.microsoft.com/barc/mbone/mping.aspx>.

Por forma a testar o funcionamento da aplicação, colocou-se o VLC a enviar uma stream para o endereço [239.1.1.239] e colocou-se o MPing por forma a verificar se o VLC estava a funcionar correctamente.

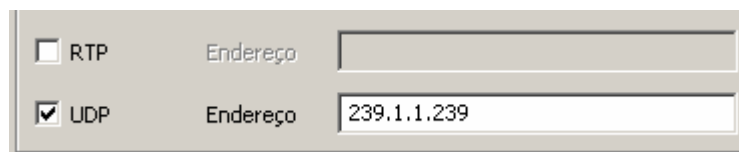


Figura 6.5 - VLC a transmitir para o IP 239.1.1.239

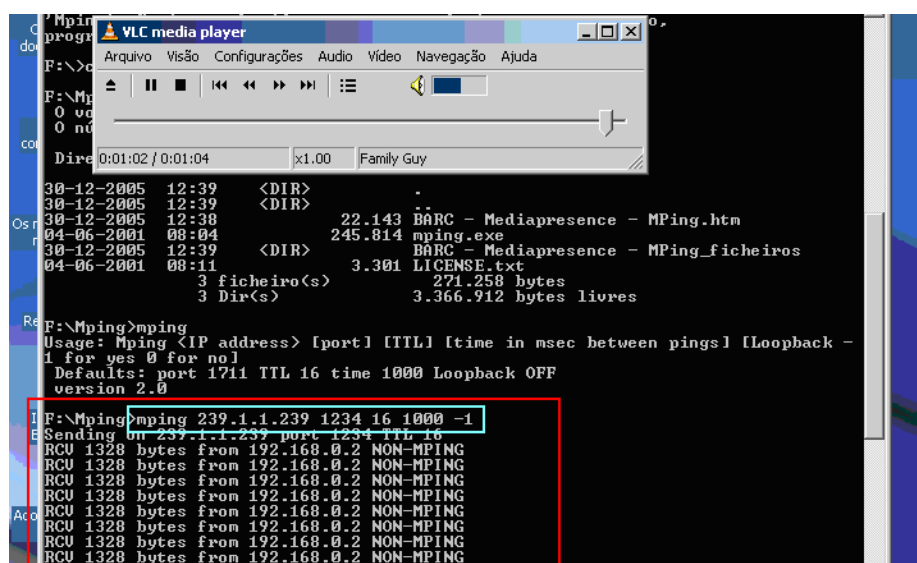


Figura 6.6 - Exemplo do funcionamento do Mping



### 6.3 Teste com multicast IPv4

Nesta secção é apresentado e documentado o primeiro teste efectuado no decorrer deste projecto. Considerou-se preferível, antes de avançar para o multicast IPv6, efectuar alguns testes usando o multicast em IPv4. Surgiram alguns problemas inesperados que acabaram por ser resolvidos.

Assim, nesta secção, é inicialmente apresentado o cenário configurado, sendo, de seguida explicada a forma de configurar as aplicações usadas. Posteriormente, são expostos os problemas surgidos e a forma encontrada para os resolver.

#### 6.3.1 Cenário

O cenário de testes, configurado para testar as aplicações e o multicast IPv4, é apresentado no esquema seguinte. Este caracteriza um cenário hipotético que pode existir numa organização, como por exemplo a ESTG – Leiria.

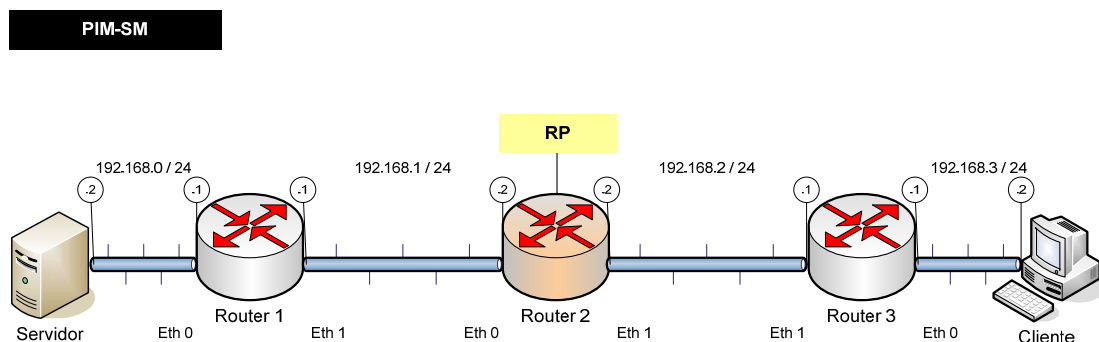


Figura 6.7 - Cenário utilizado nos testes multicast IPv4

No que se refere ao cenário em concreto, foram usados três routers (Cisco Systems da série 2600XM) e dois PCs.

#### **Configuração dos equipamentos**

Foram efectuadas um conjunto de configurações nos routers Cisco, mas pelo facto deste cenário fugir ao âmbito do projecto, estas não serão aqui expostas, encontrando-se em anexo. Convém mais uma vez referir que este foi o primeiro teste a ser efectuado e serviu apenas para facilitar a transição para o multicast IPv6.

## Configuração das aplicações

Nesta secção é detalhado todo o processo de configuração das aplicações existentes no servidor e no cliente. Desta forma, numa primeira fase é detalhado todo o processo de configuração da aplicação servidora, sendo, posteriormente, apresentada a forma de configurar a aplicação cliente.

### Aplicação servidora

Embora existissem várias aplicações que suportavam multicast IPv4, optou-se por utilizar a aplicação VLC (Vídeo Lan Cliente). Esta possui inúmeras vantagens, já mencionadas em capítulos anteriores, quando comparada com as demais existentes.

A forma mais simples de colocar o VLC a efectuar *streaming* é recorrendo ao *Wizard* (ver imagens seguintes).

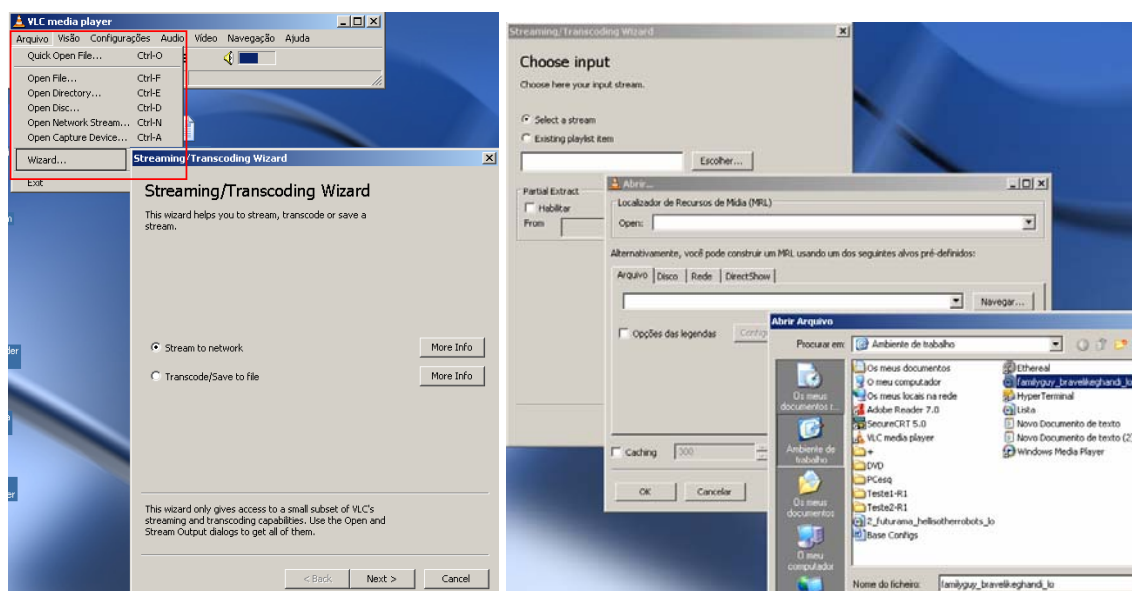


Figura 6.8 - Passos de configuração do servidor - VLC

Depois de efectuados os passos anteriores, é necessário definir qual o endereço multicast IPv4 que a aplicação irá usar para enviar os pacotes (ver imagem seguinte - *Endereço IPv4 usado para difundir vídeo - VLC*).

Dado que o cenário hipotético utilizado pretende representar um caso real de uma organização, é necessário usar endereços multicast adequados a esse fim. Desta forma, e segundo a RFC 2365, é necessário usar endereços *Limited Scope Addresses* ou *Administratively Scoped Addresses*. Ou seja, é necessário usar a gama de endereços 239.0.0.0 à 239.255.255.255. Convém, no entanto, referir que estes tipos de endereços, como é óbvio, não são encaminhados na Internet e, fazendo um paralelismo com os endereços unicast, estes correspondem aos endereços privados.

Depois de escolhida a gama de endereços a usar, é necessário definir o valor do campo TTL dos pacotes. Este campo corresponde ao número de equipamentos de *Layer3* pelos quais o pacote irá passar antes de ser eliminado. Desta forma, e para efeito de testes propriamente dito, optou-se por colocar o valor 5 na caixa de diálogo referente a esse assunto (ver imagem seguinte).

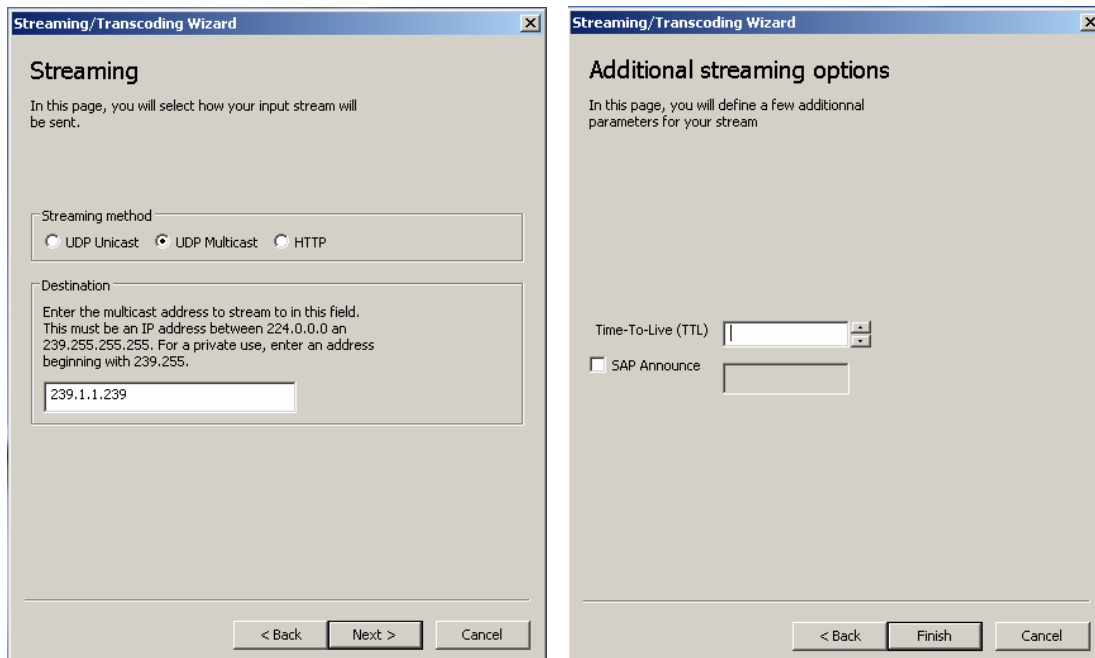


Figura 6.9 - Endereço IPv4 usado para difundir vídeo - VLC

### Aplicação Cliente

Uma vez configurado o servidor, passou-se à configuração do cliente.

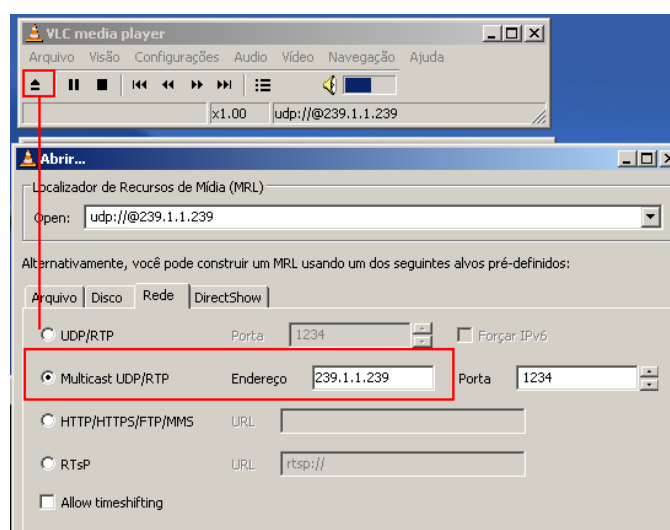


Figura 6.10 - Configurar o VLC para receber vídeo

A figura anterior demonstra como configurar o VLC para receber vídeo através do endereço multicast configurado no servidor [239.1.1.239]. É necessário clicar no botão  e escolher a opção multicast UDP/RTP para introduzir o endereço.

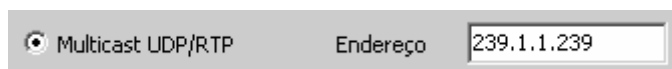


Figura 6.11 - Endereço IPv4 usado para difundir vídeo - VLC

## Problemas encontrados

Depois de se terem configurado os equipamentos e o VLC, passou-se então aos testes propriamente ditos. No entanto, ao contrário do que seria de esperar, o *streaming* não funcionou. Pensou-se que o problema estaria na aplicação cliente, que esta não estaria a fazer correctamente o *Join* ao grupo multicast usado. Desta forma, foi efectuado um conjunto de passos com vista a descobrir onde estaria eventualmente o problema.

### Passo 1: Debug na máquina cliente

Com a aplicação cliente “a correr”, resolveu-se utilizar um comando do Windows XP que permite verificar quais os grupos multicast a que o sistema está associado.

A imagem seguinte apresenta o comando introduzido (*netsh interface ip show joins*) e o resultado deste.

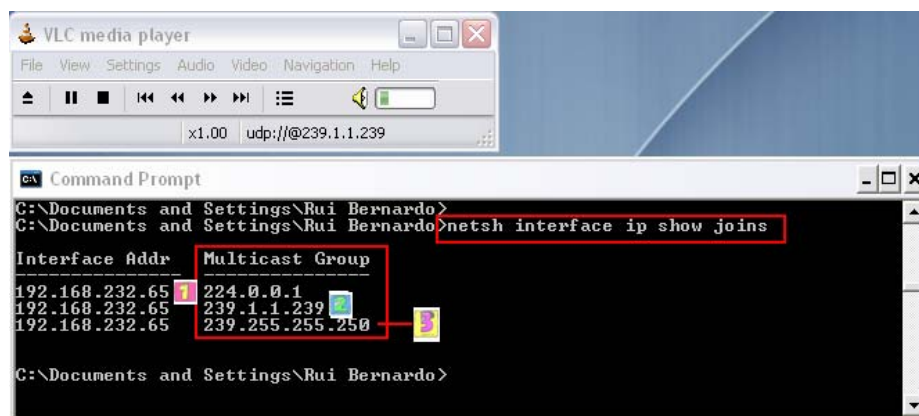


Figura 6.12 - Grupos multicast associados à máquina cliente

Como é visível pela imagem, o PC cliente está associado a três grupos multicast, sendo o primeiro e o terceiro automáticos, ou seja, estão sempre presentes. O segundo, 239.1.1.239, corresponde ao endereço configurado na aplicação VLC. Através deste comando verificamos que, em princípio, o problema não estaria do lado do cliente.

Como forma de esclarecer todas as dúvidas, foi colocado o *Ethereal* a analisar os pacotes trocados entre o PC cliente e o router mais próximo, o Router 3.

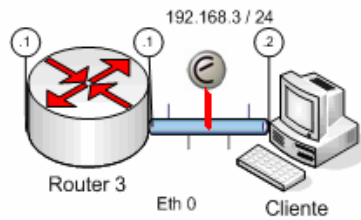


Figura 6.13 - Ethereal colocado entre o PC cliente e o Router 3

Na imagem seguinte é visível uma mensagem *IGMPv2 Report* enviada do IP [192.168.3.2], IP da máquina cliente, para o grupo multicast [239.1.1.239]. Como já foi mencionado em secções anteriores deste relatório, sempre que um *host* se associa a um grupo multicast, este envia uma mensagem IGMP membership report para o IP do grupo a que se deseja associar.

| Filter: <b>igmp</b> Expression... Clear Apply |       |             |                    |          |                      |
|-----------------------------------------------|-------|-------------|--------------------|----------|----------------------|
| No.                                           | Time  | Source      | Destination        | Protocol | Info                 |
| 14                                            | 35.54 | 192.168.3.1 | ALL-SYSTEMS.MCAST. | IGMP     | V2 Membership Query  |
| 15                                            | 40.11 | 192.168.3.2 | 239.255.255.250    | IGMP     | V2 Membership Report |
| 16                                            | 42.11 | 192.168.3.2 | 239.1.1.239        | IGMP     | V2 Membership Report |
| 31                                            | 95.63 | 192.168.3.1 | ALL-SYSTEMS.MCAST. | IGMP     | V2 Membership Query  |

|   |                                                                                   |
|---|-----------------------------------------------------------------------------------|
| + | Frame 16 (46 bytes on wire, 46 bytes captured)                                    |
| + | Ethernet II, Src: DellComp_55:02:a7 (00:06:5b:55:02:a7), Dst: 01:00:5e:01:01:ef   |
| - | Internet Protocol, Src: 192.168.3.2 (192.168.3.2), Dst: 239.1.1.239 (239.1.1.239) |
| + | Version: 4                                                                        |
| + | Header length: 24 bytes                                                           |
| + | Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)               |
| + | Total Length: 32                                                                  |
| + | Identification: 0x79b7 (31159)                                                    |
| + | Flags: 0x00                                                                       |
| + | Fragment offset: 0                                                                |
| + | Time to live: 1                                                                   |
| + | Protocol: IGMP (0x02)                                                             |
| + | Header checksum: 0xf685 [correct]                                                 |
| + | Source: 192.168.3.2 (192.168.3.2)                                                 |
| + | Destination: 239.1.1.239 (239.1.1.239)                                            |
| + | Options: (4 bytes)                                                                |
| - | Internet Group Management Protocol                                                |
| + | IGMP version: 2                                                                   |
| + | Type: Membership Report (0x16)                                                    |
| + | Max Response Time: 0,0 sec (0x00)                                                 |
| + | Header checksum: 0xf90e [correct]                                                 |
| + | Multicast Address: 239.1.1.239 (239.1.1.239)                                      |

Figura 6.14 - Envio da Mensagem IGMP Membership Report para o grupo multicast

Desta forma, como foi demonstrado, verificou-se que o problema não estava no cliente.

## Passo 2: Debug no servidor

Mais uma vez foi utilizado o Ethereal, agora no servidor, para verificar os pacotes trocados. Através deste foi possível comprovar que a aplicação servidora está a enviar os pacotes.



Foram efectuadas algumas pesquisas na Internet e colocadas dúvidas em fóruns da especialidade. Até que num deles, houve um pessoa que referiu a existência de um *Bug* no VLC, relacionado com o valor do campo TTL dos pacotes.

|     |           |             |             |     |                   |                        |
|-----|-----------|-------------|-------------|-----|-------------------|------------------------|
| 220 | 23.203316 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 221 | 23.250106 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 222 | 23.312643 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 223 | 23.359523 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 224 | 23.406461 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 225 | 23.468909 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 226 | 23.547012 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 227 | 23.625186 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 228 | 23.703322 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |
| 229 | 23.875156 | 192.168.0.2 | 239.1.1.239 | UDP | Source port: 1739 | Destination port: 1234 |

```

Frame 224 (1370 bytes on wire, 1370 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:06:5b:55:01:d8), Dst: 01:00:5e:01:01:ef (01:00:5e:01:01:ef)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 239.1.1.239 (239.1.1.239)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 1356
  Identification: 0xa227 (41511)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 1
  Protocol: UDP (0x11)
  Header checksum: 0x60df [correct]
  Source: 192.168.0.2 (192.168.0.2)
  Destination: 239.1.1.239 (239.1.1.239)
User Datagram Protocol, Src Port: 1739 (1739), Dst Port: 1234 (1234)
  Data (1328 bytes)

```

Figura 6.15 - Problemas com o campo TTL dos pacotes enviados pelo VLC

Através da análise da figura anterior pode-se concluir que o problema do cenário não estar a funcionar correctamente se deve unicamente ao facto dos pacotes estarem a ser enviados com o campo TTL a um (1). Desta forma, estes nunca poderiam ser encaminhados pelos *routers*.

### Passo 3: Resolução do problema

De forma a resolver o problema definitivamente, foi necessário aceder às propriedades da aplicação e mudar explicitamente o valor do campo TTL. A partir dessa altura, tudo funcionou perfeitamente.

A imagem seguinte ilustra como resolver o problema.

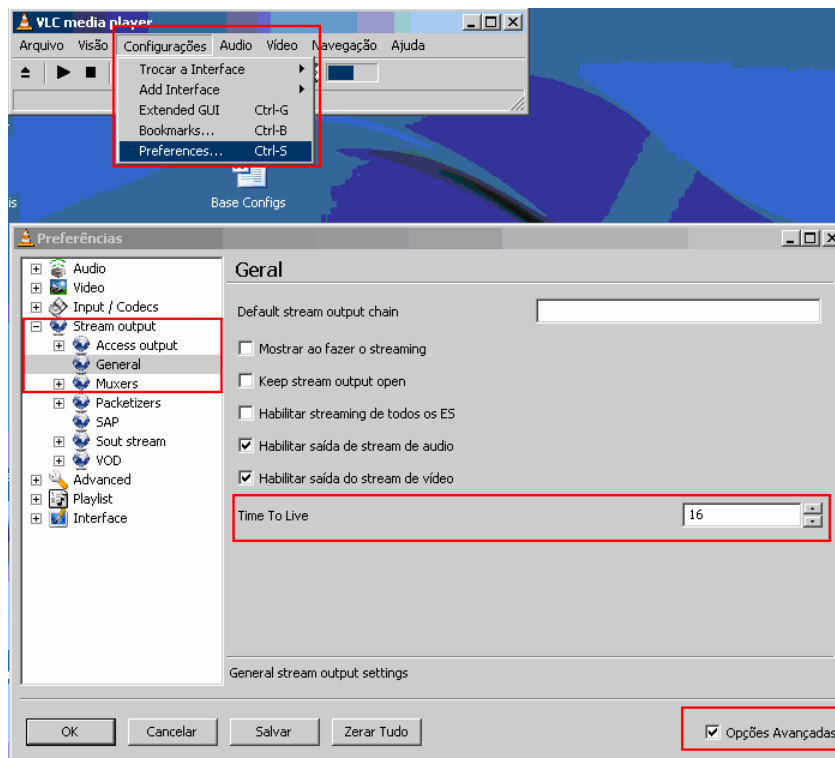


Figura 6.16 - Forma de resolver o problema do campo TTL do VLC

Depois de identificado o problema resolveu-se testar novamente o cenário e tudo funcionou correctamente.

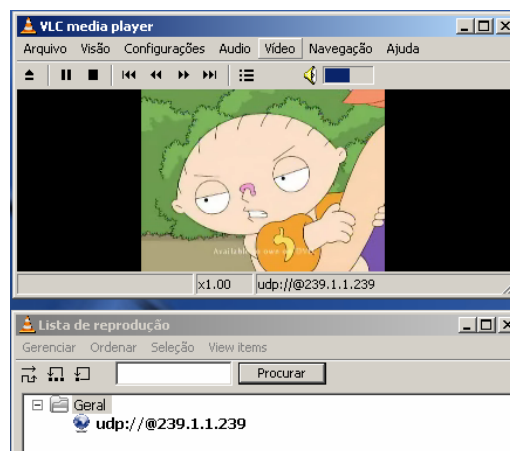


Figura 6.17 - Visualização do Stream de vídeo no cliente

## 6.4 Testes Multicast IPv6: PIM – SM

Nesta secção são apresentados diferentes cenários usando o paradigma de comunicação multicast PIM-SM. Mais concretamente, estes são esquematizados numa primeira fase, sendo de seguida para cada um deles, explicados os detalhes de implementação ao nível dos equipamentos e das aplicações.

São analisados diversos parâmetros de QoS (qualidade de serviço), enumerados os principais problemas encontrados e descrita a forma encontrada para os resolver.

### 6.4.1 Cenário I – Multicast Nativo

O esquema seguinte apresenta o primeiro cenário multicast IPv6 configurado neste projecto. Este representa um cenário hipotético onde todos os equipamentos suportam multicast IPv6.

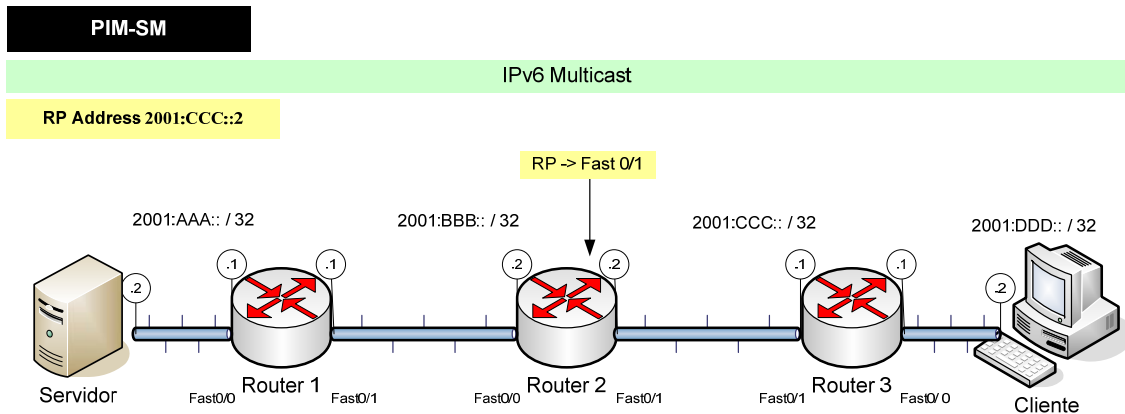


Figura 6.18 - Cenário multicast IPv6 nativo usando o paradigma PIM-SM

Neste cenário foram utilizados dois PCs, sendo o da esquerda utilizado como servidor e o da direita como cliente. No que se refere aos equipamentos responsáveis pelo encaminhamento, foram utilizados três routers Cisco da série 2600XM, com duas interfaces FastEthernet, tornando possível, desta forma, colocar o *Ethernet* entre os equipamentos e analisar os pacotes trocados.

No que se refere ao endereçamento [15], foram utilizados endereços Globais Unicast (*Global Unicast* - [RFC3513]). Mais concretamente, neste teste foram utilizados os endereços: [2001:AAA::/32], [2001:BBB::/32], [2001:CCC::/32] e [2001:DDD::/32].

Como é sabido, quando se usa o paradigma ASM é necessário configurar explicitamente em todos os equipamentos multicast (routers multicast) o ponto central da rede, ou seja, o RP (rendezvous point).

No que se refere aos equipamentos terminais, neste cenário foram usadas máquinas Windows com o sistema operativo Windows XP Service Pack 2.

### Configuração dos equipamentos

De seguida, são apresentadas as principais configurações efectuadas nos equipamentos e, para cada uma delas, é exibida uma pequena descrição da sua utilidade [25].

#### Configurações efectuadas no Router 1

| Router 1                                                                          | Descrição                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 unicast-routing                                                              | Activação do <i>forwarding</i> dos pacotes IPv6. Isto é, o comando activa o encaminhamento <i>unicast</i> e envia <i>ICMPv6-Router Advertised</i> para as interfaces que tenham configurado endereços IPv6.<br>Este comando activa, portanto, o encaminhamento ( <i>unicast</i> ) e envia rotas por omissão para os clientes ligados nas interfaces. |
| ipv6 multicast-routing                                                            | Activação do protocolo multicast PIM (PIM - <i>Protocol Independent Multicast</i> ), bem como do MLD (MLD - <i>Multicast Listener Discovery</i> ) e do encaminhamento de pacotes multicast.                                                                                                                                                          |
| ipv6 router rip cisco                                                             | Activação do protocolo de encaminhamento RIP.                                                                                                                                                                                                                                                                                                        |
| interface FastEthernet0/0<br>ipv6 address 2001:AAA::1/32<br>ipv6 rip cisco enable | Configuração de um endereço IPv6 e activação do processo IPv6 nas interfaces.                                                                                                                                                                                                                                                                        |
| interface FastEthernet0/1<br>ipv6 address 2001:BBB::1/32<br>ipv6 rip cisco enable |                                                                                                                                                                                                                                                                                                                                                      |
| ipv6 pim rp-address<br>2001:CCC::2                                                | Indicação do ponto central da rede, ou seja, a raiz da árvore de distribuição (RP ( <i>rendezvous point</i> ), isto é, indicação do <i>router</i> para onde devem ser enviados os pedidos e o tráfego multicast.                                                                                                                                     |

Tabela 6.2 - Principais configurações efectuadas no Router 1

As configurações efectuadas nos restantes *routers* são idênticas. Por esse motivo, esta não é aqui apresentada.

## Configuração das aplicações

Nesta secção é detalhado todo o processo de configuração da aplicação existente no servidor e no cliente. Desta forma, numa primeira fase é detalhado todo o processo de configuração da aplicação servidora, sendo posteriormente apresentada a forma de configurar a aplicação cliente.

### Aplicação servidora

A aplicação escolhida para difundir o *streaming* foi o VLC. As imagens seguintes ilustram a forma de colocar a referida aplicação a fazer *Streaming* para um endereço multicast IPv6.

Nos testes efectuados com o multicast IPv4, usou-se uma funcionalidade do VLC que permitia colocar a aplicação a difundir recorrendo a um *Wizard*. Verificou-se no entanto que, desta forma, se estava algo limitado visto existiam algumas limitações não se poder, por exemplo, definir a transmissão de pacotes RTP, usando-se apenas o protocolo por omissão, o UDP.

As imagens seguintes esquematizam a forma de colocar o VLC a emitir para um endereço multicast IPv6, usando os protocolos UDP e RTP.

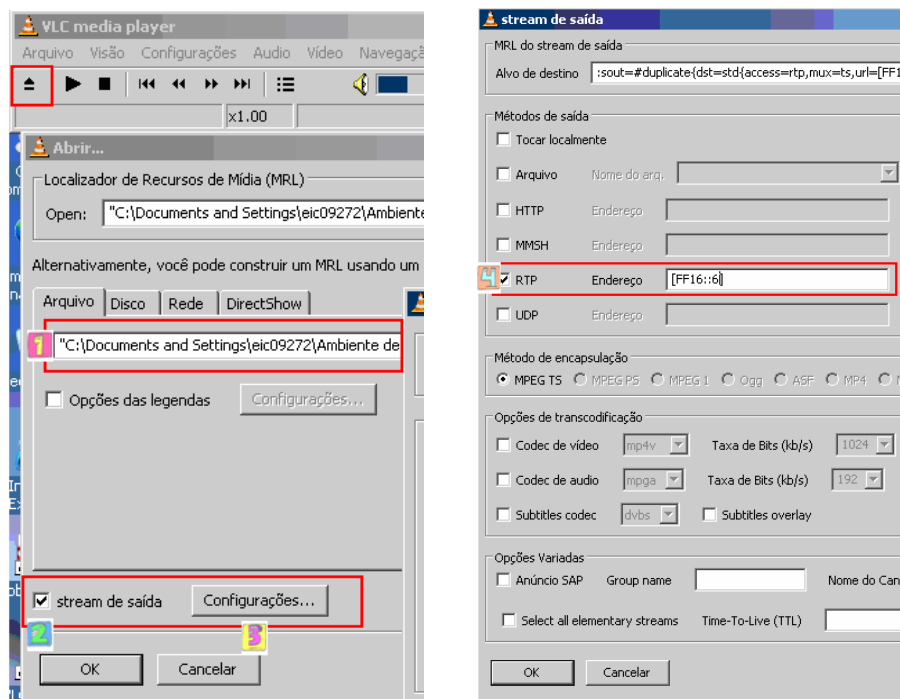


Figura 6.19 - Colocar o VLC a emitir para uma endereço multicast IPv6 usando os protocolos UDP e RTP

Convém, no entanto, detalhar os passos de configuração, uma vez que são substancialmente diferentes dos efectuados no teste anterior de multicast IPv4. Assim, para colocar o VLC a emitir *streaming*, é necessário clicar no botão  e escolher o vídeo que se pretende difundir . O passo seguinte consiste em clicar na *checkbox* 'stream de saída' - passo  - e escolher a opção configurações .

Neste cenário, foi utilizado o endereço multicast IPv6 apresentado na figura seguinte (ter em atenção que o endereço necessita de estar entre parênteses rectos).

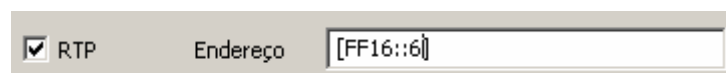


Figura 6.20 - Endereçamento multicast IPv6 utilizado neste cenário

Recorrendo à RFC 3513, concluiu-se que era necessário usar endereços temporários. Desta forma, **é-se** obrigado a colocar o 3º dígito do endereço a 1 (para mais detalhes sobre este assunto, consultar a secção 4).

Resolvida a primeira dúvida, ainda restava definir qual a abrangência do endereço multicast. Analisando a referida RFC, conclui-se que actualmente estão definidos seis valores para o campo de abrangência (ver tabela seguinte).

| Abrangências actualmente definidas para os endereços multicast |                              |
|----------------------------------------------------------------|------------------------------|
|                                                                | 1 – interface-local scope    |
|                                                                | 2 – link-local scope         |
|                                                                | 4 – admin-local scope        |
|                                                                | 5 – site-local scope         |
|                                                                | 8 – organization-local scope |
|                                                                | E – global scope             |

Tabela 6.3 - Abrangências actualmente definidas para os endereços multicast

Foi experimentado um endereço com o valor de abrangência 6, ainda não definido, verificando-se que ainda assim os testes foram efectuados com sucesso.

### Aplicação Cliente

Uma vez configurado o servidor, passou-se à configuração do cliente.

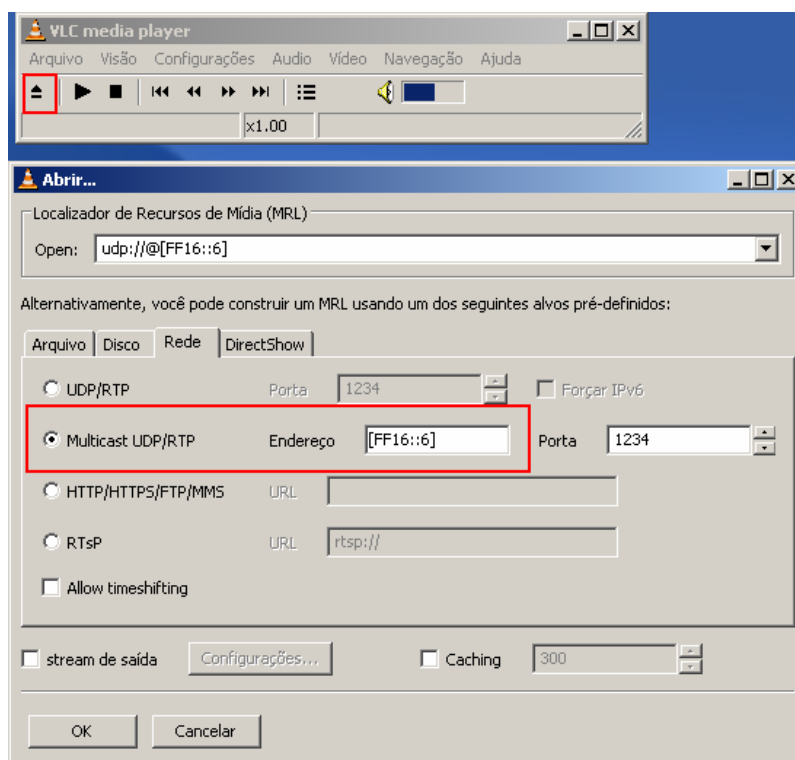


Figura 6.21 - Configurar o VLC para receber vídeo

A figura anterior mostra como configurar o VLC para receber vídeo através do endereço multicast configurado no servidor [FF16::6].

## Problemas encontrados

Uma vez configurados os equipamentos e as aplicações, resolveu-se testar se efectivamente o vídeo estava a chegar ao cliente. No entanto, mais uma vez os testes não tiveram sucesso à primeira.

Depois de efectuadas algumas pesquisas sem sucesso na Internet, resolveu-se tentar fazer um ping extremo-a-extremo entre ambas as máquinas, de modo a verificar se existia conectividade unicast entre elas. Através da análise do resultado do ping, conseguiu-se concluir que não existia conectividade unicast entre as máquinas.

A forma de resolver o problema é bastante simples e passa apenas por desactivar e voltar a activar a interface em ambas as máquinas. A figura seguinte exemplifica a forma de o fazer.

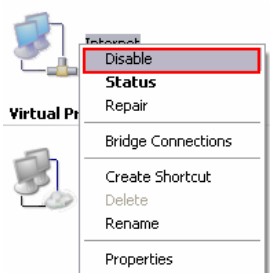


Figura 6.22 - Limpar as configurações temporárias de IPv6 na máquina

Depois de resolvidos todos os problemas, foi possível visualizar no cliente o vídeo enviado pelo servidor para o endereço [FF16::6]

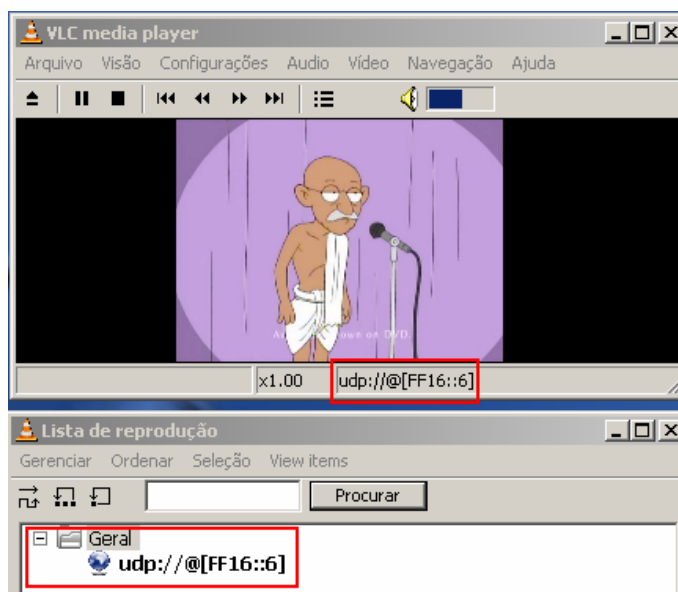


Figura 6.23 - Visualização do Stream de vídeo no cliente

## Testes

Nesta secção são apresentados e analisados diversos parâmetros de QoS (qualidade de serviço) medidos automaticamente pelo Ethereal. No entanto, esta característica só está disponível quando se utiliza o protocolo RTP.

Dado que se configurou o servidor para enviar pacotes RTP, resolveu-se colocar a aplicação Ethereal a captar os captados, conforme apresentado na imagem seguinte.

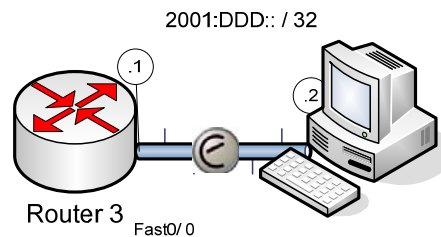


Figura 6.24 - Ethereal colocado entre o PC cliente e o Router 3

Reparou-se que os pacotes que estavam a chegar ao PC cliente eram UDP e não RTP como seria de esperar. Depois de uma pesquisa na Internet, compreendeu-se o que estava a acontecer. Segundo informação retirada da FAQ do Ethereal, o RTP não tem nenhum porto específico associado, diga-se reservado. A menos que sejam utilizados protocolos de sinalização que indiquem qual o porto utilizado na transferência actual, o ethereal não tem forma de saber qual o porto usado pelos pacotes. Desta forma, e para este cenário em particular, é necessário associar manualmente um porto aos pacotes RTP. Convém referir que, se sabia à partida que se estava a enviar pacotes RTP, daí ser possível e conveniente efectuar os passos apresentados de seguida.

### **Passo 1:** Associar manualmente um porto aos pacotes RTP

Na figura seguinte são visíveis vários pacotes UDP a serem enviados para o endereço multicast [FF16::6]. No entanto, ao contrário do que seria de esperar, não são visíveis pacotes RTP, embora se saiba que a aplicação servidora foi configurada para enviar este tipo de pacotes. Deste modo, e tendo em linha de conta o que foi mencionado em cima, a forma de configurar o Ethereal para decodificar pacotes RTP é apresentada na imagem seguinte.



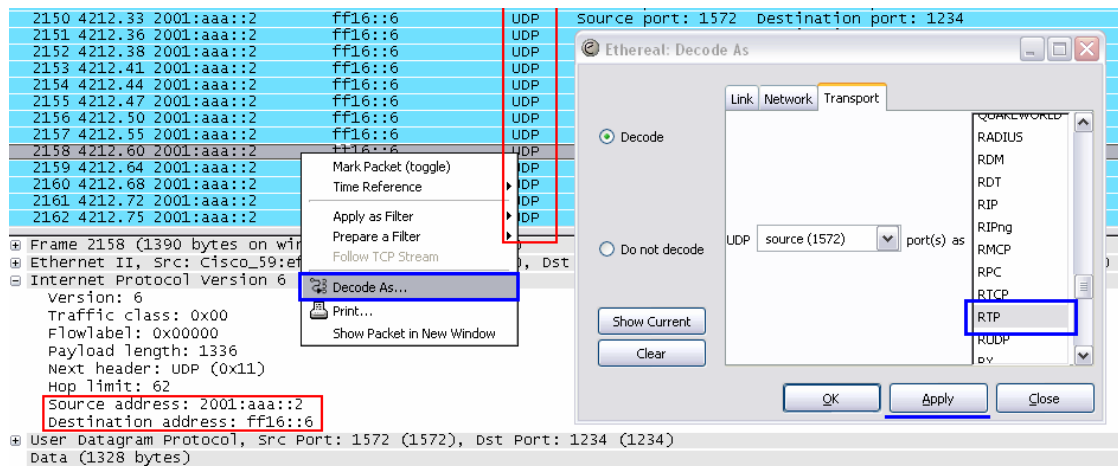


Figura 6.25 - Configurar o Ethereal para decodificar pacotes RTP

É necessário *clicar* com o botão direito do rato sobre um dos vários pacotes UDP e escolher a opção “Decode As..”. Depois, é necessário escolher o protocolo a que desejamos associar os pacotes, neste caso concreto, é o protocolo RTP.

## Passo 2: Analisar os resultados

Depois de configurada correctamente a aplicação, foi possível analisar as estatísticas disponibilizadas pela mesma. A figura seguinte demonstra a forma de obter estatísticas referentes ao tráfego RTP. Através desta, também é visível que os pacotes que antes estavam marcados como UDP, passaram a estar associados ao protocolo RTP.

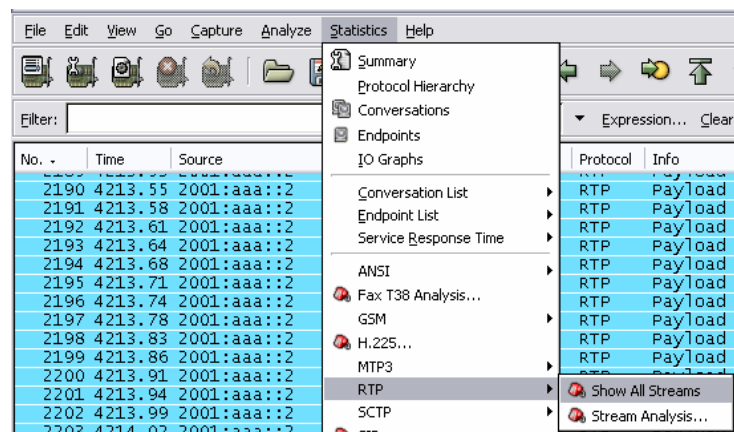


Figura 6.26 - Obtenção de estatísticas sobre o tráfego RTP usando o Ethereal

A ferramenta Ethereal é bastante poderosa e como se pode verificar pela análise da figura seguinte, através desta é possível analisar, por exemplo, a quantidade de pacotes, o número de pacotes perdidos, o atraso e a variação máxima do atraso. É também possível visualizar, em detalhe, toda a sequência de pacotes enviados, bem como atrasos e largura de banda de cada pacote.

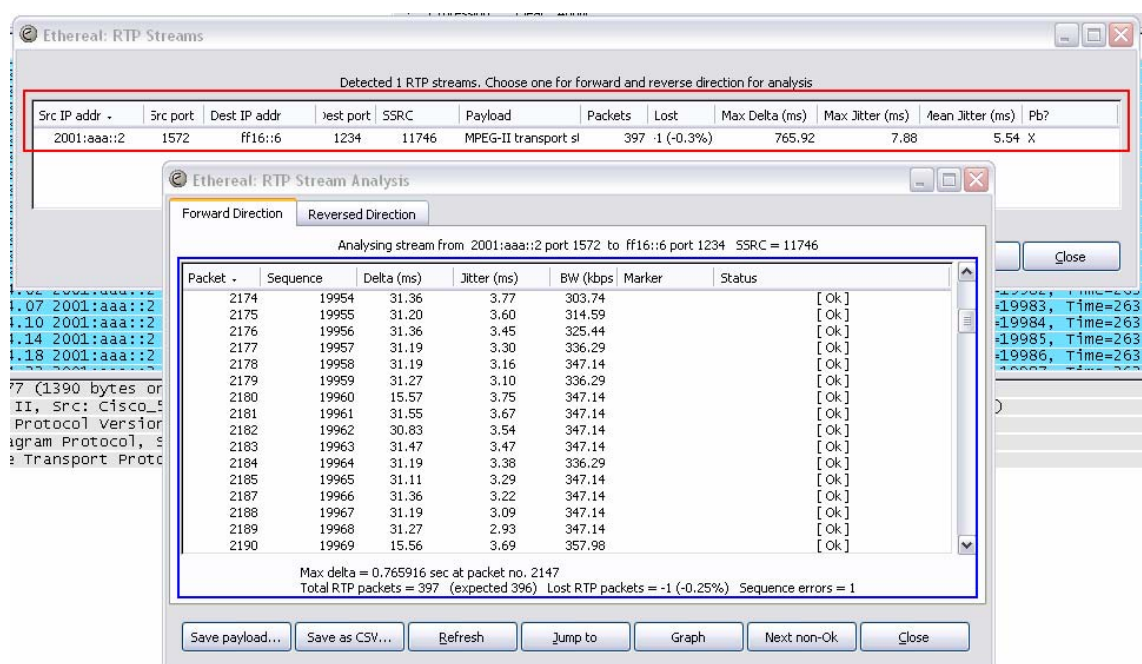


Figura 6.27 - Parâmetros de QoS medidos pelo Ethereal

#### 6.4.2 Cenário II – Simular uma Ligação à FCCN por Túnel IPv6

O cenário apresentado no esquema seguinte simula a ligação entre duas instituições que suportam multicast IPv6 e estão interligadas por redes que apenas suportam unicast IPv6. Mais concretamente este cenário pretende simular a ligação da ESTG – Leiria à plataforma testbeds fornecida pela FCCN.

Convém vez referir que o cenário seguinte foi testado apenas com os equipamentos existentes na ESTG – Leiria, não houve qualquer envolvimento da FCCN na configuração deste cenário. Assim, e como foi mencionado, este cenário simula um caso prático onde as instituições estão separadas por redes onde não existe conectividade multicast.

Na página WEB da rede M6Bone estão presentes esquemas que indicam a forma de interligar sites remotos a referida rede [26]. Desta forma, o cenário apresentado de seguida foi baseado num desses esquemas existentes.

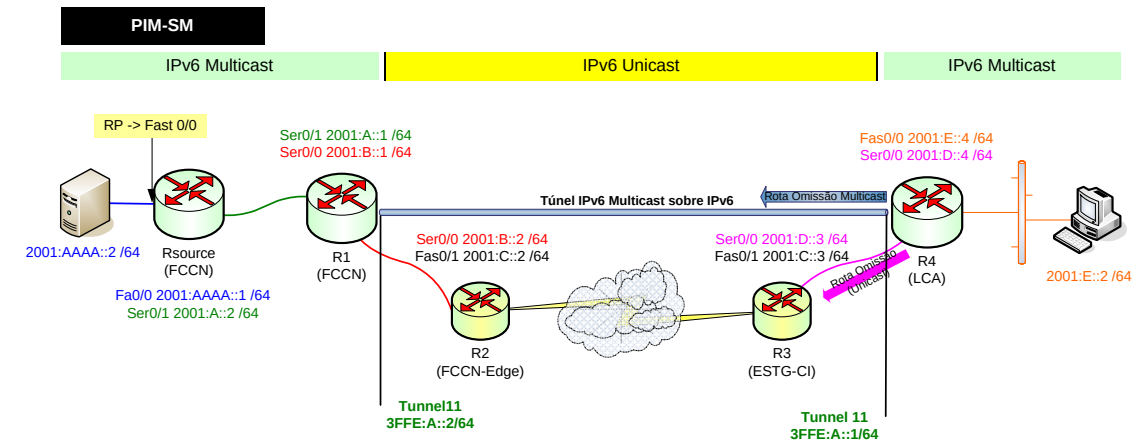


Figura 6.28 - Cenário baseado num esquema presente na M6Bone

Para este cenário em concreto, foram utilizados 5 routers Cisco System e dois PC. Conforme é visível na figura anterior, três dos routers suportam multicast IPv6, ao passo que os dois restantes, apenas suportam unicast IPv6.

A tabela seguinte “identifica” quais os equipamentos que apenas suportam unicast e quais os equipamentos que suportam multicast IPv6 e obviamente unicast IPv6 também.

| Routers Multicast             | Routers Unicast               |
|-------------------------------|-------------------------------|
| Rsource; R1 (FCCN) e R4 (LCA) | R2 (FCCN-Edge) e R3 (ESTG-CI) |

Tabela 6.4 - Suporte multicast e unicast dos equipamntos

Configuração dos equipamentos

De seguida são apresentadas as principais configurações efectuadas nos equipamentos e para cada uma delas, é exibida uma pequena descrição da sua utilidade. Convém referir que, apenas irão ser descritas as configurações efectuados nos equipamentos multicast (Rsource; R1 (FCCN) e R4 (LCA)). No que se refere as configurações dos equipamentos unicast, estás apenas são apresentadas em anexo.

Por forma a descrever correctamente a utilidade e a descrição de cada comando, foi usada seguinte referência [25].

Configurações efectuadas no **RSource, R1 (FCCN), R4 (LCA)**

| Routers RSource | Descrição |
|-----------------|-----------|
|-----------------|-----------|

|                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> hostname RSource ! ipv6 unicast-routing ipv6 multicast-routing ! interface FastEthernet0/0  ipv6 address 2001:AAAA::1/64 ! interface Serial0/1  ipv6 address 2001:A::2/64 ! ipv6 route ::/0 2001:A::1 ! ipv6 pim rp-address 2001:AAAA::1 </pre> | <p><b>ipv6 unicast-routing</b></p> <p>Este comando é responsável por activar o <i>forwarding</i> dos pacotes IPv6. Isto é, o comando activa o encaminhamento <i>unicast</i> e, envia <i>ICMPv6-Router Advertised</i> para as interfaces que tenham configurado endereços IPv6.</p> <p>Dito de uma forma mais simples, este comando activa o encaminhamento (<i>unicast</i>) e envia rotas por omissão para os clientes ligados nas interfaces directamente ligados.</p> <p><b>ipv6 multicast-routing</b></p> <p>Activar o protocolo multicast PIM (PIM - <i>Protocol Independent Multicast</i>), activar o protocolo MLD (MLD - <i>Multicast Listener Discovery</i>) e activar o encaminhamento de pacotes multicast.</p> <p><b>interface FastEthernet0/0</b></p> <p>    <b>ipv6 address 2001:AAAA::1/64</b></p> <p><b>interface Serial0/1</b></p> <p>    <b>ipv6 address 2001:A::2/64</b></p> <p>Configuração dos endereços IPv6 associados às interfaces.</p> <p><b>ipv6 route ::/0 2001:A::1</b></p> <p>Configuração de uma rota por omissão para o endereço IPv6 do Next-Hop (R1). Convém mencionar que está rota irá ser usada tanto pelos pacotes unicast, como pelos multicast.</p> <p><b>ipv6 pim rp-address 2001:AAAA::1</b></p> <p>O comando indica ao equipamento o ponto central da rede, ou seja a raiz da arvore de distribuição (RP - <b>Rendezvous Point</b>). Neste caso em concreto, o ponto central da rede irá ser o RSource.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Tabela 6.5 - Configurações efectuadas no RSource

| Router R1 | Descrição |
|-----------|-----------|
|-----------|-----------|

```

hostname R1
!
ipv6 unicast-routing
ipv6 multicast-routing
!
interface Tunnel11
 ipv6 address 3FFE:A::2/64
 tunnel source 2001:B::1
 tunnel destination 2001:D::4
 tunnel mode gre ipv6
!
interface Serial0/0
 ipv6 address 2001:B::1/64
!
interface Serial0/1
 ipv6 address 2001:A::1/64
!
ipv6 route 2001:D::/64 3FFE:A::1 multicast
ipv6 route 2001:AAAA::/64 2001:A::2
ipv6 route ::/0 2001:B::2 unicast
!
pv6 pim rp-address 2001:AAAA:1

```

```

interface Tunnel11
 ipv6 address 3FFE:A::2/64
 tunnel source 2001:B::1
 tunnel destination 2001:D::4
 tunnel mode gre ipv6

```

Os comandos anteriores configuram o túnel. Antes de se explicar em detalhe a configuração utilizada, convém mencionar que, quando se está a configurar túneis é necessário existir encaminhamento para os endereços origem e destino, definidos no túnel.

-Origem do túnel: endereço da interface Serial0/0 do R1

-Destino do túnel (extremidade remota): endereço da interface Serial0/0 do R4 (LCA).

-Tipo de túnel: o tipo de túnel usado vai indicar ao router que é necessário transportar os pacotes multicast IPv6 em pacotes GRE que, por sua vez são enviados em pacotes unicast IPv6.

(para compreender correctamente o que acabou de ser descrito, consultar X)

```

interface Serial0/0
 ipv6 address 2001:B::1/64
interface Serial0/1
 ipv6 address 2001:A::1/64

```

Configuração dos endereços IPv6 associados às interfaces

```

ipv6 route 2001:D::/64 3FFE:A::1 multicast

```

O comando anterior indica ao router que todo o tráfego multicast destinado à rede [2001:D::/64] deve ser enviado pelo túnel. Ou seja, palavra **multicast** no fim do comando indica que a rota não irá ser usada pelo processo de encaminhamento unicast, ou seja, esta nunca é colocada na tabela de encaminhamento unicast.

```

ipv6 route 2001:AAAA::/64 2001:A::2

```

Dado que neste cenário foi utilizado encaminhamento estático (rotas estáticas), é necessário garantir desta forma, encaminhamento para todas as redes existentes no cenário.

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <pre>ipv6 route ::/0 2001:B::2 unicast</pre> <p>O comando anterior indica ao router que todo o tráfego deve ser enviado para o router unicast - R2 (FCCN-Edge).</p> <p>Repare-se na palavra <b>unicast</b> no fim do comando. Esta é extremamente importante. Consultar a secção X (problemas encontrados) para compreender o que acontece quando esta palavra não é colocada no fim do comando.</p> <pre>ipv6 pim rp-address 2001:AAAA::1</pre> <p>O comando indica ao equipamento o ponto central da rede, ou seja a raiz da arvore de distribuição (RP - <b>Rendezvous Point</b>). Neste caso em concreto, o ponto central da rede irá ser o RSource.</p> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Figura 6.29 - Configurações efectuadas no R1 (FCCN)

| Router R4                                                                                                                                                                                                                                                                                                                                                                                                      | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>hostname R4 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel11 ipv6 address 3FFE:A::1/64 tunnel source 2001:D::4 tunnel destination 2001:B::1 tunnel mode gre ipv6 ! interface FastEthernet0/0 ipv6 address 2001:E::4/64 ! interface Serial0/0 ipv6 address 2001:D::4/64 ! ipv6 route ::/0 3FFE:A::2 multicast ipv6 route ::/0 2001:D::3 unicast ! ipv6 pim rp-address 2001:AAAA::1</pre> | <pre>interface Tunnel11   ipv6 address 3FFE:A::1/64   tunnel source 2001:D::4   tunnel destination 2001:B::1   tunnel mode gre ipv6</pre> <p>Os comandos anteriores configuram o túnel. Convém mencionar novamente que, o túnel só ficará bem configurado se existir encaminhamento para os endereços origem e destino, definidos no túnel.</p> <ul style="list-style-type: none"> <li>-Origem do túnel: endereço da interface Serial0/0 do R4 (LCA).</li> <li>-Destino do túnel (extremidade remota): endereço da interface Serial0/0 do R1</li> <li>-Tipo de túnel: Dado que no R1 já se configurou o tipo de túnel a utilizar, é necessário fazer o mesmo no router R4.</li> </ul> <pre>interface FastEthernet0/0   ipv6 address 2001:E::4/64 interface Serial0/0   ipv6 address 2001:D::4/64</pre> <p>Configuração dos endereços IPv6 associados às interfaces</p> |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <pre>ipv6 route ::/0 3FFE:A::2 multicast</pre> <p>O comando anterior indica ao router que todo o tráfego multicast deve ser enviado pelo túnel. Ou seja, como já foi mencionado palavra <b>multicast</b> no fim do comando indica que a rota não irá ser usada pelo processo de encaminhamento unicast.</p> <pre>ipv6 route ::/0 2001:D::3 unicast</pre> <p>O comando anterior indica ao router que todo o tráfego deve ser enviado para o router unicast - R3 (ESTG - CI).</p> <pre>ipv6 pim rp-address 2001:AAAA::1</pre> <p>O comando indica ao equipamento o ponto central da rede, ou seja a raiz da árvore de distribuição (RP - <b>Rendezvous Point</b>). Neste caso em concreto, o ponto central da rede irá ser o RSource.</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Tabela 6.6 - Configurações efectuadas R4 (LCA)

## Configuração das aplicações

Dado que para neste cenário se usou o mesmo endereço do grupo multicast [FF16::6] utilizado em cenários anteriores, optou-se por usar não repetir a explicação efectuada no capítulo anterior sendo apenas apresentado um figura que esquematiza a forma de as configurar.

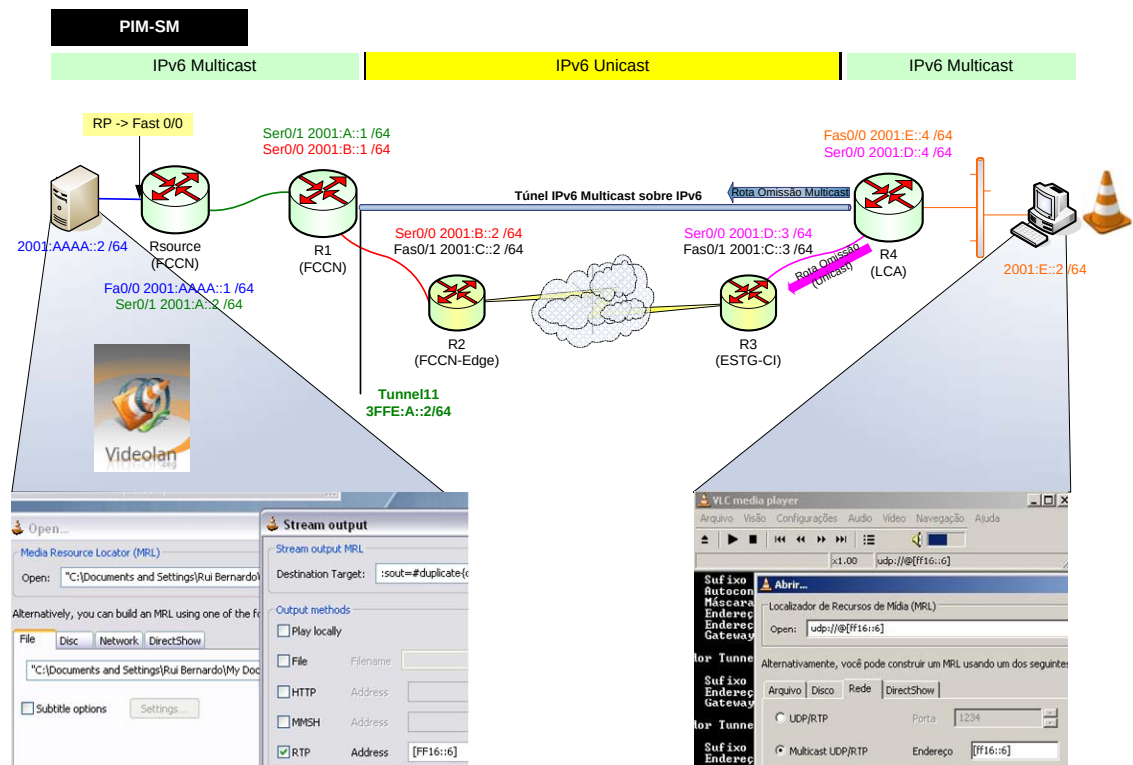


Figura 6.30 - Configuração das aplicações

### Problemas encontrados

Depois de efectuar estudo sobre o funcionamento dos túneis, passou-se para a fase de implementação nos equipamentos.

Foram introduzidas nos equipamentos as configurações apresentas nas tabelas anteriores mas com uma pequena diferença (ver palavras a negrito na tabela seguinte). Assim quando se configuraram os equipamentos, as palavras a negrito não foram colocadas nos equipamentos. A falta desta fez com que todo o cenário comprometido, dado que, no inicio não se sabia que era absolutamente necessário usa-las.

| Router R1<br>(forma incorrecta)            | Router R4 (LCA)<br>(forma incorrecta)      |
|--------------------------------------------|--------------------------------------------|
| ipv6 route ::/0 2001:D::3 <b>unicast</b> ❌ | ipv6 route ::/0 2001:B::2 <b>unicast</b> ❌ |
|                                            |                                            |

Depois de muitas tentativas fracassadas e muito tempo perdido, resolveu-se enviar um mail para a mail-list da rede M6Bone (ver imagem seguinte).



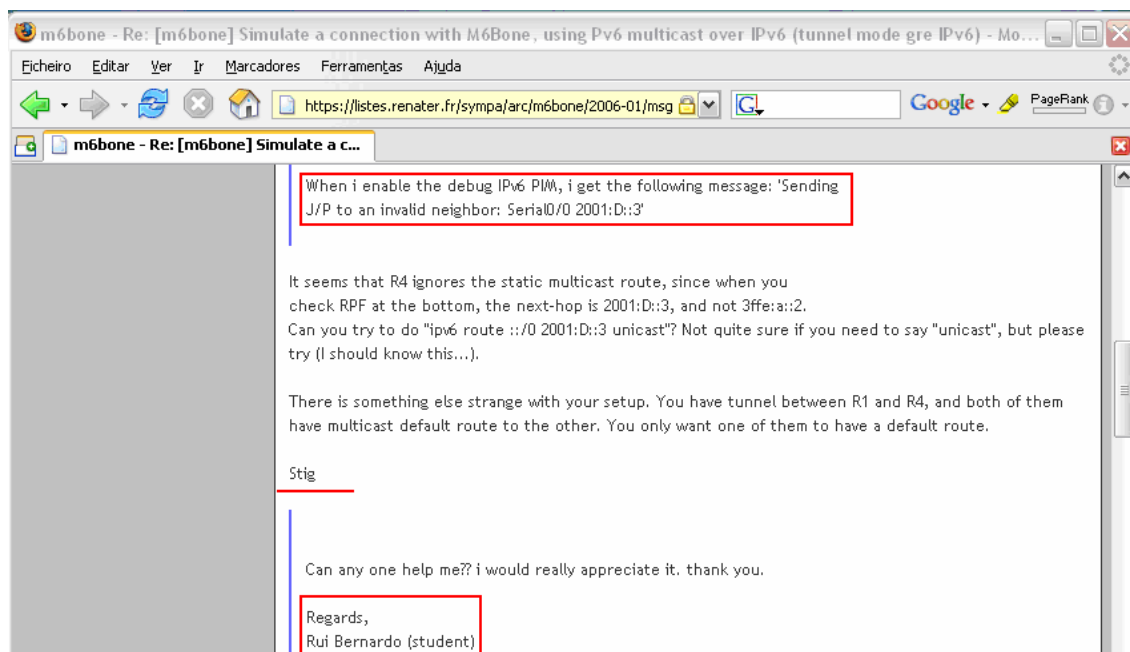


Figura 6.31 - E-Mail enviado para a Mail-List da M6Bone

Através da resposta do Stig, parece que o R4 ignora a rota estática introduzida e o endereço IP do next-hop devolvido pela verificação RPF não está correcto. Desta forma, e como é visível na imagem anterior, este aconselha o usar da palavra unicast no fim do comando.

Efectivamente e depois de se efectuada o que foi sugerido pelo Stig da M6Bone, todo o cenário funcionou perfeitamente. Por forma a compreender a necessidade da palavra unicast no final, foi consultada a seguinte referência [25].

A tabela seguinte facilita a compreensão dos conceitos(ver palavras a negrito). Assim, a palavra unicast, segundo a referência anterior, especifica que a rota não vai ser usada por uma técnica especifica do multicast (Reverse Path Forwarding – RPF). Ou seja, se retirarmos a palavra unicast, o equipamento vai utilizar sempre a rota para “comunicar” com o(s) vizinho(s) multicast, independentemente de outras rotas multicast que este possa já ter configurado. Resumidamente, quando se configura o multicast num equipamento cisco, e se usa túneis (topologia unicast distinta da multicast) é sempre necessário utilizar a palavra unicast.

| Router R4 (LCA)<br>(forma correcta)           | Router R4 (LCA)<br>(forma errada)             |
|-----------------------------------------------|-----------------------------------------------|
| ipv6 route ::/0<br>3FFE:A::2 <b>multicast</b> | ipv6 route ::/0<br>3FFE:A::2 <b>multicast</b> |
| ipv6 route ::/0 2001:D::3 <b>unicast</b>      | ipv6 route ::/0 2001:D::3                     |

Como é visível, a única diferença está precisamente no uso, ou não, da palavra **unicast**. Ou seja, na coluna da esquerda foi introduzida a palavra **unicast**, ao passo que na da direita já não.

Foram efectuados alguns testes e verificou-se que quando se usava as configurações da coluna direita, o multicast **não funcionava**. A tabela seguinte exhibe a causa do problema.

| Router R4 (LCA)<br>(forma correcta)                                                                                                                                                                                                                 | Router R4 (LCA)<br>(forma errada)                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>R4# R4#show ipv6 rpf 2001:a::1 RPF information for 2001:A::1   RPF interface: <b>Tunnel11</b>   RPF neighbor: <b>3FFE:A::2</b>   RPF route/mask: ::/0   RPF type: Mroute   RPF recursion count: 1   Metric preference: 1   Metric: 0 R4#</pre> | <pre>R4# R4#show ipv6 rpf 2001:a::1 RPF information for 2001:A::1   RPF interface: <b>Serial0/0</b> ❌   RPF neighbor: <b>2001:D::3</b> ❌   RPF route/mask: ::/0   RPF type: Mroute   RPF recursion count: 1   Metric preference: 1   Metric: 0 R4#</pre> |

Como se pode ver na coluna da esquerda, o router usa a interface **túnel11** para o calculo do RPF (está correcto), ao passo que a coluna da direita usa a interface **Serial0/1** para comunicar com a outra extremidade, o que está incorrecto.

Depois de resolvidos todos os problemas foi possível visualizar no cliente, o vídeo enviado pelo servidor para o endereço [FF16::6]



Figura 6.32 - Visualização do Stream de vídeo no cliente

Testes

Nesta secção é demonstrado, numa primeira fase, o funcionamento do túnel, sendo posteriormente analisados alguns parâmetros de QoS medidos pelo Ethereal.

**Passo 1: Funcionamento do túnel**

Para compreender o funcionamento túnel resolveu-se utilizar o Ethereal, e colocá-lo a captar os pacotes que existentes no túnel. A imagem seguinte, demonstra onde este foi colocado.

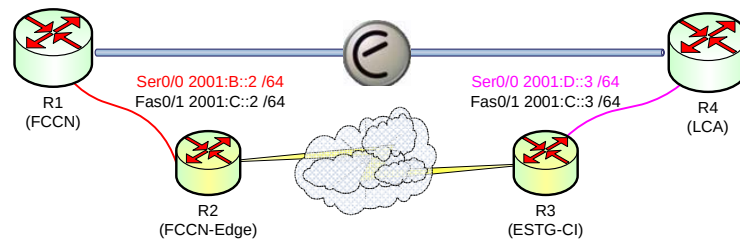


Figura 6.33 - Ethereal colocado entre o router R2 e o router R3

Como é visível pela imagem anterior, todos os pacotes enviados para o túnel serão captados pela aplicação. pacotes que existentes no túnel.

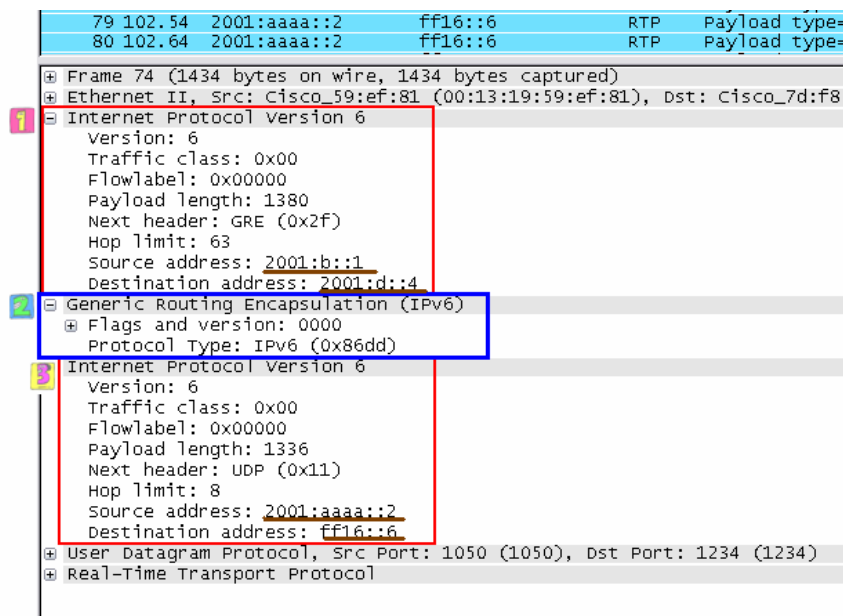


Figura 6.34 - Pacotes enviados no túnel

Observando a imagem anterior, é visível a existência de vários protocolos encapsulados uns dentro dos outros.

**Examinando a caixa 1:**

Analisando em pormenor a caixa identificada pelo número 1, é possível constatar que os pacotes estão a ser enviados com o IP origem [2001:B::1] e o IP destino [2001:D::4]. Observado também a imagem seguinte, é possível concluir que os referidos pacotes “utilizam” os endereços IPs configurados no

túnel (a imagem seguinte foi retirada do router R1). Ou seja, transporta os pacotes multicast IPv6 dentro do túnel.

```
interface Tunnel11
  ipv6 address 3FFE:A::2/64
  tunnel source 2001:B::1
  tunnel destination 2001:D::4
  tunnel mode gre ipv6
```

Figura 6.35 - Configurações do túnel efectuadas no R1

### Examinando a caixa 2:

Dado que se configurou o túnel recorrendo ao método GRE IPv6, e observando a caixa dois, conseguimos comprovar que, efectivamente, os pacotes multicast IPv6 estão a ser encapsulados dentro de pacotes GRE, sendo estes por sua vez encapsulados dentro de pacotes unicast (1).

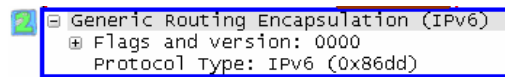


Figura 6.36 - Encapsulamento de pacotes multicast IPv6 no cabeçalho GRE

### Examinando a caixa 3:

Examinado a caixa 3, é visível que o pacote está a ser enviado pelo endereço [2001:AAAA::2], endereço correspondente à máquina servidor, para o endereço multicast [FF16::6].

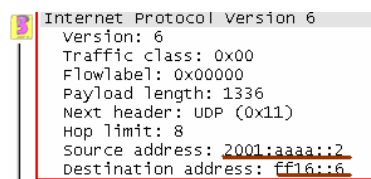
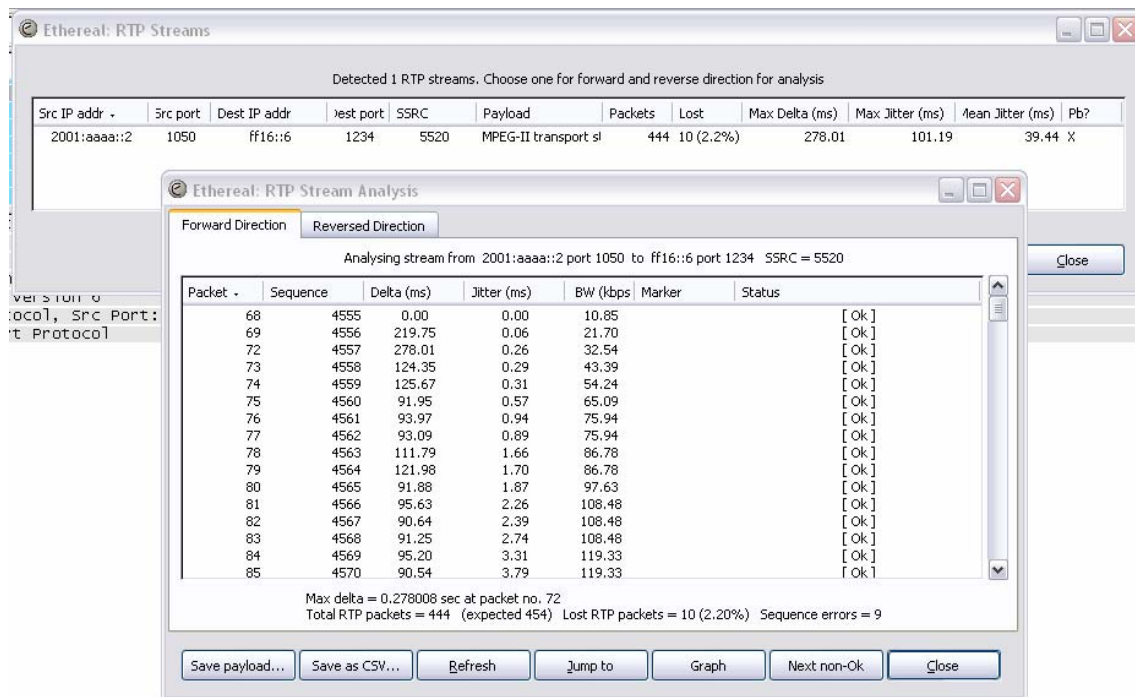


Figura 6.37 - Pacote multicast IPv6

### Passo 2: analisar os resultados

Depois configurado correctamente a aplicação foi possível analisar as estatísticas disponibilizadas pela mesma. A ferramenta Ehereal é bastante poderosa e como se pode verificar pela análise da figura seguinte, através desta é possível analisar por exemplo, a quantidade de pacotes, o número de pacotes perdidos, o atraso e a variação do atraso máxima.



Parâmetros de QoS medidos pelo Ethereal

### 6.4.3 Cenário III – IPv6 multicast em redes IPv4

Nos cenários anteriores, foram implementados cenários nativos, ou recorrendo ao uso de túneis IPv6 unicast para “transportar” os pacotes multicast. No entanto, e se não existir encaminhamento unicast IPv6, será que estamos limitados, ou existe uma outra forma de encaminhar os pacotes multicast IPv6?

Para esclarecer estas duvidas, foi implementado na ESTG –Leiria um cenário usando redes IPv4 e multicast IPv6 nos extremos. A figura seguinte esquematiza o cenário e a topologia utilizada.

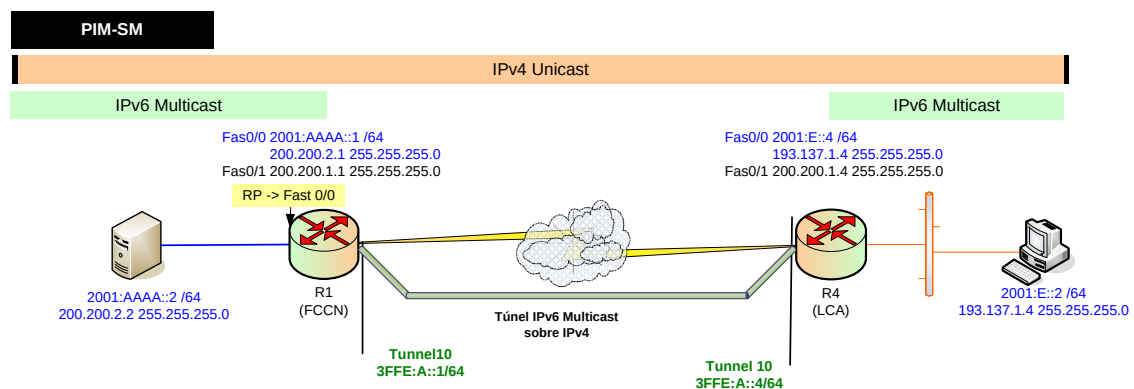


Figura 6.38 - IPv6 multicast em redes IPv4

## Configuração dos equipamentos

De seguida são apresentadas as principais configurações efectuadas nos equipamentos e para cada uma delas, é exibida uma pequena descrição da sua utilidade. Por forma a descrever correctamente a utilidade e a descrição de cada comando, foi usada seguinte referência [Cisco IOS 12.4 Command Reference].

| Router R1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> hostname R1 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel10  ipv6 address 3FFE:A::1/64  tunnel source 200.200.1.1  tunnel destination 200.200.1.4  tunnel mode ipv6ip ! interface FastEthernet0/0  ip address 200.200.2.1 255.255.255.0  ipv6 address 2001:AAAA::1/64 ! interface FastEthernet0/1  ip address 200.200.1.1 255.255.255.0 ! ip route 193.137.1.0 255.255.255.0 200.200.1.4 ! ipv6 route 2001:E::/64 3FFE:A::4 ipv6 pim rp-address 2001:AAAA::1 </pre> | <pre> interface Tunnel10  ipv6 address 3FFE:A::1/64  tunnel source 200.200.1.1  tunnel destination 200.200.1.4  tunnel mode ipv6ip </pre> <p>Os comandos anteriores configuram o túnel.</p> <ul style="list-style-type: none"> <li>-Origem do túnel: endereço da interface FastEthernet0/1 do <b>R1</b></li> <li>-Destino do túnel (extremidade remota): FastEthernet0/1 do <b>R2</b></li> <li>-Tipo de túnel: o tipo de túnel usado vai indicar ao router que é necessário transportar os pacotes multicast IPv6 imediatamente sobre os pacotes unicast IPv6. Convém mencionar que esta configuração é diferente da anterior, dado que a antiga exigia mais processamento ao router pelo facto de usar uma cabeçalho GRE. No sub capítulo testes, desta secção são apresentados imagens retiradas através do Ethereal que ajudam a compreender o funcionamento deste tipo de encapsulamento.</li> </ul> <pre> interface FastEthernet0/0  ip address 200.200.2.1 255.255.255.0  ipv6 address 2001:AAAA::1/64 </pre> <pre> interface FastEthernet0/1  ip address 200.200.1.1 255.255.255.0 </pre> <p>Configuração dos endereços IPv4 e IPv6 associados às interfaces</p> <pre> ip route 193.137.1.0 255.255.255.0 200.200.1.4 </pre> <p>O comando indica ao router qual a interface de saída a utilizar, quando é necessário enviar pacotes para a rede 193.137.1.0</p> <pre> ipv6 route 2001:E::/64 3FFE:A::4 </pre> |

|  |                                                                                                                                                              |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Rota utilizada para enviar os pacotes multicast para o túnel.</p> <pre>ipv6 pim rp-address 2001:AAAA::1</pre> <p>O comando indica ao equipamento o RP</p> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Router R2                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Descrição                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>hostname R2 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel10 ipv6 address 3FFE:A::4/64 tunnel source 200.200.1.4 tunnel destination 200.200.1.1 tunnel mode ipv6ip ! interface FastEthernet0/0 ip address 193.137.1.4 255.255.255.0 ipv6 address 2001:E::4/64 ! interface FastEthernet0/1 ip address 200.200.1.4 255.255.255.0 ! ip route 0.0.0.0 0.0.0.0 200.200.1.1 ! ipv6 route ::/0 3FFE:A::1 ipv6 pim rp-address 2001:AAAA::1</pre> | <pre>interface Tunnel10 ipv6 address 3FFE:A::4/64 tunnel source 200.200.1.4 tunnel destination 200.200.1.1 tunnel mode ipv6ip</pre> <p>Os comandos anteriores configuram o túnel.</p> <ul style="list-style-type: none"> <li>-Origem do túnel: FastEthernet0/1 do R2</li> <li>-Destino do túnel (extremidade remota): endereço da interface FastEthernet0/1 do R1</li> <li>-Tipo de túnel: Dado que no R1 já se configurou o tipo de túnel a utilizar, é necessário fazer o mesmo no router R4</li> </ul> <pre>interface FastEthernet0/0 ip address 193.137.1.4 255.255.255.0 ipv6 address 2001:E::4/64 interface FastEthernet0/1 ip address 200.200.1.4 255.255.255.0</pre> <p>Configuração dos endereços IPv4 e IPv6 associados às interfaces</p> <pre>ip route 0.0.0.0 0.0.0.0 200.200.1.1</pre> <p>Rota estática por omissão IPv4</p> <pre>ipv6 route ::/0 3FFE:A::1</pre> <p>Rota utilizada para enviar os pacotes multicast para o túnel.</p> <pre>ipv6 pim rp-address 2001:AAAA::1</pre> <p>O comando indica ao equipamento o RP</p> |

## Configuração das aplicações

Dado que nestes teste se utilizou o mesmo grupo multicast para enviar os pacotes, as configurações nas aplicações são exactamente iguais às efectuadas anteriormente.

## Problemas encontrados

Neste cenário não foram encontrados problemas de configuração. O motivo principal devou-se ao facto de já se dominar perfeitamente a tecnologia.

## Testes

conjunto de passos com vista a descobrir onde estaria eventualmente o problema.

### 6.4.4 Cenário IV – Simular uma Ligação nativa à FCCN

Para finalizar os testes usando o paradigma PIM-SM foi implementado o cenário seguinte. No entanto para este não são apresentados os detalhes de configuração dos equipamentos, nem das aplicações, dado que este cenário é idêntico ao primeiro cenário implementado.

Em anexo são apresetes as configurações efectuadas nos equipamentos.

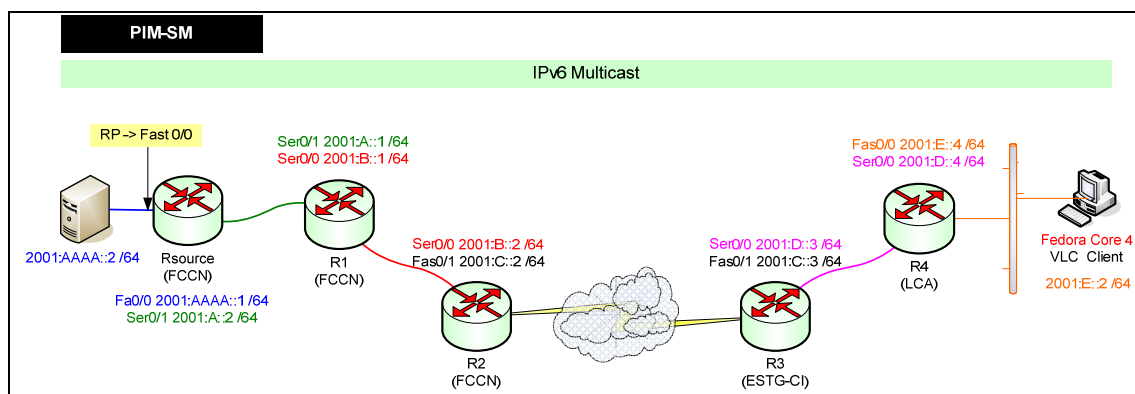


Figura 6.39 - Simular uma ligação nativa multicast IPv6

Dado que actualmente a ESTG não dispõem de uma ligação multicast IPv6 nativa com a FCCN, este cenário pretende simular o que irá acontecer num futuro breve, quando a FCCN fornecer conectividade multicast aos seus parceiros.

## 6.5 Testes Multicast IPv6: Embedded RP

Nesta secção são apresentados diferentes cenários usando o paradigma de comunicação multicast *Embedded RP*. Mais concretamente, estes são esquematizados numa primeira fase, sendo de seguida para cada um deles, explicados os detalhes de implementação ao nível dos equipamentos e das



aplicações. São analisados diversos parâmetros de QoS (qualidade de serviço), enumerados os principais problemas encontrados e descrita a forma encontrada de os resolver.

### 6.5.1 Cenário I – Multicast IPv6 Nativo

A figura seguinte apresenta um cenário configurado com *Embedded RP*. Este método, recente e projectado especificamente para IPv6, permite que o endereço do RP seja embutido no próprio endereço IPv6 do grupo *multicast*. Convém frisar que a versão do IOS usada nos testes, a mais recente até à data, compilada em Outubro de 2005, contém alguns bugs, bugs esses que se podem explicar pela imaturidade da tecnologia. Na secção *Problemas Encontrados* são apresentadas as configurações e os motivos que levam o equipamento a funcionar incorrectamente.

O esquema seguinte foi testado com sucesso nos laboratórios da ESTG – Leiria. Convém novamente referir que, com *Embedded RP*, apenas é necessário configurar um equipamento como RP. Assim, nos testes efectuados, definiu-se o RP como sendo o *Router 1*, tendo este associado o seguinte endereço [2001:AAA:BEEF:FEED::1].

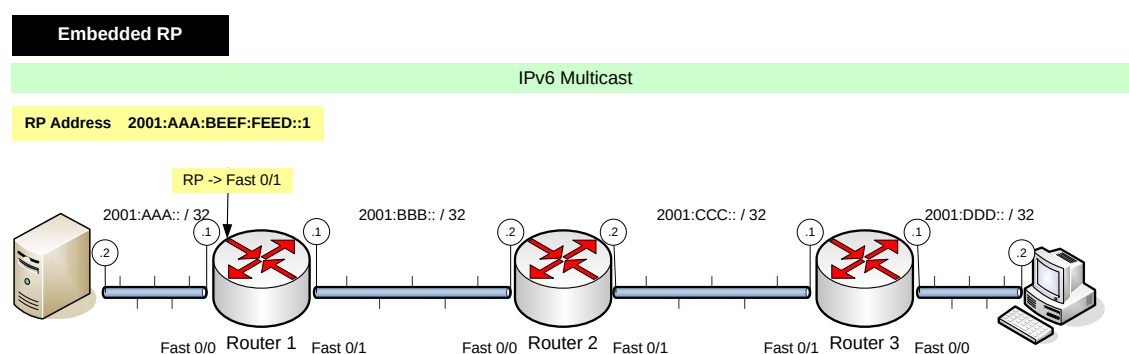


Figura 6.40 - Cenário multicast IPv6 nativo usando o paradigma *Embedded RP*

Neste cenário foram utilizados dois PCs, sendo o da esquerda utilizado como servidor e o da direita como cliente. No que se refere aos equipamentos responsáveis pelo encaminhamento, foram utilizados três routers Cisco da série 2600XM, com duas interfaces FastEthernet.

No que se refere ao endereçamento, este foi mantido, ou seja, foi utilizado o endereçamento já utilizado em testes anteriores.

## Configuração dos equipamentos

De seguida são apresentadas todas as configurações efectuadas nos equipamentos e, para as principais, é exibida uma pequena descrição da sua utilidade. Convém referir que, para se descrever a utilidade e funcionamento de cada comando foi consultada a seguinte referência [25].

```
hostname R1
!
ipv6 unicast-routing
ipv6 multicast-routing
!
interface FastEthernet0/0
  ipv6 address 2001:AAA::1/32
  ipv6 address 2001:AAA:BEEF:FEED::1/32
  ipv6 rip cisco enable
!
interface FastEthernet0/1
  ipv6 address 2001:BBB::1/32
  ipv6 rip cisco enable
!
ipv6 router rip cisco
!
ipv6 pim rp-address 2001:AAA:BEEF:FEED::1
```

**Figura 6.41** - Configurações efectuadas no **Router 1**

```
ipv6 unicast-routing
```

Activação do *forwarding* dos pacotes IPv6.

```
ipv6 multicast-routing
```

Activação do protocolo multicast PIM (PIM – *Protocol Independent Multicast*), assim como do MLD (MLD – *Multicast Listener Discovery*) e do encaminhamento de pacotes multicast

```
interface FastEthernet0/0
  ipv6 address 2001:AAA::1/32
  ipv6 address 2001:AAA:BEEF:FEED::1/32
  ipv6 rip cisco enable
```

Depois de ser ter entrado no modo de configuração da interface FastEthernet0/0, configuraram-se dois endereços IPv6 e activou-se o processo IPv6 Routing Information Protocol (RIP).

Relativamente ao endereço IPv6 a negrito, o segundo, este foi definido unicamente para identificar o endereço do RP. Não é necessário definir um endereço específico para o efeito, mas dado que este cenário foi baseado num exemplo existente na RFC 3959, resolveu-se utilizar dois endereços independentes.

```
ipv6 pim rp-address 2001:AAA:BEEF:FEED::1
```

O comando indica ao equipamento que o ponto central da rede, RP, é ele próprio (interface FastEthernet0/0)

```
interface FastEthernet0/1
  ipv6 address 2001:BBB::1/32
  ipv6 rip cisco enable
```

Activação do processo de routing na interface e atribuição de um endereço IPv6 à mesma.

```
ipv6 router rip cisco
```

Activação do protocolo de encaminhamento RIP.

Configurações efectuadas no **Router 2 e Router 3**.

As configurações efectuadas no router 2 e 3 são idênticas à efectuada no Router 1. A grande diferença reside nos IPs utilizados e na falta do comando: **ipv6 pim rp-address 2001:AAA:BEEF:FEED::1**

|                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>hostname R3 ! ipv6 unicast-routing ipv6 multicast-routing ! interface FastEthernet0/0   ipv6 address 2001:DDD::1/32   ipv6 rip cisco enable ! interface FastEthernet0/1   ipv6 address 2001:CCC::1/32   ipv6 rip cisco enable ! ipv6 router rip cisco</pre> | <pre>hostname R2 ! ipv6 unicast-routing ipv6 multicast-routing ! !interface FastEthernet0/0   ipv6 address 2001:BBB::2/32   ipv6 rip cisco enable ! interface FastEthernet0/1   ipv6 address 2001:CCC::2/32   ipv6 rip cisco enable ! ipv6 router rip cisco</pre> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Figura 6.42 - Embedded RP, cenário nativo - Principais configurações efectuadas no Router 2 e Router 3

Como é visível pela tabela anterior, no router 2 e no router 3 não foi necessário introduzir o comando que indica onde está a raiz da árvore, ou seja, onde está o RP. Este é apreendido automaticamente pelo endereço configurado nas aplicações cliente e servidora. Assim, é possível a qualquer altura alterar o endereço do RP, no router R1, não sendo necessário alterar nenhuma das configurações existentes nos restantes equipamentos.

## Configuração das aplicações

Nesta secção é detalhado todo o processo de configuração da aplicação existente no servidor e no cliente. Desta forma, numa primeira fase é detalhado todo o processo de configuração da aplicação servidora, sendo posteriormente apresentada a forma de configurar a aplicação cliente.

### Aplicação servidora

Com *Embedded RP* [RFC 3306], as aplicações, bem como os IPs usados têm um papel bastante importante. Assim, para realizar este tipo de testes tem que se usar uma gama de endereços específicos e reservados – [FF7x /12]. O 4º dígito é utilizado para definir a abrangência do endereço.

As figuras seguintes contêm as configurações efectuadas no servidor. É possível verificar que foi usado o endereço [FF76:140:2001:AAA:BEEF:FEED::4321]. Desta forma, os routers ao receberem um pacote iniciado em FF7x, sabem logo à partida que estão perante endereços *Embedded RP* e que é necessário retirar do endereço do grupo, o endereço do RP.

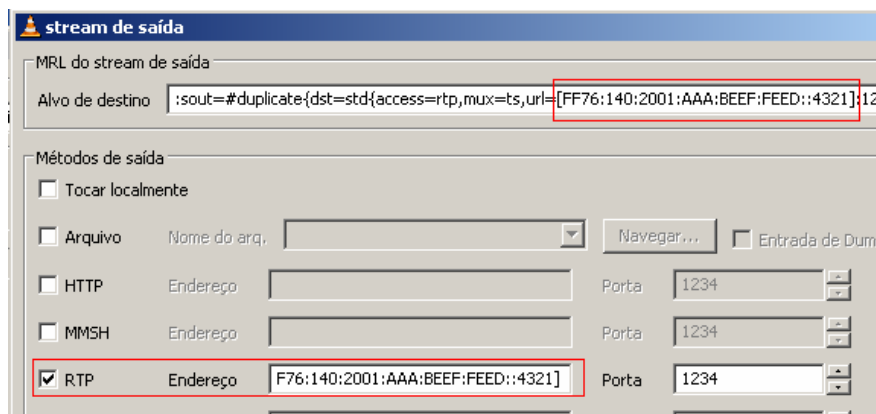


Figura 6.43 - Embedded RP, cenário nativo - Configurar o VLC para emitir vídeo

Observando com detalhe o endereço utilizado no servidor pode-se concluir o seguinte:



Figura 6.44 - Embedded RP, cenário nativo - Endereço do grupo multicast configurado no servidor

O RP terá de ter o endereço [2001:AAA:BEEF:FEED::1] (1) e o grupo multicast irá ser o [4321] – 3. Desta forma, ao retirar-se do endereço os caracteres referentes à configuração do RP e os caracteres contidos na caixa com o número 3, fica-se efectivamente com o endereço do grupo IPv6 multicast [FF76::4321].

## Aplicação Cliente

Na aplicação cliente é necessário efectuar precisamente o mesmo que foi feito na aplicação servidora, ou seja, é também necessário usar o IP [FF76:140:2001:AAA:BEEF:FEED::4321]. Assim, a figura seguinte demonstra efectivamente a configuração introduzida na máquina cliente.



Figura 6.45 - Embedded RP, cenário nativo - Configurar o VLC para receber vídeo

## Problemas encontrados

Colocar este cenário a funcionar não foi tarefa fácil. Depois de se ter estudado a tecnologia passou-se à fase de implementação. Supostamente este método seria simples de configurar, mas na prática isso não se verificou. Desta forma, na altura da implementação foi detectado um comportamento inesperado nos equipamentos, que condicionava todo o cenário, verificando-se que os equipamentos reiniciavam automaticamente.

O esquema seguinte apresenta o erro devolvido pelo equipamento. Como é visível, inesperadamente e sem se estar sequer a configurar, o equipamento lança uma excepção e reinicia automaticamente.

Press RETURN to get started.

```
15:51:59 UTC Mon Mar 4 2002: Unexpected exception to CPUvector 1200, PC =
0x814D7104, LR = 0x814D70E4
```

```
-Traceback= 0x814D7104 0x81F6CDB8 0x819528D8 0x81952914 0x827F6384 0x827F72C8
0x827E2C94 0x827E2EE8 0x827DB198 0x8280D6F0 0x8280D880 0x827DB8E4 0x8280CAF8
0x8280CCE8 0x827CC06C 0x827CB754
```

CPU Register Context:

```
MSR = 0x00009032 CR = 0x30009009 CTR = 0x806FAF98 XER = 0x80001C7F
R0 = 0x00000030 R1 = 0x85D5E0D0 R2 = 0x84AD0000 R3 = 0x00000001
R4 = 0x851AE3A0 R5 = 0x851AE1D4 R6 = 0x00000001 R7 = 0x68010000
R8 = 0x00009032 R9 = 0x00000000 R10 = 0x68010000 R11 = 0x84C10000
R12 = 0x02147698 R13 = 0xFFFF4B634 R14 = 0x8519F1A8 R15 = 0x00000000
R16 = 0x84C9DBE4 R17 = 0x00000000 R18 = 0x84ED1C1C R19 = 0x84390000
R20 = 0x84390000 R21 = 0x84ED0000 R22 = 0x00000000 R23 = 0x00000590
R24 = 0x85417140 R25 = 0x00000001 R26 = 0x00000560 R27 = 0x00000024
R28 = 0x074050D8 R29 = 0x85D42318 R30 = 0x84FD18FC R31 = 0x84FD18FC
```

```

Writing crashinfo to flash:crashinfo_20020304-155159

=== Flushing messages (15:51:59 UTC Mon Mar 4 2002) ===

Queued messages
*** System received a SegV exception ***
signal= 0xb, code= 0x1200, context= 0x84e24818
PC = 0x814d7104, Vector = 0x1200, SP = 0x85d5e0d0

System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Copyright (c) 2003 by cisco Systems, Inc.
C2600 platform with 131072 Kbytes of main memory
    
```

Tabela 6.7 - Problemas no cenário Embedded RP

Dado que os equipamentos estavam a dar problemas, pensou-se numa primeira fase que o problema seria das configurações e, como tal, foi efectuado um estudo exaustivo sobre o paradigma *Embedded RP*. De modo a tentar esclarecer o que estaria a causar o problema foram colocadas questões no site da Cisco sobre este assunto mas não se obtiveram respostas conclusivas.

Enquanto se esperava por respostas, foi efectuado em laboratório um conjunto de testes com vista a tentar descobrir a causa do problema. Depois de muitas horas perdidas, conseguiu-se empiricamente concluir que a versão do IOS usada nos testes (IOS 12.4(5)M) possuía dois bugs.

### Bug 1: o RP tem de estar na mesma rede do servidor

Embedded RP: Cenário com Erro!!!

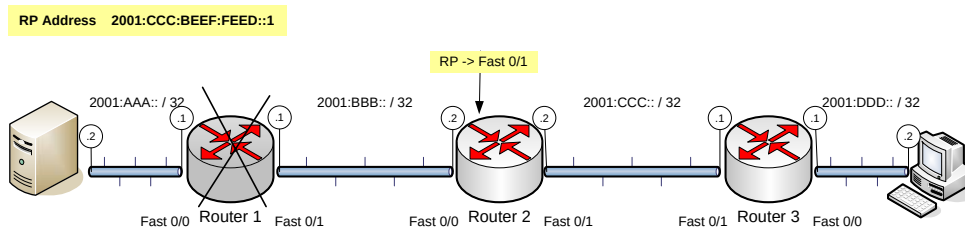


Figura 6.46 - Cenário incorrecto: o RP não está colocado no sítio certo

Como é visível na imagem anterior, o RP está configurado no 'Router 2'. Usando esta configuração e quando se coloca a servidor a enviar o *stream*, o 'Router 1' lança uma excepção e reinicia automaticamente.

### Bug 2: O endereço colocado no cliente/servidor não coincide com o RP configurado

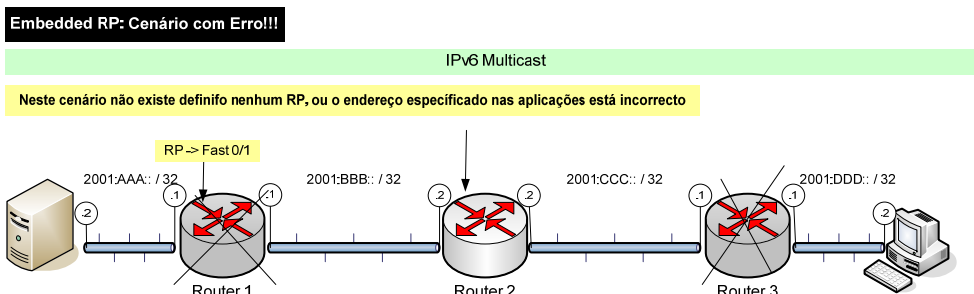


Figura 6.47 - Cenário incorrecto: não existe um RP definido

Caso não se configure correctamente no cliente ou no servidor o endereço do RP, o router mais próximo da primeira aplicação a ser executada vai *crachar*. Este problema vai acontecer mesmo que se configure o RP na mesma rede do servidor. Desta forma, é necessário introduzir com minúcia nas aplicações o endereço IPv6 multicast, dado que, como foi verificado, se se introduzir um endereço incorrecto os equipamentos falham.

Depois de se terem identificado as causas dos problemas, foi possível visualizar no cliente o vídeo difundido pelo servidor.

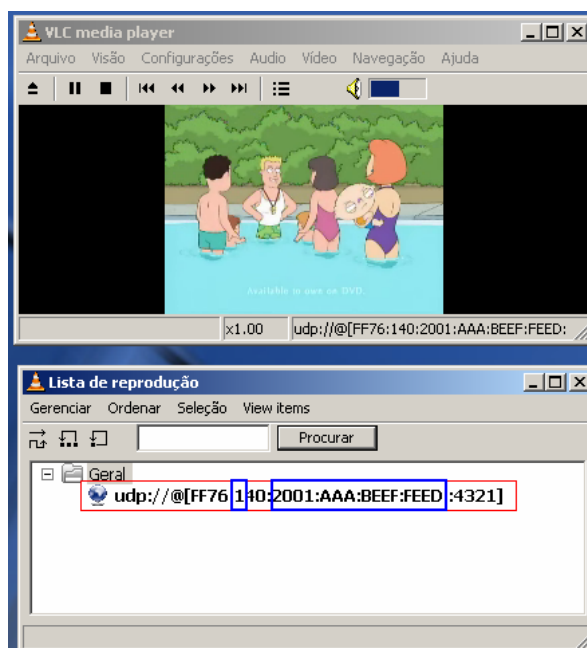


Figura 6.48 - Embedded RP, cenário nativo - Visualização do Stream de vídeo no cliente

## Testes

Nesta secção são apresentados e analisados diversos parâmetros de QoS (qualidade de serviço) usando o paradigma *Embedded RP*. Mais uma vez foi colocado o *Etherreal* no último troço de rede, ou seja, foi colocado entre o 'Router3' e o PC cliente.

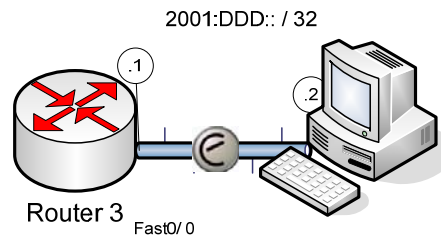


Figura 6.49 - Embedded RP, cenário nativo - Ethereal colocado entre o PC cliente e o Router 3

A imagem seguinte demonstra que os pacotes enviados pelo servidor [2001:AAA::2] têm como destinatário o endereço [FF76:140:2001:AAA:BEEF:FEED::4321]. Desta forma, dado que o cliente se registou também nesse grupo, este vai também receber o stream de vídeo.

| No. | Time  | Source      | Destination                        | Protocol | Ir |
|-----|-------|-------------|------------------------------------|----------|----|
| 44  | 43.67 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 45  | 43.70 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 46  | 43.73 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 47  | 43.76 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 48  | 43.78 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 49  | 43.81 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 50  | 43.84 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 51  | 43.87 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 52  | 43.90 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 53  | 43.93 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |
| 54  | 43.98 | 2001:aaa::2 | ff76:140:2001:aaa:beef:feed:0:4321 | RTP      | P  |

|                                                                                     |  |
|-------------------------------------------------------------------------------------|--|
| Frame 44 (1390 bytes on wire, 1390 bytes captured)                                  |  |
| Ethernet II, Src: Cisco_59:f1:e0 (00:13:19:59:f1:e0), Dst: IPv6-Neighbor-Discovery_ |  |
| Internet Protocol Version 6                                                         |  |
| Version: 6                                                                          |  |
| Traffic class: 0x00                                                                 |  |
| Flowlabel: 0x00000                                                                  |  |
| Payload length: 1336                                                                |  |
| Next header: UDP (0x11)                                                             |  |
| Hop limit: 61                                                                       |  |
| Source address: 2001:aaa::2                                                         |  |
| Destination address: ff76:140:2001:aaa:beef:feed:0:4321                             |  |
| User Datagram Protocol, Src Port: 1364 (1364), Dst Port: 1234 (1234)                |  |
| Real-Time Transport Protocol                                                        |  |

Pacotes multicast destinados ao endereço [FF76:140:2001:AAA:BEEF:FEED::4321]

## Passo 2: Analisar os resultados

Depois de configurada correctamente a aplicação, foi possível analisar as estatísticas disponibilizadas pela mesma. A figura seguinte demonstra a forma de obter estatísticas.



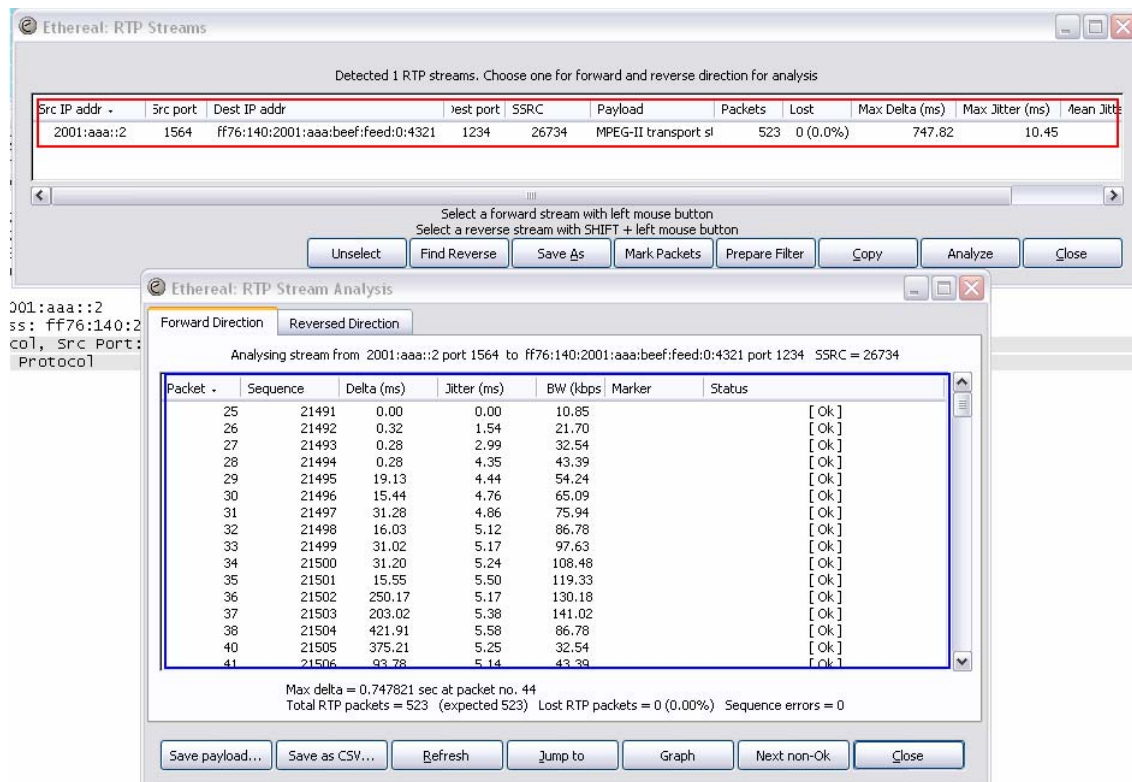


Figura 6.50 - Parâmetros de QoS medidos pelo Ethereal

## 6.5.2 Cenário II – Multicast IPv6 sobre um túnel IPv6

Depois de se ter efectuado o cenário anterior, resolveu-se efectuar um outro, mais complexo, recorrendo ao uso de túneis. Assim, o esquema seguinte apresenta o cenário Multicast IPv6 sobre um túnel IPv6.

Convém mencionar que o cenário apresentado foi apenas testado em laboratório.

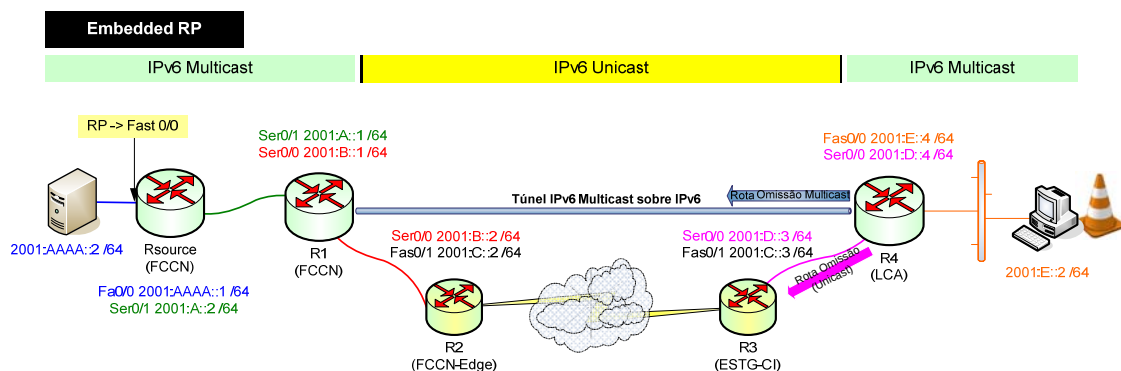


Figura 6.51 - Cenário baseado num esquema presente na M6Bone

Mais uma vez utilizaram-se 5 routers e dois PCs. A tabela seguinte identifica quais os equipamentos que apenas suportam unicast e quais os equipamentos que suportam multicast IPv6 e obviamente unicast IPv6 também.

| Routers Multicast                                  | Routers Unicast               |
|----------------------------------------------------|-------------------------------|
| Rsource; R1 (FCCN) e R4 (LCA)                      | R2 (FCCN-Edge) e R3 (ESTG-CI) |
| Equipamentos configurados como Multicast e Unicast |                               |

## **Configuração dos equipamentos**

Dado que as configurações, para o RSource – o RP, são semelhantes às efectuadas em cenários anteriores, estas serão apenas apresentadas em forma de esquema, não sendo necessário recorrer à descrição pormenorizada dos comandos. A única diferença reside no facto de, neste cenário, se ter usado o IP da interface FastEthernet como endereço RP.

```
hostname RSource
!
ipv6 unicast-routing
ipv6 multicast-routing
!
interface FastEthernet0/0
ipv6 address 2001:AAAA::1/64
ipv6 rip FCCN enable
!
interface Serial0/1
ipv6 address 2001:A::2/64
ipv6 rip FCCN enable
!
ipv6 router rip FCCN
!
ipv6 pim rp-address 2001:AAAA::1
```

Figura 6.52 - Configurações efectuadas no Router ‘RSource’

Configurações efectuadas no Router 1 e Router 4.

Como é visível pela tabela seguinte, nos restantes *routers* não foi necessário introduzir o comando [ipv6 pim rp-address 2001:AAAA::1]. As configurações efectuadas nos *routers* 1 e 4 são idênticas, diferindo apenas nos IP utilizados.

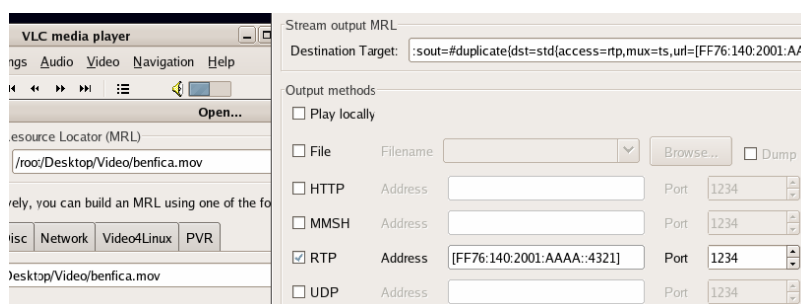
|                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> hostname R1 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel11 ipv6 address 3FFE:A::2/64 tunnel source 2001:B::1 tunnel destination 2001:D::4 tunnel mode gre ipv6 ! interface Serial0/0 ipv6 address 2001:B::1/64 ipv6 rip FCCN enable ! interface Serial0/1 ipv6 address 2001:A::1/64 ipv6 rip FCCN enable ! ipv6 route 2001:D::/64 3FFE:A::1 multicast ! ipv6 router rip FCCN </pre> | <pre> hostname R4 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel11 ipv6 address 3FFE:A::1/64 tunnel source 2001:D::4 tunnel destination 2001:B::1 tunnel mode gre ipv6 ! interface FastEthernet0/0 ipv6 address 2001:E::4/64 ipv6 rip ESTG_Leiria enable ! interface Serial0/0 ipv6 address 2001:D::4/64 ipv6 rip ESTG_Leiria enable ! ipv6 route ::/0 3FFE:A::2 multicast ! ipv6 router rip ESTG_Leiria </pre> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Principais configurações efectuadas no Router 1 e Router 4

## Configuração das aplicações

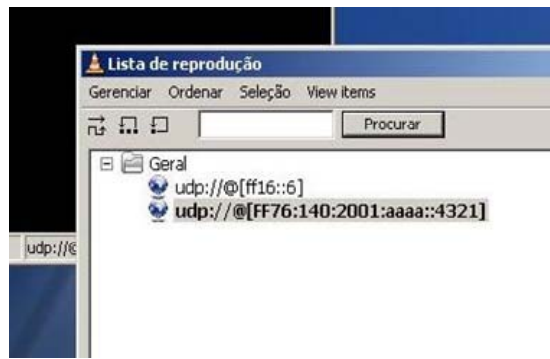
Dado que neste cenário se usou o endereço da interface FastEthernet do Router ‘RSource’ como endereço do RP, então foi necessário modificar as aplicações. A imagem seguinte ilustra as configurações introduzidas no servidor.

Como é visível, está-se a utilizar o endereço [FF76:140:2001:AAAA::4321]. Se se observar os caracteres a negrito, verifica-se que o endereço do RP é o 2001:AAAA::1, o que coincide efectivamente com o IP da interface FastEthernet do ‘RSource’.



Embedded RP, cenário com túneis - configuração da aplicação no servidor

A figura seguinte contém a configuração efectuada no VLC do PC cliente. Efectivamente, é possível verificar que esta coincide com a configuração introduzida no servidor.



Embedded RP, cenário com túneis - configuração da aplicação no cliente

## Problemas encontrados

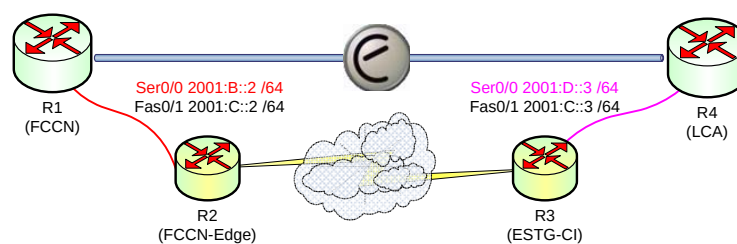
Neste cenário não foram encontrados nenhuns problemas pois foram respeitadas as limitações dos equipamentos, ou seja, foi definido o RP como o router mais próximo da fonte e foram introduzidos com minúcia os endereços das aplicações cliente e servidor. Desta forma, garantiu-se que os equipamentos não se reiniciavam automaticamente.

## Testes

Nesta secção é demonstrado, numa primeira fase, o funcionamento do túnel, sendo posteriormente analisados alguns parâmetros de QoS medidos pelo Ethereal.

### Passo 1: Funcionamento do túnel

Para compreender o funcionamento túnel do resolveu-se utilizar o Ethereal, e colocá-lo a captar os pacotes existentes no túnel. A imagem seguinte demonstra onde este foi colocado.



Ethereal colocado entre o router R2 e o router R3

Como é visível pela imagem anterior, todos os pacotes enviados para o túnel serão captados pela aplicação.

| No. | Time  | Source       | Destination              | Protocol |
|-----|-------|--------------|--------------------------|----------|
| 63  | 10.97 | 2001:aaaa::2 | ff76:140:2001:aaaa::4321 | RTP      |
| 64  | 11.06 | 2001:aaaa::2 | ff76:140:2001:aaaa::4321 | RTP      |
| 65  | 11.15 | 2001:aaaa::2 | ff76:140:2001:aaaa::4321 | RTP      |

|                                                                                               |
|-----------------------------------------------------------------------------------------------|
| Frame 63 (1434 bytes on wire, 1434 bytes captured)                                            |
| Ethernet II, Src: Cisco_59:ef:81 (00:13:19:59:ef:81), Dst: Cisco_7d:f8:41 (00:0c:29:7d:f8:41) |
| Internet Protocol Version 6                                                                   |
| Version: 6                                                                                    |
| Traffic class: 0x00                                                                           |
| Flowlabel: 0x00000                                                                            |
| Payload length: 1380                                                                          |
| Next header: GRE (0x2f)                                                                       |
| Hop limit: 63                                                                                 |
| Source address: 2001:b::1                                                                     |
| Destination address: 2001:d::4                                                                |
| Generic Routing Encapsulation (IPv6)                                                          |
| Flags and version: 0000                                                                       |
| Protocol Type: IPv6 (0x86dd)                                                                  |
| Internet Protocol Version 6                                                                   |
| Version: 6                                                                                    |
| Traffic class: 0x00                                                                           |
| Flowlabel: 0x00000                                                                            |
| Payload length: 1336                                                                          |
| Next header: UDP (0x11)                                                                       |
| Hop limit: 8                                                                                  |
| Source address: 2001:aaaa::2                                                                  |
| Destination address: ff76:140:2001:aaaa::4321                                                 |
| User Datagram Protocol, Src Port: 33096 (33096), Dst Port: 1234 (1234)                        |
| Real-time Transport Protocol                                                                  |

Pacotes enviados no túnel

Observando a imagem anterior, é perceptível a existência de vários protocolos encapsulados uns dentro dos outros.

### Examinando a caixa 1:

Analisando em pormenor a caixa identificada pelo número 1, é possível constatar que os pacotes estão a ser enviados com o IP origem [2001:B::1] e o IP destino [2001:D::4]. Observando também a imagem seguinte, é possível concluir que os referidos pacotes utilizam os endereços IP configurados no túnel (a imagem seguinte foi retirada do router R1). Ou seja, é efectuado o transporte dos pacotes multicast IPv6 dentro do túnel.

```
interface Tunnel11
  ipv6 address 3FFE:A::2/64
  tunnel source 2001:B::1
  tunnel destination 2001:D::4
  tunnel mode gre ipv6
```

Figura 6.53 - Configurações do túnel efectuadas no R1

### Examinando a caixa 2:

Dado que se configurou o túnel recorrendo ao método GRE IPv6, e observando a caixa dois, consegue-se comprovar que, efectivamente, os pacotes multicast IPv6 estão a ser encapsulados dentro de pacotes GRE, sendo estes por sua vez encapsulados dentro de pacotes unicast (1).

|                                      |
|--------------------------------------|
| Generic Routing Encapsulation (IPv6) |
| Flags and version: 0000              |
| Protocol Type: IPv6 (0x86dd)         |

Figura 6.54 - Encapsulamento de pacotes multicast IPv6 no cabeçalho GRE

## Examinando a caixa 3:

Examinando a caixa 3, é visível que o pacote está a ser enviado pelo endereço [2001:AAAA::2], endereço correspondente à máquina servidor, para o endereço multicast [FF76:140:2001:AAAA::4321].

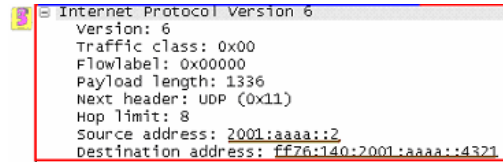


Figura 6.55 - Pacote multicast IPv6

## Passo 2: Análise dos resultados

Nesta secção são analisados, recorrendo ao Ethereal, vários parâmetros de QoS, tais como, a quantidade de pacotes, o número de pacotes perdidos, o atraso e a variação máxima do atraso dos mesmos.

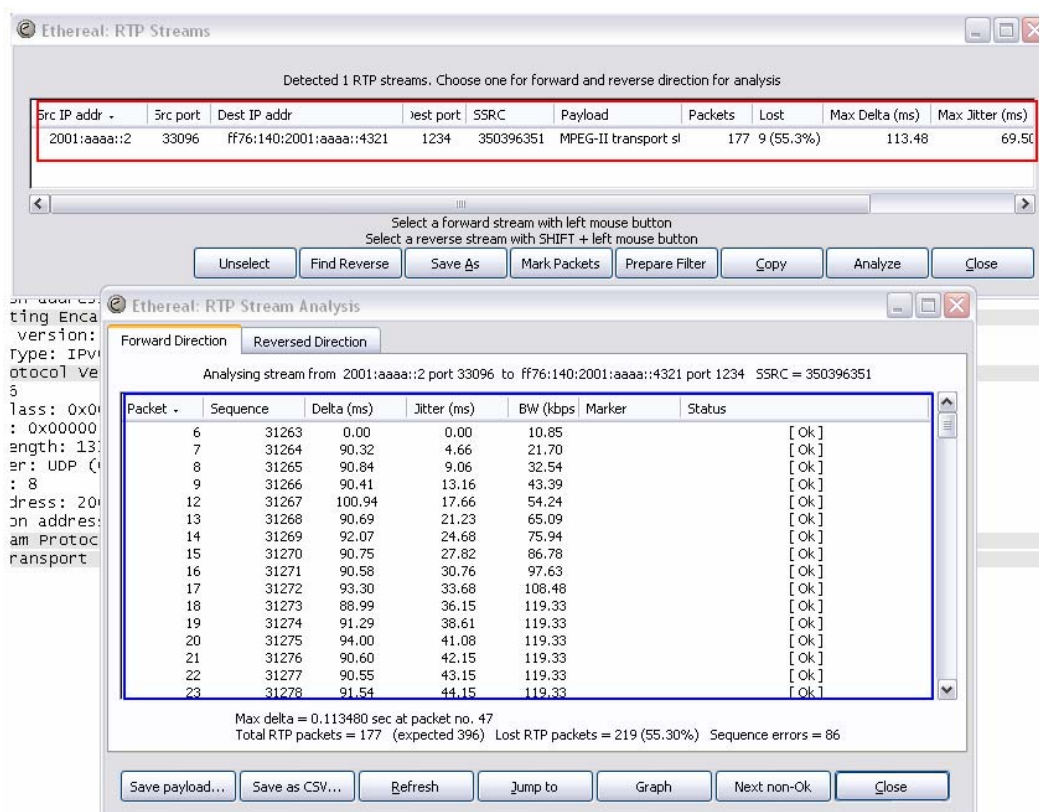


Figura 6.56 - Parâmetros de QoS medidos pelo Ethereal

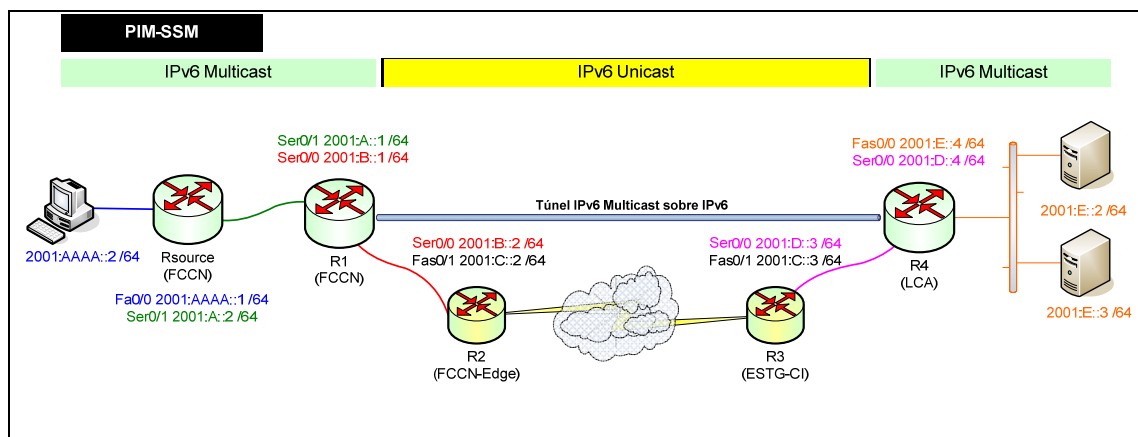
## 6.6 Testes Multicast IPv6: PIM-SSM

Como é sabido, o PIM-SSM tem inúmeras vantagens quando comparado com o seu predecessor, o PIM – SM (Sparse Mode). Com a utilização deste método, a rede não necessita de ter um ponto central, conhecido como RP, e por conseguinte não usa árvores de distribuição de tráfego. Assim, este é substancialmente mais simples que o PIM-SM e bastante mais escalável.

Apesar das vantagens evidentes, este método ainda não está muito divulgado. Um factor que tem limitado a sua utilização, é o facto de necessitar da versão dois do MLD (semelhante ao IGMPv3), sendo que, actualmente esta apenas esta disponível nos sistemas Linux [12]. Segundo responsáveis da Microsoft, a versão dois do MLD (MLDv2) irá estar disponível na próxima versão do Windows, conhecido como Windows Vista.

### 6.6.1 Cenário – Multicast IPv6 sobre um túnel IPv6

Quando se pretende implementar cenários com PIM – SSM deve-se ter em mente que os endereços tem obrigatoriamente de começar por [FF3x:: /12]



Cenário utilizado para testar o PIM-SSM

O cenário anterior, implementado no decorrer deste projecto, foi configurado recorrendo ao uso do paradigma SSM. Convém mencionar que este foi apenas testado em laboratório.

Mais uma vez, e como já tem sido habito, usaram-se 5 roteadores e dois PC. A tabela seguinte “identifica” quais os equipamentos que apenas suportam unicast e quais os equipamentos que suportam multicast IPv6 e obviamente unicast IPv6 também.

| Routers Multicast             | Routers Unicast               |
|-------------------------------|-------------------------------|
| Rsource; R1 (FCCN) e R4 (LCA) | R2 (FCCN-Edge) e R3 (ESTG-CI) |

## Configuração dos equipamentos

Como já foi referido, com PIM – SSM não é necessário configurar nada nos equipamentos, ou seja, basta apenas activar o encaminhamento *multicast*, e automaticamente os pacotes são enviados pelos servidores para os clientes registados no grupo. Esta característica deve-se ao facto de, usando o PIM-SSM, não existir um ponto central na rede, responsável por controlar a distribuição dos pacotes. Essas funções passaram a estar delegadas para os clientes.

Como tal, as configurações são extremamente simples. Assim, desta forma, nesta secção são apresentadas as configurações efectuadas nos equipamentos.

|                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>hostname RSources ! ipv6 unicast-routing ipv6 multicast-routing ! interface FastEthernet0/0 ipv6 address 2001:AAAA::1/64 ipv6 rip FCCN enable ! interface Serial0/1 ipv6 address 2001:A::2/64 ipv6 rip FCCN enable ! ipv6 router rip FCCN</pre> | <pre>hostname R4 ! ipv6 unicast-routing ipv6 multicast-routing ! interface Tunnel11 ipv6 address 3FFE:A::1/64 tunnel source 2001:D::4 tunnel destination 2001:B::1 tunnel mode gre ipv6 ! interface FastEthernet0/0 ipv6 address 2001:E::4/64 ipv6 rip ESTG_Leiria enable ! interface Serial0/0 ipv6 address 2001:D::4/64 ipv6 rip ESTG_Leiria enable ipv6 route ::0 3FFE:A::2 multicast ! ipv6 router rip ESTG_Leiria</pre> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Figura 6.57 - Configurações efectuadas no router ‘RSouce’ e no router ‘R4’

### Configurações efectuadas no router **R1**

Apesar de não ser necessário configurar o RP nos equipamentos, foi necessário, no router ‘R1’ adicionar uma rota por omissão multicast para a rede [2001:E:: /64].



```

hostname R1
!
ipv6 unicast-routing
ipv6 multicast-routing
!
interface Tunnel11
ipv6 address 3FFE:A::2/64
tunnel source 2001:B::1
tunnel destination 2001:D::4
tunnel mode gre ipv6
!
interface Serial0/0
ipv6 address 2001:B::1/64
ipv6 rip FCCN enable
!
interface Serial0/1
ipv6 address 2001:A::1/64
ipv6 rip FCCN enable
!
ipv6 route 2001:D::/64 3FFE:A::1 multicast
ipv6 route 2001:E::/64 3FFE:A::1 multicast
!
ipv6 router rip FCCN

```

Tabela 6.9 - configurações efectuadas no router R1

## Configuração das aplicações – Fase I

Nesta secção é detalhado todo o processo de configuração da aplicação existente no servidor e no cliente. Desta forma, numa primeira fase é detalhado todo o processo de configuração da aplicação servidora sendo, posteriormente apresentada a forma de configurar a aplicação cliente.

### Aplicação servidora

Dado que com PIM-SSM, as aplicações tem um importância bastante elevada, é de todo conveniente analisar a imagem seguinte. Como é visível, esta foi retirada do servidor com o endereço [2001:E::2] (ponto ) e, além disso, é visível que se está a configurar a aplicação servidora para difundir o *streaming* no endereço [FF36::6] (ponto )

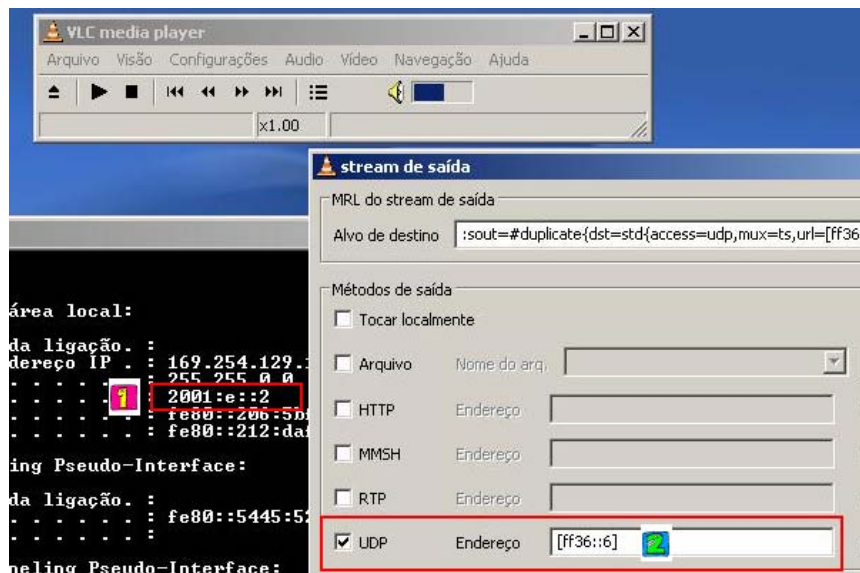


Figura 6.58 - PIM-SSM, cenário com túneis - configuração da aplicação no servidor

## Aplicação Cliente

Observando com detalhe o exemplo seguinte, retirado da máquina esquerda (cliente), é possível constatar que esta pretende-se ligar ao servidor [2001:e::2] através do grupo [FF36::6]. Por conseguinte, observando o esquema anterior verificamos que a máquina cliente está-se a ligar ao servidor 1 (**servidor ( 1 )**).

Pelo aparência da imagem seguinte é perceptível que esta foi retirada de uma máquina Linux. Obviamente, é necessário usar um cliente deste tipo pelo facto deste suportar MLDv2.



Figura 6.59 - PIM-SSM, cenário com túneis - configuração da aplicação no cliente

## Problemas encontrados – Fase I

Para configurar com sucesso este cenário foi necessário adicionar no router R1, uma rota multicast adicional à já existente.

```
ipv6 route 2001:D::/64 3FFE:A::1 multicast
```

```
ipv6 route 2001:E::/64 3FFE:A::1 multicast ###Foi necessário adicionar esta rota###
```

Para além dos problemas anteriores, também existiram problemas com o VLC no Linux. Até aqui a esta parte, para os testes, foram utilizados clips de vídeo codificados com um CODEC proprietário do Microsoft, WMV – Windows Media Vídeo. No entanto, quando se tentou visualizar esse vídeo no Linux, a aplicação era terminada abruptamente. Depois de efectuadas algumas pesquisas e tentativas, revolveu-se usar um clip codificado com um Codec standard, H 263. Efectivamente, o problema estava no ficheiro usado, dado que, com o novo, tudo funcionou perfeitamente.

## Testes – Fase I

Nesta secção é demonstrado a difusão do streaming pelo túnel.

### Passo 1: Funcionamento do túnel

Para compreender o funcionamento túnel resolveu-se utilizar o Ethereal, e colocá-lo a captar os pacotes que existentes no túnel.

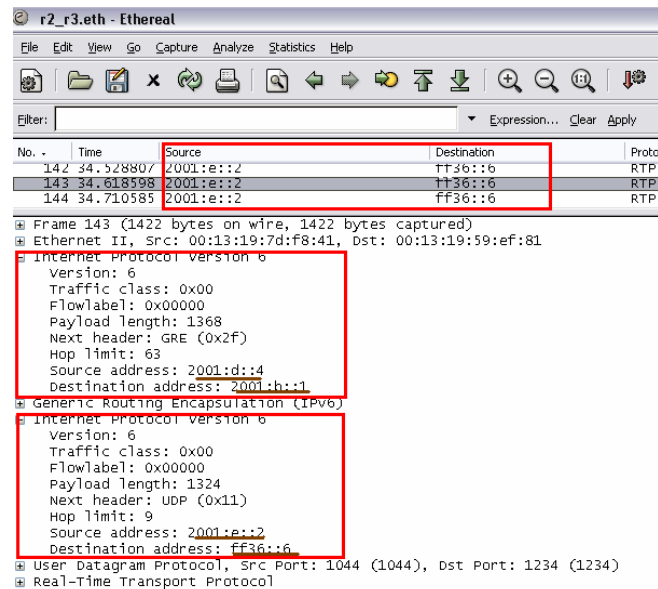


Figura 6.60 - Pacotes enviados no túnel

Observando a imagem anterior, é visível a existência de vários protocolos encapsulados uns dentro dos outros. Na última caixa, é visível também que os pacotes estão a ser enviados do PC com o IP [2001:E::2] para o endereço multicast [FF36::6]

## Configuração das aplicações – Teste II

Depois de ser ter efectuado com sucesso o testes anterior, resolveu-se colocar dois servidores a difundir para o mesmo endereço multicast. O objectivo deste teste comprovar que, efectivamente, usando o PIM-SSM é possível usar apenas um endereço multicast e, ter a ele associado vários servidores.

Na imagem seguinte está esquematizado todo o processo de configuração das aplicações servidoras e das aplicações usadas no PC cliente.

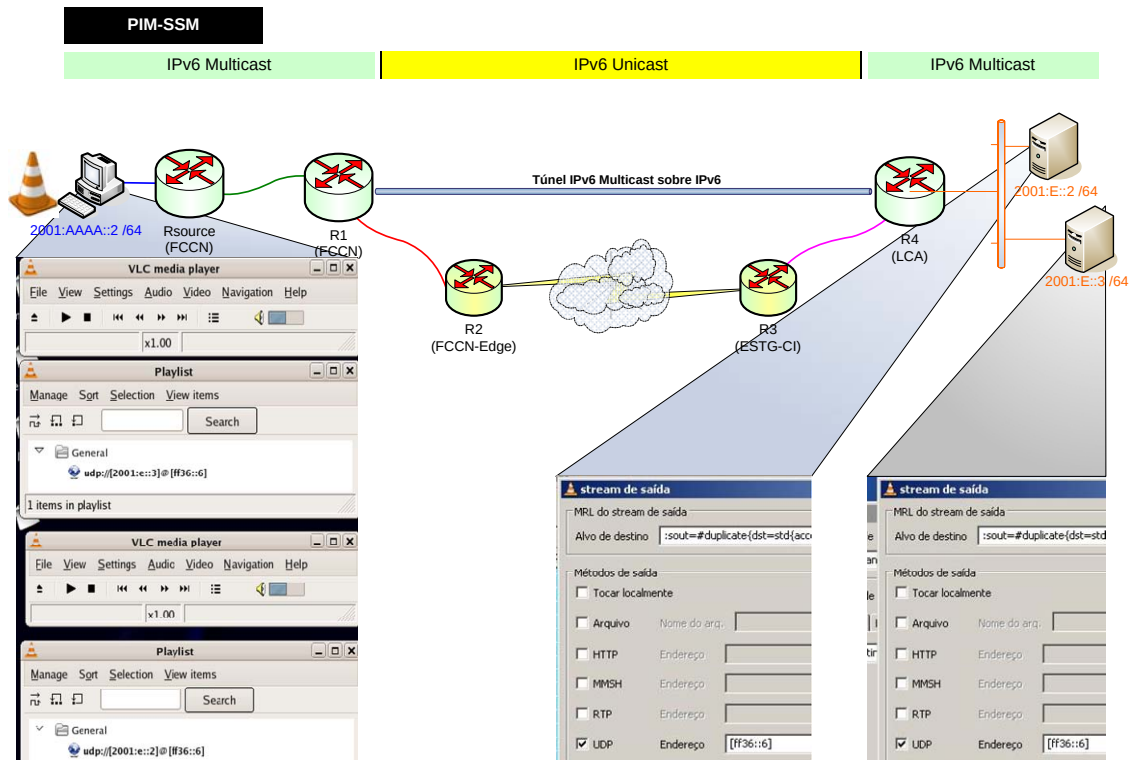


Figura 6.61 - Esquema com as configurações dos servidores e do cliente

É visível do lado direito, uso de dois servidores, [2001:E::2] e [2001:E::3], configurados com o mesmo grupo multicast [FF36::6] e, do lado esquerdo, o uso de dois clientes na mesma máquina.

A imagem seguinte apresenta com mais pormenor as configurações introduzidas na máquina Linux, máquina com o IP [2001:AAAA::2].

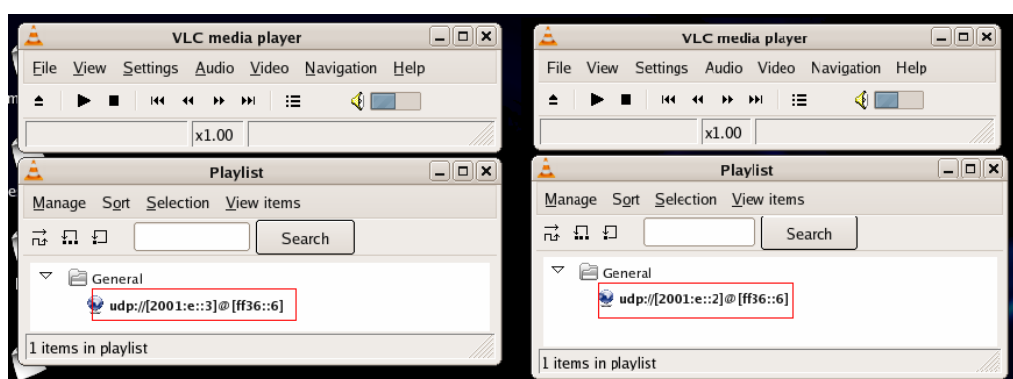


Figura 6.62 - Configurações efectuadas na máquina cliente – Linux

## Testes – Fase II

Nesta secção é demonstrado, recorrendo a imagens retiradas do Ethereal, a difusão dos dois servidores e visionamento no cliente, de ambos os clips.

| No. - | Time      | Source    | Destination | Protocol |
|-------|-----------|-----------|-------------|----------|
| 190   | 38.539277 | 2001:e::3 | ff36::6     | RTP      |
| 191   | 38.628980 | 2001:e::2 | ff36::6     | RTP      |
| 192   | 38.723503 | 2001:e::3 | ff36::6     | RTP      |
| 193   | 38.813907 | 2001:e::2 | ff36::6     | RTP      |
| 194   | 38.902907 | 2001:e::3 | ff36::6     | RTP      |
| 195   | 38.992521 | 2001:e::3 | ff36::6     | RTP      |
| 196   | 39.085904 | 2001:e::2 | ff36::6     | RTP      |
| 197   | 39.176848 | 2001:e::3 | ff36::6     | RTP      |
| 198   | 39.267513 | 2001:e::2 | ff36::6     | RTP      |
| 199   | 39.357214 | 2001:e::3 | ff36::6     | RTP      |
| 200   | 39.447178 | 2001:e::2 | ff36::6     | RTP      |
| 201   | 39.536791 | 2001:e::3 | ff36::6     | RTP      |
| 202   | 39.626672 | 2001:e::2 | ff36::6     | RTP      |

+ Frame 190 (1422 bytes on wire, 1422 bytes captured)  
 + Ethernet II, Src: 00:13:19:7d:f8:41, Dst: 00:13:19:59:ef:81  
 + Internet Protocol Version 6  
 + Generic Routing Encapsulation (IPv6)  
 - Internet Protocol Version 6  
   Version: 6  
   Traffic class: 0x00  
   Flowlabel: 0x000000  
   Payload length: 1324  
   Next header: UDP (0x11)  
   Hop limit: 63  
   Source address: 2001:e::3  
   Destination address: ff36::6  
 + User Datagram Protocol, Src Port: 1035 (1035), Dst Port: 1234 (1234)  
 + Real-Time Transport Protocol

Figura 6.63 - Ambos os servidores estão a emitir para o mesmo grupo multicast [FF36::6]

Através da imagem anterior, é visível que ambos os servidores estão a difundir para o mesmo endereço de multicast.

A imagem seguinte, retirada do PC cliente, comprova o visionamento de ambos os clips. No entanto, o vídeo apresentado no VLC têm uma péssima qualidade. Qual será o motivo?

O motivo deve-se ao facto de se estar a usar, nos equipamentos Cisco, interfaces séries com uma largura de banda máxima de 128Kbits por segundo. Dado que 128 é insuficiente para transmitir vídeo, vão existir nos *buffers* dos equipamentos muitas perdas, o que degrada no receptor a qualidade da imagem.

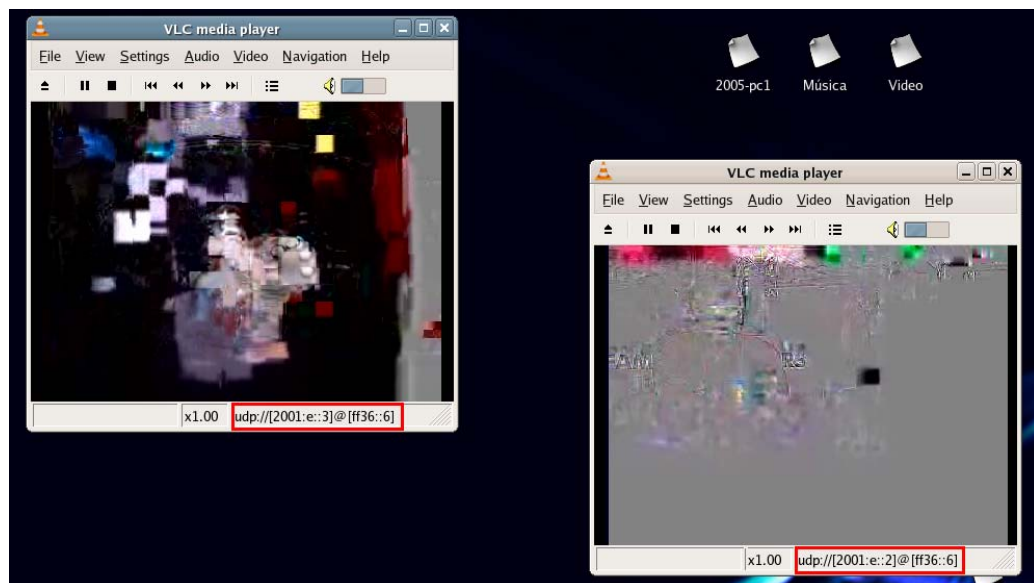


Figura 6.64 - Visionamento, no cliente, de dois filmes enviados por diferentes servidores

## **7 Túnel com a FCCN**

Até aqui a esta parte, foram efectuados vários testes, uns usando ambiente multicast nativo, e outros recorrendo ao uso de túneis. Embora os testes efectuados tenham sido extremamente importantes, foram feitos em ambiente controlado (em laboratório) e com os equipamentos limpos de configurações. Desta forma, embora estes simulam uma rede real, efectivamente não o eram. Por conseguinte, resolveu-se contactar a FCCN com vista à realização de cenários partilhados entre a plataforma de testes da FCCN e a ESTG – Leiria.

Visto que a FCCN já possui ligação multicast IPv6 com a rede M6Bone, foi estudada a viabilidade de interligar a ESTG – Leiria à rede M6Bone através da FCCN. Efectivamente e graças à disponibilidade da Eng. Mónica Domingues, foi possível configurar um túnel entre a ESTG e a FCCN que por sua vez foi reencaminhado para o router internacional, que liga à rede M6Bone.

### **7.1 Cenário dos testes**

Inicialmente pensou-se em configurar um cenário semelhante ao apresentado.

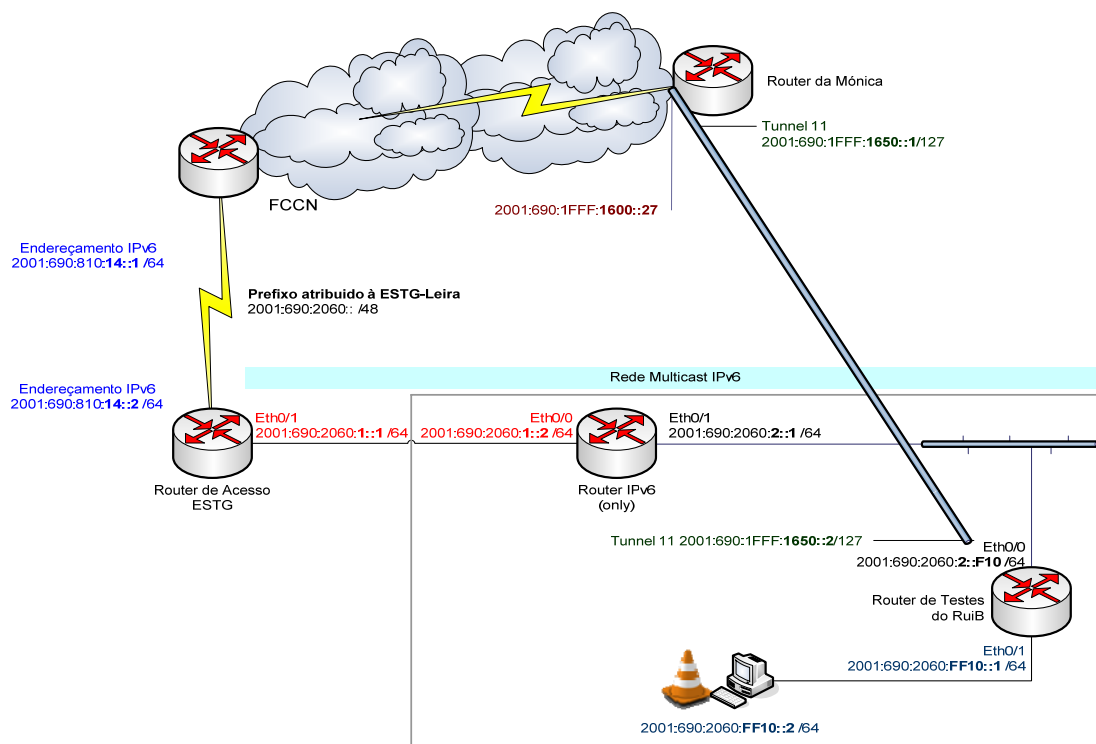


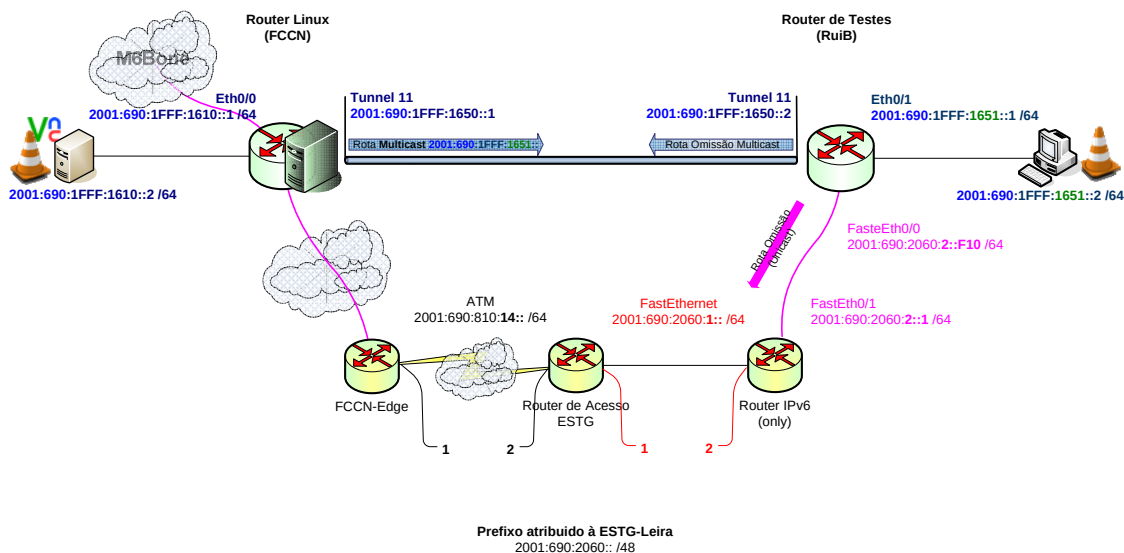
Figura 7.1 - Topologia inicial da ligação

De uma forma sucinta, o esquema apresenta a topologia e os endereços que inicialmente seriam utilizados. São visíveis vários routers dentro da rede da ESTG, ‘Router de Acesso – ESTG’, ‘Router IPv6 (only)’ e ‘Router de Testes do RuiB’. No então, o aluno apenas iria usar o último router, dado que nos outros, ou não permissões para modifica-los, como é o caso do primeiro, ou não o deve utilizar, como é o caso do segundo pois poderia comprometer toda a rede em produção. Desta forma, tal como o nome sugere, o ‘Router de Testes do RuiB’ iria ser o equipamento usado para configurar o túnel com a FCCN.

Quanto à topologia da fundação, esta é obviamente desconhecida. Apenas se sabe, que tem algures na nuvem um router que irá ser utilizado para efectuar o túnel com a ESTG – ‘Router da Mónica’.

É visível ao fundo do esquema uma máquina com um Pino. Esta pretende representar a máquina cliente, no qual foi configurado o VLC. Numa primeira fase, configurou-se a dita máquina com o endereço IPv6 [2001:690:2060:FF10::2]. Deste modo, esta iria pertencer à rede [2001:690:2060:FF10::/64], ou seja, esta estava contida dentro do prefixo atribuído à ESTG – Leiria [2001:690:2060::/48]. Depois de uma longa conversa, via skype com a técnica, esta aconselhou que seria preferível modificar a rede da máquina, para uma outra, pertencente ao prefixo da FCCN. Desta forma, segundo ela, “não quero colocar em causa a conectividade com a ESTG, por isso é preferível usar a rede que te dei...”, foi necessário modificar o endereçamento inicial para um outro ([2001:690:1FFF:1651::/64]).

O esquema seguinte ilustra, efectivamente o cenário que foi usado nos testes.



## 7.2 Fase I - Encaminhamento Unicast

A imagem anterior expõe a topologia e todos os endereços que foram efectivamente usados nos testes. De seguida são apresentados os comandos configurados até esta fase. Não é apresentada configuração final, mas sim, os comandos colocados no equipamento até esta fase – encaminhamento *unicast*.

```
ipv6 unicast-routing
```

O comando anterior, é responsável por activar o *forwarding* dos pacotes IPv6 [Cisco IOS 12.4 Command Referece]. Isto é, o comando activa o encaminhamento *unicast* e, envia *ICMPv6-Router Advertised* para as interfaces que tenham configurado endereços IPv6. Dito de uma forma mais simples, este comando activa o encaminhamento (*unicast*) e envia rotas por omissão para os clientes ligados nas interfaces directamente ligados.

```
interface FastEthernet0/0
ipv6 address 2001:690:2060:2::F10/64
```

Atribuição de um endereço IPv6 à interface que liga ao router ‘Router IPv6 (only)’.

```
interface FastEthernet0/1
ipv6 address 2001:690:1FFF:1651::1/64
```

Atribuição de um endereço IPv6 à interface “ligada” ao PC cliente.

```
interface Tunnel11
ipv6 address 2001:690:1FFF:1650::2/64
tunnel source 2001:690:2060:2::F10
tunnel destination 2001:690:1FFF:1600::27
tunnel mode ipv6
```



O primeiro comando atribui um endereço IPv6 ao túnel, endereço “sugerido” pela técnica. De seguida foram configurados os endereços de origem e destino do túnel. Como é visível, quer pelo comando, quer pela análise do esquema anterior, a origem do túnel é a interface *FastEthernet0/0* e o destino é um endereço existente na nuvem da FCCN. Por fim, o último comando, indica ao router para criar um túnel IPv6. Desta forma, é possível encaminhar tráfego multicast IPv6 “sobre ele”.

Convém no entanto fazer referência a um pormenor fundamental, que faz toda a diferença. Para se conseguir configurar com sucesso o túnel, é necessário garantir encaminhamento para os endereços que se estão a configurar no túnel, isto é, se o equipamento, não conseguir *pingar* com sucesso ao endereço de destino do túnel (2001:690:1FFF:1600::27), o túnel não vai funcionar, ficando no estado UP/DOWN.

```
ipv6 route ::/0 2001:690:2060:2::1 unicast
```

Por forma a garantir encaminhamento na rede, é necessário configurar no equipamento, uma rota por omissão. No entanto convém ver com detalhe o comando anterior que termina com a palavra **unicast** no fim. Nesta fase das configurações (ainda não estamos a configurar multicast, apenas *unicast*) a palavra não era necessária, mas numa fase posterior, esta já é, e vai fazer toda a diferença. De qualquer das formas, quando chegar a altura correcta, esta será devidamente explicada.

### 7.2.1 Encaminhamento do túnel

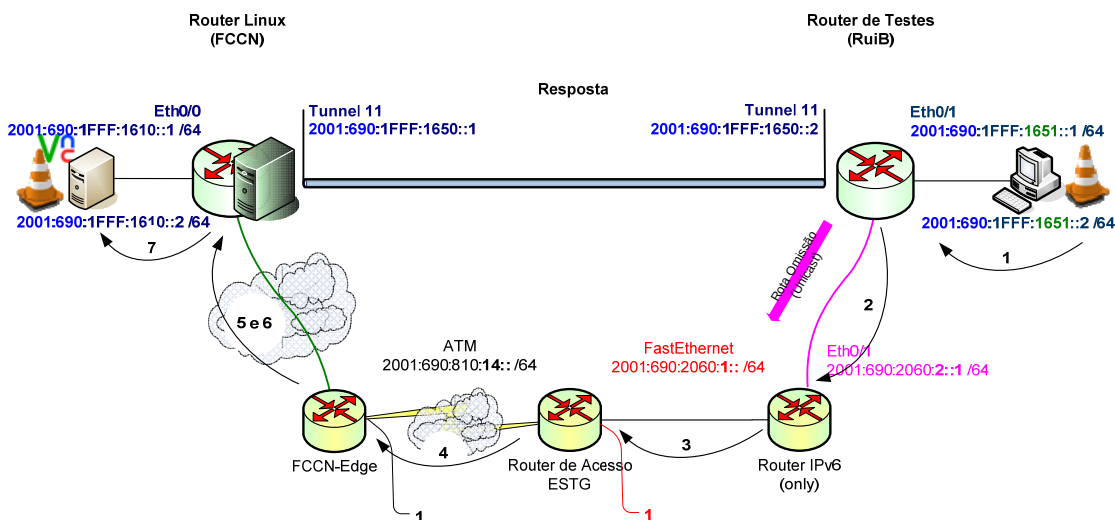
Voltando novamente ao cenário apresentado anteriormente. Convém efectivamente reparar num pormenor, que à primeira vista poderá parecer estranho, pelo menos ao aluno pareceu...

Na rede da ESTG estamos a usar um endereço da FCCN (2001:690:1fff:1651::/64). Algo estranho, dado que os routers da ESTG (*Router de Acesso* e *Router IPv6 (only)*) quando recebem um prefixo da FCCN encaminham-no para o exterior (tem rotas por omissão para a rede da FCCN). Ou seja, quando recebem um pacote IPv6 com o prefixo [2001:690::/48] encaminham-no para FCCN. Assim, como é possível existir encaminhamento para a rede de testes se os routers tem as ditas rotas por omissão? Por forma a ajudar a compreender este enigma, foi efectuado um conjunto de testes que, partindo da máquina cliente (a da direita no esquema), ajudam a esclarecer todas as dúvidas:

```
[root@localhost bin]# traceroute6 2001:690:1FFF:1610::2
traceroute to 2001:690:1FFF:1610::2 (2001:690:1fff:1610::2) from
2001:690:1fff:1651::2, 30 hops max, 16 byte packets
 1  2001:690:1fff:1651::1 (2001:690:1fff:1651::1)  5.416 ms  3.243 ms  1.245 ms
 2  2001:690:2060:2::1 (2001:690:2060:2::1)  160.624 ms  151.198 ms  126.77 ms
 3  2001:690:2060:1::1 (2001:690:2060:1::1)  147.032 ms  191.256 ms
```

|   |                                               |            |                                         |            |
|---|-----------------------------------------------|------------|-----------------------------------------|------------|
| 4 | 2001:690:810:14::1 (2001:690:810:14::1)       | 119.79 ms  | 135.584 ms                              | 173.969 ms |
| 5 | 2001:690:800:1::29 (2001:690:800:1::29)       | 178.7 ms   | 2001:690:800:2::29 (2001:690:800:2::29) | 196.348 ms |
| 6 | 2001:690:1fff:1650::1 (2001:690:1fff:1650::1) | 178.415 ms | 121.286 ms                              | 96.516 ms  |
| 7 | 2001:690:1fff:1610::2 (2001:690:1fff:1610::2) | 65.433 ms  | 90.378 ms                               | 96.24      |

Se observarmos com detalhe o comando anterior, os endereços IPs configurados na figura anterior, e os esquema seguinte conseguimos compreender todo o funcionamento, ou seja, como efectivamente se processa o encaminhamento.



Um pacote enviado pela máquina cliente (2001:690:1FFF:1651::2), destinado à máquina servidora (2001:690:1FFF:1610::1) segue o seguinte caminho:

- .Salto 1 - 2001:690:1fff:1651::1
- .Salto 2 - 2001:690:2060:2::1
- .Salto 3 - 2001:690:2060:1::1
- .Salto 4 - 2001:690:810:14::1
- .Salto 5 - Núvem FCCN
- .Salto 6 - 2001:690:1fff:1650::1
- .Salto 7 - 2001:690:1fff:1610::2

Desta forma, conclui-se com sucesso a primeira etapa, **garantir conectividade unicast, entre a ESTG – FCCN – ESTG**. Terminada a primeira etapa, é necessário configurar o que efectivamente interessa – conectividade multicast.

### 7.3 Fase II – Encaminhamento Multicast

O primeiro passo para se configurar multicast IPv6 é colocar o comando seguinte:

```
ipv6 multicast-routing
```

O comando anterior activa o encaminhamento de pacotes multicast, activa o protocolo multicast PIM (PIM – Protocol Independent Multicast) e activa também o MLD (MLD – Multicast Listener Discovery) [25].

```
ipv6 route ::/0 2001:690:1FFF:1650::1 multicast
```

Por forma a direccionar os pacotes para o túnel é necessário introduzir o comando anterior. Segundo [25], a palavra **multicast** no fim do comando indica que a rota não irá ser usada pelo processo de encaminhamento unicast, ou seja, por outras palavras a rota nunca é colocada na tabela de encaminhamento unicast.

Voltando um pouco atrás, quando se estava a configurar o encaminhamento unicast, (Fase I – Encaminhamento unicast) usou-se a seguinte rota:

```
ipv6 route ::/0 2001:690:2060:2::1 unicast
```

De seguida irá ser explicado o facto de se ter usado a palavra **unicast** no final.

Segundo [25], a palavra **unicast** especifica que a rota **não vai ser usada** por uma técnica específica do multicast (*Reverse Path Forwarding* – RPF). Ou seja, **se retirarmos** a palavra **unicast**, o equipamento vai utilizar **sempre** a rota para “comunicar” com o(s) vizinho(s) multicast, independentemente de outras rotas multicast que este possa já ter configurado. Resumidamente, quando se configura o multicast num equipamento cisco, e se usa túneis (topologia unicast distinta da multicast) é sempre necessário utilizar a palavra **unicast**.

Repare-se no exemplo seguinte que permite consolidar os conhecimentos (ver palavras a **negrito** na tabela seguinte). Convém referir que as configurações foram efectuadas no ‘*Router de Testes (RuiB)*’ usando o cenário actual.

| Router de Testes (RuiB)<br>(forma correcta)                         | Router de Testes (RuiB)<br>(forma errada)                         |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <pre>ipv6 route ::/0 2001:690:1FFF:1650::1 <b>multicast</b></pre>   | <pre>ipv6 route ::/0 2001:690:1FFF:1650::1 <b>multicast</b></pre> |
| <pre>ipv6 route ::/0 2001:690:<b>2060:2::1</b> <b>unicast</b></pre> | <pre>ipv6 route ::/0 2001:690:<b>2060:2::1</b></pre>              |

Como é visível, a única diferença está precisamente no uso, ou não, da palavra **unicast**. Ou seja, na coluna da esquerda foi introduzida a palavra **unicast**, ao passo que na da direita já não.

Foram efectuados alguns testes e verificou-se que quando se usava as configurações da coluna direita, o multicast **não funcionava**. A tabela seguinte exhibe a causa do problema.

| Router de Testes (RuiB)<br>(forma correcta)                                                                                                                                                                                                                                                 | Router de Testes (RuiB)<br>(forma errada)                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>RB#show ipv6 rpf 2001:690:1FFF:1610::2  RPF information for 2001:690:1FFF:1610::2   RPF interface: <b>Tunnel11</b>   RPF neighbor: <b>2001:690:1FFF:1650::1</b>   RPF route/mask: ::/0   RPF type: <b>Mroute</b>   RPF recursion count: 1   Metric preference: 1   Metric: 0 RB#</pre> | <pre>RB#show ipv6 rpf 2001:690:1FFF:1610::2  RPF information for 2001:690:1FFF:1610::2   RPF interface: <b>Fast0/1</b> ❌   RPF neighbor: <b>2001:690:2060:2::1</b> ❌   RPF route/mask: ::/0   RPF type: <b>Mroute</b>   RPF recursion count: 1   Metric preference: 1   Metric: 0 RB##</pre> |

Como se pode ver na coluna da esquerda, o router usa a interface **túnel11** para o calculo do RPF (está correcto), ao passo que a coluna da direita usa a interface **Fast0/1** para comunicar com a outra extremidade, o que está incorrecto.

O ‘Router de Teste (RuiB)’ está apto a receber tráfego multicast.

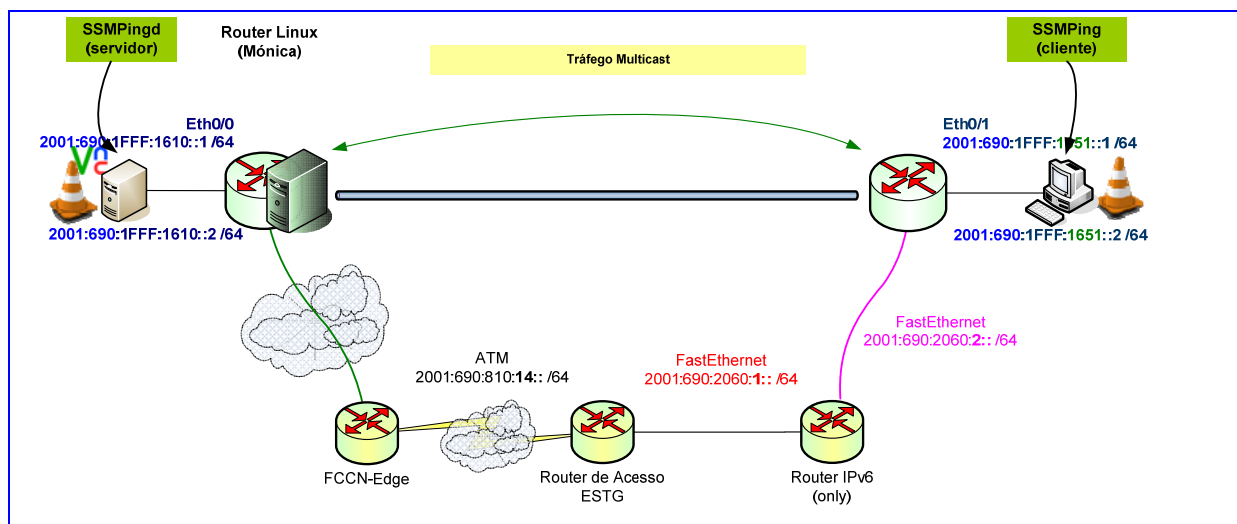
Para terminar a configuração, foi necessário a Mónica na FCCN, colocar os comandos equivalentes no equipamento que estava a configurar (‘Router Linux (Mónica)’).

Desta forma concluiu-se a configuração dos equipamentos, quer unicast quer multicast

## 7.4 Fase III – Teste de conectividade - SSM

Para testar a conectividade multicast extremo-a-extremo da rede, usou-se ao utilitário **SSMping/SSMpingd**. Como é já foi referido em secções anteriores neste relatório, a aplicação é constituída por duas partes, servidor – **SSMpingd**, e cliente – **SSMping**.

Colocou-se o SSMpingd a correr do lado da FCCN e o cliente do lado da ESTG. A figura seguinte ajuda a compreender a configuração efectuada.



O quadro seguinte contém uma copia do comando introduzido na máquina de Leiria e, mostra o resultado obtido.

```
[root@localhost bin]# ssmping -6 -I eth0 2001:690:1FFF:1610::2
ssmping joined (S,G) = (2001:690:1fff:1610::2, ff3e::4321:1234)
pinging S from 2001:690:1fff:16
multicast from 2001:690:1fff:1610::2, seq=17 dist=2 time=8.771 ms
  unicast from 2001:690:1fff:1610::2, seq=18 dist=2 time=12.539 ms
multicast from 2001:690:1fff:1610::2, seq=18 dist=2 time=12.813 ms
  unicast from 2001:690:1fff:1610::2, seq=19 dist=2 time=9.980 ms
multicast from 2001:690:1fff:1610::2, seq=19 dist=2 time=11.968 ms
  unicast from 2001:690:1fff:1610::2, seq=20 dist=2 time=14.841 ms
multicast from 2001:690:1fff:1610::2, seq=20 dist=2 time=15.116 ms
  unicast from 2001:690:1fff:1610::2, seq=21 dist=2 time=20.145 ms
multicast from 2001:690:1fff:1610::2, seq=21 dist=2 time=20.600 ms
....
--- 2001:690:1fff:1610::2 ssmping statistics ---
21 packets transmitted, time 20782 ms
unicast:
  21 packets received, 0% packet loss
  rtt min/avg/max/std-dev = 8.498/18.395/79.747/15.357 ms
multicast:
  20 packets received, 0% packet loss since first mc packet (seq 2) recvd
  rtt min/avg/max/std-dev = 8.771/20.625/79.958/17.029 ms
[root@localhost bin]#
```

Como é visível, o servidor devolveu respostas em **multicast** e **unicast**, ou seja, existe conectividade multicast SSM entre a FCCN e a ESTG – Leiria.

De seguida efectuou-se o teste oposto, ou seja, colocou-se o servidor (SSMpingd) a correr do lado da ESTG e o cliente do lado da FCCN. Mais uma vez, o resultado obtido foi o esperado, sucesso.

## 7.5 Fase IV – Configurações ASM – Ligação à M6Bone

Dado que os testes usando SSM foram bem sucedidos, passou-se então para os testes com ASM. Como é sabido, com ASM o paradigma de comunicação multicast é substancialmente diferente, uma vez que é necessário configurar explicitamente em todos os equipamentos multicast (routers multicast) o ponto central da rede, o RP (**rendezvous point**).

Depois da técnica ter configurado o RP, foi necessário efectuar o mesmo em Leiria. Assim o equipamento da ESTG passaria a conhecer o RP da rede.

```
ipv6 pim rp-address 2001:660:3007:300:1::
```

O comando anterior, inserido no equipamento de Leiria, configura o equipamento para “se ligar” ao RP com o endereço [2001:660:3007:300:1::]. Diga-se em abono da verdade que o endereço configurado no equipamento pertence, nada mais, nada menos que ao endereço de global da rede M6Bone!

## 7.6 Fase V – Teste de conectividade - ASM

Uma vez efectuadas as configurações, passou-se à fase dos testes propriamente ditos. Assim, voltou-se a colocar na FCCN o servidor **SSMpingd** e na ESTG, correu-se o utilitário **ASMping**. Convém referir que o SSMpingd aceita ASM e SSM.

```
[root@localhost bin]# asmping FF1e:: 2001:690:1FFF:1610::2
ssmping joined (S,G) = (2001:690:1fff:1610::2,ff1e::4321:1234)
pinging S from 2001:690:1fff:1651::2
  unicast from 2001:690:1fff:1610::2, seq=1 dist=2 time=22.377 ms
  unicast from 2001:690:1fff:1610::2, seq=2 dist=2 time=20.249 ms
multicast from 2001:690:1fff:1610::2, seq=2 dist=2 time=21.659 ms
  unicast from 2001:690:1fff:1610::2, seq=3 dist=2 time=18.257 ms
multicast from 2001:690:1fff:1610::2, seq=3 dist=2 time=19.480 ms
recv failed: Connection refused
errno=111
....
--- 2001:690:1fff:1610::2 ssmping statistics ---
231 packets transmitted, time 230749 ms
unicast:
```

```

200 packets received, 0% packet loss
rtt min/avg/max/std-dev = 8.165/33.320/188.618/38.705 ms
multicast:
199 packets received, 0% packet loss since first mc packet (seq 2) recvd
rtt min/avg/max/std-dev = 8.658/34.348/191.721/38.951 ms
[root@localhost bin]#

```

Desta forma se conclui que a ESTG – Leiria já tem multicast IPv6.

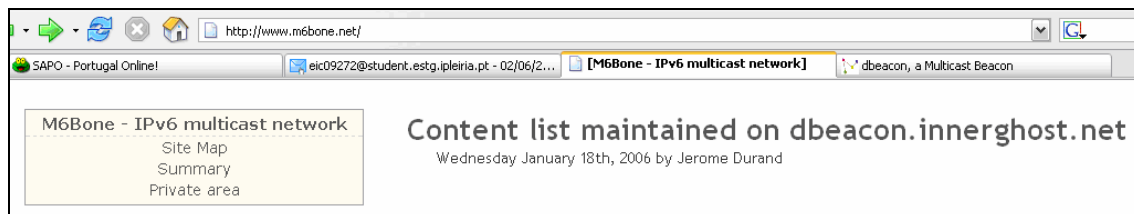
## 7.7 Como aceder aos conteúdos da rede M6Bone

Nesta secção são apresentados e explicados os passos necessários para se receber conteúdo multimédia, em *multicast*, dos servidores a difundir na rede mundial de multicast – M6Bone.

Uma vez que a ESTG já possui uma ligação multicast IPv6 à rede M6Bone via FCCN, é perfeitamente transparente e possível, a qualquer pessoa dentro da rede da ESTG receber conteúdo da rede M6Bone.

Actualmente, a M6Bone possui uma página Web onde são apresentados todos os emissores a difundir, bem como o estado destes. Existe também uma outra onde são apresentados diversos parâmetros de QoS dos servidores ligados à rede.

A forma mais simples de aceder aos conteúdos da M6Bone é através do seu site, [www.M6Bone.net](http://www.M6Bone.net).



O link para a página que contém os emissores está em destaque (ver imagem anterior).

| Name                          | Address                                    | Description                                                                   | Status |
|-------------------------------|--------------------------------------------|-------------------------------------------------------------------------------|--------|
| Frequence3 Radio              | vlc udp://@[ff1e::8888]:8888               | This is a well known <a href="#">French Internet radio</a> , 270kb/s required | ✓      |
| Frequence 3 Radio             | udp://@[ff0e::2:ffdd]:1234                 | "                                                                             | ✗      |
| Frequence 3 Radio             | vlc udp://[gluon.q2s.ntnu.no]@[ff3e::8888] | SSM transported version of the radio                                          | ✓      |
| University of Bergen Kamera 1 | vlc udp://[gluon.q2s.ntnu.no]@[ff3e::8886] | A nice high resolution view from the university of bergen                     | ✓      |

Figura 7.2 - Servidores ligados na rede M6Bone

Esta página é refrescada de 10 em 10 minutos, pela Universidade de Strasbourg [] e permite analisar a disponibilidade dos servidores ligados à rede. O funcionamento interno desta é simples: são enviados *Joins* para os grupos multicast e aguardados 10 segundos pela resposta. Se o pacote chegar, então assume-se que o grupo está a funcionar correctamente, se isso não acontecer, então é porque o servidor não se encontra disponível. O estado dos servidores é representado pelas imagens seguintes:

| Ícons representativos | Descrição      |
|-----------------------|----------------|
| ✓                     | Disponível     |
| ✗                     | Não disponível |

Desta forma, para aceder aos conteúdos multicast da rede M6Bone, basta consultar a página anterior e configurar o VLC. A imagem seguinte contém o exemplo de configuração. Convém, no entanto, não esquecer que o Windows XP não suporta MLDv2, ou seja, com este não é possível, por enquanto, ver conteúdos de servidores que usam o paradigma SSM.



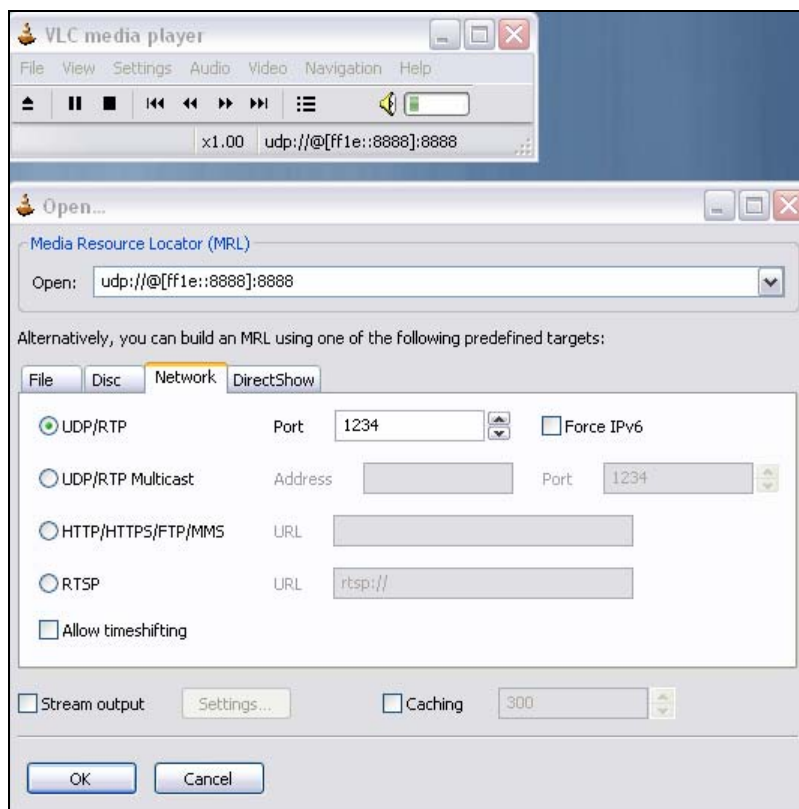


Figura 7.3 - Forma de configurar o VLC para receber conteúdos da M6Bone

## 8 Conclusão

O objectivo do projecto, numa primeira fase, abrangia o estudo e experimentação das tecnologias envolvidas no multicast IPv6 e a produção de um relatório técnico que documentasse o trabalho realizado e servisse de referência para trabalhos futuros. No entanto, com o decorrer do projecto, verificou-se que, para além de efectuar testes na plataforma *testbeds*, também existia a possibilidade de ligar a escola de Leiria à rede M6Bone.

Assim, numa primeira fase, foram contactados os responsáveis da rede com vista a estudar as melhores possibilidades de ligação. Uma vez que a ESTG – Leiria está conectada à rede da FCCN e esta já possui ligação nativa IPv6 multicast com a rede M6Bone, chegou-se à conclusão que era necessário entrar em contacto com os responsáveis da FCCN, com vista a estudar a possibilidade desta fornecer o serviço. Desta forma, foi contactada a Eng. Mónica Domingues, e foram estudadas as melhores possibilidades de ligação.

Em paralelo, com vista a estudar a tecnologia, foram implementados vários cenários em laboratório, usando os diversos recursos disponíveis, nomeadamente routers Cisco. Dado que estes, no início do projecto, não dispunham de suporte para multicast IPv6, foi necessário actualizar o software, e resolveu-se também estudar a possibilidade de actualizar o equipamento *Edge* do Politécnico que faz fronteira com o exterior. Depois de efectuados alguns contactos com os responsáveis do Centro de Informática da ESTG, foi actualizado o equipamento, numa primeira fase, e de seguida foi configurado neste o serviço multicast IPv6.

Actualmente, a ESTG – Leiria dispõe de encaminhamento nativo de pacotes IPv6 multicast em parte da sua rede interna. No entanto, o seu fornecedor de Internet, FCCN, ainda não disponibiliza esse serviço aos seus parceiros. Por conseguinte, para interligar a escola à plataforma e à rede M6Bone, foi necessário recorrer ao uso de túneis.

A figura seguinte esquematiza o trabalho efectuado ao longo deste projecto. Além desta configuração, foram efectuados vários cenários em laboratório que serão apresentados no capítulo dos testes. Nesta é visível a ligação da ESTG – Leiria à rede M6Bone, e à plataforma TestBeeds (FCCN).

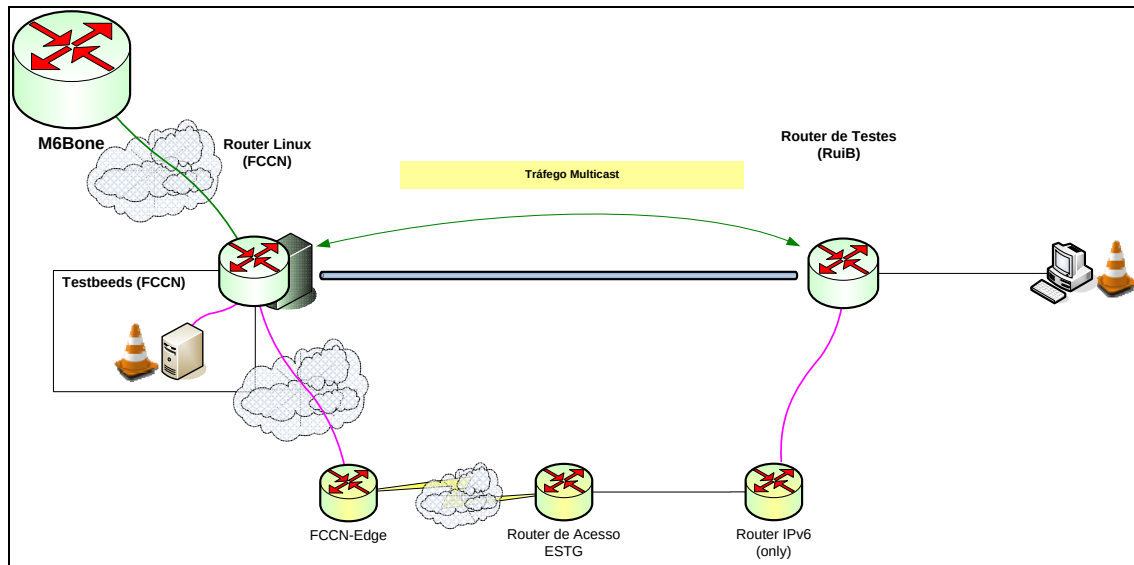


Figura 8.1 - Topologia existente da ESTG –Leiria, ligação à M6Bone

## 9 Referências

- [1] <http://www-r2.u-strasbg.fr/~hoerd/libssmsdp/?topic=Intro>
- [2] 6Net
- [3] CCNP
- [4] <http://abilene.internet2.edu/about/>
- [5] [domen.uninett.no/~venaas/ipv6mcdepsrv.pdf](http://domen.uninett.no/~venaas/ipv6mcdepsrv.pdf)
- [6] [internetng.dit.upm.es/ponencias-jing/2002/durand/m6bone.pdf](http://internetng.dit.upm.es/ponencias-jing/2002/durand/m6bone.pdf)
- [7] [www.terena.nl/tech/task-forces/tf-ngn/tf-ngn14/20040510\\_JD\\_M6Bone.pdf](http://www.terena.nl/tech/task-forces/tf-ngn/tf-ngn14/20040510_JD_M6Bone.pdf)
- [8] [www4.renater.fr/Telechargement/FICHE\\_MulticastV6SXA.PDF](http://www4.renater.fr/Telechargement/FICHE_MulticastV6SXA.PDF)
- [9] [http://www.m6bone.net/article.php3?id\\_article=92](http://www.m6bone.net/article.php3?id_article=92)
- [10] [www.m6bone.net](http://www.m6bone.net)
- [11] RFC 1112
- [12] RFC 3569
- [13] Cisco, Deployment IPv6 Multicast
- [14] FCCN, Monica Dominges - Deliverebals
- [15] <http://www.iana.org/assignments/ipv6-multicast-addresses>
- [16] [www.rnp.br/newsgen/0111/mld5.html](http://www.rnp.br/newsgen/0111/mld5.html)
- [17] RIVERSTONE NETWORKS ADVANCED TECHNICAL PAPER SERIES Internet Group Management Protocol Michael Gibbs, Riverstone Networks
- [18] RFC 2710
- [19] <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/3725bcdcf-210b-4ed2-9ddf-10721285a7d2.mspx>
- [20] [http://en.wikipedia.org/wiki/Protocol\\_Independent\\_Multicast](http://en.wikipedia.org/wiki/Protocol_Independent_Multicast)
- [21] Cisco, Multicast IPv6 at-a-glance
- [22] <http://www.javvin.com/protocolMBGP.html>
- [23] <http://www.ethereal.com/>
- [24] <http://www.venaas.no/multicast/ssmping/>

- [25] [http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/ipv6\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/ipv6_r/index.htm)
- [26] [[http://www.m6bone.net/article.php3?id\\_article=55](http://www.m6bone.net/article.php3?id_article=55)]



## Apêndice

### 9.1 O essencial do IOS da Cisco

O IOS (IOS® – *Internetwork Operacion System*), desenvolvido pela Cisco, é actualmente o sistema operativo de redes mais utilizado do mundo [2] e têm como característica principal, a grande versatilidade e adaptabilidade face ao aparecimento de novas tecnologias.

Nesta secção pretende-se dar uma visão geral da nomenclatura que a cisco usa para caracterizar o seu sistema operativo (IOS) e a relação desta com as novas funcionalidades que vão aparecendo à medida que a tecnologia evolui. De uma forma sucinta, a nomenclatura usada possui três números: um número para a **versão principal** (*Major Version*), um outro para a **versão secundaria** (*Minor Version*) e por fim, um outro que aparece dentro de parênteses e representa o **número da actualização** (*Maintenance Version*) [1].

#### Version 12.2(8)

Figura 9.1 - Nomenclatura usada para representar as versões dos IOS

O exemplo anterior permite-nos concluir que a versão base usada é a 12.2. Além disso, devido à existência do 8, indica-nos que já existiram 8 actualizações críticas depois do lançamento da primeira versão (12.2(0)).

Durante vários anos a cisco disponibilizou uma “única linha” de versões, contendo correcções incrementais aos erros descobertos, acréscimo de novas funcionalidades e novas características. De uma forma simplificada, pode-se comparar a evolução do IOS como uma linha para comboios (*trains*) que, vai crescendo à medida que é necessário satisfazer novas localidades. No caso da Cisco, as necessidades não são as localidades, mas sim as novas tecnologias, características e correcções críticas de erros. Dito de outra forma, cada versão principal/secundária (*Major* ou *Minor Version*) que a Cisco lança no mercado, corresponde uma nova linha, diferente das anteriores que, depois “cresce” à medida

que vão surgindo novas funcionalidades/correcções. A figura apresentada em baixo demonstra parte do que acabou se ser explicado.

O modelo apresentado no parágrafo anterior foi usado durante vários anos, mas verificou-se que era inviável. Pensou-se que a melhor solução seria criar várias linhas, uma linha por cada tipo de cliente. Foi criada a linha para a evolução tecnológica, a linha para os serviços empresariais e uma outra para os ISPs. Estas linhas ficaram conhecidas respectivamente como, linha T, E e S [2]. No entanto este aumento veio geral alguma dificuldade na escolha IOS e actualmente a Cisco possui apenas duas linhas principais.

**.Major release:** uma linha que cresce à medida que vão surgindo novas correcções face a erros encontrados. Este tipo de versão é também conhecido como *M Release (M de mainline)*[2].

**.T-release:** idêntico ao anterior mas difere pelo facto de as actualizações não conterem apenas correcções de erros, passando a conter também suporte para novas tecnologias, funcionalidades e suporte para novo Hardware – esta versão é internamente referida com *T train*.

Além das duas linhas apresentadas, existe um outra de menor importância – semelhante a uma versão *Beta*, mas para a versão T. Esta versão tem um tempo de vida muito curto e é conhecida como *Application Specific release*.

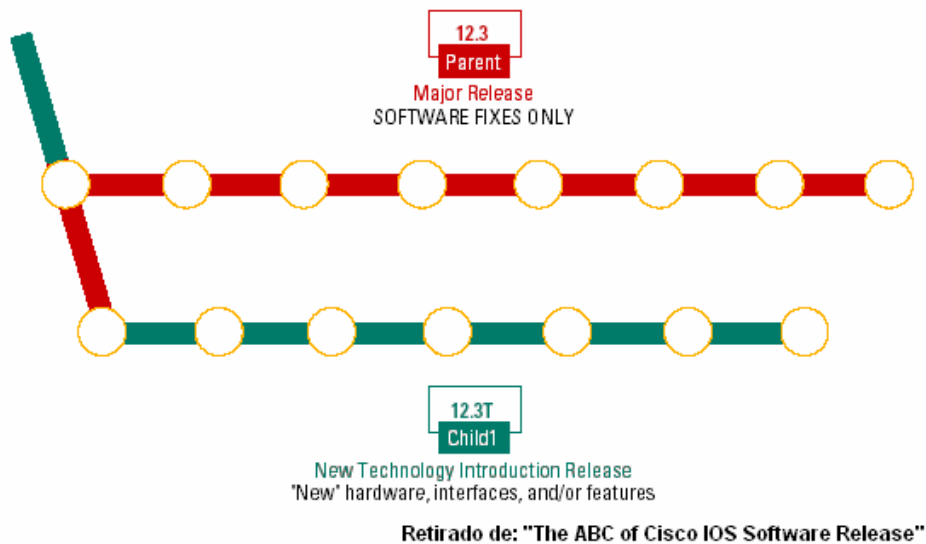


Figura 9.2 - Evolução da versão 12.3

Com a criação da versão T, a cisco consegue introduzir novas funcionalidades sem afectar a estabilidade das versões da linha principal (M). Assim, a escolha de uma ou outra versão fica a cargo dos clientes, sabendo à partida que se escolherem a versão T, por uma lado estão a utilizar uma versão que permite ganhar vantagem ao nível empresarial – no leque de serviços oferecidos, por outro lado, estão a comprometer até certo ponto, a estabilidade do seu sistema.



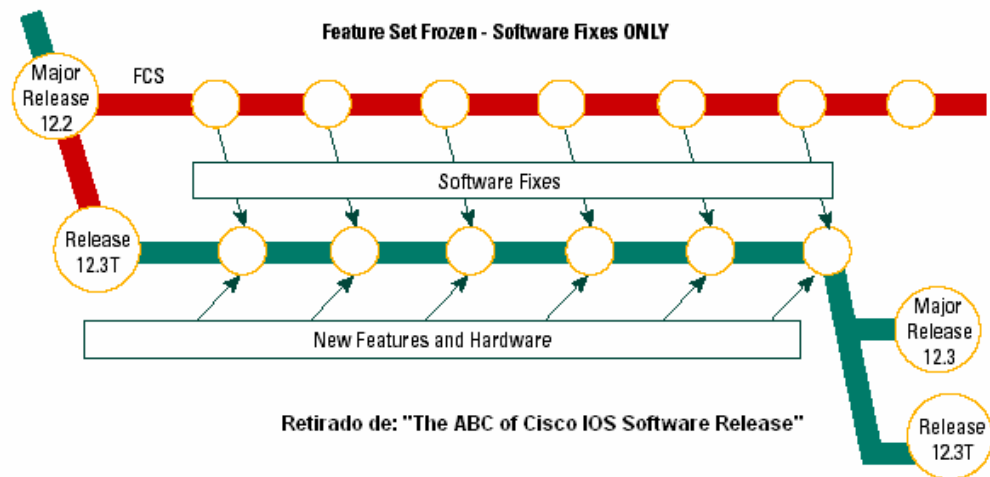


Figura 9.3 - Evolução da versão T e M dos IOSs

A figura anterior demonstra que todas as actualizações críticas introduzidas sequencialmente na versão M, também são introduzidas na versão T. A grande diferença deve-se ao facto de inverso não se verificar, ou seja, a versão M não herda nada da versão T.

### 9.1.2 Escolha das funcionalidades – Cisco IOS Packaging

Antes de mais, convém referir que as funcionalidades disponibilizadas pelos IOSs da Cisco estão em constante actualização e mudança. Nesta secção pretende dar uma visão geral da forma como estão agrupadas as diferentes funcionalidades no IOS. Note-se que apenas se esta a tomar em consideração a versão principal (*Mainline release*).

Diferentes utilizadores têm diferentes necessidades. Tendo por base esta premissa, a cisco agrupou as funcionalidades oferecidas pelo seu sistema operativo de uma forma hierárquica. Isto é, existem versões com um conjunto reduzido de comandos, para empresas de dimensão pequena e versões que além de terem os comandos básicos, também disponibilizam muitos mais. A Figura 9.4 - permite compreender o que acabou se ser explicado.

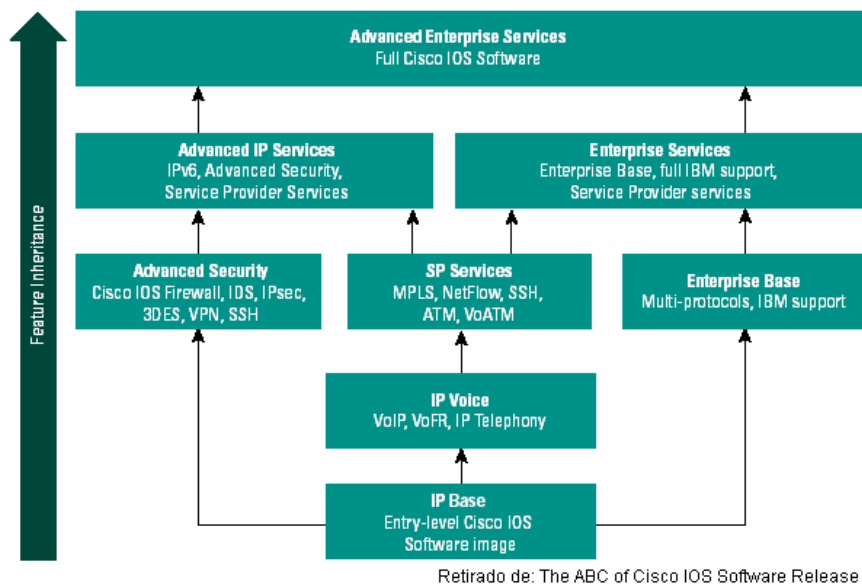


Figura 9.4 - Hierarquia de serviços oferecidos na versão 12.3

Como forma de facilitar a escolha de um IOSs a cisco reagrupou recentemente, a partir da versão 12.3, a sua hierarquia, passando de um total de 44 pacotes para 8 (ver imagem anterior) [2]. Essencialmente passaram a existir quatro grandes categorias:

| Categoria | Descrição                                                                                                     | Pacotes                                 |
|-----------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Base      | Services básicos essenciais                                                                                   | IP Base; Enterprise Base                |
| Serviços  | Serviços adicionais IP, tais como Telefonia IP, MPLS, VoIP, VoFR e ATM                                        | SP Services; Enterprise Services        |
| Avançado  | Adição de suporte para VTP, Firewall, encriptação 3DES, shell segura, IPsec e sistema de detecção de intrusão | Advanced Security; Advanced IP Services |
| Empresa   | Protocolo adicionais, incluindo IBM, IPX, Apple Talk                                                          | Enterprise Base; Enterprise Services    |

Tabela 9.1 - Descrição dos pacotes existentes na versão 12.3 do Cisco IOS

Actualmente na versão mais recente do IOS, 12.4, a Cisco introduziu algumas modificações à tabela anterior, mas o essencial mantêm-se. Isto é, apenas foram acrescentados alguns serviços adicionais, mas a hierarquia apresentada na Figura 9.4 - mantêm a mesma.

## 9.2 Aplicações H.264/x264

Nesta secção é efectuado um pequeno enquadramento à tecnologia x264, numa primeira fase, sendo posteriormente apresentados os projectos que actualmente já suportam ou pretendem vir a suportar a tecnologia.

### 9.2.1 Tecnologia H.264

O H.264 usa as últimas inovações na tecnologia de compressão por forma a fornecer uma qualidade de vídeo fabulosa e com ficheiros de reduzidas dimensões. Desta forma, é possível visualizar vídeo em ficheiros bastante mais pequenos, poupar largura de banda, e poupar nos custos de armazenamento.

Usando a actual qualidade do MPEG-2 [1], a tecnologia H.264 consegue reduzir a taxa de transferência de dados, para um terço, ou até mesmo metade. Se for usado o mesmo débito produzido por um codificador MPEG-2, a tecnologia H.264 consegue obter frames com tamanhos até 4 vezes maiores.

A tecnologia H.264 fornece actualmente o método mais eficiente para a maior parte das aplicações, desde a difusão, passando pela vídeo-conferência, *vídeo-on-demand*, e *streaming multimédia*. Visto possuir uma excelente relação qualidade/débito gerado, esta pode ser usada nos mais diversos ambientes, quer seja na telefonia móvel, Internet, ou até difusão por satélite.

| Cenário de Utilização       | Resolução e Frame rate | Exemplo de Data Rates |
|-----------------------------|------------------------|-----------------------|
| Conteúdos Multimédia        | 176x144 @ 10-15 fps    | 50-60 Kbps            |
| Padrão da Internet          | 640x480 @ 24 fps       | 1-2 Mbps              |
| Televisão de Alta Definição | 1280x720 @ 24fps       | 5-6 Mbps              |
| Televisão de Alta Definição | 1920x1080 @ 24fps      | 7-8 Mbps              |

Cenários de utilização da tecnologia H.264, resoluções suportadas e Data Rates

### 9.2.2 x264 – O codificador H.264 Open-Source

O **x264** é uma *frame-work* para codificar streams de vídeo H.264/MPEG-4 AVC, sendo usado pelo VLC (*VídeoLAN Cliente*) e pelo MEncoder<sup>3</sup>. Este usa uma licença GPL (*GNU General Public License*) e, em Dezembro de 2005, foi considerado a única implementação *open-source* aceitável do standard (H.264), suportando o perfil principal e o alto - *Main and High Profile*. Actualmente ainda não possui, no entanto, suporte para vídeo entrelaçado [2].

O código foi inicialmente escrito por Laurent Aimar, Loren Merritt, Eric Petit (OS X), Min Chen (vfw/nasm), Justin Clay (vfw), Måns Rullgård, Alex Izvorski, Alex Wright, e por Christian Heine.

<sup>3</sup> **MEncoder** é uma ferramenta, em linha de comandos, para codificar e decodificar vídeo. Esta é distribuída livremente usando uma licença GPL. O site oficial é: <http://www.mplayerhq.hu/>

Actualmente o x264 possui uma vasta comunidade, que dá sugestões e efectua desenvolvimentos ao software. Estas comunicam através do fórum *Doom9* [3]

### 9.2.3 Projectos que usam o x264

Actualmente existem vários projectos que usam o codificador *open-source* x264. Segundo [2][4] a lista dos projectos que usam o referido codificador é a seguinte

#### Projectos que usam x264

|                             |                           |                                  |
|-----------------------------|---------------------------|----------------------------------|
| <a href="#">Avidemux</a>    | <a href="#">ffdshow</a>   | <a href="#">ffmpeg</a>           |
| <a href="#">GordianKnot</a> | <a href="#">Handbrake</a> | <a href="#">MeGUI</a>            |
| <a href="#">MEncoder</a>    | <a href="#">pspVideo9</a> | <a href="#">RealAnime</a>        |
| <a href="#">StaxRip</a>     | <a href="#">TCVP</a>      | <a href="#">VLC media player</a> |
| <a href="#">MPlayer</a>     |                           |                                  |

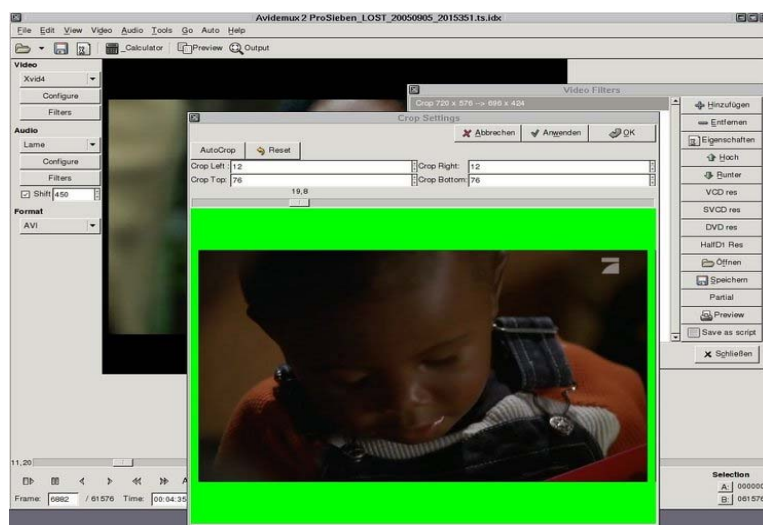
Projectos actuais que usam o codificador x264

### Avidemux



**Avidemux** é um programa *open-source* destinado ao processamento, produção e edição de Vídeo. Escrito em C/C++, usando a palette gráfica [GTK+](#) (GIMP Toolkit +), este trata-se de uma plataforma universal e independente para processamento de vídeo. Actualmente está disponível para a maior parte das distribuições Linux, mas existem também versões para Windows, para Mac OS X, FreeBSD e NetBSD.

O site oficial da aplicação é: <http://avidemux.org/>

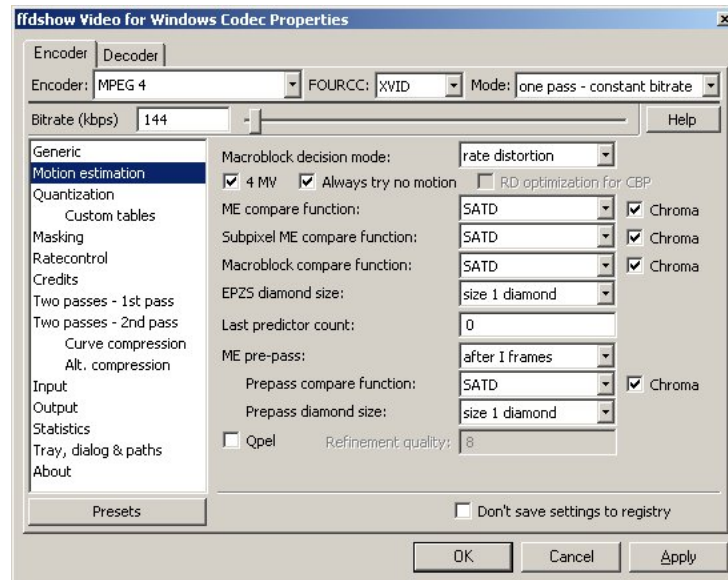


Screen Shot da aplicação **Avidemux**

## Ffdshow

**Ffdshow** é um codec *Video for Windows* e *DirectShow open-source* que permite codificar/descodificar diversos formatos de vídeo e áudio, incluindo vídeos DivX e XviD usando a biblioteca de codecs fornecida pela [libavcodec](http://libavcodec.org)<sup>4</sup>.

O site oficial da aplicação é: <http://sourceforge.net/projects/ffdshow>



Janela de configuração do codificador de vídeo ffdshow

## Ffmpeg



**FFmpeg** são um conjunto de programas que permitem gravar, converter e efectuar posteriormente a difusão digital de *stream* áudio e vídeo. Inicialmente foi desenvolvido para sistemas linux, mas actualmente já existem versões para Windows.

Através da técnica de *reverse-engineered*, a aplicação re-implementou vários codecs [5]:

- [Sorenson 3 Codec](#)
- [Advanced Streaming Format](#)
- [Windows Media Audio](#)
- [Windows Media Video](#)
- [QDesign Music Codec 2](#),

<sup>4</sup> **Libavcodec** é uma livreria de codecs, programada em C, que permite codificar e descodificar vídeo e áudio. Esta é parte do projecto FFmpeg, e é usada em diversas aplicações.

O site oficial é: <http://www.ffmpeg.org/>

## GordianKnot

Embora inicialmente tenha sido projectado para apenas para calcular o *bitrate* da codificação DivX, actualmente também codifica DivX/XviD.

O site oficial é: <http://sourceforge.net/projects/gordianknot>

## Handbrake



**HandBrake** é uma aplicação multi-plataforma, com capacidade de converter DVD para MPEG-4. Embora inicialmente esta tenha sido desenvolvida para BeOS, actualmente já existem versões para MacOS X e Linux.

Actualmente esta ferramenta permite efectuar várias formas de transcodificação, sendo estas apresentadas na tabela seguinte.

| Fontes Suportadas    | Saídas                                                  |
|----------------------|---------------------------------------------------------|
| Qualquer tipo de DVD | Formato do ficheiro: MP4, AVI ou OGM                    |
| PAL ou NTSC          | Video: MPEG-4 ou H.264<br>(constant quantizer encoding) |
| AC-3, LPCM           | Audio: AAC, MP3, AC-3                                   |

Formas de transcodificação suportadas pelo HandBrake

## MeGUI

**MeGUI** é uma ferramenta gráfica extremamente intuitiva que opera sobre o standard MPEG-4. Possui um leque vasto de potencialidades, suportando MPEG-4 ASP (XviD & libavcodec MPEG-4), usando o codificador *mencoder*. Suporta MPEG-4 AVC usando o codificador *x264* e *mencoder* e, suporta também (HE)AAC usando para tal o codificador AAC BeSweet.

## MEncoder

**MEncoder** é uma ferramenta, em linha de comandos, para codificar e decodificar vídeo. Esta é distribuída livremente usando uma licença GPL.

O site oficial é: <http://www.mplayerhq.hu/>

## PspVideo9

A aplicação **PSPVideo9**, desenvolvida por um estudante de engenharia da Universidade de Carleton, permite converter um vasto leque de formatos (avi, mpeg, etc) no formato de vídeo suportado pela *Play Station Portable* (PSP).

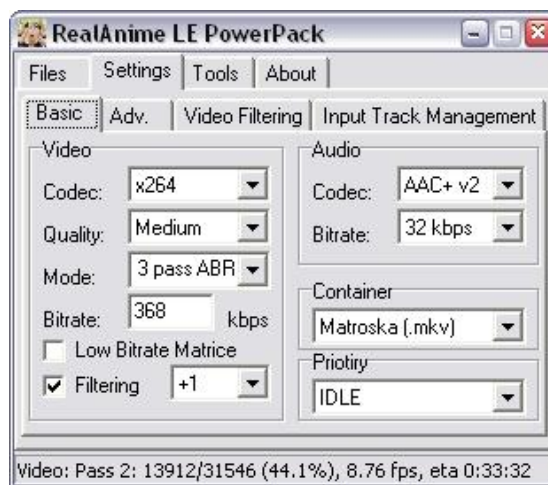
O site oficial é: <http://www.pspvideo9.com/lang/pt-BR/>

## RealAnime

**RealAnime** é uma ferramenta gráfica, bastante intuitiva e fácil de utilizar, capaz de converter diversos formatos de ficheiros de vídeo, usando diferentes codificadores:

| Codecs Vídeo | Codecs Áudio | Codificadores     |
|--------------|--------------|-------------------|
| x264         | AAC+ v2      | x264              |
| XviD         | Vorbis       | BeSweet           |
| RV10         | MP3          | mEncoder          |
| Snow         |              | Helix Producer 11 |

Funcionalidades da ferramenta RealAnime



Frontend da ferramenta RealAnime

## StaxRip

O **StaxRip** é uma ferramenta *open-source* para converter DVD, DVB, entre outros, para praticamente qualquer tipo de formato.

| Codecs Vídeo | Codecs Áudio |
|--------------|--------------|
| DivX         | MP3          |

|        |            |
|--------|------------|
| XviD   | AC3        |
| x264   | MP3        |
| MPEG-2 | MP2/MPA    |
| MPEG-4 | AAC        |
|        | Ogg Vorbis |
|        | DTS        |
|        | WAV        |

O site oficial é: <http://www.planetdvd.net/staxrip/index.htm>

## TCVP



TCVP é um player de vídeo e música com capacidades de codificação e transcodificação para sistemas operativos Unix. Actualmente o desenvolvimento desta aplicação está estagnado.

## VLC media player



O VLC é um player multimédia de *open-source*, possuindo suporte para vários formatos de vídeo, tais como o MPEG-1, MPEG-2, MPEG-4, DivX, DVD, VCDs, etc. Além disso, tem suporte a vários protocolos de *streaming*, podendo ser usado como servidor de vídeo numa rede. Possui suporte para transmissão em unicast ou multicast. Além disso, opera em redes IPv4 e IPv6 [6].

O VLC tem versões para vários sistemas operativos, tais como Windows, Mac OS, FreeBSD, Linux, BeOS, entre outros e possui suporte a vários protocolos como UDP, HTTP, RTP, etc.

O VLC é um dos melhores softwares usados para transmissão e reprodução de vídeos. Isso devido a gama de plataformas suportadas, formatos de arquivos tocados, dentre outras funcionalidades que vêm sendo agregadas ao VLC constantemente. Mais informações sobre as características do VLC podem ser obtidas através da página oficial:

<http://www.videolan.org/vlc/>

## Referencias

---

[1] <http://www.apple.com/quicktime/technologies/h264/>



- [2] <http://www.videolan.org/x264.html>
- [3] <http://en.wikipedia.org/wiki/Doom9>
- [4] <http://en.wikipedia.org/wiki/X264>
- [5] <http://en.wikipedia.org/wiki/FFmpeg>
- [6] <http://www.videolan.org/vlc/>

### 9.3 Configurações efectuadas nos Testes

### 9.3.1 IPv4 – PIM-SM (nativo)

[illegible]

| Router 1                                                                                                                                                                                                                                         | Router 2                                                                                                                                                                                                                                                   | Router 3                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> R1#sh run Building configuration...  Current configuration : 1067 bytes ! version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname R1 ! boot-start-marker </pre> | <pre> R2#sh R2#show run R2#show running-config Building configuration...  Current configuration : 989 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname R2 </pre> | <pre> R3#sh run Building configuration...  Current configuration : 891 bytes ! version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname R3 ! boot-start-marker </pre> |

|                                     |                                     |                                     |
|-------------------------------------|-------------------------------------|-------------------------------------|
| boot-end-marker                     | !                                   | boot-end-marker                     |
| !                                   | boot-start-marker                   | !                                   |
| !                                   | boot-end-marker                     | !                                   |
| memory-size iomem 10                | !                                   | memory-size iomem 10                |
| no network-clock-participate slot 1 | !                                   | no network-clock-participate slot 1 |
| no network-clock-participate wic 0  | !                                   | no network-clock-participate wic 0  |
| no aaa new-model                    | resource policy                     | no aaa new-model                    |
| ip subnet-zero                      | !                                   | ip subnet-zero                      |
| !                                   | no aaa new-model                    | !                                   |
| !                                   | no network-clock-participate slot 1 | !                                   |
| !                                   | no network-clock-participate wic 0  | !                                   |
| !                                   | !                                   | !                                   |
| ip cef                              | !                                   | ip cef                              |
| ip ips po max-events 100            | !                                   | ip ips po max-events 100            |
| ipv6 unicast-routing                | !                                   | ipv6 unicast-routing                |
| ipv6 multicast-routing              | ip cef                              | ipv6 multicast-routing              |
| no ftp-server write-enable          | ipv6 unicast-routing                | no ftp-server write-enable          |
| !                                   | ipv6 multicast-routing              | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | !                                   | !                                   |
| interface FastEthernet0/0           | !                                   | interface FastEthernet0/0           |
| no ip address                       | !                                   | no ip address                       |
| duplex auto                         | !                                   | duplex auto                         |
| speed auto                          | !                                   | speed auto                          |
| ipv6 address 2001:AAA::1/32         | interface FastEthernet0/0           | ipv6 address 2001:DDD::1/32         |
| ipv6 rip cisco enable               | no ip address                       | ipv6 rip cisco enable               |
| !                                   | duplex auto                         | !                                   |
| interface Serial0/0                 | speed auto                          | interface FastEthernet0/1           |
| no ip address                       | ipv6 address 2001:BBB::2/32         | no ip address                       |
| shutdown                            | ipv6 rip cisco enable               | duplex auto                         |
| !                                   | !                                   | speed auto                          |
| interface BRI0/0                    | interface Serial0/0                 | ipv6 address 2001:CCC::1/32         |
| no ip address                       | no ip address                       | ipv6 rip cisco enable               |
| shutdown                            | shutdown                            | !                                   |
| !                                   | no fair-queue                       | ip classless                        |
| interface FastEthernet0/1           | no dce-terminal-timing-enable       | !                                   |
| no ip address                       | !                                   | !                                   |
| duplex auto                         | interface FastEthernet0/1           | ip http server                      |
| speed auto                          | no ip address                       | no ip http secure-server            |
| ipv6 address 2001:BBB::1/32         | duplex auto                         | !                                   |
| ipv6 rip cisco enable               | speed auto                          | ipv6 router rip cisco               |
| !                                   | ipv6 address 2001:CCC::2/32         | !                                   |
| interface Serial0/1                 | ipv6 rip cisco enable               | ipv6 pim rp-address 2001:CCC::2     |
| no ip address                       | !                                   | !                                   |
| shutdown                            | interface Serial0/1                 | !                                   |
| !                                   | no ip address                       | control-plane                       |
| ip classless                        | shutdown                            | !                                   |
| !                                   | no dce-terminal-timing-enable       | !                                   |
| !                                   | !                                   | !                                   |
| ip http server                      | !                                   | !                                   |
| no ip http secure-server            | !                                   | !                                   |
| !                                   | ip http server                      | !                                   |
| ipv6 router rip cisco               | no ip http secure-server            | !                                   |
| !                                   | !                                   | !                                   |
| ipv6 pim rp-address 2001:CCC::2     | ipv6 router rip cisco               | !                                   |
| !                                   | !                                   | !                                   |
| !                                   | ipv6 pim rp-address 2001:CCC::2     | line con 0                          |
| !                                   | !                                   | line aux 0                          |
| control-plane                       | !                                   | line vty 0 4                        |







|                               |                           |                     |                     |                      |
|-------------------------------|---------------------------|---------------------|---------------------|----------------------|
| !                             | no ip address             | no ip address       | interface           | !                    |
| interface Serial0/0           | ipv6 address              | shutdown            | FastEthernet0/0     | interface Tunnel11   |
| no ip address                 | 3FFE:A::2/64              | duplex auto         | no ip address       | no ip address        |
| shutdown                      | tunnel source 2001:B::1   | speed auto          | shutdown            | ipv6 address         |
| no dce-terminal-timing-enable | tunnel destination        | !                   | duplex auto         | 3FFE:A::1/64         |
| !                             | 2001:D::4                 | interface Serial0/0 | speed auto          | tunnel source        |
| interface Serial0/1           | tunnel mode gre ipv6      | no ip address       | !                   | 2001:D::4            |
| no ip address                 | !                         | ipv6 address        | interface Serial0/0 | tunnel destination   |
| ipv6 address 2001:A::2/64     | interface FastEthernet0/0 | 2001:B::2/64        | no ip address       | 2001:B::1            |
| clock rate 128000             | no ip address             | no fair-queue       | ipv6 address        | tunnel mode gre ipv6 |
| no dce-terminal-timing-enable | shutdown                  | clock rate 128000   | 2001:D::3/64        | !                    |
| !                             | duplex auto               | no dce-terminal-    | no fair-queue       | interface            |
| !                             | speed auto                | timing-enable       | no dce-terminal-    | FastEthernet0/0      |
| !                             | no ipv6 mfib forwarding   | !                   | timing-enable       | no ip address        |
| ip http server                | !                         | interface           | !                   | duplex auto          |
| no ip http secure-server      | interface Serial0/0       | FastEthernet0/1     | interface BRI0/0    | speed auto           |
| !                             | no ip address             | no ip address       | no ip address       | ipv6 address         |
| ipv6 route ::0 2001:A::1      | ipv6 address 2001:B::1/64 | duplex auto         | encapsulation hdlc  | 2001:E::4/64         |
| ipv6 pim rp-address           | clock rate 128000         | speed auto          | shutdown            | !                    |
| 2001:AAAA::1                  | no dce-terminal-timing-   | ipv6 address        | !                   | interface BRI0/0     |
| !                             | enable                    | 2001:C::2/64        | interface           | no ip address        |
| !                             | !                         | !                   | FastEthernet0/1     | encapsulation hdlc   |
| !                             | interface Serial0/1       | interface Serial0/1 | no ip address       | shutdown             |
| control-plane                 | no ip address             | no ip address       | --More--            | !                    |
| !                             | ipv6 address 2001:A::1/64 | shutdown            | duplex auto         | interface Serial0/0  |
| !                             | no dce-terminal-timing-   | no dce-terminal-    | speed auto          | no ip address        |
| !                             | enable                    | timing-enable       | ipv6 address        | ipv6 address         |
| !                             | !                         | !                   | 2001:C::3/64        | 2001:D::4/64         |
| !                             | !                         | !                   | !                   | clock rate 128000    |
| !                             | !                         | !                   | interface Serial0/1 | no dce-terminal-     |
| !                             | ip http server            | ip http server      | no ip address       | timing-enable        |
| !                             | no ip http secure-server  | no ip http secure-  | shutdown            | !                    |
| !                             | !                         | server              | no dce-terminal-    | interface Serial0/1  |
| !                             | ipv6 route 2001:D::/64    | !                   | timing-enable       | no ip address        |
| line con 0                    | 3FFE:A::1 multicast       | ipv6 route          | !                   | shutdown             |
| line aux 0                    | ipv6 route                | 2001:A::/64         | !                   | no dce-terminal-     |
| line vty 0 4                  | 2001:AAAA::/64            | 2001:B::1           | !                   | timing-enable        |
| !                             | 2001:A::2                 | ipv6 route          | ip http server      | !                    |
| !                             | ipv6 route ::0 2001:B::2  | 2001:AAAA::/64      | no ip http secure-  | !                    |
| end                           | unicast                   | 2001:B::1           | server              | !                    |
| RSources#                     | ipv6 pim rp-address       | ipv6 route ::0      | !                   | ip http server       |
|                               | 2001:AAAA::1              | 2001:C::3           | ipv6 route          | no ip http secure-   |
|                               | !                         | !                   | 2001:E::/64         | server               |
|                               | !                         | !                   | 2001:D::4           | !                    |
|                               | !                         | !                   | ipv6 route ::0      | ipv6 route ::0       |
|                               | control-plane             | control-plane       | 2001:C::2           | 3FFE:A::2 multicast  |
|                               | !                         | !                   | !                   | ipv6 route ::0       |
|                               | !                         | !                   | !                   | 2001:D::3 unicast    |
|                               | !                         | !                   | !                   | ipv6 pim rp-address  |
|                               | !                         | !                   | control-plane       | 2001:AAAA::1         |
|                               | !                         | !                   | !                   | !                    |
|                               | !                         | !                   | !                   | !                    |
|                               | !                         | !                   | --More--            | control-plane        |
|                               | !                         | !                   | !                   | !                    |
|                               | !                         | !                   | !                   | !                    |
|                               | line con 0                | line con 0          | control-plane       | !                    |
|                               | line aux 0                | line aux 0          | !                   | !                    |
|                               | line vty 0 4              | line vty 0 4        | !                   | !                    |
|                               | !                         | login               | !                   | !                    |
|                               | end                       | !                   | voice-port 1/0/0    | !                    |
|                               |                           | end                 | !                   | !                    |
|                               | R1#                       |                     | voice-port 1/0/1    | !                    |
|                               |                           | R2#                 | !                   | !                    |
|                               |                           |                     | !                   | line con 0           |
|                               |                           |                     | !                   | line aux 0           |
|                               |                           |                     | line con 0          | line vty 0 4         |
|                               |                           |                     | line aux 0          | !                    |
|                               |                           |                     | line vty 0 4        | !                    |
|                               |                           |                     | !                   | end                  |
|                               |                           |                     | !                   |                      |
|                               |                           |                     | end                 | R4#                  |
|                               |                           |                     |                     |                      |
|                               |                           |                     | R3#                 |                      |





## IPv6@ESTG-Leiria: Vídeo-Difusão sobre Multicast IPv6

|                               |                               |                               |                               |                               |
|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| ipv6 rip FCCN enable          | no ip address                 | shutdown                      | 2001:D::3/64                  | !                             |
| !                             | ipv6 address                  | duplex auto                   | ipv6 rip                      | !                             |
| interface Serial0/0           | 3FFE:A::2/64                  | speed auto                    | ESTG_Leiria enable            | interface Tunnel11            |
| no ip address                 | tunnel source 2001:B::1       | !                             | no fair-queue                 | no ip address                 |
| shutdown                      | tunnel destination            | interface Serial0/0           | clock rate 128000             | ipv6 address                  |
| no dce-terminal-timing-enable | 2001:D::4                     | no ip address                 | no dce-terminal-timing-enable | 3FFE:A::1/64                  |
| !                             | tunnel mode gre ipv6          | ipv6 address                  | !                             | tunnel source                 |
| interface Serial0/1           | !                             | 2001:B::2/64                  | interface BRI0/0              | 2001:D::4                     |
| no ip address                 | interface FastEthernet0/0     | ipv6 rip FCCN                 | no ip address                 | tunnel destination            |
| ipv6 address 2001:A::2/64     | no ip address                 | enable                        | encapsulation hdlc            | 2001:B::1                     |
| ipv6 rip FCCN enable          | shutdown                      | no fair-queue                 | shutdown                      | tunnel mode gre ipv6          |
| no dce-terminal-timing-enable | duplex auto                   | clock rate 128000             | !                             | !                             |
| !                             | speed auto                    | no dce-terminal-timing-enable | interface                     | FastEthernet0/0               |
| !                             | !                             | !                             | FastEthernet0/1               | no ip address                 |
| !                             | interface Serial0/0           | interface                     | no ip address                 | duplex auto                   |
| ip http server                | no ip address                 | FastEthernet0/1               | duplex auto                   | speed auto                    |
| no ip http secure-server      | ipv6 address 2001:B::1/64     | no ip address                 | speed auto                    | ipv6 address                  |
| !                             | ipv6 rip FCCN enable          | duplex auto                   | ipv6 address                  | 2001:E::4/64                  |
| ipv6 router rip FCCN          | no dce-terminal-timing-enable | speed auto                    | 2001:C::3/64                  | ipv6 rip                      |
| !                             | !                             | ipv6 address                  | !                             | ESTG_Leiria enable            |
| ipv6 pim rp-address           | interface Serial0/1           | 2001:C::2/64                  | interface Serial0/1           | !                             |
| 2001:AAAA::1                  | no ip address                 | !                             | no ip address                 | interface BRI0/0              |
| !                             | ipv6 address 2001:A::1/64     | interface Serial0/1           | shutdown                      | no ip address                 |
| !                             | ipv6 rip FCCN enable          | no ip address                 | no dce-terminal-timing-enable | encapsulation hdlc            |
| control-plane                 | clock rate 128000             | shutdown                      | !                             | shutdown                      |
| !                             | no dce-terminal-timing-enable | no dce-terminal-timing-enable | !                             | !                             |
| !                             | !                             | !                             | !                             | interface Serial0/0           |
| !                             | !                             | !                             | ip http server                | no ip address                 |
| !                             | !                             | !                             | no ip http secure-server      | ipv6 address                  |
| !                             | ip http server                | ip http server                | !                             | 2001:D::4/64                  |
| !                             | no ip http secure-server      | no ip http secure-server      | !                             | ipv6 rip                      |
| !                             | !                             | !                             | ipv6 route ::/0               | ESTG_Leiria enable            |
| !                             | ipv6 route 2001:D::/64        | !                             | 2001:C::2 unicast             | no dce-terminal-timing-enable |
| !                             | 3FFE:A::1 multicast           | ipv6 route ::/0               | ipv6 router rip               | !                             |
| line con 0                    | ipv6 router rip FCCN          | 2001:C::3 unicast             | ESTG_Leiria                   | interface Serial0/1           |
| line aux 0                    | !                             | ipv6 router rip FCCN          | redistribute static           | no ip address                 |
| line vty 0 4                  | !                             | redistribute static           | !                             | shutdown                      |
| login                         | !                             | !                             | control-plane                 | no dce-terminal-timing-enable |
| !                             | !                             | !                             | !                             | !                             |
| !                             | control-plane                 | !                             | !                             | !                             |
| end                           | !                             | control-plane                 | !                             | !                             |
| RSources#                     | !                             | !                             | voice-port 1/0/0              | ip http server                |
| RSources#                     | !                             | !                             | !                             | no ip http secure-server      |
| RSources#                     | !                             | !                             | voice-port 1/0/1              | server                        |
|                               | !                             | !                             | !                             | !                             |
|                               | !                             | !                             | !                             | ipv6 route ::/0               |
|                               | !                             | !                             | !                             | 3FFE:A::2 multicast           |
|                               | !                             | !                             | !                             | ipv6 router rip               |
|                               | !                             | !                             | !                             | ESTG_Leiria                   |
|                               | !                             | !                             | !                             | !                             |
|                               | line con 0                    | !                             | !                             | !                             |
|                               | line aux 0                    | !                             | !                             | !                             |
|                               | line vty 0 4                  | line con 0                    | !                             | !                             |
|                               | login                         | line aux 0                    | line con 0                    | control-plane                 |
|                               | !                             | line vty 0 4                  | line aux 0                    | !                             |
|                               | !                             | login                         | line vty 0 4                  | !                             |
|                               | end                           | !                             | login                         | line con 0                    |
|                               |                               | !                             | !                             | line aux 0                    |
|                               | R1#                           | end                           | !                             | line vty 0 4                  |
|                               |                               |                               | end                           | login                         |
|                               |                               | R2#                           |                               | !                             |
|                               |                               | R2#                           | R3#                           | !                             |
|                               |                               | R2#                           |                               | end                           |
|                               |                               |                               |                               | R4#                           |
|                               |                               |                               |                               | R4#                           |

### 9.3.6 IPv6 – PIM-SSM (túnel)

| RSource                           | R1                        | R2                    | R3                   | R4                     |
|-----------------------------------|---------------------------|-----------------------|----------------------|------------------------|
| RSource#shy                       | R1>en                     | R2#sh                 | R3#show run          | R4#show running-       |
| RSource#sh run                    | R1#sh                     | R2#show run           | Current              | config                 |
| RSource#sh running-config         | R1#show run               | R2#show running-      | configuration : 1123 | Building               |
| Building configuration...         | R1#show running-config    | config                | bytes                | configuration...       |
|                                   | Building configuration... | Building              | !                    |                        |
| Current configuration : 894 bytes | Current configuration :   | configuration...      | version 12.4         | Current configuration  |
| !                                 | 1130 bytes                | Current configuration | service timestamps   | : 1146 bytes           |
| version 12.4                      | !                         | : 1007 bytes          | debug datetime msec  | !                      |
| service timestamps debug          | version 12.4              | !                     | service timestamps   | version 12.4           |
| datetime msec                     | service timestamps debug  | version 12.4          | log datetime msec    | service timestamps     |
| service timestamps log datetime   | datetime msec             | service timestamps    | no service password- | debug datetime msec    |
| msec                              | service timestamps log    | debug datetime msec   | encryption           | service timestamps     |
| no service password-encryption    | datetime msec             | service timestamps    | !                    | log datetime msec      |
| !                                 | no service password-      | log datetime msec     | hostname R3          | no service password-   |
| hostname RSource                  | encryption                | no service password-  | !                    | encryption             |
| !                                 | !                         | encryption            | boot-start-marker    | !                      |
| boot-start-marker                 | hostname R1               | !                     | boot-end-marker      | hostname R4            |
| boot-end-marker                   | !                         | hostname R2           | !                    | !                      |
| !                                 | boot-start-marker         | !                     | !                    | boot-start-marker      |
| !                                 | boot-end-marker           | boot-start-marker     | resource policy      | boot-end-marker        |
| resource policy                   | !                         | boot-end-marker       | !                    | !                      |
| !                                 | !                         | !                     | no aaa new-model     | !                      |
| no aaa new-model                  | !                         | !                     | memory-size iomem    | resource policy        |
| memory-size iomem 10              | resource policy           | !                     | 10                   | !                      |
| no network-clock-participate slot | !                         | resource policy       | no network-clock-    | no aaa new-model       |
| 1                                 | no aaa new-model          | !                     | participate slot 1   | memory-size iomem      |
| no network-clock-participate wic  | memory-size iomem 10      | no aaa new-model      | no network-clock-    | 10                     |
| 0                                 | no network-clock-         | memory-size iomem     | participate wic 0    | no network-clock-      |
| !                                 | participate slot 1        | 10                    | !                    | participate slot 1     |
| !                                 | no network-clock-         | no network-clock-     | !                    | no network-clock-      |
| !                                 | participate wic 0         | participate slot 1    | !                    | participate wic 0      |
| !                                 | !                         | no network-clock-     | ip cef               | !                      |
| ip cef                            | !                         | participate wic 0     | ipv6 unicast-routing | !                      |
| ipv6 unicast-routing              | !                         | !                     | !                    | !                      |
| ipv6 multicast-routing            | !                         | !                     | !                    | !                      |
| !                                 | ip cef                    | !                     | !                    | ip cef                 |
| !                                 | ipv6 unicast-routing      | !                     | !                    | ipv6 unicast-routing   |
| !                                 | ipv6 multicast-routing    | ip cef                | !                    | ipv6 multicast-routing |
| !                                 | !                         | ipv6 unicast-routing  | !                    | !                      |
| !                                 | !                         | !                     | !                    | !                      |
| !                                 | !                         | !                     | interface            | !                      |
| !                                 | !                         | !                     | FastEthernet0/0      | !                      |
| !                                 | !                         | !                     | no ip address        | !                      |
| !                                 | !                         | !                     | shutdown             | !                      |
| !                                 | !                         | !                     | duplex auto          | !                      |
| !                                 | !                         | !                     | speed auto           | !                      |
| !                                 | !                         | !                     | !                    | !                      |
| !                                 | !                         | !                     | interface Serial0/0  | !                      |
| !                                 | !                         | !                     | no ip address        | !                      |
| !                                 | !                         | !                     | ipv6 address         | !                      |
| !                                 | !                         | !                     | 2001:D::3/64         | !                      |
| !                                 | !                         | !                     | ipv6 rip             | !                      |
| !                                 | !                         | !                     | ESTG_Leiria enable   | !                      |
| !                                 | !                         | !                     | no fair-queue        | !                      |
| !                                 | !                         | !                     | clock rate 128000    | !                      |
| !                                 | !                         | !                     | no dce-terminal-     | !                      |
| !                                 | !                         | !                     | timing-enable        | !                      |
| !                                 | !                         | !                     | !                    | !                      |
| interface FastEthernet0/0         | !                         | !                     | interface BRI0/0     | !                      |
| no ip address                     | !                         | !                     | no ip address        | !                      |
| duplex auto                       | !                         | !                     | encapsulation hdlc   | !                      |
| speed auto                        | interface Tunnel11        | !                     | shutdown             | interface Tunnel11     |
| ipv6 address 2001:AAAA::1/64      | no ip address             | interface             | !                    | no ip address          |
| ipv6 rip FCCN enable              | ipv6 address              | FastEthernet0/0       | interface            | ipv6 address           |
| !                                 | 3FFE:A::2/64              | no ip address         | FastEthernet0/1      | 3FFE:A::1/64           |
| interface Serial0/0               | tunnel source 2001:B::1   | shutdown              | no ip address        | tunnel source          |

## IPv6@ESTG-Leiria: Vídeo-Difusão sobre Multicast IPv6

|                               |                           |                      |                     |                      |
|-------------------------------|---------------------------|----------------------|---------------------|----------------------|
| no ip address                 | tunnel destination        | duplex auto          | duplex auto         | 2001:D::4            |
| shutdown                      | 2001:D::4                 | speed auto           | speed auto          | tunnel destination   |
| no dce-terminal-timing-enable | tunnel mode gre ipv6      | !                    | ipv6 address        | 2001:B::1            |
| !                             | !                         | interface Serial0/0  | 2001:C::3/64        | tunnel mode gre ipv6 |
| interface Serial0/1           | interface FastEthernet0/0 | no ip address        | !                   | !                    |
| no ip address                 | no ip address             | ipv6 address         | interface Serial0/1 | interface            |
| ipv6 address 2001:A::2/64     | shutdown                  | 2001:B::2/64         | no ip address       | FastEthernet0/0      |
| ipv6 rip FCCN enable          | duplex auto               | ipv6 rip FCCN        | shutdown            | no ip address        |
| no dce-terminal-timing-enable | speed auto                | enable               | no dce-terminal-    | duplex auto          |
| !                             | !                         | no fair-queue        | timing-enable       | speed auto           |
| !                             | interface Serial0/0       | clock rate 128000    | !                   | ipv6 address         |
| !                             | no ip address             | no dce-terminal-     | !                   | 2001:E::4/64         |
| ip http server                | ipv6 address 2001:B::1/64 | timing-enable        | !                   | ipv6 rip             |
| no ip http secure-server      | ipv6 rip FCCN enable      | !                    | ip http server      | ESTG_Leiria enable   |
| !                             | no dce-terminal-timing-   | interface            | no ip http secure-  | !                    |
| ipv6 router rip FCCN          | enable                    | FastEthernet0/1      | server              | interface BRI0/0     |
| !                             | !                         | no ip address        | !                   | no ip address        |
| !                             | interface Serial0/1       | duplex auto          | ipv6 route ::/0     | encapsulation hdlc   |
| !                             | no ip address             | speed auto           | 2001:C::2 unicast   | shutdown             |
| !                             | ipv6 address 2001:A::1/64 | ipv6 address         | ipv6 router rip     | !                    |
| control-plane                 | ipv6 rip FCCN enable      | 2001:C::2/64         | ESTG_Leiria         | interface Serial0/0  |
| !                             | clock rate 128000         | !                    | redistribute static | no ip address        |
| !                             | no dce-terminal-timing-   | interface Serial0/1  | !                   | ipv6 address         |
| !                             | enable                    | no ip address        | !                   | 2001:D::4/64         |
| !                             | !                         | shutdown             | !                   | ipv6 rip             |
| !                             | !                         | no dce-terminal-     | !                   | ESTG_Leiria enable   |
| !                             | ip http server            | timing-enable        | control-plane       | no dce-terminal-     |
| !                             | no ip http secure-server  | !                    | !                   | timing-enable        |
| !                             | !                         | !                    | control-plane       | !                    |
| !                             | ipv6 route 2001:D::/64    | ip http server       | !                   | interface Serial0/1  |
| line con 0                    | 3FFE:A::1 multicast       | no ip http secure-   | !                   | no ip address        |
| line aux 0                    | ipv6 route 2001:E::/64    | server               | !                   | shutdown             |
| line vty 0 4                  | 3FFE:A::1 multicast       | !                    | voice-port 1/0/0    | no dce-terminal-     |
| login                         | ipv6 router rip FCCN      | ipv6 route ::/0      | !                   | timing-enable        |
| !                             | !                         | 2001:C::3 unicast    | !                   | !                    |
| !                             | !                         | ipv6 router rip FCCN | !                   | !                    |
| end                           | !                         | redistribute static  | !                   | ip http server       |
|                               | !                         | !                    | !                   | no ip http secure-   |
| RSources#                     | control-plane             | !                    | !                   | server               |
| RSources#                     | !                         | !                    | !                   | !                    |
|                               | !                         | !                    | !                   | ipv6 route ::/0      |
|                               | !                         | control-plane        | !                   | 3FFE:A::2 multicast  |
|                               | !                         | !                    | line con 0          | ipv6 router rip      |
|                               | !                         | !                    | line aux 0          | ESTG_Leiria          |
|                               | !                         | !                    | line vty 0 4        | !                    |
|                               | !                         | !                    | login               | !                    |
|                               | !                         | !                    | !                   | !                    |
|                               | !                         | !                    | !                   | !                    |
|                               | !                         | !                    | end                 | control-plane        |
|                               | line con 0                | !                    |                     | !                    |
|                               | line aux 0                | !                    | R3#                 | !                    |
|                               | line vty 0 4              | !                    |                     | !                    |
|                               | login                     | line con 0           |                     | !                    |
|                               | !                         | line aux 0           |                     | !                    |
|                               | !                         | line vty 0 4         |                     | !                    |
|                               | end                       | login                |                     | !                    |
|                               |                           | !                    |                     | !                    |
|                               | R1#                       | !                    |                     | !                    |
|                               | R1#                       | end                  |                     | !                    |
|                               | R1#                       |                      |                     | line con 0           |
|                               |                           | R2#                  |                     | line aux 0           |
|                               |                           | R2#                  |                     | line vty 0 4         |
|                               |                           | R2#                  |                     | login                |
|                               |                           |                      |                     | !                    |
|                               |                           |                      |                     | !                    |
|                               |                           |                      |                     | end                  |
|                               |                           |                      |                     |                      |
|                               |                           |                      |                     | R4#                  |
|                               |                           |                      |                     | R4#                  |

## 10 Anexos

### 10.1 IETF – Grupos de Trabalho

Como já foi referenciado ao longo deste relatório, o IETF é uma entidade a nível mundial que, entre outras actividades, desenvolve um vasto trabalho técnico na área dos protocolos para a Internet. Mais concretamente, este trabalho é efectuado por grupos de trabalho (WG – *Working Groups*) que são agrupados por diversas áreas (*routing, transport, security, etc.*)

Nesta secção são apresentados os WG que desenvolvem a sua actividade nas áreas deste projecto.

| Área                                                                                                                                                                                                                  | Grupos                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Internet</b><br>Directores:<br><a href="mailto:townsley@cisco.com">Mark Townsley &lt;townsley@cisco.com&gt;</a><br><a href="mailto:margaret@thingmagic.com">Margaret Wasserman &lt;margaret@thingmagic.com&gt;</a> | <b>IP Version 6 (<a href="#">ipv6</a>)</b><br><b>Multicast &amp; Anycast Group Membership (<a href="#">magma</a>)</b> |
| <b>Encaminhamento</b><br>Directores:<br><a href="mailto:fenner@research.att.com">Bill Fenner &lt;fenner@research.att.com&gt;</a><br><a href="mailto:zinin@psg.com">Alex Zinin &lt;zinin@psg.com&gt;</a>               | <b>Protocol Independent Multicast (<a href="#">pim</a>)</b><br><b>Source-Specific Multicast (<a href="#">ssm</a>)</b> |
| <b>Transporte</b><br>Directores:<br><a href="mailto:mankin@psg.com">Allison Mankin &lt;mankin@psg.com&gt;</a><br><a href="mailto:jon.peterson@neustar.biz">Jon Peterson &lt;jon.peterson@neustar.biz&gt;</a>          | <b>Audio/Video Transport (<a href="#">avt</a>)</b><br><b>Reliable Multicast Transport (<a href="#">rmt</a>)</b>       |

Tabela 10.1 - Grupos de trabalho do IETF que trabalham na área deste projecto

#### 10.1.1 IPv6

O grupo IPv6 é responsável pela especificação e pela padronização da versão 6 do Protocolo Internet (IPv6 – *Internet Protocol*). O novo protocolo que, entre outras características, aumenta consideravelmente (por um factor de quatro) o espaço de endereçamento do IPv4 – o seu predecessor.

O grupo de trabalho IPv6 foi originalmente denominado pelo IESG de grupo de trabalho do Protocolo Internet da Nova Geração – (IPng – *IP Next Generation*). O seu objectivo inicial era implementar as recomendações dos directores de área (AD – *Area Directors*) delineadas em Julho de 1994 e RFC 1752 (*Recommendation for the IP Next Generation Protocol*) publicada em Janeiro de 1995.

Actualmente a função principal do grupo é completar a padronização do IPv6, rever e actualizar as especificações tendo por base o conhecimento adquirido através do desenvolvimento e das implementações praticas desenvolvidas ao longo dos últimos anos.

### **10.1.2 Multicast & Anycast**

O grupo de Multicast & Anycast tem um papel de extrema importância no funcionamento da Internet. É responsável pelo desenvolvimento de funcionalidades, relatórios e outras características necessárias aos grupos de Multicast. Além disso, é também responsável pelo endereçamento e, em conjunto com os membros do grupo Anycast, pelo desenvolvimento de mecanismos (simples) de segurança até a camada dois do modelo de OSI.

De uma forma simplista, desenvolve protocolos que permitem aos PCs trocar informações referentes a grupos Multicast. Os principais desenvolvimentos elaborados pelo grupo são apresentados de seguida:

- .Novos Protocolos – IGMPv3 e MLDv2 (este último anda se encontra em draft). Em termos concretos, estes protocolos não são completamente novos, são uma actualização aos seus antecessores.

- .Gestão de MIBs – actualização para IGMPv3 e MLDv2 das RFCs 2933 e 3019 respectivamente.

- .Interoperabilidade entre protocolos – IGMP com MLD; IGMP e MLD com protocolos de encaminhamento

- .Criação de uma Interface Programática de Aplicação – Multicast Source Filtering API responsável pela interacção de IGMPv3 com MLDv2.

### **10.1.3 Protocol Independent Multicast**

O grupo de trabalho PIM (PIM – *Protocol Independent Multicast*) está enquadrado na área de Encaminhamento do IETF, e é caracterizado por padronizar e promover o Protocolo Independente de Multicast, modo espaçado e denso (Sparse Mode, Dense Mode), como um protocolo escalável, eficiente e robusto, capaz de suportar milhares de grupos e diferentes tipos de aplicações. Além disso, o grupo é também responsável pela gestão, com o desenvolvimento de uma MIB especificamente para o protocolo PIM.

#### 10.1.4 Source-Specific Multicast

Tal como o PIM, o grupo de trabalho SSM (Source-Specific Multicast) encaixa-se na área de Encaminhamento e têm como função definir, de uma forma bastante clara, a semântica para que os desenhadores de protocolos e interfaces dos *host* usam em conjunção com a Especificação Multicast da fonte de Origem (Source-Specific Multicast). De uma forma mais concreta e acessível, o grupo cria documentos que servem de referência aos autores de RFCs na área do Multicast.

O grupo tem como função publicar RFCs que definam claramente o modelo Multicast Source-Specific e a sua relação com a RFC 1112. Definição de regras que os *Host* e os *Routers* devem seguir quando pretendam usar e/ou reservar os endereços específicos do Multicast.

#### 10.1.5 Audio/Video Transport

O grupo Transporte de Áudio/Vídeo (AVT - *Áudio/Vídeo Transport*) esta agrupado na área de transporte do IETF e foi formado com o propósito de desenvolver um protocolo para a transmissão de áudio e vídeo em tempo real, assente em Multicast e Unicast IDP/IP. Esse é conhecido como RTP (*Real-Time Transport Protocol*).

Actualmente o grupo está envolvido em vários projectos. O esquema seguinte apresenta alguns dos mais importantes.

- .Vários – desenvolver novos formatos para os novos Codec; documentar as melhores práticas (*best-current practices*) para o design de formatos do *payload*; completar o trabalho desenvolvido na correcção de erros; etc.

- .Gestão – actualização da MIB RTP para suportar as alterações introduzidas pela RFC 3550; desenvolver uma MIB para a RFC 3611 (RTCP-XR)

- .Perfis – desenvolver novos perfis para SRTP (RFC 3448); RTP/SAVPF; etc.

Convém para finalizar referir que, o grupo de trabalho disponibiliza na sua página um link que contém informação adicional, extremamente bem organizada e actual, sendo o conteúdo desta da responsabilidade do grupo.

### **10.1.6 Reliable Multicast Transport**

O grupo Reliable Multicast Transport (RMT) tem como objectivo definir mecanismos **confiáveis** de transporte de tráfego Multicast. Actualmente têm como alvo futuro a atingir, a definição de dois protocolos:

.Baseado em NACK (Negative Acknowledgment)

.ALC "Asynchronous Layered Coding" Protocol – usa correcção de erros de transferência dianteira (*Forward Error Correction*). Actualmente a RFC 3450 promove, de forma informativa, este tipo de protocolo (RFC 3450 – *Asynchronous Layered Coding (ALC) Protocol Instantiation*).

O grupo trabalha em parceria com os grupos *Reliable Multicast Transport* e *Multicast Security*, especialmente nas áreas de controlo de congestão e requisitos de segurança "forçados" pela RFC 2357 (RFC 2357 – *IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols*).

## **10.2 RFCs**

Com o decorrer dos anos, os membros do IETF foram desenvolvendo diversos documentos, conhecidos como RFC. Nas secções seguintes estão agrupadas, de uma forma tabelada, os diversos documentos desenvolvido pelos grupos de trabalhos nas áreas do IPv6; Multicast e Vídeo/Áudio.

Visto que com o amadurecimento das tecnologias/protocolos vão saindo novas versões de documentos que se "absorvem" alguns deles, nas tabelas seguintes apenas estão presentes os que se mantêm actualizados, isto é, todas as RFCs que estão desactualizadas não aparecem listadas nas tabelas seguintes.

O principal objectivo de sistematizar as RFCs neste relatório, deveu-se ao facto de se agrupar num único documento, as principais referências necessárias para aprofundar o trabalho desenvolvido. Convém também frisar que estas referências foram actualizadas, pela última vez em Outubro de 2005.

### **10.2.1 IPv6**



| Número                  | Título                                                                                                                                                                                                                                                                                                     | Data          | Inf                                                                                                       | Tipo                                   |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------|
| <a href="#">RFC1809</a> | <b>Using the Flow Label Field in IPv6</b>                                                                                                                                                                                                                                                                  | June 1995     |                                                                                                           | INFORMATIONAL                          |
| <b>Abstract</b>         | The purpose of this memo is to distill various opinions and suggestions of the End-to-End Research Group regarding the handling of Flow Labels into a set of suggestions for IPv6. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. |               |                                                                                                           |                                        |
| <a href="#">RFC1810</a> | <b>Report on MD5 Performance</b>                                                                                                                                                                                                                                                                           | June 1995     |                                                                                                           | INFORMATIONAL                          |
| <b>Abstract</b>         | This RFC addresses how fast MD5 can be implemented in software and hardware, and whether it supports currently available IP bandwidth. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind.                                             |               |                                                                                                           |                                        |
| <a href="#">RFC1825</a> | <b>Security Architecture for the Internet Protocol</b>                                                                                                                                                                                                                                                     | August 1995   | Obsoleted by <a href="#">RFC2401</a>                                                                      | PROPOSED STANDARD                      |
| <a href="#">RFC1826</a> | <b>IP Authentication Header</b>                                                                                                                                                                                                                                                                            | August 1995   | Obsoleted by <a href="#">RFC2402</a>                                                                      | PROPOSED STANDARD                      |
| <a href="#">RFC1827</a> | <b>IP Encapsulating Security Payload (ESP)</b>                                                                                                                                                                                                                                                             | August 1995   | Obsoleted by <a href="#">RFC2406</a>                                                                      | PROPOSED STANDARD                      |
| <a href="#">RFC1881</a> | <b>IPv6 Address Allocation Management</b>                                                                                                                                                                                                                                                                  | December 1995 |                                                                                                           | INFORMATIONAL                          |
| <b>Abstract</b>         | The IPv6 address space will be managed by the IANA for the good of the Internet community, with advice from the IAB and the IESG, by delegation to the regional registries. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind.        |               |                                                                                                           |                                        |
| <a href="#">RFC1883</a> | <b>Internet Protocol, Version 6 (IPv6) Specification</b>                                                                                                                                                                                                                                                   | December 1995 | Obsoleted by <a href="#">RFC2460</a>                                                                      | PROPOSED STANDARD                      |
| <a href="#">RFC1884</a> | <b>IP Version 6 Addressing Architecture</b>                                                                                                                                                                                                                                                                | December 1995 | Obsoleted by <a href="#">RFC2373</a>                                                                      | HISTORIC<br>[pub as:PROPOSED STANDARD] |
| <a href="#">RFC1885</a> | <b>Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)</b>                                                                                                                                                                                                               | December 1995 | Obsoleted by <a href="#">RFC2463</a>                                                                      | PROPOSED STANDARD                      |
| <a href="#">RFC1886</a> | <b>DNS Extensions to support IP version 6</b>                                                                                                                                                                                                                                                              | December 1995 | Obsoleted by <a href="#">RFC3596</a> ,<br>Updated by <a href="#">RFC2874</a> ,<br><a href="#">RFC3152</a> | PROPOSED STANDARD                      |
| <a href="#">RFC1887</a> | <b>An Architecture for IPv6 Unicast Address Allocation</b>                                                                                                                                                                                                                                                 | December 1995 |                                                                                                           | INFORMATIONAL                          |
| <b>Abstract</b>         | This document provides an architecture for allocating IPv6 [1] unicast addresses in the Internet. This document provides information for the Internet community. This memo does not specify an Internet standard of any kind.                                                                              |               |                                                                                                           |                                        |
| <a href="#">RFC1888</a> | <b>OSI NSAPs and IPv6</b>                                                                                                                                                                                                                                                                                  | August 1996   |                                                                                                           | HISTORIC<br>[pub as:EXPERIMENTAL]      |
| <b>Abstract</b>         | This document recommends that network implementors who have planned or deployed an OSI NSAP addressing plan, and who wish to deploy or transition to IPv6, should redesign a native IPv6 addressing plan to meet their needs. This memo defines an Experimental Protocol for the Internet community.       |               |                                                                                                           |                                        |
| <a href="#">RFC1897</a> | <b>IPv6 Testing Address Allocation</b>                                                                                                                                                                                                                                                                     | January 1996  | Obsoleted by <a href="#">RFC2471</a>                                                                      | EXPERIMENTAL                           |
| <a href="#">RFC1924</a> | <b>A Compact Representation of IPv6 Addresses</b>                                                                                                                                                                                                                                                          | Apr-01-1996   |                                                                                                           | INFORMATIONAL                          |
| <b>Abstract</b>         | This document specifies a more compact representation of IPv6 addresses, which permits encoding in a                                                                                                                                                                                                       |               |                                                                                                           |                                        |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                         |                |                                                          |                                           |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------------|-------------------------------------------|
|                                                    | mere 20 bytes. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind.                                                                                                                                                                                                                                                                  |                |                                                          |                                           |
| <a href="#">RFC1933</a>                            | Transition Mechanisms for IPv6 Hosts and Routers                                                                                                                                                                                                                                                                                                                                                        | April 1996     | Obsoleted by <a href="#">RFC2893</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC1970</a>                            | Neighbor Discovery for IP Version 6 (IPv6)                                                                                                                                                                                                                                                                                                                                                              | August 1996    | Obsoleted by <a href="#">RFC2461</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC1971</a>                            | IPv6 Stateless Address Autoconfiguration                                                                                                                                                                                                                                                                                                                                                                | August 1996    | Obsoleted by <a href="#">RFC2462</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC1972</a>                            | A Method for the Transmission of IPv6 Packets over Ethernet Networks                                                                                                                                                                                                                                                                                                                                    | August 1996    | Obsoleted by <a href="#">RFC2464</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC1981</a>                            | Path MTU Discovery for IP version 6                                                                                                                                                                                                                                                                                                                                                                     | August 1996    |                                                          | DRAFT STANDARD [pub as:PROPOSED STANDARD] |
| <b>Abstract</b>                                    | This document describes Path MTU Discovery for IP version 6. It is largely derived from RFC 1191, which describes Path MTU Discovery for IP version 4. [STANDARDS-TRACK]                                                                                                                                                                                                                                |                |                                                          |                                           |
| <a href="#">RFC2019</a>                            | Transmission of IPv6 Packets Over FDDI                                                                                                                                                                                                                                                                                                                                                                  | October 1996   | Obsoleted by <a href="#">RFC2467</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC2023</a>                            | IP Version 6 over PPP                                                                                                                                                                                                                                                                                                                                                                                   | October 1996   | Obsoleted by <a href="#">RFC2472</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC2030</a>                            | Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI                                                                                                                                                                                                                                                                                                                                    | October 1996   | Obsoletes <a href="#">RFC1769</a> <a href="#">Errata</a> | INFORMATIONAL                             |
| <b>Abstract</b>                                    | This memorandum describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind.                                                                                     |                |                                                          |                                           |
| <a href="#">RFC2073</a>                            | An IPv6 Provider-Based Unicast Address Format                                                                                                                                                                                                                                                                                                                                                           | January 1997   | Obsoleted by <a href="#">RFC2374</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC2080</a>                            | RIPng for IPv6                                                                                                                                                                                                                                                                                                                                                                                          | January 1997   |                                                          | PROPOSED STANDARD                         |
| <b>Abstract</b>                                    | This document specifies a routing protocol for an IPv6 internet. It is based on protocols and algorithms currently in wide use in the IPv4 Internet [STANDARDS-TRACK]                                                                                                                                                                                                                                   |                |                                                          |                                           |
| <a href="#">RFC2133</a>                            | Basic Socket Interface Extensions for IPv6                                                                                                                                                                                                                                                                                                                                                              | April 1997     | Obsoleted by <a href="#">RFC2553</a>                     | INFORMATIONAL                             |
| <a href="#">RFC2147</a>                            | TCP and UDP over IPv6 Jumbograms                                                                                                                                                                                                                                                                                                                                                                        | May 1997       | Obsoleted by <a href="#">RFC2675</a>                     | PROPOSED STANDARD                         |
| <a href="#">RFC2185</a>                            | Routing Aspects of IPv6 Transition                                                                                                                                                                                                                                                                                                                                                                      | September 1997 |                                                          | INFORMATIONAL                             |
| <b>Abstract</b>                                    | This document gives an overview of the routing aspects of the IPv6 transition. It is based on the protocols defined in the document "Transition Mechanisms for IPv6 Hosts and Routers." Readers should be familiar with the transition mechanisms before reading this document. This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. |                |                                                          |                                           |
| <a href="#">RFC2292</a>                            | Advanced Sockets API for IPv6                                                                                                                                                                                                                                                                                                                                                                           | February 1998  | Obsoleted by <a href="#">RFC3542</a>                     | INFORMATIONAL                             |
| <a href="#">RFC2365</a><br><a href="#">BCP0023</a> | Administratively Scoped IP Multicast                                                                                                                                                                                                                                                                                                                                                                    | July 1998      |                                                          | BEST CURRENT PRACTICE                     |
| <b>Abstract</b>                                    | This document defines the "administratively scoped IPv4 multicast space" to be the range 239.0.0.0 to 239.255.255.255. In addition, it describes a simple set of semantics for the implementation of                                                                                                                                                                                                    |                |                                                          |                                           |

|                         |                                                                                                                                                                                                                                                                                                                |                |                                                                             |                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------------------------------------------------------------------------|----------------------------------------|
|                         | Administratively Scoped IP Multicast. Finally, it provides a mapping between the IPv6 multicast address classes [RFC1884] and IPv4 multicast address classes. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. |                |                                                                             |                                        |
| <a href="#">RFC2374</a> | <b>An IPv6 Aggregatable Global Unicast Address Format</b>                                                                                                                                                                                                                                                      | July 1998      | Obsoletes <a href="#">RFC2073</a> ,<br>Obsoleted by <a href="#">RFC3587</a> | HISTORIC<br>[pub as:PROPOSED STANDARD] |
| <a href="#">RFC2375</a> | <b>IPv6 Multicast Address Assignments</b>                                                                                                                                                                                                                                                                      | July 1998      |                                                                             | INFORMATIONAL                          |
| <b>Abstract</b>         | This document defines the initial assignment of IPv6 multicast addresses. This memo provides information for the Internet community. It does not specify an Internet standard of any kind.                                                                                                                     |                |                                                                             |                                        |
| <a href="#">RFC2401</a> | <b>Security Architecture for the Internet Protocol</b>                                                                                                                                                                                                                                                         | November 1998  | Obsoletes <a href="#">RFC1825</a> ,<br>Updated by <a href="#">RFC3168</a>   | PROPOSED STANDARD                      |
| <b>Abstract</b>         | This memo specifies the base architecture for IPsec compliant systems. [STANDARDS-TRACK]                                                                                                                                                                                                                       |                |                                                                             |                                        |
| <a href="#">RFC2402</a> | <b>IP Authentication Header</b>                                                                                                                                                                                                                                                                                | November 1998  | Obsoletes <a href="#">RFC1826</a>                                           | PROPOSED STANDARD                      |
| <b>Abstract</b>         | The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "authentication"), and to provide protection against replays. [STANDARDS-TRACK]                                                                   |                |                                                                             |                                        |
| <a href="#">RFC2406</a> | <b>IP Encapsulating Security Payload (ESP)</b>                                                                                                                                                                                                                                                                 | November 1998  | Obsoletes <a href="#">RFC1827</a>                                           | PROPOSED STANDARD                      |
| <b>Abstract</b>         | The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. [STANDARDS-TRACK]                                                                                                                                                                          |                |                                                                             |                                        |
| <a href="#">RFC2428</a> | <b>FTP Extensions for IPv6 and NATs</b>                                                                                                                                                                                                                                                                        | September 1998 |                                                                             | PROPOSED STANDARD                      |
| <b>Abstract</b>         | This paper specifies extensions to FTP that will allow the protocol to work over IPv4 and IPv6. [STANDARDS-TRACK]                                                                                                                                                                                              |                |                                                                             |                                        |
| <a href="#">RFC2450</a> | <b>Proposed TLA and NLA Assignment Rule</b>                                                                                                                                                                                                                                                                    | December 1998  |                                                                             | INFORMATIONAL                          |
| <b>Abstract</b>         | This document proposes rules for Top-Level Aggregation Identifiers (TLA ID) and Next-Level Aggregation Identifiers (NLA ID). This memo provides information for the Internet community.                                                                                                                        |                |                                                                             |                                        |
| <a href="#">RFC2452</a> | <b>IP Version 6 Management Information Base for the Transmission Control Protocol</b>                                                                                                                                                                                                                          | December 1998  | Obsoleted by <a href="#">RFC4022</a>                                        | PROPOSED STANDARD                      |
| <a href="#">RFC2454</a> | <b>IP Version 6 Management Information Base for the User Datagram Protocol</b>                                                                                                                                                                                                                                 | December 1998  | Obsoleted by <a href="#">RFC4113</a>                                        | HISTORIC<br>[pub as:PROPOSED STANDARD] |
| <a href="#">RFC2460</a> | <b>Internet Protocol, Version 6 (IPv6) Specification</b>                                                                                                                                                                                                                                                       | December 1998  | Obsoletes <a href="#">RFC1883</a>                                           | DRAFT STANDARD                         |
| <b>Abstract</b>         | This document specifies version 6 of the Internet Protocol (IPv6), also sometimes referred to as IP Next Generation or IPng. [STANDARDS-TRACK]                                                                                                                                                                 |                |                                                                             |                                        |
| <a href="#">RFC2461</a> | <b>Neighbor Discovery for IP Version 6 (IPv6)</b>                                                                                                                                                                                                                                                              | December 1998  | Obsoletes <a href="#">RFC1970</a>                                           | DRAFT STANDARD                         |
| <b>Abstract</b>         | This document specifies the Neighbor Discovery protocol for IP Version 6. [STANDARDS-TRACK]                                                                                                                                                                                                                    |                |                                                                             |                                        |
| <a href="#">RFC2462</a> | <b>IPv6 Stateless Address Autoconfiguration</b>                                                                                                                                                                                                                                                                | December 1998  | Obsoletes <a href="#">RFC1971</a><br><a href="#">Errata</a>                 | DRAFT STANDARD                         |
| <b>Abstract</b>         | This document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6. [STANDARDS-TRACK]                                                                                                                                                                              |                |                                                                             |                                        |
| <a href="#">RFC2463</a> | <b>Internet Control Message Protocol</b>                                                                                                                                                                                                                                                                       | December       | Obsoletes                                                                   | DRAFT                                  |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |                                                                                                                                     |                                          |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
|                         | <b>(ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification</b>                                                                                                                                                                                                                                                                                                                                                                                               | 1998          | <a href="#">RFC1885</a>                                                                                                             | STANDARD                                 |
| <b>Abstract</b>         | This document specifies a set of Internet Control Message Protocol (ICMP) messages for use with version 6 of the Internet Protocol (IPv6). [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                           |               |                                                                                                                                     |                                          |
| <a href="#">RFC2464</a> | <b>Transmission of IPv6 Packets over Ethernet Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                             | December 1998 | Obsoletes <a href="#">RFC1972</a><br><a href="#">Errata</a>                                                                         | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on Ethernet networks. It also specifies the content of the Source/Target Link-layer Address option used in Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages when those messages are transmitted on an Ethernet. [STANDARDS-TRACK] |               |                                                                                                                                     |                                          |
| <a href="#">RFC2465</a> | <b>Management Information Base for IP Version 6: Textual Conventions and General Group</b>                                                                                                                                                                                                                                                                                                                                                                             | December 1998 |                                                                                                                                     | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document is one in the series of documents that provide MIB definitions for for IP Version 6. Specifically, the IPv6 MIB textual conventions as well as the IPv6 MIB General group is defined in this document. [STANDARDS-TRACK]                                                                                                                                                                                                                                 |               |                                                                                                                                     |                                          |
| <a href="#">RFC2466</a> | <b>Management Information Base for IP Version 6: ICMPv6 Group</b>                                                                                                                                                                                                                                                                                                                                                                                                      | December 1998 |                                                                                                                                     | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document is one in the series of documents that define various MIB object groups for IPv6. Specifically, the ICMPv6 group is defined in this document. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                          |               |                                                                                                                                     |                                          |
| <a href="#">RFC2467</a> | <b>Transmission of IPv6 Packets over FDDI Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                 | December 1998 | Obsoletes <a href="#">RFC2019</a>                                                                                                   | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on FDDI networks. [STANDARDS-TRACK]                                                                                                                                                                                                                                                             |               |                                                                                                                                     |                                          |
| <a href="#">RFC2470</a> | <b>Transmission of IPv6 Packets over Token Ring Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                           | December 1998 |                                                                                                                                     | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This memo specifies the MTU and frame format for transmission of IPv6 packets on Token Ring networks. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                                                |               |                                                                                                                                     |                                          |
| <a href="#">RFC2471</a> | <b>IPv6 Testing Address Allocation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                 | December 1998 | Obsoletes <a href="#">RFC1897</a> ,<br>Obsoleted by <a href="#">RFC3701</a>                                                         | HISTORIC<br>[pub<br>as:EXPERIMENTAL<br>] |
| <a href="#">RFC2472</a> | <b>IP Version 6 over PPP</b>                                                                                                                                                                                                                                                                                                                                                                                                                                           | December 1998 | Obsoletes <a href="#">RFC2023</a>                                                                                                   | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document defines the method for transmission of IP Version 6 packets over PPP links as well as the Network Control Protocol (NCP) for establishing and configuring the IPv6 over PPP. It also specifies the method of forming IPv6 link-local addresses on PPP links. [STANDARDS- TRACK]                                                                                                                                                                          |               |                                                                                                                                     |                                          |
| <a href="#">RFC2473</a> | <b>Generic Packet Tunneling in IPv6 Specification</b>                                                                                                                                                                                                                                                                                                                                                                                                                  | December 1998 |                                                                                                                                     | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document defines the model and generic mechanisms for IPv6 encapsulation of Internet packets, such as IPv6 and IPv4. [STANDARDS- TRACK]                                                                                                                                                                                                                                                                                                                           |               |                                                                                                                                     |                                          |
| <a href="#">RFC2474</a> | <b>Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</b>                                                                                                                                                                                                                                                                                                                                                                         | December 1998 | Obsoletes <a href="#">RFC1455</a> ,<br><a href="#">RFC1349</a> ,<br>Updated by <a href="#">RFC3168</a> ,<br><a href="#">RFC3260</a> | PROPOSED STANDARD                        |
| <b>Abstract</b>         | This document defines the IP header field, called the DS (for differentiated services) field. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                                                        |               |                                                                                                                                     |                                          |
| <a href="#">RFC2491</a> | <b>IPv6 over Non-Broadcast Multiple Access (NBMA) networks</b>                                                                                                                                                                                                                                                                                                                                                                                                         | January 1999  |                                                                                                                                     | PROPOSED STANDARD                        |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |              |                                                                                                                     |                   |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">Abstract</a> | This document describes a general architecture for IPv6 over NBMA networks. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                |              |                                                                                                                     |                   |
| <a href="#">RFC2492</a>  | <b>IPv6 over ATM Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | January 1999 |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document is a companion to the ION working group's architecture document, "IPv6 over Non Broadcast Multiple Access (NBMA) networks". It provides specific details on how to apply the IPv6 over NBMA architecture to ATM networks. This architecture allows conventional host-side operation of the IPv6 Neighbor Discovery protocol, while also supporting the establishment of 'shortcut' ATM forwarding paths (when using SVCs). Operation over administratively configured Point to Point PVCs is also supported. [STANDARDS-TRACK] |              |                                                                                                                     |                   |
| <a href="#">RFC2497</a>  | <b>Transmission of IPv6 Packets over ARCnet Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | January 1999 |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This memo specifies a frame format for transmission of IPv6 packets and the method of forming IPv6 link-local and statelessly autoconfigured addresses on ARCnet networks. It also specifies the content of the Source/Target Link-layer Address option used by the Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages described in, when those messages are transmitted on an ARCnet. [STANDARDS-TRACK]                                                                         |              |                                                                                                                     |                   |
| <a href="#">RFC2526</a>  | <b>Reserved IPv6 Subnet Anycast Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | March 1999   |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document defines a set of reserved anycast addresses within each subnet prefix, and lists the initial allocation of these reserved subnet anycast addresses. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                                                          |              |                                                                                                                     |                   |
| <a href="#">RFC2529</a>  | <b>Transmission of IPv6 over IPv4 Domains without Explicit Tunnels</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | March 1999   |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This memo specifies the frame format for transmission of IPv6 (IPv6) packets and the method of forming IPv6 link-local addresses over IPv4 domains. It also specifies the content of the Source/Target Link-layer Address option used in the Router Solicitation, Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement and Redirect messages, when those messages are transmitted on an IPv4 multicast network. [STANDARDS-TRACK]                                                                                         |              |                                                                                                                     |                   |
| <a href="#">RFC2545</a>  | <b>Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | March 1999   |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | BGP-4 Multiprotocol Extensions (BGP-MP) defines the format of two BGP attributes (MP_REACH_NLRI and MP_UNREACH_NLRI) that can be used to announce and withdraw the announcement of reachability information. This document defines how compliant systems should make use of those attributes for the purpose of conveying IPv6 routing information. [STANDARDS-TRACK]                                                                                                                                                                        |              |                                                                                                                     |                   |
| <a href="#">RFC2546</a>  | <b>6Bone Routing Practice</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | March 1999   | Obsoleted by <a href="#">RFC2772</a>                                                                                | INFORMATIONAL     |
| <a href="#">RFC2553</a>  | <b>Basic Socket Interface Extensions for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | March 1999   | Obsoletes <a href="#">RFC2133</a> ,<br>Obsoleted by <a href="#">RFC3493</a> ,<br>Updated by <a href="#">RFC3152</a> | INFORMATIONAL     |
| <a href="#">RFC2590</a>  | <b>Transmission of IPv6 Packets over Frame Relay Networks Specification</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | May 1999     |                                                                                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This memo describes mechanisms for the transmission of IPv6 packets over Frame Relay networks. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                             |              |                                                                                                                     |                   |
| <a href="#">RFC2675</a>  | <b>IPv6 Jumbograms</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | August 1999  | Obsoletes <a href="#">RFC2147</a>                                                                                   | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document describes the IPv6 Jumbo Payload option, which provides the means of specifying such large payload lengths. It also describes the changes needed to TCP and UDP to make use of jumbograms. [STANDARDS-TRACK]                                                                                                                                                                                                                                                                                                                   |              |                                                                                                                     |                   |
| <a href="#">RFC2710</a>  | <b>Multicast Listener Discovery (MLD) for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | October 1999 | Updated by <a href="#">RFC3590</a> ,<br><a href="#">RFC3810</a>                                                     | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document specifies the protocol used by an IPv6 router to discover the presence of multicast                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |                                                                                                                     |                   |

|                         |                                                                                                                                                                                                                                                                                                                  |                |                                                                                                                                                                |                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
|                         | listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. [STANDARDS TRACK]                                                                                             |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2711</a> | <b>IPv6 Router Alert Option</b>                                                                                                                                                                                                                                                                                  | October 1999   |                                                                                                                                                                | PROPOSED STANDARD                          |
| <b>Abstract</b>         | This memo describes a new IPv6 Hop-by-Hop Option type that alerts transit routers to more closely examine the contents of an IP datagram. [STANDARDS TRACK]                                                                                                                                                      |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2732</a> | <b>Format for Literal IPv6 Addresses in URL's</b>                                                                                                                                                                                                                                                                | December 1999  | Obsoleted by <a href="#">RFC3986</a> ,<br>Updates <a href="#">RFC2396</a>                                                                                      | PROPOSED STANDARD                          |
| <a href="#">RFC2740</a> | <b>OSPF for IPv6</b>                                                                                                                                                                                                                                                                                             | December 1999  | <a href="#">Errata</a>                                                                                                                                         | PROPOSED STANDARD                          |
| <b>Abstract</b>         | This document describes the modifications to OSPF to support version 6 of the Internet Protocol (IPv6). [STANDARDS TRACK]                                                                                                                                                                                        |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2765</a> | <b>Stateless IP/ICMP Translation Algorithm (SIIT)</b>                                                                                                                                                                                                                                                            | February 2000  |                                                                                                                                                                | PROPOSED STANDARD                          |
| <b>Abstract</b>         | This document specifies a transition mechanism algorithm in addition to the mechanisms already specified. [STANDARDS TRACK]                                                                                                                                                                                      |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2766</a> | <b>Network Address Translation - Protocol Translation (NAT-PT)</b>                                                                                                                                                                                                                                               | February 2000  | Updated by <a href="#">RFC3152</a>                                                                                                                             | PROPOSED STANDARD                          |
| <b>Abstract</b>         | This document specifies an IPv4-to-IPv6 transition mechanism, in addition to those already specified. [STANDARDS TRACK]                                                                                                                                                                                          |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2767</a> | <b>Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)</b>                                                                                                                                                                                                                                              | February 2000  |                                                                                                                                                                | INFORMATIONAL                              |
| <b>Abstract</b>         | This memo proposes a mechanism of dual stack hosts using the technique called "Bump-in-the-Stack" in the IP security area. This memo provides information for the Internet community.                                                                                                                            |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2874</a> | <b>DNS Extensions to Support IPv6 Address Aggregation and Renumbering</b>                                                                                                                                                                                                                                        | July 2000      | Updates <a href="#">RFC1886</a> ,<br>Updated by <a href="#">RFC3152</a> ,<br><a href="#">RFC3226</a> ,<br><a href="#">RFC3363</a> ,<br><a href="#">RFC3364</a> | EXPERIMENTAL<br>[pub as:PROPOSED STANDARD] |
| <b>Abstract</b>         | This document defines changes to the Domain Name System to support renumberable and aggregatable IPv6 addressing. [STANDARDS TRACK]                                                                                                                                                                              |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2893</a> | <b>Transition Mechanisms for IPv6 Hosts and Routers</b>                                                                                                                                                                                                                                                          | August 2000    | Obsoletes <a href="#">RFC1933</a> ,<br>Obsoleted by <a href="#">RFC4213</a>                                                                                    | PROPOSED STANDARD                          |
| <a href="#">RFC2894</a> | <b>Router Renumbering for IPv6</b>                                                                                                                                                                                                                                                                               | August 2000    |                                                                                                                                                                | PROPOSED STANDARD                          |
| <b>Abstract</b>         | This document defines a mechanism called Router Renumbering ("RR") which allows address prefixes on routers to be configured and reconfigured almost as easily as the combination of Neighbor Discovery and Address Autoconfiguration works for hosts. [STANDARDS TRACK]                                         |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2921</a> | <b>6BONE pTLA and pNLA Formats (pTLA)</b>                                                                                                                                                                                                                                                                        | September 2000 |                                                                                                                                                                | INFORMATIONAL                              |
| <b>Abstract</b>         | This memo defines how the 6bone uses the 3FFE::/16 IPv6 address prefix, allocated in RFC 2471, "IPv6 Testing Address Allocation", to create pseudo Top-Level Aggregation Identifiers (pTLA's) and pseudo Next-Level Aggregation Identifiers (pNLA's). This memo provides information for the Internet community. |                |                                                                                                                                                                |                                            |
| <a href="#">RFC2928</a> | <b>Initial IPv6 Sub-TLA ID Assignments</b>                                                                                                                                                                                                                                                                       | September 2000 |                                                                                                                                                                | INFORMATIONAL                              |



|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |               |                        |                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------------------|-------------------|
| <a href="#">Abstract</a> | This document defines initial assignments of IPv6 Sub-Top-Level Aggregation Identifiers (Sub-TLA ID) to the Address Registries. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                      |               |                        |                   |
| <a href="#">RFC3019</a>  | <b>IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol</b>                                                                                                                                                                                                                                                                                                                                                                                   | January 2001  |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document defines a portion of the Management Information Base (MIB) for use with network management protocols in Internet Protocol Version 6 internets. Specifically, this document is the MIB module that defines managed objects for implementations of the Multicast Listener Discovery Protocol [RFC2710]. [STANDARDS TRACK]                                                                                                                                           |               |                        |                   |
| <a href="#">RFC3041</a>  | <b>Privacy Extensions for Stateless Address Autoconfiguration in IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                       | January 2001  |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document describes an extension to IPv6 stateless address autoconfiguration for interfaces whose interface identifier is derived from an IEEE identifier. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                |               |                        |                   |
| <a href="#">RFC3053</a>  | <b>IPv6 Tunnel Broker</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                       | January 2001  |                        | INFORMATIONAL     |
| <a href="#">Abstract</a> | The motivation for the development of the tunnel broker model is to help early IPv6 adopters to hook up to an existing IPv6 network (e.g., the 6bone) and to get stable, permanent IPv6 addresses and DNS names. The concept of the tunnel broker was first presented at Orlando's IETF in December 1998. Two implementations were demonstrated during the Grenoble IPng & NGtrans interim meeting in February 1999. This memo provides information for the Internet community. |               |                        |                   |
| <a href="#">RFC3056</a>  | <b>Connection of IPv6 Domains via IPv4 Clouds</b>                                                                                                                                                                                                                                                                                                                                                                                                                               | February 2001 | <a href="#">Errata</a> | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This memo specifies an optional interim mechanism for IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup, and for them to communicate with native IPv6 domains via relay routers. [STANDARDS TRACK]                                                                                                                                                                                                                                  |               |                        |                   |
| <a href="#">RFC3089</a>  | <b>A SOCKS-based IPv6/IPv4 Gateway Mechanism</b>                                                                                                                                                                                                                                                                                                                                                                                                                                | April 2001    |                        | INFORMATIONAL     |
| <a href="#">Abstract</a> | This document describes a SOCKS-based IPv6/IPv4 gateway mechanism that enables smooth heterogeneous communications between the IPv6 nodes and IPv4 nodes. This memo provides information for the Internet community.                                                                                                                                                                                                                                                            |               |                        |                   |
| <a href="#">RFC3111</a>  | <b>Service Location Protocol Modifications for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                         | May 2001      |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document defines the Service Location Protocol Version 2's (SLPv2) use over IPv6 networks. Since this protocol relies on UDP and TCP, the changes to support its use over IPv6 are minor. [STANDARDS TRACK]                                                                                                                                                                                                                                                                |               |                        |                   |
| <a href="#">RFC3122</a>  | <b>Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification</b>                                                                                                                                                                                                                                                                                                                                                                                                | June 2001     |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This memo describes extensions to the IPv6 Neighbor Discovery that allow a node to determine and advertise an IPv6 address corresponding to a given link-layer address. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                       |               |                        |                   |
| <a href="#">RFC3142</a>  | <b>An IPv6-to-IPv4 Transport Relay Translator</b>                                                                                                                                                                                                                                                                                                                                                                                                                               | June 2001     |                        | INFORMATIONAL     |
| <a href="#">Abstract</a> | The document describes an IPv6-to-IPv4 transport relay translator (TRT). This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                             |               |                        |                   |
| <a href="#">RFC3146</a>  | <b>Transmission of IPv6 Packets over IEEE 1394 Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                     | October 2001  |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE1394 networks. [STANDARDS TRACK]                                                                                                                                                                                                                                                                  |               |                        |                   |
| <a href="#">RFC3162</a>  | <b>RADIUS and IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                          | August 2001   |                        | PROPOSED STANDARD |
| <a href="#">Abstract</a> | This document specifies the operation of RADIUS (Remote Authentication Dial In User Service) when run over IPv6 as well as the RADIUS attributes used to support IPv6 network access. [STANDARDS TRACK]                                                                                                                                                                                                                                                                         |               |                        |                   |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                |                                                                                                                                                    |                   |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">RFC3175</a> | <b>Aggregation of RSVP for IPv4 and IPv6 Reservations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | September 2001 |                                                                                                                                                    | PROPOSED STANDARD |
| <b>Abstract</b>         | This document describes the use of a single RSVP (Resource ReSerVation Protocol) reservation to aggregate other RSVP reservations across a transit routing region, in a manner conceptually similar to the use of Virtual Paths in an ATM (Asynchronous Transfer Mode) network. It proposes a way to dynamically create the aggregate reservation, classify the traffic for which the aggregate reservation applies, determine how much bandwidth is needed to achieve the requirement, and recover the bandwidth when the sub-reservations are no longer required. It also contains recommendations concerning algorithms and policies for predictive reservations. [STANDARDS TRACK] |                |                                                                                                                                                    |                   |
| <a href="#">RFC3177</a> | <b>IAB/IESG Recommendations on IPv6 Address Allocations to Sites</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | September 2001 |                                                                                                                                                    | INFORMATIONAL     |
| <b>Abstract</b>         | This document provides recommendations to the addressing registries (APNIC, ARIN and RIPE-NCC) on policies for assigning IPv6 address blocks to end sites. In particular, it recommends the assignment of /48 in the general case, /64 when it is known that one and only one subnet is needed and /128 when it is absolutely known that one and only one device is connecting.                                                                                                                                                                                                                                                                                                        |                |                                                                                                                                                    |                   |
| <a href="#">RFC3178</a> | <b>IPv6 Multihoming Support at Site Exit Routers</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | October 2001   |                                                                                                                                                    | INFORMATIONAL     |
| <b>Abstract</b>         | The document describes a mechanism for basic IPv6 multihoming support, and its operational requirements. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                |                                                                                                                                                    |                   |
| <a href="#">RFC3226</a> | <b>DNSSEC and IPv6 A6 aware server/resolver message size requirements</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | December 2001  | Updates <a href="#">RFC2535</a> , <a href="#">RFC2874</a> , Updated by <a href="#">RFC4033</a> , <a href="#">RFC4034</a> , <a href="#">RFC4035</a> | PROPOSED STANDARD |
| <b>Abstract</b>         | This document mandates support for EDNS0 (Extension Mechanisms for DNS) in DNS entities claiming to support either DNS Security Extensions or A6 records. This requirement is necessary because these new features increase the size of DNS messages. If EDNS0 is not supported fall back to TCP will happen, having a detrimental impact on query latency and DNS server load. This document updates RFC 2535 and RFC 2874, by adding new requirements. [STANDARDS TRACK]                                                                                                                                                                                                             |                |                                                                                                                                                    |                   |
| <a href="#">RFC3266</a> | <b>Support for IPv6 in Session Description Protocol (SDP)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | June 2002      | Updates <a href="#">RFC2327</a> <a href="#">Errata</a>                                                                                             | PROPOSED STANDARD |
| <b>Abstract</b>         | This document describes the use of Internet Protocol Version 6 (IPv6) addresses in conjunction with the Session Description Protocol (SDP). Specifically, this document clarifies existing text in SDP with regards to the syntax of IPv6 addresses. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                 |                |                                                                                                                                                    |                   |
| <a href="#">RFC3306</a> | <b>Unicast-Prefix-based IPv6 Multicast Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | August 2002    | Updated by <a href="#">RFC3956</a>                                                                                                                 | PROPOSED STANDARD |
| <a href="#">RFC3307</a> | <b>Allocation Guidelines for IPv6 Multicast Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | August 2002    |                                                                                                                                                    | PROPOSED STANDARD |
| <a href="#">RFC3314</a> | <b>Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | September 2002 |                                                                                                                                                    | INFORMATIONAL     |
| <a href="#">RFC3315</a> | <b>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | July 2003      |                                                                                                                                                    | PROPOSED STANDARD |
| <a href="#">RFC3316</a> | <b>Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | April 2003     |                                                                                                                                                    | INFORMATIONAL     |
| <a href="#">RFC3363</a> | <b>Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | August 2002    | Updates <a href="#">RFC2673</a> , <a href="#">RFC2874</a>                                                                                          | INFORMATIONAL     |



|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |               |                                                           |                   |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------|-------------------|
| <a href="#">RFC3364</a>                                                             | <b>Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | August 2002   | Updates <a href="#">RFC2673</a> , <a href="#">RFC2874</a> | INFORMATIONAL     |
| <a href="#">RFC3484</a>                                                             | <b>Default Address Selection for Internet Protocol version 6 (IPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | February 2003 |                                                           | PROPOSED STANDARD |
|    | This document describes two algorithms, for source address selection and for destination address selection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. They do not override choices made by applications or upper-layer protocols, nor do they preclude the development of more advanced mechanisms for address selection. The two algorithms share a common context, including an optional mechanism for allowing administrators to provide policy that can override the default behavior. In dual stack implementations, the destination address selection algorithm can consider both IPv4 and IPv6 addresses - depending on the available source addresses, the algorithm might prefer IPv6 addresses over IPv4 addresses, or vice-versa. All IPv6 nodes, including both hosts and routers, must implement default address selection as defined in this specification. [STANDARDS TRACK]                                                                                                                                                                                |               |                                                           |                   |
| <a href="#">RFC3493</a>                                                             | <b>Basic Socket Interface Extensions for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | February 2003 | Obsoletes <a href="#">RFC2553</a>                         | INFORMATIONAL     |
|    | The de facto standard Application Program Interface (API) for TCP/IP applications is the "sockets" interface. Although this API was developed for Unix in the early 1980s it has also been implemented on a wide variety of non-Unix systems. TCP/IP applications written using the sockets API have in the past enjoyed a high degree of portability and we would like the same portability with IPv6 applications. But changes are required to the sockets API to support IPv6 and this memo describes these changes. These include a new socket address structure to carry IPv6 addresses, new address conversion functions, and some new socket options. These extensions are designed to provide access to the basic IPv6 features required by TCP and UDP applications, including multicasting, while introducing a minimum of change into the system and providing complete compatibility for existing IPv4 applications. Additional extensions for advanced IPv6 features (raw sockets and access to the IPv6 extension headers) are defined in another document. This memo provides information for the Internet community. |               |                                                           |                   |
| <a href="#">RFC3513</a>                                                             | <b>Internet Protocol Version 6 (IPv6) Addressing Architecture</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | April 2003    | Obsoletes <a href="#">RFC2373</a>                         | PROPOSED STANDARD |
|  | This specification defines the addressing architecture of the IP Version 6 (IPv6) protocol. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 node's required addresses. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |               |                                                           |                   |
| <a href="#">RFC3531</a>                                                             | <b>A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | April 2003    |                                                           | INFORMATIONAL     |
|  | This document proposes a method to manage the assignment of bits of an IPv6 address block or range. When an organisation needs to make an address plan for its subnets or when an ISP needs to make an address plan for its customers, this method enables the organisation to postpone the final decision on the number of bits to partition in the address space they have. It does it by keeping the bits around the borders of the partition to be free as long as possible. This scheme is applicable to any bits addressing scheme using bits with partitions in the space, but its first intended use is for IPv6. It is a generalization of RFC 1219 and can be used for IPv6 assignments. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                        |               |                                                           |                   |
| <a href="#">RFC3542</a>                                                             | <b>Advanced Sockets Application Program Interface (API) for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | May 2003      | Obsoletes <a href="#">RFC2292</a> <a href="#">Errata</a>  | INFORMATIONAL     |
|  | This document provides sockets Application Program Interface (API) to support "advanced" IPv6 applications, as a supplement to a separate specification, RFC 3493. The expected applications include Ping, Traceroute, routing daemons and the like, which typically use raw sockets to access IPv6 or ICMPv6 header fields. This document proposes some portable interfaces for applications that use raw sockets under IPv6. There are other features of IPv6 that some applications will need to access: interface identification (specifying the outgoing interface and determining the incoming interface), IPv6 extension headers, and path Maximum Transmission Unit (MTU) information. This document provides API access to these features too. Additionally, some extended interfaces to libraries for the "r" commands are defined. The extension will provide better backward compatibility to existing implementations that are not IPv6-capable. This memo provides information for the Internet community.                                                                                                             |               |                                                           |                   |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                |                                      |                      |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------------------|----------------------|
| <a href="#">RFC3572</a> | <b>Internet Protocol Version 6 over MAPOS<br/>(Multiple Access Protocol Over<br/>SONET/SDH)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | July 2003      |                                      | INFORMATIONAL        |
| <b>Abstract</b>         | Multiple Access Protocol over SONET/SDH (MAPOS) is a high-speed link- layer protocol that provides multiple access capability over a Synchronous Optical NETwork/Synchronous Digital Hierarchy (SONET/SDH). This document specifies the frame format for encapsulating an IPv6 datagram in a MAPOS frame. It also specifies the method of forming IPv6 interface identifiers, the method of detecting duplicate addresses, and the format of the Source/Target Link-layer Addresses option field used in IPv6 Neighbor Discovery messages. This memo provides information for the Internet community.                                 |                |                                      |                      |
| <a href="#">RFC3574</a> | <b>Transition Scenarios for 3GPP Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | August 2003    |                                      | INFORMATIONAL        |
| <b>Abstract</b>         | This document describes different scenarios in Third Generation Partnership Project (3GPP) defined packet network, i.e., General Packet Radio Service (GPRS) that would need IP version 6 and IP version 4 transition. The focus of this document is on the scenarios where the User Equipment (UE) connects to nodes in other networks, e.g., in the Internet. GPRS network internal transition scenarios, i.e., between different GPRS elements in the network, are out of scope. The purpose of the document is to list the scenarios for further discussion and study. This memo provides information for the Internet community. |                |                                      |                      |
| <a href="#">RFC3582</a> | <b>Goals for IPv6 Site-Multihoming<br/>Architectures</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | August 2003    |                                      | INFORMATIONAL        |
| <b>Abstract</b>         | This document outlines a set of goals for proposed new IPv6 site- multihoming architectures. It is recognised that this set of goals is ambitious and that some goals may conflict with others. The solution or solutions adopted may only be able to satisfy some of the goals presented here. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                            |                |                                      |                      |
| <a href="#">RFC3587</a> | <b>IPv6 Global Unicast Address Format</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | August 2003    | Obsoletes<br><a href="#">RFC2374</a> | INFORMATIONAL        |
| <b>Abstract</b>         | This document obsoletes RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format". It defined an IPv6 address allocation structure that includes Top Level Aggregator (TLA) and Next Level Aggregator (NLA). This document makes RFC 2374 and the TLA/NLA structure historic. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                         |                |                                      |                      |
| <a href="#">RFC3590</a> | <b>Source Address Selection for the Multicast<br/>Listener Discovery (MLD) Protocol</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | September 2003 | Updates<br><a href="#">RFC2710</a>   | PROPOSED<br>STANDARD |
| <b>Abstract</b>         | It has come to light that there is an issue with the selection of a suitable IPv6 source address for Multicast Listener Discovery (MLD) messages when a node is performing stateless address autoconfiguration. This document is intended to clarify the rules on selecting an IPv6 address to use for MLD messages. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                |                |                                      |                      |
| <a href="#">RFC3595</a> | <b>Textual Conventions for IPv6 Flow Label</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | September 2003 |                                      | PROPOSED<br>STANDARD |
| <b>Abstract</b>         | This MIB module defines textual conventions to represent the commonly used IPv6 Flow Label. The intent is that these textual conventions (TCs) will be imported and used in MIB modules that would otherwise define their own representations. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                      |                |                                      |                      |
| <a href="#">RFC3633</a> | <b>IPv6 Prefix Options for Dynamic Host<br/>Configuration Protocol (DHCP) version 6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | December 2003  |                                      | PROPOSED<br>STANDARD |
| <b>Abstract</b>         | The Prefix Delegation options provide a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCP). This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router, across an administrative boundary, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.                                                                                                                                                                                     |                |                                      |                      |
| <a href="#">RFC3646</a> | <b>DNS Configuration options for Dynamic<br/>Host Configuration Protocol for IPv6<br/>(DHCPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | December 2003  |                                      | PROPOSED<br>STANDARD |
| <b>Abstract</b>         | This document describes Dynamic Host Configuration Protocol for IPv6 (DHCPv6) options for passing a list of available DNS recursive name servers and a domain search list to a client.                                                                                                                                                                                                                                                                                                                                                                                                                                                |                |                                      |                      |
| <a href="#">RFC3697</a> | <b>IPv6 Flow Label Specification</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | March 2004     |                                      | PROPOSED<br>STANDARD |
| <b>Abstract</b>         | This document specifies the IPv6 Flow Label field and the minimum requirements for IPv6 source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                |                                      |                      |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |                                   |                   |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------|-------------------|
|                         | nodes labeling flows, IPv6 nodes forwarding labeled packets, and flow state establishment methods. Even when mentioned as examples of possible uses of the flow labeling, more detailed requirements for specific use cases are out of scope for this document. The usage of the Flow Label field enables efficient IPv6 flow classification based only on IPv6 main header fields in fixed positions. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |                                   |                   |
| <a href="#">RFC3701</a> | <b>6bone (IPv6 Testing Address Allocation) Phaseout</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | March 2004 | Obsoletes <a href="#">RFC2471</a> | INFORMATIONAL     |
| <b>Abstract</b>         | The 6bone was established in 1996 by the IETF as an IPv6 Testbed network to enable various IPv6 testing as well as to assist in the transitioning of IPv6 into the Internet. It operates under the IPv6 address allocation 3FFE::/16 from RFC 2471. As IPv6 is beginning its production deployment it is appropriate to plan for the phaseout of the 6bone. This document establishes a plan for a multi-year phaseout of the 6bone and its address allocation on the assumption that the IETF is the appropriate place to determine this. This document obsoletes RFC 2471, "IPv6 Testing Address Allocation", December, 1998. RFC 2471 will become historic. This memo provides information for the Internet community.                                                                                                                                                                                                                   |            |                                   |                   |
| <a href="#">RFC3736</a> | <b>Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | April 2004 |                                   | PROPOSED STANDARD |
| <b>Abstract</b>         | Stateless Dynamic Host Configuration Protocol service for IPv6 (DHCPv6) is used by nodes to obtain configuration information, such as the addresses of DNS recursive name servers, that does not require the maintenance of any dynamic state for individual clients. A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address autoconfiguration. This document explains which parts of RFC 3315 must be implemented in each of the different kinds of DHCP agents so that agent can support stateless DHCP. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                       |            |                                   |                   |
| <a href="#">RFC3750</a> | <b>Unmanaged Networks IPv6 Transition Scenarios</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | April 2004 |                                   | INFORMATIONAL     |
| <b>Abstract</b>         | This document defines the scenarios in which IPv6 transition mechanisms are to be used in unmanaged networks. In order to evaluate the suitability of these mechanisms, we need to define the scenarios in which these mechanisms have to be used. One specific scope is the "unmanaged network", which typically corresponds to a home or small office network. The scenarios are specific to a single subnet, and are defined in terms of IP connectivity supported by the gateway and the Internet Service Provider (ISP). We first examine the generic requirements of four classes of applications: local, client, peer to peer and server. Then, for each scenario, we infer transition requirements by analyzing the needs for smooth migration of applications from IPv4 to IPv6. This memo provides information for the Internet community.                                                                                        |            |                                   |                   |
| <a href="#">RFC3756</a> | <b>IPv6 Neighbor Discovery (ND) Trust Models and Threats</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | May 2004   |                                   | INFORMATIONAL     |
| <a href="#">RFC3769</a> | <b>Requirements for IPv6 Prefix Delegation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | June 2004  |                                   | INFORMATIONAL     |
| <b>Abstract</b>         | This document describes requirements for how IPv6 address prefixes should be delegated to an IPv6 subscriber's network (or "site"). This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |                                   |                   |
| <a href="#">RFC3775</a> | <b>Mobility Support in IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | June 2004  |                                   | PROPOSED STANDARD |
| <b>Abstract</b>         | This document specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, Mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes. [STANDARDS TRACK] |            |                                   |                   |
| <a href="#">RFC3776</a> | <b>Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | June 2004  |                                   | PROPOSED STANDARD |
| <b>Abstract</b>         | Mobile IPv6 uses IPsec to protect signaling between the home agent and the mobile node. Mobile IPv6 base document defines the main requirements these nodes must follow. This document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |                                   |                   |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                |                                 |                       |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|---------------------------------|-----------------------|
| <a href="#">RFC3810</a>                            | <b>Multicast Listener Discovery Version 2 (MLDv2) for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | June 2004      | Updates <a href="#">RFC2710</a> | PROPOSED STANDARD     |
| <b>Abstract</b>                                    | This document updates RFC 2710, and it specifies Version 2 of the Multicast Listener Discovery Protocol (MLDv2). MLD is used by an IPv6 router to discover the presence of multicast listeners on directly attached links, and to discover which multicast addresses are of interest to those neighboring nodes. MLDv2 is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses. [STANDARDS TRACK]                                                                                                                                                                 |                |                                 |                       |
| <a href="#">RFC3831</a>                            | <b>Transmission of IPv6 Packets over Fibre Channel</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | July 2004      |                                 | PROPOSED STANDARD     |
| <b>Abstract</b>                                    | This document specifies the way of encapsulating IPv6 packets over Fibre Channel, and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on Fibre Channel networks. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                |                                 |                       |
| <a href="#">RFC3849</a>                            | <b>IPv6 Address Prefix Reserved for Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | July 2004      |                                 | INFORMATIONAL         |
| <b>Abstract</b>                                    | To reduce the likelihood of conflict and confusion when relating documented examples to deployed systems, an IPv6 unicast address prefix is reserved for use in examples in RFCs, books, documentation, and the like. Since site-local and link-local unicast addresses have special meaning in IPv6, these addresses cannot be used in many example situations. The document describes the use of the IPv6 address prefix 2001:DB8::/32 as a reserved prefix for use in documentation. This memo provides information for the Internet community.                                                                                                                                                                                                                  |                |                                 |                       |
| <a href="#">RFC3879</a>                            | <b>Deprecating Site Local Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | September 2004 |                                 | PROPOSED STANDARD     |
| <b>Abstract</b>                                    | This document describes the issues surrounding the use of IPv6 site-local unicast addresses in their original form, and formally deprecates them. This deprecation does not prevent their continued use until a replacement has been standardized and implemented. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                |                                 |                       |
| <a href="#">RFC3898</a>                            | <b>Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | October 2004   |                                 | PROPOSED STANDARD     |
| <b>Abstract</b>                                    | This document describes four options for Network Information Service (NIS) related configuration information in Dynamic Host Configuration Protocol for IPv6 (DHCPv6): NIS Servers, NIS+ Servers, NIS Client Domain Name, NIS+ Client Domain name. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                |                                 |                       |
| <a href="#">RFC3901</a><br><a href="#">BCP0091</a> | <b>DNS IPv6 Transport Operational Guidelines</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | September 2004 |                                 | BEST CURRENT PRACTICE |
| <b>Abstract</b>                                    | This memo provides guidelines and Best Current Practice for operating DNS in a world where queries and responses are carried in a mixed environment of IPv4 and IPv6 networks. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.                                                                                                                                                                                                                                                                                                                                                                                                                                     |                |                                 |                       |
| <a href="#">RFC3904</a>                            | <b>Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | September 2004 |                                 | INFORMATIONAL         |
| <b>Abstract</b>                                    | This document analyzes issues involved in the transition of "unmanaged networks" from IPv4 to IPv6. Unmanaged networks typically correspond to home networks or small office networks. A companion paper analyzes out the requirements for mechanisms needed in various transition scenarios of these networks to IPv6. Starting from this analysis, we evaluate the suitability of mechanisms that have already been specified, proposed, or deployed. This memo provides information for the Internet community.                                                                                                                                                                                                                                                  |                |                                 |                       |
| <a href="#">RFC3919</a>                            | <b>Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | October 2004   |                                 | INFORMATIONAL         |
| <b>Abstract</b>                                    | This memo defines additional (to those in RFC 2896) protocol identifier examples for IP version 6 and MPLS protocols. These can be used to produce valid protocolIdentifierTable INDEX encodings, as defined by the Remote Network Monitoring MIB (Management Information Base) Version 2 [RFC2021] and the RMON Protocol Identifier Reference [RFC2895].<br>This document contains additional (to those in RFC 2896) protocol identifier macros for well-known protocols. A conformant implementation of the RMON-2 MIB [RFC2021] can be accomplished without the use of these protocol identifiers, and accordingly, this document does not specify any IETF standard. It is published to encourage better interoperability between RMON-2 agent implementations, |                |                                 |                       |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |                                 |                   |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------------|-------------------|
|                         | by providing RMON related IPv6 and MPLS protocol information. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |               |                                 |                   |
| <a href="#">RFC3956</a> | <b>Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | November 2004 | Updates <a href="#">RFC3306</a> | PROPOSED STANDARD |
| <b>Abstract</b>         | This memo defines an address allocation policy in which the address of the Rendezvous Point (RP) is encoded in an IPv6 multicast group address. For Protocol Independent Multicast - Sparse Mode (PIM-SM), this can be seen as a specification of a group-to-RP mapping mechanism. This allows an easy deployment of scalable inter-domain multicast and simplifies the intra-domain multicast configuration as well. This memo updates the addressing format presented in RFC 3306. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                 |               |                                 |                   |
| <a href="#">RFC3963</a> | <b>Network Mobility (NEMO) Basic Support Protocol</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | January 2005  |                                 | PROPOSED STANDARD |
| <b>Abstract</b>         | This document describes the Network Mobility (NEMO) Basic Support protocol that enables Mobile Networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves. It also allows every node in the Mobile Network to be reachable while moving around. The Mobile Router, which connects the network to the Internet, runs the NEMO Basic Support protocol with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network. [STANDARDS TRACK]                                                                                                                                                                   |               |                                 |                   |
| <a href="#">RFC3974</a> | <b>SMTP Operational Experience in Mixed IPv4/v6 Environments</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | January 2005  |                                 | INFORMATIONAL     |
| <b>Abstract</b>         | This document discusses SMTP operational experiences in IPv4/v6 dual stack environments. As IPv6-capable SMTP servers are deployed, it has become apparent that certain configurations of MX records are necessary for stable dual-stack (IPv4 and IPv6) SMTP operation. This document clarifies the existing problems in the transition period between IPv4 SMTP and IPv6 SMTP. It also defines operational requirements for stable IPv4/v6 SMTP operation. This document does not define any new protocol. This memo provides information for the Internet community.                                                                                                                                                                                                                                |               |                                 |                   |
| <a href="#">RFC4007</a> | <b>IPv6 Scoped Address Architecture</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | March 2005    |                                 | PROPOSED STANDARD |
| <b>Abstract</b>         | This document specifies the architectural characteristics, expected behavior, textual representation, and usage of IPv6 addresses of different scopes. According to a decision in the IPv6 working group, this document intentionally avoids the syntax and usage of unicast site-local addresses. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |               |                                 |                   |
| <a href="#">RFC4029</a> | <b>Scenarios and Analysis for Introducing IPv6 into ISP Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | March 2005    | <a href="#">Errata</a>          | INFORMATIONAL     |
| <b>Abstract</b>         | This document describes different scenarios for the introduction of IPv6 into an ISP's existing IPv4 network without disrupting the IPv4 service. The scenarios for introducing IPv6 are analyzed, and the relevance of already defined transition mechanisms are evaluated. Known challenges are also identified. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                          |               |                                 |                   |
| <a href="#">RFC4038</a> | <b>Application Aspects of IPv6 Transition</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | March 2005    |                                 | INFORMATIONAL     |
| <b>Abstract</b>         | As IPv6 networks are deployed and the network transition is discussed, one should also consider how to enable IPv6 support in applications running on IPv6 hosts, and the best strategy to develop IP protocol support in applications. This document specifies scenarios and aspects of application transition. It also proposes guidelines on how to develop IP version-independent applications during the transition period. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                            |               |                                 |                   |
| <a href="#">RFC4057</a> | <b>IPv6 Enterprise Network Scenarios</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | June 2005     | <a href="#">Errata</a>          | INFORMATIONAL     |
| <b>Abstract</b>         | This document describes the scenarios for IPv6 deployment within enterprise networks. It defines a small set of basic enterprise scenarios and includes pertinent questions to allow enterprise administrators to further refine their deployment scenarios. Enterprise deployment requirements are discussed in terms of coexistence with IPv4 nodes, networks and applications, and in terms of basic network infrastructure requirements for IPv6 deployment. The scenarios and requirements described in this document will be the basis for further analysis to determine what coexistence techniques and mechanisms are needed for enterprise IPv6 deployment. The results of that analysis will be published in a separate document. This memo provides information for the Internet community. |               |                                 |                   |
| <a href="#">RFC4068</a> | <b>Fast Handovers for Mobile IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | July 2005     |                                 | EXPERIMENTAL      |
| <b>Abstract</b>         | Mobile IPv6 enables a Mobile Node to maintain its connectivity to the Internet when moving from one                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |               |                                 |                   |



|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |             |                        |                       |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------|-----------------------|
|                                                    | Access Router to another, a process referred to as handover. During handover, there is a period during which the Mobile Node is unable to send or receive packets because of link switching delay and IP protocol operations. This "handover latency" resulting from standard Mobile IPv6 procedures, namely movement detection, new Care of Address configuration, and Binding Update, is often unacceptable to real-time traffic such as Voice over IP. Reducing the handover latency could be beneficial to non-real-time, throughput-sensitive applications as well. This document specifies a protocol to improve handover latency due to Mobile IPv6 procedures. This document does not address improving the link switching latency. This memo defines an Experimental Protocol for the Internet community.                                                                                                                           |             |                        |                       |
| <a href="#">RFC4074</a>                            | <b>Common Misbehavior Against DNS Queries for IPv6 Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | May 2005    |                        | INFORMATIONAL         |
| <b>Abstract</b>                                    | There is some known misbehavior of DNS authoritative servers when they are queried for AAAA resource records. Such behavior can block IPv4 communication that should actually be available, cause a significant delay in name resolution, or even make a denial of service attack. This memo describes details of known cases and discusses their effects. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |                        |                       |
| <a href="#">RFC4076</a>                            | <b>Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | May 2005    |                        | INFORMATIONAL         |
| <b>Abstract</b>                                    | IPv6 hosts using Stateless Address Autoconfiguration are able to configure their IPv6 address and default router settings automatically. However, further settings are not available. If these hosts wish to configure their DNS, NTP, or other specific settings automatically, the stateless variant of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) could be used. This combination of Stateless Address Autoconfiguration and stateless DHCPv6 could be used quite commonly in IPv6 networks. However, hosts using this combination currently have no means by which to be informed of changes in stateless DHCPv6 option settings; e.g., the addition of a new NTP server address, a change in DNS search paths, or full site renumbering. This document is presented as a problem statement from which a solution should be proposed in a subsequent document. This memo provides information for the Internet community. |             |                        |                       |
| <a href="#">RFC4135</a>                            | <b>Goals of Detecting Network Attachment in IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | August 2005 |                        | INFORMATIONAL         |
| <b>Abstract</b>                                    | When a host establishes a new link-layer connection, it may or may not have a valid IP configuration for Internet connectivity. The host may check for link change (i.e., determine whether a link change has occurred), and then, based on the result, it can automatically decide whether its IP configuration is still valid. During link identity detection, the host may also collect necessary information to initiate a new IP configuration if the IP subnet has changed. In this memo, this procedure is called Detecting Network Attachment (DNA). DNA schemes should be precise, sufficiently fast, secure, and of limited signaling. This memo provides information for the Internet community.                                                                                                                                                                                                                                  |             |                        |                       |
| <a href="#">RFC4140</a>                            | <b>Hierarchical Mobile IPv6 Mobility Management (HMIPv6)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | August 2005 |                        | EXPERIMENTAL          |
| <b>Abstract</b>                                    | This document introduces extensions to Mobile IPv6 and IPv6 Neighbour Discovery to allow for local mobility handling. Hierarchical mobility management for Mobile IPv6 is designed to reduce the amount of signalling between the Mobile Node, its Correspondent Nodes, and its Home Agent. The Mobility Anchor Point (MAP) described in this document can also be used to improve the performance of Mobile IPv6 in terms of handover speed. This memo defines an Experimental Protocol for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                         |             |                        |                       |
| <a href="#">RFC4147</a>                            | <b>Proposed Changes to the Format of the IANA IPv6 Registry</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | August 2005 | <a href="#">Errata</a> | INFORMATIONAL         |
| <b>Abstract</b>                                    | This document proposes a revised format for the IANA IPv6 address registries. Rather than providing a formal definition of the format, it is described by giving examples of the (current as of preparation of this document) contents of the registries in the proposed format. The proposed format would bring the IANA IPv6 address registries into alignment with the current IPv6 Address Architecture specification, as well as update it to a more useful and generally accepted format. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                   |             |                        |                       |
| <a href="#">RFC4159</a><br><a href="#">BCP0109</a> | <b>Deprecation of ip6.int</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | August 2005 |                        | BEST CURRENT PRACTICE |
| <b>Abstract</b>                                    | This document advises of the deprecation of the use of "ip6.int" for Standards Conformant IPv6 implementations. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |             |                        |                       |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                |                                   |                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------------------------------|-------------------|
| <a href="#">RFC4177</a> | <b>Architectural Approaches to Multi-homing for IPv6</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | September 2005 |                                   | INFORMATIONAL     |
| <b>Abstract</b>         | This memo provides an analysis of the architectural aspects of multi-homing support for the IPv6 protocol suite. The purpose of this analysis is to provide a taxonomy for classification of various proposed approaches to multi-homing. It is also an objective of this exercise to identify common aspects of this domain of study, and also to provide a framework that can allow exploration of some of the further implications of various architectural extensions that are intended to support multi-homing. This memo provides information for the Internet community.                                                                                                                                                                                   |                |                                   |                   |
| <a href="#">RFC4192</a> | <b>Procedures for Renumbering an IPv6 Network without a Flag Day</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | September 2005 | Updates <a href="#">RFC2072</a>   | INFORMATIONAL     |
| <b>Abstract</b>         | This document describes a procedure that can be used to renumber a network from one prefix to another. It uses IPv6's intrinsic ability to assign multiple addresses to a network interface to provide continuity of network service through a "make-before-break" transition, as well as addresses naming and configuration management issues. It also uses other IPv6 features to minimize the effort and time required to complete the transition from the old prefix to the new prefix. This memo provides information for the Internet community.                                                                                                                                                                                                            |                |                                   |                   |
| <a href="#">RFC4193</a> | <b>Unique Local IPv6 Unicast Addresses</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | October 2005   |                                   | PROPOSED STANDARD |
| <b>Abstract</b>         | This document defines an IPv6 unicast address format that is globally unique and is intended for local communications, usually inside of a site. These addresses are not expected to be routable on the global Internet. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                |                                   |                   |
| <a href="#">RFC4213</a> | <b>Basic Transition Mechanisms for IPv6 Hosts and Routers</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | October 2005   | Obsoletes <a href="#">RFC2893</a> | PROPOSED STANDARD |
| <b>Abstract</b>         | This document specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. Two mechanisms are specified, dual stack and configured tunneling. Dual stack implies providing complete implementations of both versions of the Internet Protocol (IPv4 and IPv6), and configured tunneling provides a means to carry IPv6 packets over unmodified IPv4 routing infrastructures. This document obsoletes RFC 2893. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                    |                |                                   |                   |
| <a href="#">RFC4215</a> | <b>Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | October 2005   |                                   | INFORMATIONAL     |
| <b>Abstract</b>         | This document analyzes the transition to IPv6 in Third Generation Partnership Project (3GPP) packet networks. These networks are based on General Packet Radio Service (GPRS) technology, and the radio network architecture is based on Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS)/Wideband Code Division Multiple Access (WCDMA) technology. The focus is on analyzing different transition scenarios and applicable transition mechanisms and finding solutions for those transition scenarios. In these scenarios, the User Equipment (UE) connects to other nodes, e.g., in the Internet, and IPv6/IPv4 transition mechanisms are needed. This memo provides information for the Internet community. |                |                                   |                   |

### 10.2.2 Vídeo

|             |                                                                            |                                                |                                                            |                                             |
|-------------|----------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------|---------------------------------------------|
| Figura 10.1 | Figura 10.2 - <b>Título</b>                                                | Figura 10.3 - <b>a</b><br><b>t</b><br><b>a</b> | Figura 10.4 - <b>I</b><br><b>n</b><br><b>f</b><br><b>.</b> | Figura 10.5 - <b>Estado</b>                 |
| Figura 10.6 | Figura 10.7 - <b>A Comment on Packet Video Remote Conferencing and the</b> | Figura 10.8 - <b>p</b>                         | Figura 10.9 -                                              | Figura 10.10 - <b>INFO</b><br><b>RMATIO</b> |

|              |                                                                                                                                                                                                                                                                                                                                              |                                               |                                                                         |                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------------|----------------------------------|
|              | Transport/Network Layers                                                                                                                                                                                                                                                                                                                     | 1993                                          |                                                                         | NAL                              |
| Figura 10.11 | Figura 10.12 - This RFC is a vehicle to inform the Internet community about XTP as it benefits from past Internet activity and targets general-purpose applications and multimedia applications with the emerging ATM networks in mind. This memo provides information for the Internet community. It does not specify an Internet standard. |                                               |                                                                         |                                  |
| Figura 10.13 | Figura 10.14 - <b>RTP: A Transport Protocol for Real-Time Applications</b>                                                                                                                                                                                                                                                                   | Figura 10.15<br>annu-<br>ar-y<br>1996         | Figura 10.16 -<br>bsol-<br>et-<br>ed-<br>by<br><a href="#">RFC 3550</a> | Figura 10.17 - PROPOSED STANDARD |
| Figura 10.18 | Figura 10.19 - <b>RTP Profile for Audio and Video Conferences with Minimal Control</b>                                                                                                                                                                                                                                                       | Figura 10.20<br>annu-<br>ar-y<br>1996         | Figura 10.21 -<br>bsol-<br>et-<br>ed-<br>by<br><a href="#">RFC 51</a>   | Figura 10.22 - PROPOSED STANDARD |
| Figura 10.23 | Figura 10.24 - <b>RTP Payload Format of Sun's CellB Video Encoding</b>                                                                                                                                                                                                                                                                       | Figura 10.25<br>cto-<br>b-<br>e-<br>r<br>1996 | Figura 10.26 -                                                          | Figura 10.27 - PROPOSED STANDARD |
| Figura 10.28 | Figura 10.29 - This memo describes a packetization scheme for the CellB video encoding. The scheme proposed allows applications to transport CellB video flows over protocols used by RTP. This document is meant for implementors of video applications that want to use RTP and CellB. [STANDARDS-TRACK]                                   |                                               |                                                                         |                                  |
| Figura 10.30 | Figura 10.31 - <b>RTP Payload Format for H.261 Video Streams</b>                                                                                                                                                                                                                                                                             | Figura 10.32<br>cto-<br>b-<br>e-<br>r<br>19   | Figura 10.33 -                                                          | Figura 10.34 - PROPOSED STANDARD |



|              |                                                                                                                                                                                                                                                                                                                                                                                         |                                     |                                     |                                  |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|----------------------------------|
|              |                                                                                                                                                                                                                                                                                                                                                                                         | 96                                  |                                     |                                  |
| Figura 10.35 | Figura 10.36 - This memo describes a scheme to packetize an H.261 video stream for transport using the Real-time Transport Protocol, RTP, with any of the underlying protocols that carry RTP. [STANDARDS-TRACK]                                                                                                                                                                        |                                     |                                     |                                  |
| Figura 10.37 | Figura 10.38 - <b>RTP Payload Format for JPEG-compressed Video</b>                                                                                                                                                                                                                                                                                                                      | Figura 10.39 - Proposed by RFC 2435 | Figura 10.40 - Proposed by RFC 2435 | Figura 10.41 - PROPOSED STANDARD |
| Figura 10.42 | Figura 10.43 - <b>RTP Payload Format for MPEG1/MPEG2 Video</b>                                                                                                                                                                                                                                                                                                                          | Figura 10.44 - Proposed by RFC 2250 | Figura 10.45 - Proposed by RFC 2250 | Figura 10.46 - PROPOSED STANDARD |
| Figura 10.47 | Figura 10.48 - <b>VEMMI URL Specification</b>                                                                                                                                                                                                                                                                                                                                           | Figura 10.49 - Archived             | Figura 10.50 -                      | Figura 10.51 - PROPOSED STANDARD |
| Figura 10.52 | Figura 10.53 - A new URL scheme, "vemmi" is defined. VEMMI is a new international standard for on-line multimedia services, that is both an ITU-T (International Telecommunications Union, ex. CCITT) International Standard (T.107) and an European Standard (ETSI European Telecommunications Standard Institute) standard (ETS 300 382, obsoleted by ETS 300 709). [STANDARDS-TRACK] |                                     |                                     |                                  |
| Figura 10.54 | Figura 10.55 - <b>RTP Payload Format for H.263 Video Streams</b>                                                                                                                                                                                                                                                                                                                        | Figura 10.56 - Proposed by RFC 1997 | Figura 10.57 -                      | Figura 10.58 - PROPOSED STANDARD |
| Figura 10.59 | Figura 10.60 - This document specifies the payload format for encapsulating an H.263 bitstream in the Real-Time Transport Protocol (RTP). [STANDARDS TRACK]                                                                                                                                                                                                                             |                                     |                                     |                                  |
| Figura 10.61 | Figura 10.62 - <b>RTP Payload Format for</b>                                                                                                                                                                                                                                                                                                                                            | Figura 10.63                        | Figura 10.64 -                      | Figura 10.65 - PROP              |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                         |                |                                     |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|----------------|-------------------------------------|
|              | MPEG1/MPEG2 Video                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | annuaries               | bsolutes       | OSD<br>STAND<br>ARD                 |
| Figura 10.66 | <p>Figura 10.67 - This memo describes a packetization scheme for MPEG video and audio streams. [STANDARDS-TRACK] The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.</p> |                         |                |                                     |
| Figura 10.68 | Figura 10.69 - <b>Real Time Streaming Protocol (RTSP)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Figura 10.70<br>payload | Figura 10.71 - | Figura 10.72 - PROPOSED<br>STANDARD |
| Figura 10.73 | <p>Figura 10.74 - The Real Time Streaming Protocol, or RTSP, is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. [STANDARDS-TRACK]</p>                                                                                                                                                                                                                                                                                                                                                          |                         |                |                                     |
| Figura 10.75 | Figura 10.76 - <b>RTP Payload Format for Bundled MPEG</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Figura 10.77<br>payload | Figura 10.78 - | Figura 10.79 - EXPERIMENTAL         |
| Figura 10.80 | <p>Figura 10.81 - This document describes a payload type for bundled, MPEG-2 encoded video and audio data that may be used with RTP, version 2. This memo defines an Experimental Protocol for the Internet community. This memo does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested.</p>                                                                                                                                                                                                                                                                                                                        |                         |                |                                     |
| Figura 10.82 | Figura 10.83 - <b>WAVE and AVI Codec Registries</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Figura 10.84<br>update  | Figura 10.85 - | Figura 10.86 - INFORMATIONAL        |
| Figura 10.87 | <p>Figura 10.88 - The purpose of this paper is to establish a mechanism by which codecs registered within Microsoft's WAVE and AVI Registries may be referenced within the IANA Namespace by Internet applications. This memo provides information for the Internet community. It does not specify an Internet standard of any kind.</p>                                                                                                                                                                                                                                                                                                                                 |                         |                |                                     |
| Figura 10.89 | Figura 10.90 - <b>RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Figura 10.91<br>content | Figura 10.92 - | Figura 10.93 - PROPOSED<br>STANDARD |

|               |                                                                                                                                                                                                                                                                       |                                                                          |                                                     |                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------|
|               |                                                                                                                                                                                                                                                                       | o<br>b<br>e<br>r<br><br>1<br>9<br>9<br>8                                 |                                                     | ARD                                   |
| Figura 10.94  | Figura 10.95 - This document specifies an RTP payload header format applicable to the transmission of video streams generated based on the 1998 version of ITU-T Recommendation H.263. [STANDARDS-TRACK]                                                              |                                                                          |                                                     |                                       |
| Figura 10.96  | Figura 10.97 - <b>RTP Payload Format for BT.656 Video Encoding</b>                                                                                                                                                                                                    | Figura 10.98<br>c<br>t<br>o<br>b<br>e<br>r<br><br>1<br>9<br>9<br>8       | Figura 10.99 -                                      | Figura 10.100 - PROPOSED STANDARD     |
| Figura 10.101 | Figura 10.102 - This document specifies the RTP payload format for encapsulating ITU Recommendation BT.656-3 video streams in the Real-Time Transport Protocol (RTP). [STANDARDS-TRACK]                                                                               |                                                                          |                                                     |                                       |
| Figura 10.103 | Figura 10.104 - <b>RTP Payload Format for JPEG-compressed Video</b>                                                                                                                                                                                                   | Figura 10.105<br>c<br>t<br>o<br>b<br>e<br>r<br><br>1<br>9<br>9<br>8      | Figura 10.106 - bsol et es <a href="#">RFC 2035</a> | Figura 10.107 - PROPOSED STANDARD     |
| Figura 10.108 | Figura 10.109 - This memo describes the RTP payload format for JPEG video streams. [STANDARDS-TRACK]                                                                                                                                                                  |                                                                          |                                                     |                                       |
| Figura 10.110 | Figura 10.111 - <b>AT&amp;T's Error Resilient Video Transmission Technique</b>                                                                                                                                                                                        | Figura 10.112<br>o<br>v<br>e<br>n<br>b<br>e<br>r<br><br>1<br>9<br>9<br>8 | Figura 10.113 -                                     | Figura 10.114 - INFORMATIONAL         |
| Figura 10.115 | Figura 10.116 - This document describes a set of techniques for packet loss resilient transmission of compressed video bitstreams based on reliable delivery of their vital information-carrying segments. This memo provides information for the Internet community. |                                                                          |                                                     |                                       |
| Figura 10.117 | Figura 10.118 - <b>Guidelines for Writers of RTP Payload Format Specifications</b>                                                                                                                                                                                    | Figura 10.119<br>e<br>c<br>e<br>m                                        | Figura 10.120 -                                     | Figura 10.121 - BEST CURRENT PRACTICE |

|              |                                                                                                                                                                                                                                                                                                             |                                                                     |                                                                                              |                                              |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------|
|              |                                                                                                                                                                                                                                                                                                             | b<br>e<br>r<br><br>1<br>9<br>9<br>9                                 |                                                                                              | CE                                           |
| Figura 10.12 | Figura 10.123 - This document provides general guidelines aimed at assisting the authors of RTP Payload Format specifications in deciding on good formats. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. |                                                                     |                                                                                              |                                              |
| Figura 10.12 | Figura 10.125 - <b>RTP Payload for Text Conversation</b>                                                                                                                                                                                                                                                    | Figura 10.126<br>a<br>y<br><br>2<br>0<br>0<br>0                     | Figura 10.127 -<br>bs<br>ol<br>et<br>ed<br>by<br><a href="#">R<br/>F<br/>C<br/>41<br/>03</a> | Figura 10.128 - PRO<br>POSED<br>STAND<br>ARD |
| Figura 10.12 | Figura 10.130 - <b>RTP Payload Format for Real-Time Pointers</b>                                                                                                                                                                                                                                            | Figura 10.131<br>u<br>n<br>e<br><br>2<br>0<br>0<br>0                | Figura 10.132 -                                                                              | Figura 10.133 - PRO<br>POSED<br>STAND<br>ARD |
| Figura 10.13 | Figura 10.135 - This document describes an RTP payload format for transporting the coordinates of a dynamic pointer that may be used during a presentation. [STANDARDS TRACK]                                                                                                                               |                                                                     |                                                                                              |                                              |
| Figura 10.13 | Figura 10.137 - <b>RTP Payload Format for DV (IEC 61834) Video</b>                                                                                                                                                                                                                                          | Figura 10.138<br>a<br>n<br>u<br>a<br>r<br>y<br><br>2<br>0<br>0<br>2 | Figura 10.139 -                                                                              | Figura 10.140 - PRO<br>POSED<br>STAND<br>ARD |
| Figura 10.14 | Figura 10.142 - This document specifies the packetization scheme for encapsulating the compressed digital video data streams commonly known as "DV" into a payload format for the Real-Time Transport Protocol (RTP). [STANDARDS TRACK]                                                                     |                                                                     |                                                                                              |                                              |
| Figura 10.14 | Figura 10.144 - <b>One-way Loss Pattern Sample Metrics</b>                                                                                                                                                                                                                                                  | Figura 10.145<br>u<br>g<br>u<br>s<br>t<br><br>2                     | Figura 10.146 -                                                                              | Figura 10.147 - INF<br>ORMATI<br>ONAL        |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                         |                                                                     |                                   |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------|
|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0<br>0<br>2                                             |                                                                     |                                   |
| Figura 10.14 | Figura 10.149 - <b>RTP Payload Format for Society of Motion Picture and Television Engineers (SMPTE) 292M Video</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Figura 10.150 -<br>a<br>r<br>c<br>h<br>2<br>0<br>0<br>3 | Figura 10.151 -                                                     | Figura 10.152 - PROPOSED STANDARD |
| Figura 10.15 | Figura 10.154 - This memo specifies an RTP payload format for encapsulating uncompressed High Definition Television (HDTV) as defined by the Society of Motion Picture and Television Engineers (SMPTE) standard, SMPTE 292M. SMPTE is the main standardizing body in the motion imaging industry and the SMPTE 292M standard defines a bit-serial digital interface for local area HDTV transport. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                         |                                                                     |                                   |
| Figura 10.15 | Figura 10.156 - <b>The Ogg Encapsulation Format Version 0</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Figura 10.157 -<br>a<br>y<br>2<br>0<br>0<br>3           | Figura 10.158 -                                                     | Figura 10.159 - INFORMATIONAL     |
| Figura 10.16 | Figura 10.161 - This document describes the Ogg bitstream format version 0, which is a general, freely-available encapsulation format for media streams. It is able to encapsulate any kind and number of video and audio encoding formats as well as other data streams in a single bitstream. This memo provides information for the Internet community. This memo provides information for the Internet community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                         |                                                                     |                                   |
| Figura 10.16 | Figura 10.163 - <b>RTP: A Transport Protocol for Real-Time Applications</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Figura 10.164 -<br>u<br>l<br>y<br>2<br>0<br>0<br>3      | Figura 10.165 -<br>bs<br>ol<br>et<br>es<br><a href="#">RFC 1889</a> | Figura 10.166 - STANDARD          |
| Figura 10.16 | Figura 10.168 - This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of- service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers. Most of the text in this memorandum is identical to RFC 1889 which it obsoletes. There are no changes in the packet formats on the wire, only changes to the rules and algorithms governing how the protocol is used. The biggest change is an enhancement to the scalable timer algorithm for calculating when to send RTCP packets in order to minimize transmission in excess of the intended rate when many participants join a session simultaneously. [STANDARDS TRACK] |                                                         |                                                                     |                                   |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                          |                                                                                        |                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------|
| Figura 10.16 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Figura 10.171                                                            | Figura 10.172 -<br>bs<br>ol<br>et<br>es<br><a href="#">R<br/>F<br/>C<br/>18<br/>90</a> | Figura 10.173 - STA<br>NDARD                 |
|              | Figura 10.170 - <b>RTP Profile for Audio and Video Conferences with Minimal Control</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2<br>0<br>0<br>3                                                         |                                                                                        |                                              |
| Figura 10.17 | Figura 10.175 - This document describes a profile called "RTP/AVP" for the use of the real-time transport protocol (RTP), version 2, and the associated control protocol, RTCP, within audio and video multiparticipant conferences with minimal control. It provides interpretations of generic fields within the RTP specification suitable for audio and video conferences. In particular, this document defines a set of default mappings from payload type numbers to encodings. This document also describes how audio and video data may be carried within RTP. It defines a set of standard encodings and their names when used within RTP. The descriptions provide pointers to reference implementations and the detailed standards. This document is meant as an aid for implementors of audio, video and other real-time multimedia applications. This memorandum obsoletes RFC 1890. It is mostly backwards-compatible except for functions removed because two interoperable implementations were not found. The additions to RFC 1890 codify existing practice in the use of payload formats under this profile and include new payload formats defined since RFC 1890 was published. [STANDARDS TRACK] |                                                                          |                                                                                        |                                              |
| Figura 10.17 | Figura 10.177 - <b>RTP Payload Format for Transport of MPEG-4 Elementary Streams</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Figura 10.178<br>o<br>v<br>e<br>n<br>b<br>e<br>r<br><br>2<br>0<br>0<br>3 | Figura 10.179 -                                                                        | Figura 10.180 - PRO<br>POSED<br>STAND<br>ARD |
| Figura 10.18 | Figura 10.182 - The Motion Picture Experts Group (MPEG) Committee (ISO/IEC JTC1/SC29 WG11) is a working group in ISO that produced the MPEG-4 standard. MPEG defines tools to compress content such as audio-visual information into elementary streams. This specification defines a simple, but generic RTP payload format for transport of any non-multiplexed MPEG-4 elementary stream.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                          |                                                                                        |                                              |
| Figura 10.18 | Figura 10.184 - <b>Video-Message Message-Context</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Figura 10.185<br>c<br>t<br>o<br>b<br>e<br>r<br><br>2<br>0<br>0<br>4      | Figura 10.186 -<br>pd<br>at<br>es<br><a href="#">R<br/>F<br/>C<br/>34<br/>58</a>       | Figura 10.187 - PRO<br>POSED<br>STAND<br>ARD |
| Figura 10.18 | Figura 10.189 - The Message-Context header defined in RFC 3458 describes the context of a message (for example: fax-message or voice-message). This specification extends the Message-Context header with one additional context value: "video-message".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                          |                                                                                        |                                              |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                             |                                                                     |                                   |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------|
|              | A receiving user agent (UA) may use this information as a hint to optimally present the message. [STANDARDS TRACK]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                             |                                                                     |                                   |
| Figura 10.19 | Figura 10.191 - <b>RTP Payload Format for H.264 Video</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Figura 10.192 -<br>e<br>b<br>r<br>u<br>a<br>r<br>y<br>2<br>0<br>0<br>5      | Figura 10.193 -                                                     | Figura 10.194 - PROPOSED STANDARD |
| Figura 10.19 | Figura 10.196 - This memo describes an RTP Payload format for the ITU-T Recommendation H.264 video codec and the technically identical ISO/IEC International Standard 14496-10 video codec. The RTP payload format allows for packetization of one or more Network Abstraction Layer Units (NALUs), produced by an H.264 video encoder, in each RTP payload. The payload format has wide applicability, as it supports applications from simple low bit-rate conversational usage, to Internet video streaming with interleaved transmission, to high bit-rate video-on-demand. [STANDARDS TRACK] |                                                                             |                                                                     |                                   |
| Figura 10.19 | Figura 10.198 - <b>RTP Payload for Text Conversation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Figura 10.199 -<br>u<br>n<br>e<br>2<br>0<br>0<br>5                          | Figura 10.200 -<br>bs<br>ol<br>et<br>es<br><a href="#">RFC 2793</a> | Figura 10.201 - PROPOSED STANDARD |
| Figura 10.20 | Figura 10.203 - This memo obsoletes RFC 2793; it describes how to carry real-time text conversation session contents in RTP packets. Text conversation session contents are specified in ITU-T Recommendation T.140.<br>One payload format is described for transmitting text on a separate RTP session dedicated for the transmission of text.<br>This RTP payload description recommends a method to include redundant text from already transmitted packets in order to reduce the risk of text loss caused by packet loss.<br>[STANDARDS TRACK]                                               |                                                                             |                                                                     |                                   |
| Figura 10.20 | Figura 10.205 - <b>RTP Payload Format for Uncompressed Video</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Figura 10.206 -<br>e<br>p<br>t<br>e<br>m<br>b<br>e<br>r<br>2<br>0<br>0<br>5 | Figura 10.207 -                                                     | Figura 10.208 - PROPOSED STANDARD |
| Figura 10.20 | Figura 10.210 - This memo specifies a packetization scheme for encapsulating uncompressed video into a payload format for the Real-time Transport Protocol, RTP. It supports a range of standard- and high-definition video formats, including common television formats such as ITU BT.601, and standards from the Society of Motion Picture and Television Engineers (SMPTE), such as SMPTE 274M and SMPTE 296M. The format is designed to be applicable and extensible to new video formats as they are developed. [STANDARDS TRACK]                                                           |                                                                             |                                                                     |                                   |

### 10.3 FCCN - Projecto Estúdios

A FCCN – Fundação para a Computação Científica Nacional, desde 1996, tem vindo a prestar junto da comunidade académica portuguesa um conjunto de serviços de banda larga no âmbito do áudio e do vídeo através da implementação de sistemas difusão de vídeo.

O projecto Estúdios financiado pelo POSI (Programa Operacional da Sociedade do Conhecimento), pretende **motivar e divulgar a investigação de técnicas e tecnologias relacionadas com a video-conferência**, através da montagem de um conjunto de Estúdios em instituições de ensino superior, e a sua utilização regular em actividades como o ensino à distancia ou provas académicas, de forma a testar e validar os diversos cenários propostos **Error! Reference source not found..**

De uma forma sucinta, o projecto têm como objectivo a implementação, nas instalações das Intituições ligadas à RCTS, de um conjunto de Estúdios dotados dos meios audiovisuais que permitem uma utilização multifuncional, nomeadamente:

- .Reuniões em Videoconferência
- .Sessões de Ensino à Distância
- .Produção de conteúdos de Vídeo
- .Auditório – Visionamento de Conteúdos de Alta Qualidade
- .Experimentação nas áreas de video-conferência e video-difusão

No que se refere ao último tópico (Experimentação nas áreas de video-conferência e video-difusão), pretende-se que seja possível a exploração de várias tecnologias relacionadas com video-conferência e video-difusão, em particular o *AcessGrid* e a Video-conferência em 3D.



O AccessGrid é um projecto que permite a video-conferência sobre IP utilizando Multicast. Tem como objectivo fornecer um ambiente de colaboração de grupos bastante rico e envolve grandes grupos de participantes com uma distribuição diversificada. Pretende-se que o Estúdio seja compatível com um nó de AccessGrid. Assim, será dotado de equipamento necessário para permitir a experimentação utilizando desta tecnologia.

A Video-conferência em 3D é possível através da utilização de uma tela polarizada e um posicionamento adequado das câmaras e projectores. É também necessário que os projectores se encontrem equipados com filtros polarizadores. O Estúdio pretende integrar o equipamento necessário para a exploração da videoconferência em 3D.

Outras tecnologias que se pretende explorar no Estúdio são o ConferenceXP, o VRVS, o VideoLan, o Windows Media, o QuickTime Pro, o Real Media, o Isabel e o DVTS.

Apenas a titulo de curiosidade, a Universidade de Évora já estabeleceu um protocolo, em Outubro de 2004, com a FCCN afim de desta implementar nas suas instalações um Estúdio

## 10.4 FCCN – Formulário de inscrição nos Testbeds IPv6

# Formulário de Candidatura

### **Dados**

Nome: Rui Manuel Ferreira Bernardo

Instituição: ESTG - Instituto Politécnico de Leiria

### **Projecto/Tese**

Título: **IPv6@ESTG-Leiria Vídeo-Difusão sobre Multicast IPv6**

Descrição Sumária:

O objectivo deste projecto é o estudo e experimentação de uma solução de Vídeo-Difusão sobre Multicast IPv6, envolvendo a investigação e estudo das tecnologias envolvidas, a definição de cenários e a realização de testes.

Descrição da Componente IPv6 do Projecto/Tese:

Pretende-se que este projecto seja implementado totalmente em maquinas IPv6, quer sejam host linux ou Windows, quer sejam routers da Cisco System

Data prevista de produção de documentos: Fevereiro de 2006

### **Utilização das Plataformas**

Capacidade de Actuar de Forma Remota: Sim

Necessidade de Apoio Humano por parte da FCCN (em horas/semana): ???

Período de Utilização da(s) plataforma(s): \_14/11.2005\_ a \_2/12/2005\_

Testbed/Lisboa: Sim

Testbed/Porto: Não

Lista de Recursos Necessários (da plataforma, a disponibilizar pela FCCN):

| Descrição                                         | Local |
|---------------------------------------------------|-------|
| 4 routers com suporte para IPv6 Multicast Routing |       |

|                                                           |  |
|-----------------------------------------------------------|--|
| Aplicação de Acesso Remoto – VNC ou a Embutida no Windows |  |
| Aplicação servidora de streaming – VLC                    |  |
|                                                           |  |
|                                                           |  |
|                                                           |  |
|                                                           |  |
|                                                           |  |

Lista de Recursos Próprios a alojar junto da plataforma:

| Descrição Sumária                                        | Local |
|----------------------------------------------------------|-------|
| DVD com o conteúdo multimédia a difundir pela plataforma |       |
|                                                          |       |
|                                                          |       |
|                                                          |       |
|                                                          |       |
|                                                          |       |
|                                                          |       |
|                                                          |       |

**Data: 8.11.2005**

**Assinatura:**

## 10.5 Conceitos relacionados com o Vídeo

O aparecimento do áudio e do vídeo digital, a redução de preço dos leitores e dos suportes de gravação, o crescimento da Internet, a divulgação e instalação de redes sem fios e o crescente desenvolvimento de animações interactivas têm contribuído de forma inquestionável para que os conteúdos de multimédia estejam cada vez mais presentes no quotidiano de todos nós.

Actualmente estamos a assistir a uma gradual integração de sistemas de comunicação multimédia nas redes *wireless*. Mas tal integração é ainda um grande desafio pelo facto de estas redes oferecerem pouca largura de banda. O desafio torna-se ainda maior quando se trata de integrar sistemas de transmissão em tempo real. A integração de conteúdos multimédia, produzidos em tempo real, no protocolo IP não causa problemas. O desafio está em conseguir garantir uma boa qualidade de serviço quando as comunicações são feitas através de redes *wireless*. Uma das soluções que tem vindo a ser desenvolvida é a criação de sistemas de transmissão capazes de se adaptar à situação actual do meio e ao tipo de ligação.

A possibilidade de transmitir conteúdos de multimédia sobre redes *wireless* é uma realidade que atrai cada vez mais utilizadores e prestadores de serviço, apesar de todas as dificuldades em desenvolver sistemas que garantam uma boa qualidade de serviço. A sensibilidade a atrasos do tráfego em tempo real, a pouca largura de banda que as redes *wireless* oferecem e as limitações dos terminais móveis são problemas que a pouco e pouco vão sendo ultrapassados graças ao interesse dos utilizadores e das empresas com mais influência na área das telecomunicações.

### ***Protocolos de comunicação multimédia***

Os conteúdos de multimédia, nomeadamente o áudio e o vídeo, começam cada vez mais a invadir os computadores e as redes. A possibilidade de transmitir tal informação através das redes, como a Internet, desperta o aparecimento de novas aplicações ou mesmo indústrias, tais como a televisão digital, teleconferência, ou sistemas de informação multimédia. As aplicações de multimédia colocam novas exigências às redes e aos protocolos envolvidos nas comunicações de rede: os protocolos de transporte. É o caso do protocolo TCP (*Transmission Control Protocol*) que, apesar de ser um protocolo de transporte bastante robusto, não é ideal para aplicações em tempo real. Os mecanismos que usa para controlar o fluxo e a congestão provocam um atraso, que não é bem-vindo quando os dados são vídeo ou áudio. É neste sentido que surgem os protocolos RTP, RTCP e RTSP que foram especialmente concebidos para facilitar a transmissão de conteúdos multimédia sobre as redes.

## **RTP (Real-time Transport Protocol)**

### **1.1.1.1 Descrição**

RTP, Real-time Transport Protocol, é um protocolo desenhado para transportar informação sensível a atraso, tal como o áudio e o vídeo, através de redes. O objectivo é facilitar o envio, a monitorização, a sincronização e a reconstrução dos dados multimédia. Foi desenvolvido pelo IETF<sup>5</sup> (*Internet Engineering Task Force*), num grupo denominado de “*Audio-Video Transport Working Group*” no sentido de suportar vídeo-conferências entre participantes geograficamente dispersos. Originalmente o protocolo RTP era apenas utilizado como um protocolo de *multicast*, no entanto começou rapidamente a ser também usado como protocolo de *unicast*. Assim, actualmente o protocolo RTP suporta os dois

---

<sup>5</sup> Sítio do IETF: <http://www.ietf.org>

tipos de comunicação, o método *unicast* que permite enviar a informação apenas para um destino, e o método *multicast* que permite o envio simultâneo da informação para um grupo de destinatários. Obviamente o método *multicast* é bastante mais flexível porque permite a obtenção dos conteúdos multimédia em tempo real por mais do que um utilizador. No entanto, o método *unicast* não deixa ser útil até porque as ligações ponto a ponto são bastante utilizadas. RTP tem algumas características de um protocolo de transporte, mas não o é, e tipicamente é encapsulado noutros protocolos de transporte, nomeadamente o TCP e UDP (*User Datagram Protocol*). A escolha entre estes dois protocolos de transporte é uma questão antiga em algumas discussões sobre redes, essencialmente porque cada um deles tem vantagens e desvantagens. As vantagens do TCP são a capacidade de correcção de erros e controle de congestão. Mas para comunicações em tempo real estas vantagens tornam-se desvantagens pois certamente irão provocar atraso, o que não é bom. O protocolo UDP, aparentemente tem a desvantagem de não garantir a entrega dos dados. Mas esta desvantagem pode ser considerada uma vantagem, porque assim o protocolo torna-se mais simples e rápido quando comparado com o TCP. A escolha recai maioritariamente sobre o UDP, que é assim eleito como o melhor protocolo para transportar dados relativos a aplicações de multimédia em tempo real. O protocolo RTP não implementa directamente nenhum mecanismo de controlo de fluxo nem de recuperação de erros, no entanto, o seu *header* contém um número de sequência através do qual é possível detectar perdas de pacotes e posteriormente efectuar retransmissão dos dados, caso isso se justifique.

RTP é um protocolo relativamente recente, amplamente usado em aplicações como “*RealPlayer*”, “*QuickTime*” e “*NetMeeting*”. Normalmente é utilizado nessas aplicações para *streaming* de áudio e vídeo, e para vídeo-conferências. A simplicidade deste protocolo, sobretudo pelo facto de não transportar endereços de rede, permite que este esteja já adaptado à nova realidade que é o IPv6 (*Internet Protocol Version 6*).



Figura -1. Encapsulamento das mensagens RTP nos restantes protocolos

### 1.1.1.2 Estrutura do protocolo RTP

Cada pacote RTP é constituído por um cabeçalho (*header*) de tamanho fixo e por um *payload* que contém os dados multimédia. O *header* é composto pelos seguintes campos:

- **V, version.** Identifica a versão do pacote RTP. Usualmente tem o valor ‘2’, pois a versão 1 serviu apenas para realizar os primeiros testes e já não se utiliza.
- **P, padding.** Se estiver activo significa que o pacote contém um ou mais *bytes* adicionais que não fazem parte do *payload*.
- **X, extension.** Se estiver activo o tamanho fixo do *header* deve ser seguido por, exactamente uma extensão de *header*.
- **CSRC count.** Contém o número de identificadores CSRC que seguem o *header*.
- **M, marker.** A interpretação deste campo é definida por um perfil. Serve para marcar acontecimentos importantes, tais como o limite de uma *frame*.
- **Payload type.** Identifica o formato do *payload* do pacote RTP e determina a sua interpretação por parte da aplicação. Para cada tipo de dados está associado um valor, por exemplo o áudio PCMA (*Paired Carrier Multiple Access*) é representado pelo valor ‘8’, o vídeo H263 pelo valor ‘34’ e o vídeo MPEG (*Moving Picture Experts Group*) por ‘26’. Existem ainda alguns tipos de dados que são identificados por valores dinâmicos.
- **Sequence number.** O número de sequência é incrementado um a um por cada pacote RTP enviado, e poderá ser usado pelo receptor para detectar a perda de pacotes. O primeiro valor desta sequência deverá ser gerado aleatoriamente.

- **Timestamp.** Reflete o instante de amostragem do pacote RTP. O instante de amostragem deve derivar de um relógio, cuja frequência depende do tipo de dados transportados, de modo a permitir sincronização e cálculos de atraso. Essencialmente serve para que os dados sejam mostrados no receptor com a mesma frequência com que foram adquiridos e no tempo correcto.
- **SSRC.** Representa o código de sincronização. Este valor é escolhido aleatoriamente, de modo a que dois códigos de sincronização na mesma sessão RTP não tenham o mesmo SSRC.
- **CSRC.** Identifica o tipo de contribuição que o conteúdo do *payload* irá ter. Este campo é útil quando existem várias fontes que contribuem para a produção de dados, que serão multiplexados antes de chegarem ao receptor.

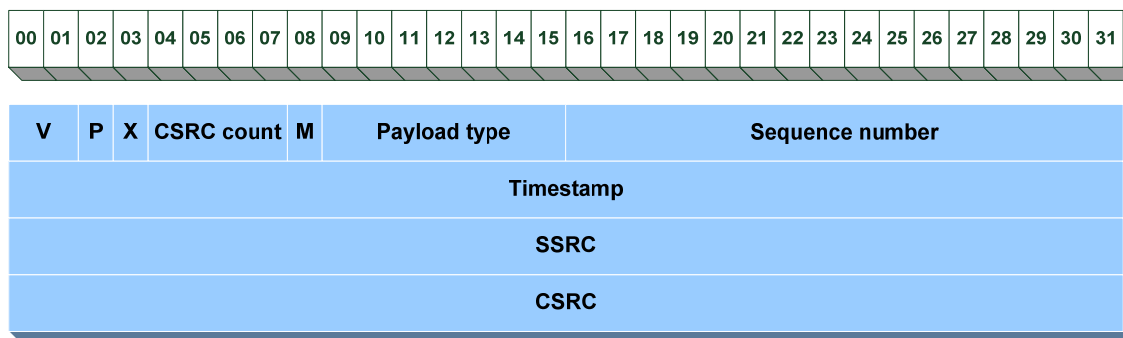


Figura 2. header do protocolo RTP

### 1.1.1.3 RTP – segurança e qualidade de serviço

O protocolo RTP é muitas vezes usado na Internet, uma rede considerada insegura. Nas comunicações *broadcast* a segurança e confidencialidade não são absolutamente necessárias, mas se se tratar de uma vídeo-conferência, por exemplo usada para telemedicina, a confidencialidade dos dados é extremamente importante. Este protocolo é bastante flexível no que diz respeito à encriptação dos pacotes, e permite o uso de qualquer algoritmo com tais funcionalidades, sendo o DES-CBC (*Data Encryption Standard-Cipher Block Chaining*) o algoritmo mais utilizado. Seja qual for o algoritmo deve existir negociação entre as duas partes, emissor e receptor, e deve ser sempre tido em conta que o RTP serve para comunicações muito sensíveis, e por isso os mecanismos de segurança devem ser implementados com o mínimo de atraso.

Apesar de tudo o protocolo RTP não é seguro, por si só. Não implementa mecanismos de segurança porque esses mecanismos já estão implementados noutros protocolos. Por isso RTP é um protocolo que desempenha apenas as suas funções ligadas às comunicações em tempo real, e que confia em outros protocolos para garantir a segurança. Não implementa também, qualquer mecanismo que garanta a entrega dos dados no tempo correcto, nem garante qualidade de serviço nas redes IP (*Internet Protocol*), mas deixa essas tarefas entregues aos protocolos das camadas mais baixas. Não previne que os pacotes sejam entregues fora de ordem, no entanto o facto de estes terem um número de sequência permite ao receptor efectuar a respectiva ordenação. É também possível criar duas sessões RTP para a mesma origem de dados, sendo que uma dessas sessões funcionará de forma redundante. A segurança é entregue a outros protocolos já existentes e a qualidade de serviço é garantida por um outro protocolo, o RTCP. Além do mais, as redes devem funcionar com mecanismos QoS (*Quality of Service*), como o RSVP, para reservar recursos.

### RSVP (ReSerVation Protocol)

O protocolo RSVP é um protocolo proposto pelo IETF para definir níveis de qualidade de serviço (QoS) nas redes IP, nomeadamente a Internet.

Este protocolo faz parte de um enorme esforço que tem vindo a ser desenvolvido no sentido de aumentar a qualidade serviço na Internet e em redes privadas no que diz respeito à transmissão de áudio e vídeo. As aplicações, usualmente de *streaming*, utilizam-no para reservar uma determinada qualidade de serviço à rede, ou seja, ao tráfego de *streaming*, produzido continuamente, são atribuídos níveis de prioridade que o fazem ter vantagem em relação ao tráfego gerado por outras aplicações. Após o pedido de reserva de recursos por parte dos terminais, os *routers* enviam pedidos QoS para todos os nós da rede por onde passa o respectivo tráfego. Assim, consegue-se que a largura de banda disponível para a ligação de *streaming* seja suficiente.

## RTCP (Real-time Transport Control Protocol)

### 1.1.1.4 Descrição

O RTCP é parceiro do protocolo RTP na transmissão e empacotamento de dados multimédia, mas não transporta quaisquer dados desse tipo. Ele é usado para enviar periodicamente pacotes de controlo relativos à sessão de *streaming*. A principal função do RTCP é fornecer feedback em relação à qualidade de serviço oferecida pelo RTP. Reúne estatísticas acerca da comunicação multimédia, e informações tais como número de *bytes* enviados, pacotes perdidos, *jitter* e atraso. Esta informação pode ser utilizada pelo emissor para controlar a transmissão, de modo a melhorar a qualidade serviço, por exemplo diminuindo o débito, ou transmitindo os dados mais comprimidos. Fundamentalmente o protocolo RTCP desempenha três funções:

Fornecer feedback em relação à qualidade dos dados enviados. Esta é uma tarefa que leva o protocolo RTP a ser considerado um protocolo de transporte uma vez que lhe atribui funções de controlo de fluxo e de congestão.

Gerir a transmissão para os vários participantes, ou seja, uma vez que cada participante envia os seus pacotes de controlo ao emissor, este pode controlar o débito de modo a garantir qualidade a todos e a permitir um aumento do número de participantes.

Uma função opcional é transportar pequenas informações acerca da sessão, por exemplo a identificação do receptor.

O RTCP dever ser usado em todos os ambientes de *streaming*, mas especialmente em *multicast* no sentido de garantir a melhor qualidade de serviço possível a todos os utilizadores.

### 1.1.1.5 Estrutura do protocolo RTCP

O *header* do pacote RTCP é composto pelos seguintes campos:

- **V, version.** Identifica a versão do pacote RTCP.
- **P, padding.** Se estiver activo significa que o pacote contém um ou mais bytes adicionais que não fazem parte da informação de controlo.
- **Count.** Indica o número de relatórios de blocos de recepção contidos no pacote.
- **Type.** Identifica o tipo do pacote RTCP. Existem vários, tais como:
  - 193** - NACK, negative acknowledgement.
  - 200** - SR, sender report.
  - 201** - RR, receiver report.
  - 203** - BYE, goodbye.
- **Length.** Representa o tamanho do pacote RTCP.

- **Data.** Este campo contém o relatório em si. Pode conter várias informações, nomeadamente as referidas anteriormente.

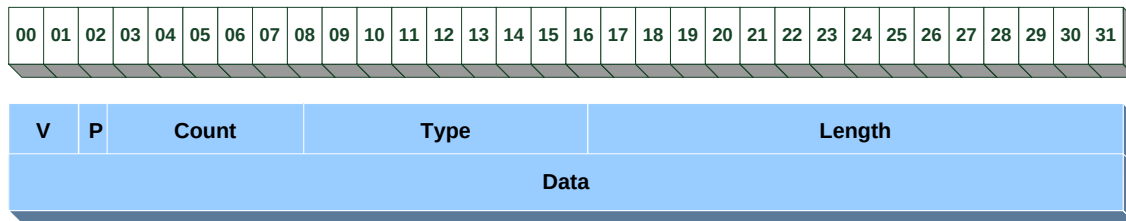


Figura 3. header do protocolo RTCP

## RTSP (Real-time Streaming Protocol)

Nos últimos anos, paralelamente ao desenvolvimento das técnicas de *streaming*, as interfaces gráficas dos utilizadores também têm vindo a evoluir no sentido de implementar algo semelhante aos controlos existentes nos gravadores de vídeo. Este tipo de interface, que permite um maior controlo na reprodução do ficheiro multimédia por parte do utilizador, exige a implementação de um protocolo de comunicação, através do qual o cliente e o servidor possam comunicar de forma simétrica. O RTSP é o protocolo mais utilizado para este fim.

O protocolo RTSP foi também desenvolvido pelo IETF. Este protocolo é usado em sistemas de *streaming* que permitem ao receptor controlar remotamente a informação multimédia, ou seja, utilizar comandos VCR (*Video Cassette Recorder*) tais como, *PLAY* e *PAUSE* ou ainda aceder a ficheiros no emissor. O RTSP permite estabelecer comunicação e controlar um ou vários *streams* de multimédia. Por outras palavras, ele não transporta a informação multimédia, apenas a controla, actuando assim como um controlador remoto de servidores multimédia. Os *streams* de multimédia controlados pelo RTSP deverão ser transportados pelo RTP, no entanto o seu funcionamento não depende do protocolo usado para transportar a informação.

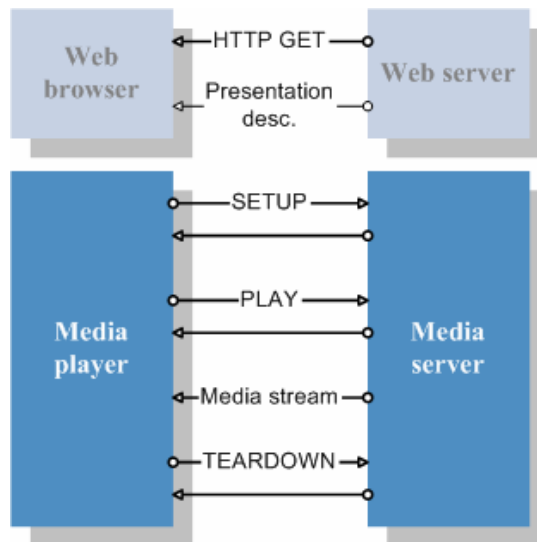
Este protocolo é intencionalmente similar, em sintaxe e funcionamento, ao HTTP/1.1 (*Hyper Text Transfer Protocol*) de modo a que mecanismos adicionais ao HTTP podem por vezes ser também aplicados ao RTSP. Contudo, o RTSP difere em vários aspectos do HTTP:

- HTTP não mantém o estado da sessão (*stateless*), ao contrário do RTSP que precisa manter-se ciente do estado do fluxo.
- Enquanto que o HTTP é um protocolo assimétrico onde apenas os clientes fazem requisições ao servidor, no RTSP existe uma simetria, onde o servidor também pode enviar requisições aos clientes.
- Tanto o servidor como o cliente RTSP podem emitir pedidos.
- Utiliza caracteres ISO 10646<sup>6</sup> em vez de ISO 8859-1<sup>7</sup>.

<sup>6</sup> Codificação mais actual que abrange mais caracteres. Também conhecida como UTF-8.

<sup>7</sup> Codificação dos caracteres do alfabeto Latim nº 1.





**Figura 4.** Diferença entre comunicação Web browser/Web server e Media player/Media server

### 1.1.1.6 Estrutura do protocolo RTSP

RTSP é um protocolo textual (*text-based*) que utiliza os caracteres ISO 10646 definidos na codificação UTF-8. As linhas são terminadas por CRLF ([Carriage Return Line Feed](#)), mas os receptores devem estar também preparados para interpretar os comandos CR ([Carriage Return](#)) e LF ([Line Feed](#)) como identificadores de fim de linha. A sua estrutura não é ilustrada como foi anteriormente nos protocolos RTP e RTCP precisamente porque se trata de um protocolo textual, e como tal o seu conteúdo são mensagens de texto. Assim segue-se um exemplo simples de como o receptor poderá iniciar a recepção de um vídeo.

- **Receptor:** PLAY rtsp://exemplo.com/videos/video.mpg RTSP/1.0
- **Servidor:** RTSP/1.0 200 OK

Após esta troca de mensagens o servidor inicia o envio do vídeo “video.mpg”

Além da mensagem iniciada por *PLAY*, existem ainda mais três que importa referir: *SETUP*, utilizada para anunciar ao servidor algumas configurações relativas à transmissão, *PAUSE*, usado para efectuar uma pausa na transmissão e *TEARDOWN* para terminar o envio dos dados multimédia.

## RTP, RTCP, RTSP – conclusões

Em suma, RTP, RTCP e RTSP são protocolos utilizados na transmissão de dados multimédia, em tempo real, com características muito próprias. O protocolo RTP assume o papel mais importante porque é ele que transporta os dados, podendo até funcionar sem os outros dois. É importante deixar claro que este protocolo não fornece nenhum mecanismo de controlo de fluxo e congestão, e que por isso não é um protocolo de transporte. Assim, RTP é sempre encapsulado noutro protocolo, normalmente o UDP. O RTCP surge aqui como o protocolo que garante qualidade de serviço na transmissão. Consiste em relatórios enviados para o servidor, cuja finalidade é fazer com que este possa adaptar a forma como os dados são enviados, à qualidade da ligação. Finalmente, para dar mais flexibilidade à transmissão, aparece o protocolo RTSP. Este último é ideal para que o receptor possa utilizar comandos VCR para controlar o envio dos dados de vídeo ou áudio. Assim a melhor forma de transmitir multimédia através de uma rede, é utilizando os três protocolos em conjunto, aproveitando as suas diferentes potencialidades.

## Compressão de vídeo

A compressão de dados não é mais do que um processo que visa reduzir o tamanho de um determinado ficheiro. Consiste essencialmente em substituir partes do ficheiro por códigos, que serão posteriormente usados para restabelecer o ficheiro original. Assim, codificação de dados e compressão de dados são aqui interpretados como sendo a mesma coisa. A forma como se comprime a informação difere de acordo com o tipo de dados. Por exemplo no caso do texto, a compressão não origina perda de dados. Já o mesmo não acontece nas imagens, onde a compressão reduz a sua qualidade. Contudo, a perda de qualidade das imagens é muitas vezes imperceptível para o olho humano. A enorme redução de tamanho dos ficheiros codificados em relação aos originais leva a que a utilização de compressão de vídeo seja uma realidade que todos compreendem facilmente.

Este sub-capítulo surge no sentido de apresentar alguns conceitos gerais sobre o vídeo digital e a sua respectiva compressão, antes da abordagem às normas em no sub-capítulo 0.

## Imagens digitais

A palavra “imagem” tem vários significados. De acordo com o dicionário, sabemos que “imagem” é a representação visual de uma pessoa, uma figura, um animal ou uma coisa. Contudo, tecnicamente falando, uma imagem é um sinal bidimensional que o sistema visual humano consegue compreender. As imagens adquirem um novo significado quando se movem, formando assim os vídeo, tal como vimos na televisão. A definição de imagem varia também de acordo com o suporte onde esta se encontra. Assim uma imagem digitalizada torna-se uma imagem digital, que é representada através de uma estrutura de *pixels*.

As imagens podem ser agrupadas em três categorias diferentes:

- **Imagens a preto e branco:** nestas imagens cada *pixel* é representado por um *bit*.
- **Imagens em tons de cinza:** onde cada *pixel* é representado por um nível de luminosidade. Normalmente estas imagens são representadas por 256 níveis de cinzento, ou 8 *bits*. Estas imagens, bem como as anteriores, apesar da sua simplicidade, continuam a ser muito utilizadas, por exemplo em sistemas de recolha de imagens para fins de segurança, em sistemas medicinais, ou mesmo para trabalhos de fotografia.
- **Imagens a cores:** as mais complexas, pela sua variedade de componentes. Nestas imagens cada *pixel* pode ser representado por dois componente (*luminance* e *chrominance*). As imagens a cores são as que mais se vêem no nosso dia-a-dia e as que mais agradam às pessoas. Por exemplo, a norma de compressão MPEG, utiliza um valor Y de *luminance* e dois ( $C_B$  e  $C_R$ ) de *chrominance*.

## Pixel

*Pixel* é visto como o elemento completo mais pequeno de uma imagem representada digitalmente. Cada *pixel* é composto por três *sub-pixels*, cada um deles com uma cor (RGB). Os *pixels* são tão pequenos e existem em tão grandes quantidades numa imagem, que se tornam praticamente imperceptíveis. Quantos mais *pixels* usarmos numa imagem, mais perfeita ela fica. A sua cor e intensidade são escolhidas de modo a conseguir representar pequenas áreas da figura. *Pixel*, ou *px*, é também usado como uma medida de resolução. Quem não ouviu já falar de câmaras fotográficas digitais com 5, 6 ou 8 mega *pixels*? Esse valor não é mais do que a quantidade de *pixels* que o equipamento utiliza para representar cada imagem. Por exemplo, uma câmara que consegue tirar fotografias com uma resolução de  $2048 \times 1536$  *pixels* é vista como uma máquina de 3.1 *megapixels* ( $2048 \times 1536 = 3,145,728$ ).

## Modelo YUV

### 1.1.1.7 Definição

O modelo YUV define o espaço de cores através de um componente de *luminance*<sup>8</sup> e dois de *chrominance*<sup>9</sup>. O Y representa o componente *luminance* e o U e V representam os componentes *chrominance*. YUV é usado nos sistemas de televisão PAL (*Phase Alternation Line*), um dos maiores sistemas televisivos mundiais. Este modelo está mais próximo da percepção humana do que o conhecido RGB (*Red Green Blue*) utilizado nos grafismos dos computadores, mas não tanto como o espaço de cores HSV (*Hue Saturation Value*). Os engenheiros que inventaram este sistema de representação da cor fizeram-no porque precisavam de encontrar uma forma de garantir a compatibilidade entre a televisão a cores e a já existente a preto e branco. Combinando a informação relativa à cor, YUV usa menos largura de banda do que o RGB.

YUV usa informação RGB, constituindo uma matriz que combina as três cores para reduzir a quantidade de informação do sinal. O componente Y representa o valor *luma*<sup>10</sup> que é a amplitude entre o valor mais claro e mais escuro. *Luma* é o sinal “visto” pelos televisores a preto e branco e o seu valor é calculado pela seguinte fórmula:  **$luma = 30\% R + 59\% G + 11\% B$** . Os componentes U e V retiram os valores de *luminance* do vermelho (R) e azul (B) afim de reduzir a informação de cor. Estes três componentes podem posteriormente ser combinados para determinar a quantidade de vermelho (R), verde (G) e azul (B).

Essencialmente, existem duas razões para a existência do modelo YUV. Primeiro, a conversão de um sinal RGB para YUV é linear, consegue-se com pequenos circuitos ou com alguns cálculos numéricos. Segundo, este modelo permite fazer a separação da informação relativa à cor e do componente *luminance*. Esta razão leva a que o YUV seja utilizado por sistemas de televisão PAL ou SECAM<sup>11</sup> (*Séquentiel Couleur Avec Mémoire*) e por alguns mecanismos de compressão de imagem, nomeadamente o MPEG. Num sinal de televisão o canal *luminance* é modelado separadamente (ou seja, a informação de cor é enviada separadamente). Assim, os televisores a preto e branco funcionam na mesma porque retêm apenas o canal Y ignorando os outros dois. Uma vez que o olho humano é também muito mais sensível ao brilho, os mecanismos de compressão comprimem maioritariamente os canais de *chrominance* em vez do canal de *luminance* para tornar as alterações à imagem menos perceptíveis.

### 1.1.1.8 Conversão

Tal como acima referido a conversão entre os sinais RGB e YUV é relativamente simples e consegue-se com as seguintes fórmulas:

- **De RGB para YUV**

$$Y = 0.299R + 0.587G + 0.114B$$

$$U = 0.492(B - Y)$$

$$V = 0.877(R - Y)$$

- **De YUV para RGB**

<sup>8</sup> Relativo à luminosidade das imagens.

<sup>9</sup> Relativo à core das imagens.

<sup>10</sup> Semelhante a *luminance*.

<sup>11</sup> A primeira norma europeia para a televisão a cores. Desenvolvida em França, um dos poucos países que continua a utilizá-la.

R=Y+1.140V  
G=Y-0.395U-0.581V  
B=Y+2.032U

Podemos ainda efectuar a conversão através de matrizes:

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Figura 5. Fórmula matricial para conversão YUV – RGB.

Onde R, G e B assumem valores entre 0 e 1, com o 1 a representar o máximo de intensidade e 0 o mínimo.

### 1.1.1.9 Sub-amostragem cromática

A sub-amostragem cromática, *chroma subsampling*, consiste em usar menos definição para definir a cor de uma imagem do que para definir a sua luminosidade. É usado quando um vídeo analógico ou um sinal YUV é digitalmente amostrado. O olho humano é menos sensível à cor do que à intensidade, por isso o componente *chroma* de uma imagem não precisa de ser tão bem definido como o componente *luma*. Assim, muitos sistemas de vídeo efectuem uma amostragem mais baixa dos canais que contêm a cor, ou seja, a amostragem desses canais é feita com uma frequência mais lenta. Esta técnica permite reduzir a largura de banda global do sinal de vídeo sem provocar uma aparente perda de qualidade das imagens.

A sub-amostragem de vídeo é usualmente expressão por uma relação constituída por três valores numéricos: o número de amostras do componente Y, seguido de amostras dos outros dois componentes U e V respectivamente. Para fins de comparação de qualidade apenas os dois últimos valores são importantes uma vez que, tradicionalmente, o valor Y é sempre 4.

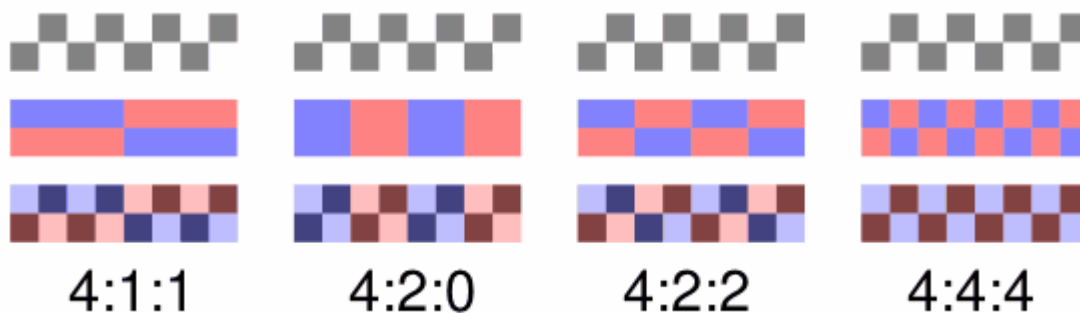


Figura -6. Tipos de sub amostragem cromática.

Por vezes, podem ser usados quatro valores para definir esta relação (por exemplo 4:2:2:4). Neste caso o quarto termo representa a frequência de amostragem.

De seguida apresentamos alguns exemplos de relações de sub amostragem.

- 4:4:4

Cada um dos três canais tem a mesma frequência de amostragem e cada *pixel* da imagem é representado por 3 *bytes*, quando usamos 8 *bits* de quantificação. Esta é a melhor relação de amostragem, e é usada como um formato intermédio em *scanners* e produções cinematográficas.

▪ **4:2:2**

Cada um dos dois canais que representam a cor (U, V) tem metade da amostragem usada no canal que representa o brilho (Y). No vídeo quantificado com 8 *bits*, cada *macropixel* de dois *pixels* próximos usa 4 *bytes* de memória. Esta relação consegue ainda garantir uma qualidade bastante aceitável, e é usada por muitos formatos de vídeo.

▪ **4:2:0**

Esta relação não significa que não existe informação V armazenada. Significa sim, que em cada linha é apenas armazenado um canal de cor com metade da resolução horizontal. O canal de cor armazenado muda em cada linha, ou seja, se numa linha temos 4:2:0, na próxima teremos 4:0:2, e na seguinte voltaremos a ter 4:2:0, etc. Esta resolução é especialmente utilizada nos sistemas PAL e SECAM, bem como em implementações de DVD (*Digital Versatile Disk*), MPEG-2, JPEG (*Joint Photographic Experts Group*) ou MJPEG (*Motion Joint Photographic Experts Group*). Para uma quantificação de 8 *bits* cada *macropixel* usa 6 *bytes* (2x2 *pixels*).

## PSNR (Peak Signal-to-Noise Ratio)

PSNR é uma medida objectiva de avaliação de qualidade de imagem, relacionando o valor máximo de um sinal e a magnitude do ruído de fundo. É normalmente utilizado para medir a qualidade de imagens reconstruídas a partir de um vídeo codificado. Uma vez que os sinais podem variar muito, o PSNR é usualmente expresso em valores logarítmicos. Tipicamente os valores do PSNR variam entre 20 e 40dB, aproximadamente.

## A importância da compressão de vídeo

Uma sequência de imagens em formato digital gera um ficheiro de vídeo que necessita de muito espaço para ser armazenado. Por exemplo, se numa sequência cada imagem tiver 288 linha e 360 elementos em cada linha, teremos uma imagem cuja dimensão é 288x360. Se cada uma dessas imagens, a cores, tiver uma precisão de 8 *bits*, então o seu tamanho será de aproximadamente 311 KBytes cada. Se as imagens deste vídeo forem enviadas a uma velocidade de 24 imagens/segundo, então teremos uma taxa de transmissão de 60 Mbits/s, e um minuto deste vídeo ocuparia cerca de 448 MBytes. Assim, a compressão, também usada em dados como áudio e texto, é para o vídeo uma necessidade fundamental.

## Compressão de vídeo – termos e conceitos

As técnicas usadas em compressão de vídeo, nomeadamente o MPEG, são divididas em duas classes, “*intra*” e “*nonintra*”. A primeira técnica, *intra*, consiste em comprimir a imagem usando informação apenas dessas imagens. Ao passo que na segunda técnica, *nonintra*, também é usada informação de outras imagens separadas no tempo.

Chama-se “*source data*” aos dados que entram no compressor, e “*reconstructed data*” aos dados que saem do algoritmo de descompressão.

Algumas técnicas de compressão são desenhadas de tal forma que os dados reconstruídos são exactamente iguais aos dados de origem, essas técnicas chamam-se “*lossless*” e são usadas maioritariamente em ficheiros de texto. Em outras técnicas, denominadas de “*lossy*”, a informação final é apenas uma boa aproximação da inicial (o caso do vídeo). A distinção entre estas duas técnicas é absolutamente importante, pois a eficiência de cada uma delas é diferente (menos eficiência na

técnica *lossless*). Uma boa compressão de dados resulta da combinação destas duas técnicas, e é também conseguida quando se utiliza a técnica *lossy* em elementos da imagem que os nossos olhos não vêem. **Error! Reference source not found.**

## Compressão de vídeo – funcionamento básico

Apesar do vídeo ser uma forma de representação da informação bastante complexa, existem muitas razões que facilitam a sua compressão. O aspecto chave desta questão é a similaridade que normalmente existe entre as imagens que constituem o vídeo, tal como ilustra a Figura 7. Como regra geral, menos diferenças entre as imagens conduzem a uma melhor compressão. Se não existirem diferenças, a sequência de vídeo será codificada como uma imagem seguida de alguns *bits* que dizem ao decodificador para simplesmente repetir a imagem. Parece estranho, mas é exactamente o que os algoritmos de compressão fazem. Claro que este é um caso bastante particular, e muito mais terá de ser feito para codificar uma sequência de imagens com muitas diferenças entre elas. A técnica consiste em codificar e referenciar a primeira imagem da sequência e fazer com que de seguida surjam *bits* que indicam as alterações que as imagens seguintes irão ter em relação à referência. No entanto, é fundamental que ocasionalmente sejam referenciadas e codificadas imagens independentemente das vizinhas de modo a que estas não dependam todas da primeira, mas também de imagens intermédias. A grande taxa de compressão é assim conseguida codificando a maior parte das imagens como diferenças relativamente a imagens vizinhas. Mas, as imagens podem conter elementos que não existiam nas anteriores, não sendo assim possível fazer a codificação apenas através do processo de diferenças. Esta situação é, normalmente resolvida codificando esses elementos de forma independente. **Error! Reference source not found.**

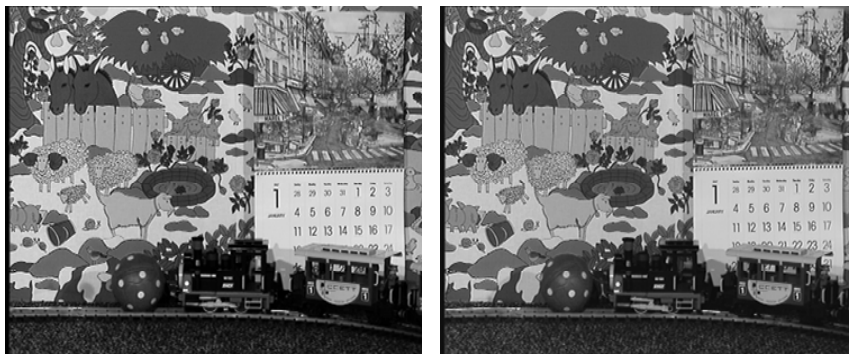


Figura 7. Semelhança entre imagens.

## Normas de compressão de sinais audiovisuais

Neste sub-capítulo são abordados conceitos sobre as mais conhecidas normas de compressão de sinais audiovisuais não proprietárias. De entre as várias normas é dado um destaque especial ao MPEG-4 por ser uma norma recente e cada vez mais utilizada e sobretudo por ser a norma que utilizamos nos testes de *streaming*.

Cada uma das normas foi desenvolvida com diferentes características de acordo com os objectivos que se pretendiam alcançar. Essencialmente, existem as normas MPEG e H26x desenvolvidas pelo ISO<sup>12</sup>/IEC<sup>13</sup> (*International Organization for Standardization/International Electrotechnical*

---

<sup>12</sup> Sítio do ISO: <http://www.iso.org>

<sup>13</sup> Sítio do IEC: <http://www.iec.org>

Commission) e ITU-T<sup>14</sup> ([International Telecommunication Union-Telecommunication Standardization Sector](http://www.itu.int)) respectivamente, sendo que algumas foram desenvolvidas em parcerias entre estas duas entidades.

## H261

*“...designed for transmission over [ISDN](#) lines on which data rates are multiples of 64 kbit/s”*

H261 foi desenvolvido em 1990 pelo ITU-T para ser utilizado em ligações ISDN (*Integrated Services Digital Network*) com velocidades múltiplas de 64 Kbit/s e particularmente em videoconferências. Capaz de suportar resoluções de imagem de 352x288 (CIF) e de 176x144 (QCIF), o H261 foi a primeira norma de compressão de vídeo a ser desenvolvida. O desenvolvimento desta norma resulta de um esforço pioneiro, e todas as normas que surgiram posteriormente são parcialmente baseadas nela. O H261 é actualmente uma norma obsoleta mas que continua a ser lembrado como um marco histórico na área da codificação de vídeo.

## H262

*“It is identical in content to the video part of the [ISO/IEC MPEG-2](#) standard”.*

A norma H262 foi desenvolvida numa parceria entre o ITU-T e o ISO/IEC uma vez que o seu funcionamento é bastante idêntico ao MPEG-2 (sub-capítulo 0). No entanto, a publicação destas duas normas foi feita separadamente, mas o conteúdo dos documentos é, tal como a norma em si, muito semelhante.

## H263

*“...designed as a low-bitrate encoding solution for videoconferencing”*

H263 é uma norma de compressão desenhada para comunicações de *low-bitrate* em aplicações de videoconferência, cuja primeira versão foi publicada em 1995 pelo ITU-T. Foi desenvolvido para substituir o H261 na maioria das aplicações. O algoritmo do H263 é similar ao usado no H261, mas com algumas alterações que permite melhor performance e correcção de erros. Suporte cinco resoluções de imagem. Adicionalmente ao CIF e QCIF suportados pelo H261 suporta também SQCIF, 4CIF e 16CIF. A resolução associada a cada um destes nomes é apresentada na Tabela 1.

| Formato | Resolução                   |                            |
|---------|-----------------------------|----------------------------|
|         | <i>Luminance<br/>pixels</i> | <i>Luminance<br/>lines</i> |
| CIF     | 352                         | 288                        |
| QCIF    | 176                         | 144                        |
| SQCIF   | 128                         | 96                         |
| 4CIF    | 704                         | 576                        |
| 16CIF   | 1408                        | 1152                       |

**Tabela 1.** Formatos de imagens.

<sup>14</sup> Sítio do ITU: <http://www.itu.int>

## H264

“...to create a standard that would be capable of providing good video quality at bit rates that are substantially lower”**Error! Reference source not found.**

H264, ou MPEG-4 part 10, é uma norma de compressão de vídeo digital desenvolvido por um grupo que ficou conhecido por JVT (*Joint Video Team*) e que é resultado de um trabalho colectivo de duas entidades que já trabalhavam separadamente no desenvolvimento deste tipo de normas, VCEG<sup>15</sup> (*Video Coding Experts Group*) e MPEG<sup>16</sup>. As normas H264 do ITU-T e MPEG-4 part 10 do ISO/IEC são tecnicamente muito semelhantes, e são parte de uma tecnologia conhecida como AVC (*Advanced Video Coding*). A primeira versão desta norma conjunta ficou completa em 2003.

O nome H264 deriva do modelo de normas de vídeo H26x do ITU-T, ao passo que AVC está relacionado com o trabalho do ISO/IEC neste projecto colectivo. É usual chamar a esta norma H.264/AVC, AVC/H.264, H.264/MPEG-4 AVC ou ainda MPEG-4/H.264 AVC. Por vezes, é também denominado de “*the JVT codec*” como referencia ao grupo JVT que o desenvolveu. Este múltiplo conjunto de nomes não é de estranhar, pois o MPEG-2 é também conhecido como H262 na comunidade ITU-T.

O projecto H.264/AVC foi desenvolvido com a finalidade de criar uma norma que pudesse ser capaz de garantir uma boa qualidade de vídeo em taxas de transmissão relativamente baixas, e sem que a sua implementação se tornasse complexa ou impraticável. Um objectivo adicional era desenhar esta norma de tal modo flexível, que pudesse ser usada na maioria das aplicações (isto é, aplicações de alto ou de baixo débito e aplicações de muita ou pouca resolução de vídeo), e em conjunto com uma vasta quantidade de sistemas (isto é, aplicações de *broadcast*, armazenamento em DVD, empacotamento RTP e sistemas de telefone).

Recentemente o projecto JVT completou o desenvolvimento de algumas extensões à norma inicial que ficaram conhecidas como FRExt (*Fidelity Range Extensions*). Esta extensão permite codificação de vídeo de alta-fidelidade através do aumento da taxa de amostragem (codificação de 10 e 12 *bits*) e maior resolução na representação da cor (usando relações YUV 4:2:2 e YUV 4:4:4) (ver sub-capítulo 1.1.1.9).

H264/AVC contém um conjunto de novas características que permitem comprimir o vídeo de forma mais eficiente do que as normas anteriores e que promovem uma maior flexibilidade em relação ao tipo de ambientes onde se pode utilizar. Tais características tornam o H264 radicalmente melhor que o MPEG-2 e tipicamente consegue obter a mesma qualidade de imagem com metade do *bit rate*.

## MPEG (Moving Pictures Experts Group)

Desde o final dos anos 80 que este comité tem trabalhado com grande entusiasmo e sucesso no desenvolvido de normas de compressão de vídeo.

### 1.1.1.10 Introdução histórica

O processo de universalização da norma de compressão de vídeo MPEG teve início em 1988, e tinha como principal objectivo a descompressão, em tempo real, de vídeo armazenado em suportes digitais. Já o trabalho tinha começado quando um novo projecto surgiu, motivado pela necessidade de uma maior taxa de transmissão e melhor qualidade de imagem exigidos pelos meios televisivos. Assim, foram criados dois projectos que ficaram conhecidos como MPEG-1 e MPEG-2 respectivamente. Um terceiro projecto, MPEG-3, foi antecipado no sentido se satisfazer mais algumas necessidades exigidas

---

<sup>15</sup> Propriedade do ITU-T.

<sup>16</sup> Propriedade do ISO/IEC.



pela televisão HDTV, no entanto, o MPEG-2 mostrou-se capaz de preencher essas necessidades e o MPEG-3 nunca chegou a ser muito desenvolvido. Para taxas de transmissão mais baixas, foi iniciado um novo projecto, MPEG-4.

O grupo<sup>17</sup> responsável pela criação do MPEG reuniu-se inúmeras vezes e em diversos países, até que em 1990 surgiu a primeira versão, MPEG-1.

As potencialidades que se pretendiam obter com o MPEG-2 levaram a que o seu desenvolvimento durasse vários anos. Durante esse tempo o projecto MPEG-2 foi dividido em nove partes, que foram sendo publicadas até 1997. O formato MPEG-2 é o mais conhecido e utilizado graças à sua vasta aplicabilidade tanto ao nível do vídeo como do áudio. No entanto, o MPEG-4 começa a ser utilizado e a mostrar que é o novo líder da geração MPEG.

Quando o processo se iniciou, já muitas indústrias convergiam para uma tecnologia digital. A indústria dos computadores procurava substituir as tradicionais linhas de texto por imagens paradas, vídeo e áudio. As imagens digitais eram vistas como uma forma de aperfeiçoar os jogos de vídeo e os sistemas de entretenimento baseados em multimédia. Nesta altura os CDs (*Compact Disc*) já eram utilizados para armazenamento digital, e as suas capacidades eram suficientes para o vídeo digital comprimido. A indústria das telecomunicações já levava vantagem na área de compressão de vídeo digital, e tinha já iniciado o desenvolvimento da norma H261 que pretendia uniformizar as teleconferências. O debate acerca de uma televisão digital, com uma melhor definição de imagem (HDTV), também já tinha começado. A televisão por cabo também pretendia usar o vídeo digital nas ligações com os satélites, e até mesmo faze-lo chegar até à casa dos clientes. Com a partilha de tecnologia entre estes diversos interesses industriais, esta normalização foi um progresso natural. A convergência destes interesses quebrou barreiras que normalmente impedem o crescimento tecnológico.

#### 1.1.1.11 Envolvimento e colaboração internacional

Centenas de técnicos especializados estiveram presentes nos vários encontros que visavam o desenvolvimento do MPEG. E muitos mais deram o seu contributo a nível nacional. Foram muitas as companhias envolvidas nas várias áreas dos três projectos (MPEG-1, MPEG-2 e MPEG-4) e foram muitos os encontros internacionais, nacionais, oficiais e não oficiais representados por um ou mais elementos de cada entidade envolvida. Com tal nível de participação, torna-se impossível saber ao certo o contributo de cada um.

Uma norma tão complexa como esta não surgiu facilmente, foi necessário muitos debates e discussões até se chegar a níveis de consenso. O tempo dispendido deve-se sobretudo aos processos de refinamento e adaptação às necessidades de algumas aplicações. A versão MPEG-1 está completamente finalizada e documentada, no entanto, considera-se que o MPEG-2 pode ainda sofrer alterações mesmo apesar da vasta documentação existente. Os utilizadores costumam preferir sempre uma versão preliminar do produto que satisfaça as necessidades actuais, e que este seja actualizado consoante as exigências que vão surgindo.

A melhor fonte de informação acerca das normas e das actividades em volta do MPEG é o seu sítio na Internet<sup>18</sup>. E porque esta norma é utilizada por muitos, ela continua a crescer através de processos de refinamento e actualização, e a sua conclusão poderá nunca vir a acontecer.

#### 1.1.1.12 Inter e intraframes

Uma sequência de vídeo é simplesmente um conjunto de imagens mostradas em intervalos de tempo muito próximos. A maior parte dessas imagens são normalmente muito semelhantes. Não será então de estranhar que os sistemas de compressão de vídeo, como o MPEG, tirem proveito disso. As técnicas de compressão que, para codificar uma imagem, usam informação de outras são normalmente

<sup>17</sup> Constituído pelas entidades ISO, IEC JTC1, SC2 e WG8.

<sup>18</sup> Sítio do grupo MPEG: <http://www.mpeg.org>

denominadas de “*técnicas interframe*”. Quando ocorre uma grande mudança de uma imagem para a outra, esta técnica não funciona e deverá ser utilizada outra mais adequada. Nesta situação, a técnica a utilizar, “*técnica intraframe*”, deverá ser capaz de tirar proveito de similaridades existentes na própria imagem.

Estas duas técnicas de compressão, *interframe* e *intraframe*, estão previstas no algoritmo de compressão do MPEG. Contudo, também podemos abreviar estes dois nomes para *inter* e *intra*, respectivamente. É ainda usual utilizar o termo *non-intra* em vez de *inter*.

### 1.1.1.13 Macroblock

Chama-se *macroblock* ao bloco mais elementar de uma imagem MPEG. Um *macroblock* é constituído por uma grelha 16×16 de amostras de *luminance* e por duas grelhas 8×8, cada uma delas com as amostras dos dois componentes de cor, *chrominance*. A grelha com as amostras de *luminance* é constituída por quatro blocos 8×8. E são todos esses blocos 8×8 que formam a unidade básica de informação usada pelos modelos de compressão.

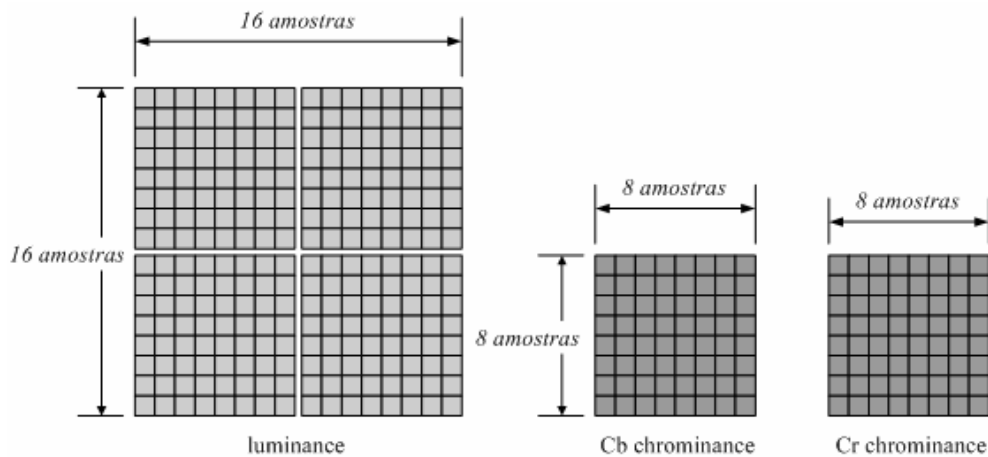


Figura 8. Macroblock MPEG.

### 1.1.1.14 Imagens I-, P- e B-

Cada sequência de vídeo é dividida em um ou mais grupos de imagens, e cada grupo de imagens é composto por uma ou mais imagens de três tipos diferentes, I, P e B. As imagens I (*intra-coded pictures*) são codificadas de forma independente, ou seja, sem referencia a outras imagens. Já as imagens P e B dependem de outras. As imagens P (*predictive-coded pictures*) são deduzidas das anteriores I ou B e não podem ser construídas se o decodificador não tiver decodificado as imagens antecedentes. As imagens B (*bidirectionally predictive-coded pictures*) são obtidas a partir das anteriores e próximas imagens P e I

### 1.1.1.15 Start codes

*Start codes*, tal como o nome sugere, são códigos que marcam o início de determinado segmento de informação num *stream* de vídeo, por exemplo o início de uma imagem ou de um grupo de imagens. Os *start codes* são todos constituídos por 32 *bits*, sendo que os 23 primeiros são zeros e o 24º tem o

valor '1'. Assim, o último *byte*<sup>19</sup> é o mais importante de todos e é ele que realmente identifica um *start code* em particular. O *byte alignment* é sempre obtido uma vez que os *start codes* podem ser precedidos da quantidade de zeros que for necessária para conseguir esse alinhamento. Neste projecto, e como se verá mais à frente, o *start code* das imagens codificadas em MPEG-4<sup>20</sup> foi fundamental para que se conseguísse desenvolver um servidor de *streaming* em que cada pacote RTP transporta uma *frame* do vídeo.

## MPEG-1

*“The MPEG-1 codec targets a bandwidth of 1-1.5 Mbps...”* **Error! Reference source not found.**

A norma MPEG-1 foi a primeira a ser desenvolvida pelo grupo MPEG para codificar vídeo com taxas entre 1 e 1.5 Mbps. Permitindo resoluções de imagem CIF e 30 *frames* por segundo, esta norma requer *hardware* muito dispendioso para efectuar codificação em tempo real. A grande quantidade de dependências entre as *frames* do vídeo leva a que a qualidade da imagem seja muito influenciada pela perda de pacotes. Mantendo-se popular durante muitos anos, a norma MPEG-1 foi pioneira na revolução multimédia dos computadores. MPEG-1 é actualmente uma norma em desuso e pode apenas ser lembrada pelo popular formato de áudio MP3 que deriva de “MPEG-1 audio layer 3”.

## MPEG-2

*“MPEG-2 is typically used to encode audio and video for broadcast signals...”*

MPEG-2 é a designação usada para uma norma de compressão de áudio e vídeo também desenvolvida pelo MPEG. O MPEG-2 é o sucessor do MPEG-1, e foi inicialmente projectado para suportar débitos de transmissão elevados, imagens grandes e *interlaced frames*. O algoritmo de compressão de vídeo disponibilizado por esta norma permite codificação com *bit rates* elevados através da remoção da redundância temporal e espacial presente nas sequências de vídeo. A redundância temporal ocorre quando existem sucessivas imagens iguais. Já a redundância espacial deve-se à replicação de *pixels* numa imagem. Permitindo uma boa compressão de vídeo através de algoritmos normalizados esta norma é tipicamente utilizado para codificação de sinais destinados a *broadcast*, incluindo a TV por cabo e a televisão de alta definição (HDTV). O MPEG-2 pode também ser utilizado em comunicações por satélite, redes com ou sem fios, cinema digital, armazenamento em suportes digitais, sistemas de videoconferência, entre muitos outros.

MPEG-2 é certamente a norma de compressão de áudio e vídeo mais desenvolvida e por isso mais conhecida e utilizada quer pelos produtores quer pelos consumidores de multimédia.

### 1.1.1.16 Multiplexagem MPEG-2

A norma MPEG-2 também define a forma como os vários componentes multimédia são combinados num único *stream* sincronizado. O processo de combinar todos os componentes é conhecido como “multiplexagem”.

Os componentes são conhecidos como *Elementary Stream* e dizem respeito a dados de vídeo, áudio, controlo, entre outros. À combinação de *Elementary Streams* chama-se *Programme*. Cada *Elementary*

<sup>19</sup> Denominado de *start code value* no MPEG-2.

<sup>20</sup> *Start code* representado por 0x000001B6, em hexa-décimal.

*Streams* é enviado para o codificador que por sua vez acumula a informação em pacotes PES (*Packetised Elementary Stream*).



Figura -9. Dois *elementary streams* multiplexados no mesmo *stream* MPEG-2

MPEG-2 permite duas formas de multiplexagem que originam dois tipos de *streams* diferentes:

- **MPEG Program Stream.** Cada *Program Stream* transporta um grupo de PES com o mesmo *Timestamp*. Utiliza-se em situações onde se pretende apenas guardar o *stream* ou em ambientes que garantem poucos erros de transmissão.
- **MPEG Transport Stream.** Consiste em dividir os *Packetised Elementary Streams* em unidades de tamanho fixo. Esta técnica é usada para transmissões em que existe probabilidade de perder muitos pacotes. Cada *Transport Stream* é constituído por um *header* de 32 bits e por um *payload* (de acordo com a Figura 10).

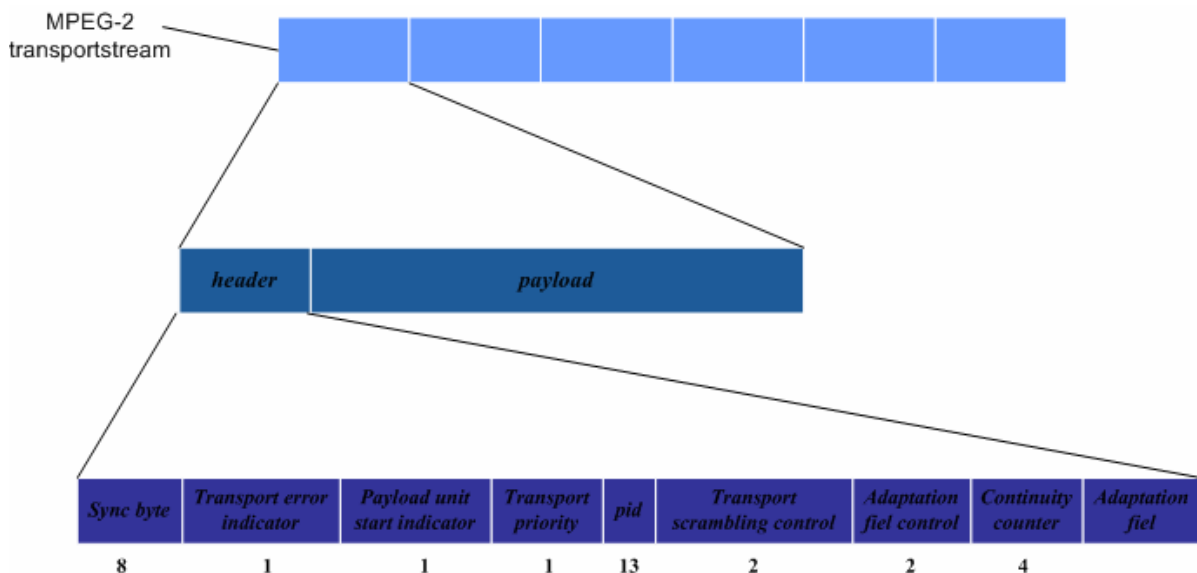


Figura 10. Constituição do *header* de cada *transport stream*.

## MPEG-3

“MPEG-3 was designed to handle [HDTV](#) signals... Shortly thereafter, work on MPEG-3 was discontinued”**Error! Reference source not found.**

O MPEG-3 foi inicialmente previsto para codificar sinais HDTV. Contudo, foi descoberto que resultados semelhantes poderiam ser alcançados fazendo ligeiras alterações ao MPEG-2. Assim, os trabalhos com o MPEG-3 foram abandonados. A sigla MPEG-3 é muitas vezes confundida com MP3, porém, e tal como já foi referido no sub-capítulo 0, MP3 diz respeito ao “MPEG-1 Audio Layer 3”.

## MPEG-4<sup>21</sup>

“MPEG-4 absorbs many of the features of [MPEG-1](#) and [MPEG-2](#)... adding new features such as... various types of interactivity.”

MPEG-4 é uma norma de compressão bastante recente e que está a ser cada vez mais utilizada. Decidimos descreve-la com maior detalhe pela razão referida e porque é a norma que vamos utilizar nos testes de *streaming*.

MPEG-4 é o resultado de muitos anos de trabalho partilhado por centenas de entidades, em particular MPEG, ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*). Nenhuma outra tecnologia tem o potencial de se tornar, tão rapidamente, a mais usada por múltiplas indústrias e utilizadores. É também a única norma capaz de enfrentar e acompanhar a era da “revolução digital”, desdobrando facilmente os conteúdos de multimédia para qualquer tipo de plataformas. A compressão MPEG-4 permite a distribuição de conteúdos áudio e vídeo através de redes fixas ou móveis com muita ou pouca largura de banda. MPEG-4 fornece um conjunto de ferramentas *open source* para codificar, de várias formas, todos os tipos de multimédia incluindo imagens, animações, objectos 2D (*2-Dimensional*) e 3D (*3-Dimensional*) os quais podem ser apresentados de forma interactiva e personalizada. A tecnologia MPEG-4 adapta-se a qualquer largura de banda, e o *software* que a implementa é facilmente acessível através de Internet.

MPEG-4 vem revolucionar os sistemas de multimédia, pelas novas experiências e funcionalidades que proporciona. Ao mesmo tempo, é parte de uma evolução progressiva, pois funciona sobre estruturas existentes, incluindo ambientes MPEG-2.

### 1.1.1.17 Interactividade

MPEG-4 é uma norma “object-based”, permitindo uma interacção separada com cada um dos objectos que forma uma imagem. É possível construir cenas de multimédia, as quais revolucionam todas as possibilidades de interactividade. Os autores de um vídeo podem permitir que os utilizadores finais interajam com os objectos da cena: para mudar a cor de um carro, escolher o melhor ângulo de visão ou etiquetar um jogador de futebol para mais facilmente observar os seus movimentos.

Com o MPEG-4 é possível realizar programas interactivos. Por exemplo, o utilizador pode navegar interactivamente através das filmagens de um evento desportivo, seleccionar as informações que mais lhe agradam, ouvir comentários e ver determinado anúncio publicitário. Tudo isto com apenas um *stream* de vídeo onde os objectos estão codificados separadamente. Este mesmo estilo de interactividade pode ser usado em DVDs ou em *streaming*, algo que até há bem pouco tempo era impossível.

### 1.1.1.18 Evolução e compatibilidade

“*in with the new – out with the old*”. Esta é uma das teorias com a qual o MPEG-4 não convive, pois o seu desenvolvimento é feito de maneira a garantir uma integração nos outros ambientes já desenvolvidos. Foi por isso que o grupo MPEG especificou métodos de incorporar conteúdos MPEG-4 em *streams* MPEG-2 e planeou a melhor forma de transportar MPEG-4 através de pacotes RTP.

MPEG-4 é uma norma dinâmica. A primeira parte<sup>22</sup> foi publicada em 1999, e o trabalho continua. Uma vez que o MPEG-4 não pretende acabar com as normas que já existem, todas as alterações que ocorrem são sempre feitas com garantia de compatibilidade. As alterações são sempre feitas de modo

<sup>21</sup> Sítio do fórum MPEG-4 (The MPEG-4 Industry Forum): <http://www.m4if.org>

<sup>22</sup> Part 1 (ISO/IEC 14496-1): Systems: Describes synchronization and multiplexing of video and audio.

adicional, e geralmente consistem em adicionar uma nova parte à norma. Existem dois tipos de alterações: as que adicionam novas funcionalidades e as que aperfeiçoam o que já existe.

### 1.1.1.19 A aceitação da norma

MPEG-4 tem sido progressivamente adoptado por um grande número de indústrias, quebrando até algumas barreiras que impediam o desenvolvimento de uma tecnologia como esta. É já a norma usada nas comunicações de multimédia dos terminais 3G (*3rd Generation*). Actualmente os grupos mais envolvidos no desenvolvimento da televisão digital estão a discutir a sua integração nesta área. Alguns serviços de *streaming*, como o “QuickTime” ou o “RealNetworks”, também já adoptaram o MPEG-4. De facto, a maioria, se não todos os maiores *players* que suportam *streaming* descodificam MPEG-4 de forma nativa ou através de *plug-ins*. O “Quicktime” e o “RealNetworks” descodificam MPEG-4 de forma nativa e o “Windows Media Player” tem ao seu dispor uma série de *plug-ins* que permitem a integração de MPEG-4.

Em termos de *hardware*, diversos construtores desenvolvem os seus equipamentos com suporte para MPEG-4. Muitas das câmaras digitais disponíveis no mercado permitem codificação MPEG-4 das imagens capturadas. Também muitos dos equipamentos domésticos de DVD estão configurados para suporte de MPEG-4, mas nunca deixando de lado as normas já existentes, sobretudo o MPEG-2.

### 1.1.1.20 Perspectiva tecnológica

A melhor forma de perceber o novo paradigma MPEG-4 é comparando-o com o MPEG-2. No mundo MPEG-2 os conteúdos podem ser criados a partir de vários recursos tais como vídeo, áudio, gráficos e texto. Mas após a digitalização todos os objectos são codificados em conjunto. MPEG-2 oferece uma apresentação estática das imagens. É possível adicionar gráficos e texto à apresentação final das imagens, mas é impossível eliminar esses elementos.

O modelo MPEG-4 revoluciona tudo isto. É dinâmico, em vez de estático. Diferentes objectos podem ser codificados e enviados separadamente para o descodificador. A composição final da imagem é feita depois da descodificação (*after decoding*) e não antes da codificação (*before encoding*). A mesma ideia é válida para composições de áudio, todavia o conceito é mais fácil de explicar para imagens.

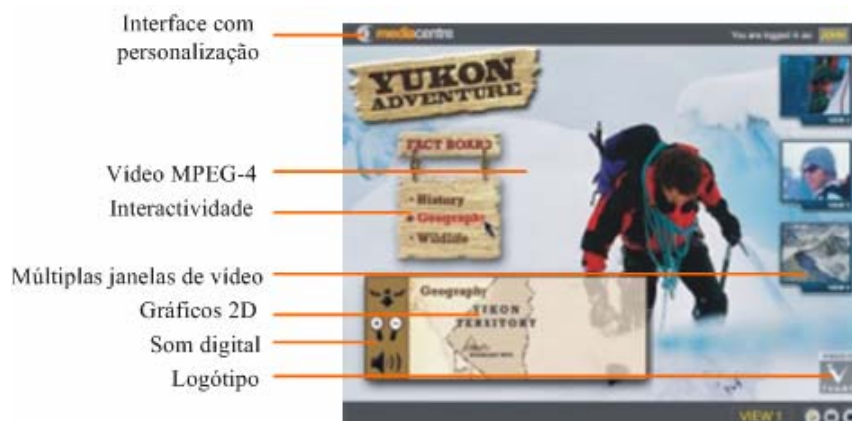


Figura 11. Cena MPEG-4 com múltiplos objectos.

De modo a conseguir efectuar este tipo de codificação, MPEG-4 recorre a uma linguagem específica para descrição de imagens, BiFS (*Binary Format for Scenes*). A linguagem BiFS descreve onde e quando os objectos aparecem na cena e também os seus comportamentos. Os objectos actuam em resposta a determinado evento, usualmente um *input* do utilizador, provocando assim a tal interactividade. Todos os objectos são codificados com o seu próprio esquema de codificação: vídeo é

codificado como vídeo, áudio como áudio, texto como texto, gráficos como gráficos, em vez de se codificar todos os *pixels* de igual forma. Assim, o MPEG-4 inclui diferentes codificadores para cada tipo de informação.

### 1.1.1.21 Profiles

MPEG-4 é constituído por um imenso número de ferramentas, e nem todas são úteis para determinadas aplicações. Por isso existem grupos de ferramentas denominados de *profiles* que permitem aos utilizadores escolher apenas os conjuntos que contêm as funcionalidades que lhes interessam.

### 1.1.1.22 MPEG-4 parts

MPEG-4, e à semelhança de outras normas como o MPEG-2, é constituído por diversas partes (*parts*) que podem ser implementadas individualmente ou combinadas umas com as outras (por exemplo, a parte de áudio pode ser implementada separadamente). Os *profiles* podem ser definidos dentro dessas partes, ou seja, ao implementarmos um *profile* poderemos não estar a implementar uma parte completa. Até ao momento foram desenvolvidas 22 partes na norma MPEG-4.

## MPEG e o futuro

Actualmente estão a ser desenhadas duas normas, MPEG-7 e MPEG-21, que constituem um conjunto de ferramentas capazes de adicionar novas funcionalidades inovadoras para a manipulação dos conteúdos de multimédia. Ambas estão a ser desenvolvidas de maneira a funcionarem em conjunto com o MPEG-4. As descrições e meta dados do MPEG-7 podem ser transportadas nos *streams* MPEG-4, e as especificações do MPEG-21 estão a ser escritas para complementar a representação de conteúdos MPEG-4.

### 1.1.1.23 MPEG-7

*“...it offers metadata information for áudio and vídeo files”*

Em Outubro de 1996, MPEG iniciou um novo projecto designado “Multimedia Content Discription Interface” e também conhecido como MPEG-7 que tem por objectivo proporcionar um conjunto de ferramentas para descrever os conteúdos de multimédia. Será usado para indexar, catalogar e proporcionar pesquisas avançadas nos ficheiros de multimédia. MPEG-7 não é uma norma que lida directamente com a codificação de vídeo ou áudio, como o MPEG-1, MPEG-2 e MPEG-4. Esta norma usa XML<sup>23</sup> (*Extensible Markup Language*) para adicionar meta dados, tais como título, ano de produção, legendas ou créditos, aos vídeos e sons. Actualmente é possível procurar um determinado filme numa rede, através do seu nome. Mas, o objectivo chave do MPEG-7 é fazer com que seja possível procurar determinados objectos ou cenas dentro desses filmes. Por exemplo nos filmes que têm muitas cenas com explosões, o MPEG-7 pode ser usado para indexar essas cenas. Assim, utilizando uma simples pesquisa de texto, podemos encontrar todas essas cenas de explosões, inclusive em vários filmes. Nos ficheiros de áudio o processo é idêntico, sendo possível indexar determinadas palavras da letra da música, para facilmente as podermos encontrar através de uma simples pesquisa.

---

<sup>23</sup> W3C Recommendation, 6 October 2000.

A combinação do MPEG-4 e do MPEG-7 é designada pelo MPEG como “*Tools for Killer Applications*”. A combinação destas duas normas é vista como a solução ideal para *streaming*, manipulação e indexação de conteúdos.

MPEG-7 está ainda em processo de desenvolvimento e espera-se que em poucos anos seja possível ter acesso a todas as suas funcionalidades.

#### **1.1.1.24 MPEG-21**

*“...the vision for MPEG-21 is to define a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices...”*

Actualmente, existem muitos elementos que definem uma infra-estrutura para comunicações multimédia, desde as redes aos equipamentos terminais passando pelas diferentes aplicações de envio e visualização dos dados. Porém, não existe nenhum mecanismo que descreva a forma de como todos esses elementos se relacionam entre si. O objectivo do MPEG-21 é descrever o modo de como esses elementos se relacionam, através de uma norma que proporciona uma utilização transparente dos conteúdos multimédia nas várias redes e pelas diferentes comunidades de utilizadores.

Especificamente, o MPEG-21 pretende regulamentar os direitos dos conteúdos digitais que são partilhados entre os criadores e os consumidores. Esta norma irá fornecer uma ferramenta que permite aos utilizadores expressarem os seus direitos e interesses sobre determinado conteúdo.

### ***Streaming multimédia***

*“Streaming media is [media](#) that is consumed (read, heard, viewed) while it is being delivered”*

Uma técnica que vem assumindo grande importância na área da multimédia é a denominada “*media streaming*”. Esta técnica consiste, basicamente, em uma forma de possibilitar a reprodução de dados multimédia em tempo real, sem a necessidade de aguardar a transferência completa do ficheiro. Até há bem pouco tempo, a reprodução remota de um ficheiro de vídeo ou áudio envolvia, necessariamente, a transferência completa do mesmo para um disco local, antes do início da sua reprodução. Quando a duração do vídeo ou áudio é muita longa, a espera pela sua transferência pode demorar vários minutos, tornando-se assim bastante desconfortável. Informação multimédia é, normalmente, aquela que se armazena em livros, CDs, DVDs. A sua vertente de *streaming* é, por outro lado, associada à radio, televisão ou mais recentemente a redes de computadores com ou sem fios.

### **História**

As tentativas de exibir informação multimédia nos computadores remetem-nos para os primeiros anos da computação, na segunda metade do século XX. Contudo, durante várias décadas muito pouco foi feito nesta área, especialmente devido aos elevados custos e limitação a nível de *hardware*. Na década de 70, experiências académicas provaram que o *streaming* de multimédia era perfeitamente praticável nos computadores. Na segunda metade da década de 80, os computadores tornaram-se suficientemente eficazes, com a introdução de processadores mais potentes e sistemas operativos mais fiáveis em termos de latência, para permitirem a visualização de multimédia. Mas apesar da evolução tecnológica dos computadores, as redes informáticas continuavam a ser muito limitadas para fins de distribuição multimédia. Foi nos anos 90 que as técnicas de *streaming* começaram a ganhar terreno, graças ao aumento da largura de banda nas redes, ao crescimento das ligações à Internet e ao aparecimento de protocolos normalizados (TCP/IP, HTTP). Este avanço nas redes de computadores em conjunto com



os poderosos computadores pessoais, e modernos sistemas operativos tornam o *streaming* de multimédia acessível ao mais comum dos utilizadores.

## Tecnologia envolvida

Um sistema de *streaming* resulta da combinação de várias tecnologias. As câmaras de vídeo e os gravadores de áudio criam informação RAW<sup>24</sup>. Os servidores são utilizados para armazenar os ficheiros de multimédia e torna-los disponíveis. Os clientes retiram esses ficheiros do servidor e mostram-nos aos utilizadores. Servidores e clientes comunicam entre si utilizando protocolos específicos. A informação multimédia é, normalmente, comprimida para fins de armazenamento ou de *streaming*. Utilizam-se *codecs* (*encoding*, *decoding*) para codificar e decodificar os dados.

Podemos assim, reter várias tecnologias: os equipamentos de captura, os servidores, os clientes, os protocolos de comunicação, os codificadores e decodificadores e os vários tipos de formatos codificados.

## Tipos de streaming

À semelhança de muitas outras aplicações de rede que envolvem clientes e servidores, também as técnicas de *streaming* permitem dois tipos de comunicação bem conhecidos, *unicast* e *multicast*. Quando a comunicação é feita apenas entre duas entidades, um servidor e um cliente, então estamos a falar de *unicast*. Neste tipo a comunicação é, normalmente, controlada pelo cliente. *Multicast* aplica-se quando o servidor envia os dados para vários clientes em simultâneo. Também aqui cada cliente pode controlar a transmissão que lhe diz respeito. No entanto, este tipo de transmissão pode por vezes ser associado a difusão, onde os clientes simplesmente se limitam a receber os dados sem qualquer controle sobre eles.

## Técnicas de streaming

Existem três técnicas para aceder a conteúdos multimédia<sup>25</sup> através de uma rede de computadores: *Downloading*, *True Streaming* e *Progressive Downloading*.

### 1.1.1.25 Downloading

Nesta técnica o utilizador efectua o *download* completo do ficheiro, que é gravado no disco (normalmente numa directoria temporária), e posteriormente abre-o e visualiza-o. Esta técnica tem a vantagem de se poder aceder mais rapidamente a determinadas partes do ficheiro, aquando da sua reprodução. Mas tem, no entanto, a grande desvantagem de termos que esperar pela transferência completa do ficheiro antes de podermos iniciar a sua visualização. Se o ficheiro for relativamente pequeno, isto pode não ser um grande inconveniente, mas se for muito grande torna-se certamente uma espera muito aborrecida. A melhor forma de disponibilizar ficheiros de multimédia com esta técnica é através de *hyperlink's* em páginas *Web*, ou através da inclusão do ficheiro no próprio código HTML (*HyperText Mark-up Language*).

Contudo, é importante deixar claro que, tecnicamente, esta não é verdadeiramente uma técnica de *streaming*, mas sim uma técnica normal de *download*. Apenas o facto de envolver transferência e multimédia, leva a que se considere como técnica de *streaming*.

---

<sup>24</sup> Dados não processados, capturados directamente do sensor (informação no seu estado natural).

<sup>25</sup> Vídeo, áudio ou outro tipo de animações.

### **1.1.1.26 True Streaming**

A técnica de *True Streaming* obriga à existência de novos servidores especialmente concebidos para disponibilizarem conteúdos multimédia. Esta obrigação deve-se às limitações dos actuais servidores *Web* que não têm a capacidade de transportar vídeo e áudio em tempo real. O funcionamento desta técnica é bem diferente da anterior, pois aqui o utilizador pode iniciar a visualização do ficheiro imediatamente após o início da sua transferência. De facto, o ficheiro é enviado de tal forma que o utilizador consegue visualizá-lo à medida que este chega. No entanto, em situações de congestionamento da rede, a reprodução é momentaneamente congelada. A grande vantagem é que não existe espera. *True Streaming* é uma técnica extremamente importante quando pretendemos transmitir determinados eventos em directo, tais como conferências ou eventos desportivos. É também possível o envio de conteúdos multimédia que estejam gravados em ficheiro no servidor.

### **1.1.1.27 Progressive Download**

Esta técnica é vista como uma simulação de *True Streaming*, mas não contempla todas as suas vantagens. Consiste também no *download* completo do ficheiro, mas permitindo a visualização das partes que vão sendo recebidas.

Esta técnica é mais simples, pois não exige grandes mudanças na forma de funcionamento dos actuais servidores *Web*. Contudo, apresenta uma grande desvantagem quando comparada com a técnica anterior, pois ao contrário dos servidores *Web*, os servidores de multimédia podem adaptar a transmissão à qualidade da ligação, alterando dinamicamente as taxas de transmissão de vídeo. Usualmente, são utilizadas “*applets Java*”<sup>26</sup> para implementar clientes que reproduzem a informação ao mesmo tempo que esta é recebida. Já, a técnica anterior exige a utilização de programas específicos que o utilizador tem de instalar obrigatoriamente antes de iniciar a recepção dos dados. Para facilitar a reprodução de vídeo ou áudio através dos *browsers* de Internet, esta técnica utiliza, normalmente, as tecnologias de “*helper application*”<sup>27</sup> ou de “*plugin*”<sup>28</sup>, existentes nos principais *browsers*.

### **1.1.1.28 HTTP streaming**

Esta é a forma mais simples e económica para enviar multimédia a partir de um *Website*. A utilização de HTTP streaming torna-se mais acessível especialmente para entidades de pequenas dimensões, que desta forma não precisam de investir em servidores especializados em streaming. Para esta técnica não é necessário nenhum tipo especial de alojamento ou *Website*. Basta apenas colocar os ficheiros de multimédia no servidor, e criar uma página com ligações para os mesmos.

É, no entanto, importante ter em mente as limitações do HTTP streaming:

- HTTP streaming é uma boa opção para *websites* com pouco tráfego, ou seja, *websites* onde no máximo cerca de dez pessoas acedam simultaneamente ao ficheiro. Para situações de maior tráfego deve optar-se por uma solução mais séria de streaming, um servidor especialmente concebido para o efeito.

---

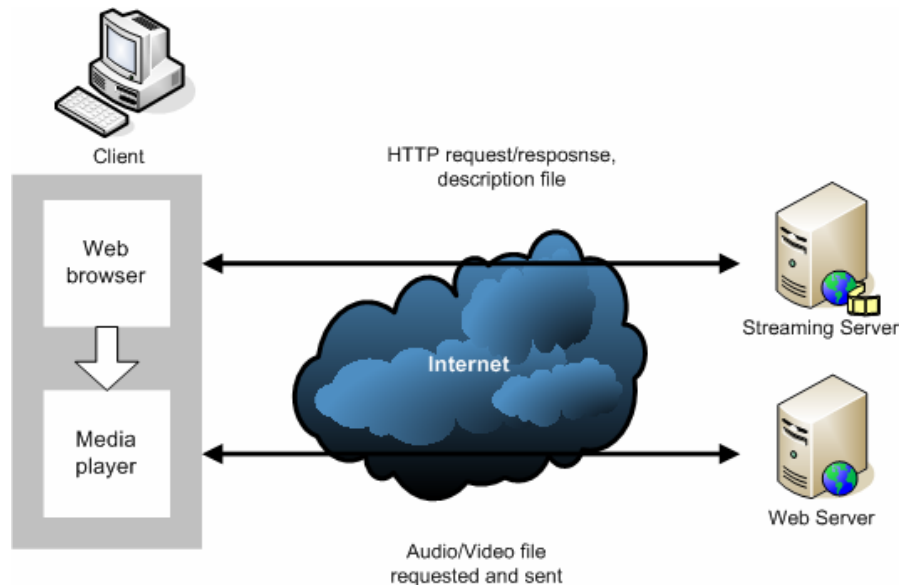
<sup>26</sup> Desenvolvidas em linguagem Java e utilizadas para fornecer aos *browsers* funcionalidades interactivas que não podem ser fornecidas pelo HTML.

<sup>27</sup> Um “*helper application*” é uma pequena aplicação chamada a partir do *browser*, e que apresenta a informação multimédia numa janela separada.

<sup>28</sup> Um “*plugin*” é ligeiramente diferente do “*helper application*”, pois possui a capacidade de reproduzir os dados dentro da janela do próprio *browser*.

- É impossível efectuar *streaming* de vídeos em directo, uma vez que este método apenas funciona para ficheiros que estejam gravados no servidor HTTP.
- Não é possível detectar o tipo e a velocidade da ligação que chega ao utilizador usando HTTP. Assim, se queremos ter várias versões dos conteúdos de acordo com as várias velocidades existentes, temos obrigatoriamente que armazenar diferentes ficheiros para cada velocidade.

Este tipo de *streaming* é muito simples de implementar. Para isso basta codificar um ficheiro, por exemplo de vídeo, num dos formatos conhecidos, coloca-lo no servidor e estabelecer um *hyperlink* que lhe dê acesso. Assim, quando o utilizador “clica” no *hyperlink*, o seu *player* de vídeo entra em funcionamento iniciando a sua reprodução.



**Figura -12.** Diferença entre *streaming* através de *Streaming Server* e de *Web Server*.

Todas estas técnicas continuam a ser utilizadas e a existência de uma não desfavorece as outras. Cada uma delas tem vantagens e desvantagens, e por isso a sua escolha depende de caso para caso. Mas a maioria das pessoas optam pelas técnicas que tiram proveito dos servidores *Web* por estarem já familiarizadas com os *browsers*. O protocolo HTTP é utilizado na transferência de páginas *Web*, por isso a transferência de multimédia com este protocolo torna-se simples e sem a necessidade de recorrer a outro *software* adicional.

## Servidores de streaming

### 1.1.1.29 Server-less

A utilização dos tradicionais servidores *Web* para efectuar *streaming* é uma técnica denominada de *server-less*. Ao *streaming* feito através destes servidores chama-se HTTP streaming (ver sub-capítulo 1.1.1.28).

### 1.1.1.30 Server-based

Um servidor de streaming do tipo *server-based* é uma aplicação especializada no envio de conteúdos multimédia, que é normalmente instalada num computador ligado a uma rede, por exemplo a Internet. Este tipo de servidores está associado à técnica de *True Streaming*, uma vez que as outras apenas

simulam *streaming*. Existem inúmeros servidores deste tipo, muitos dos quais encontramos facilmente na Internet em *open source*. Segue-se uma lista com alguns deles.

- **FFmpeg**<sup>29</sup> é um conjunto de programas em *open source* através dos quais é possível gravar, converter e efectuar *streaming* de áudio e vídeo. Foi desenvolvido em “Linux” mas pode ser executado em outros sistemas operativos, nomeadamente o “Windows”. O projecto foi iniciado por [Fabrice Bellard](#), mas actualmente é gerido por Michael Niedermayer. É constituído pelos seguintes componentes:

**ffmpeg**, é uma aplicação de linha de comando que converte um tipo de ficheiro para outro. Pode ser utilizado, por exemplo para converter o formato YUV para MPEG-4. Esta conversão não é mais do que uma técnica de compressão de vídeo. Suporta também codificação em tempo real.

**ffserver**, é utilizado como servidor de HTTP *streaming*. Funcionalidades de comunicação utilizando o protocolo RTSP estão também a ser desenvolvidas.

**ffplay**, é um *player* de multimédia baseado nas livrarias do FFmpeg.

**libavcodec**, é uma livraria que contém todos os codificadores e decodificadores de áudio e vídeo incluídos no FFmpeg.

**libavformat**, é uma livraria que contém geradores de formatos de áudio e vídeo.

- **VideoLAN**<sup>30</sup> é um projecto para *streaming* de multimédia de uma vasta quantidade de formatos de vídeo incluindo MPEG-1, MPEG-2, MPEG-4 e DivX<sup>31,32</sup>. Foi inicialmente desenvolvido no meio académico da escola Francesa de engenharia “École Centrale Paris”<sup>33</sup>. Permite *streaming unicast* e *multicast* em redes de banda larga IPv6 ou IPv4 (*Internet Protocol Version 4*). VideoLAN é um *software* desenvolvido em *open source* sob licença GNU GPL (também conhecido por GPL, *General Public License*). Este projecto também disponibiliza um *player*, VLC (*Video Lan Client*), que pode ser usado para visualizar ficheiros de vídeo provenientes de *streaming* ou apenas de ficheiros locais. Funciona em vários sistemas operativos incluindo “Windows”, “Solaris”, “Linux” e “Mac OS”.
- **FreeJ**<sup>34</sup> é uma plataforma para manipulação de vídeo em tempo real, que permite a combinação de vários *inputs* para produzir efeitos finais. FreeJ permite “misturar” informação proveniente de *webcams*, câmaras de vídeo, televisão e ficheiros de vídeo, imagem e texto. Este servidor pode ser manipulado remotamente através de sessões SSH (*Secure Shell*) e foi desenhado de maneira que vários utilizadores podem aceder simultaneamente às suas configurações. É completamente gratuito e a sua construção foi e continua a ser feita sob licença GNU GPL.
- **Peercasting**<sup>35</sup> é um método de *streaming multicast*, normalmente de áudio e vídeo, que utiliza a tecnologia P2P (*Peer-to-peer*). Pode ser usado para *multicast* comercial ou amador. Funciona com a existência de vários utilizadores ligados à Internet e com este programa a funcionar. Assim quando um utilizador pretende determinado *stream* a rede P2P encaminha-o para outro utilizador que tenha esse *stream*. Contudo Peercasting, sofre de pouca qualidade de serviço especialmente

---

<sup>29</sup> Sítio do FFmpeg: <http://ffmpeg.sourceforge.net>

<sup>30</sup> Sítio do videoLAN: <http://www.videolan.org>

<sup>31</sup> Codec de vídeo desenvolvido por [DivX, Inc.](#), conhecido pelas suas capacidades de converter grandes segmentos de vídeo em tamanhos pequenos.

<sup>32</sup> Sítio do DivX: <http://www.divx.com>

<sup>33</sup> Sítio da École Centrale Paris: <http://www.ecp.fr>

<sup>34</sup> Sítio do FreeJ: <http://freej.org>

<sup>35</sup> Sítio do Peercasting: <http://www.peercast.org>

quando um cliente se desliga durante uma transmissão para outro cliente. Este é também um software gratuito e desenvolvido sob licença GNU GPL e pode ser modificado e distribuído desde que de acordo com as normas desta entidade licenciadora.

- **SHOUTcast**<sup>36</sup> é uma tecnologia *freeware* para streaming de áudio através da Internet (*Internet radio*), desenvolvida pela “NullSoft”. SHOUTcast utiliza codificação MP3 para codificação dos conteúdos áudio que são enviados pelo protocolo HTTP. Este software permite aos utilizadores configurar as suas próprias estações (servidores) de rádio digital. Os ficheiros de áudio produzidos por este servidor podem ser lidos por inúmeros clientes de áudio como o “[Nullsoft Winamp](#)” e o “[Apple iTunes](#)”.

## Largura de banda e tamanho de armazenamento

O tamanho de armazenamento de um ficheiro recebido por streaming é calculado através da largura de banda da ligação e da duração do ficheiro pela seguinte fórmula:

Tamanho de armazenamento (em *mebibyte*) = tamanho (em segundos) × *bitrate* (em *Kbit/s*) / 8,388.608

Onde,

(1 *mebibyte* =  $8 \times 1,048,576$  bits = 8,388.608 *kbits*) **Error! Reference source not found.**

Por exemplo, se se tiver uma hora de vídeo (3600 segundos) codificado a 300 *Kbit/s* então o tamanho de armazenamento será de 128.7 *MiB* [ $(3600 \times 300) / 8,388.608$ ]. Se o vídeo for acedido por mil utilizadores, precisamos de 300 *Mbit/s* de largura de banda ( $300 \text{ Kbit/s} \times 1000 = 300000 \text{ Kbit/s}$ ), o que é equivalente a 128.7 *Mib* por hora.

Mas para tornar os cálculos ainda mais simples, e acima de tudo mais precisos e completos, existe um *Website* que disponibiliza uma página através da qual podemos efectuar os cálculos de acordo com as nossas condições de *streaming*.

## Formatos e *players* de vídeo

Existem muitos formatos de ficheiros que podem ser utilizados para *streaming* de multimédia. Cada um deles tem vantagens e desvantagens, mas as preferências pessoais de cada utilizador acabam por ser o factor mais importante na decisão de usar um ou outro formato. No que diz respeito ao vídeo, considerámos mais importantes os três seguintes formatos: “*Windows media*”, “*Real media*” e “*Quicktime*”. Assim, quando se pretende implementar um servidor de *streaming* deve ter-se em conta que cada utilizador tem a sua preferência e por isso só utiliza determinados formatos. Esta preferência é muitas vezes influenciada pelo *software* que o utilizador tem instalado no seu PC (*Personal Computer*). Por exemplo, se um utilizador não tiver o *software* “*Quicktime Player*” instalado, ele certamente não irá optar pelo formato “*Quicktime*”, mas sim por um cujo *player* esteja no seu computador. O ideal é que o servidor de *streaming* forneça a mesma informação em vários formatos, ou que pelo menos disponibilize os *players* necessários, quando isso é possível.

“*Microsoft*”, “*RealNetworks*” e “*Apple*” usam os seus próprios formatos para codificação de vídeo. No mundo perfeito o ideal era que todos os formatos de vídeo pudessem ser visualizados em todos os *players*. Mas na verdade, os conteúdos gerados por um determinado codificador proprietário podem, normalmente, apenas ser vistos pelo *player* desse mesmo proprietário. Poderão ainda existir incompatibilidades de versão entre os conteúdos e os *players*. Por exemplo, conteúdos codificados com uma versão mais actual de determinado codificador podem não ser compatíveis com um *player* mais antigo do mesmo proprietário. Este problema ocorre com versões do “*RealOne Player*” e do

<sup>36</sup> Sítio do SHOUTcast: <http://www.shoutcast.com>

“Windows Media Player”. De seguida enumeramos alguns dos *players* mais conhecidos, apresentando as suas principais características, vantagens e desvantagens, não deixando de fazer referência aos respectivos formatos de vídeo.

#### 1.1.1.31 Windows Media Player<sup>37</sup>



“Windows Media Player” tem a vantagem de estar protegido pelo maior fabricante de *software*. É uma aposta segura que a “Microsoft” não quererá certamente perder. Quase todas as versões do sistema operativo “Windows” trazem este *player* cujas actualizações são fáceis de realizar. É desenhado no sentido de poder ser controlado através de código HTML, permitindo assim que *browsers* compatíveis o possam utilizar para apresentar elementos multimédia. O desempenho deste *player* é bastante bom e as imagens que produz são, regra geral, de óptima qualidade. A grande desvantagem deste *software* é o facto de ser propriedade da “Microsoft”, e por isso ser desenhado no sentido de funcionar, no seu melhor, em conjunto com outros produtos desta empresa. Esta desvantagem limita a utilização do *player* noutros sistemas operativos bem como noutros *browsers*.

- Vantagens:

Grátis. Todas as aplicações de vídeo da “Microsoft” são gratuitas, e o seu uso é ilimitado;

Fácil integração com o código HTML;

Óptima qualidade de vídeo e áudio acima de 128 Kbps.

- Desvantagens:

Fraca qualidade de áudio quando o *streaming* é feito através de ligações de modem;

É necessário ter o *browser* “Internet Explorer” para visualizar vídeo embutido em código HTML;

Funciona apenas no sistema operativo “Windows” ou em computadores “Macintosh”;

É necessário um *plug-in* para funcionar no *browser* “Netscape”.

#### 1.1.1.32 Real Media Player<sup>38</sup>



“Real Media Player” é propriedade da “RealNetworks”, empresa que tem uma ilustre história e que foi uma das primeiras a desenvolver aplicações de *streaming*. Até a bem pouco tempo os seus formatos de vídeo eram considerados os melhores para esta tecnologia. Actualmente os formatos da “RealNetworks” continuam a ser muito bons, mas começam a perder terreno para outros formatos. As imagens apresentadas pelo *player* tendem a ser pouco definidas e as perdas de detalhe nos vídeos são evidentes. Contudo, a qualidade de imagem é perfeitamente adequada para a maioria das situações. A principal desvantagem é a dificuldade que existe em conseguir uma versão completa do *player*. A “RealNetworks” insiste em manter um modelo comercial dos seus produtos, e por isso disponibiliza apenas versões de demonstração encorajando a compra da versão completa. Este facto tem afastado as

---

<sup>37</sup> Sítio do Windows Media Player: <http://www.windowsmedia.com>

<sup>38</sup> Sítio do Real Media Player: <http://www.realnetworks.com>

peçoas da sua utilização dando vantagem a outros sistemas gratuitos. Apesar de tudo, o “*Real Media Player*” continua a ser dos poucos *software* que funciona em qualquer sistema operativo.

- Vantagens:

É o formato de vídeo mais utilizado em *streaming*;

Excelente qualidade em ligações através de modem. Em muitos casos, garante a melhor qualidade de *streaming* possível;

O servidor da “*RealNetworks*” permite fazer *streaming* dos três principais formatos (*WindowsMedia*, *QuickTime* e *RealMedia*).

- Desvantagens:

O custo. São disponibilizadas apenas versões de demonstração, as versões completas têm de ser pagas.

### 1.1.1.33 Quicktime<sup>39</sup>



#### QuickTime

“*Quicktime*” é um formato e *player* de vídeo que merece o devido respeito, até porque o seu aparecimento remete-nos ao início das produções de vídeo digital. “*Quicktime*” é, em muitos aspectos, mais complicado do que o “*Windows Media Player*” e do que o “*Real Media Player*”, mas para a maioria dos produtores e utilizadores de vídeo digital as complexidades não são obstáculo. Se explorarmos as opções avançadas do “*Quicktime*” descobrimos que é possível criar vídeo interactivo ou mesmo efeitos de realidade virtual. As ferramentas “*Quicktime*”, nomeadamente o seu *player*, são consideradas as melhores no que diz respeito ao tratamento de vídeo. No entanto, torna-se um desafio explorar todas as suas potencialidades únicas, e é por isso que muitas pessoas optam por algo menos complexo. A sua integração com outros produtos é uma das suas principais vantagens.

- Vantagens:

Excelente qualidade de reprodução de vídeo em ligações de banda larga (acima de 1 Mbps);

O *player* permite visualizar vários formatos de video;

Suporta imagens panorâmicas de 360° e objectos 3D.

- Desvantagens:

Fraca qualidade de *streaming* em tempo real, especialmente quando a ligação não permite débitos superiores a 1 Mbps.

A tabela seguinte apresenta algumas comparações em os *players* referidos:

| Player | Compatibilidade | Formatos | Compatibilidade de browsers | Disponibilidade |
|--------|-----------------|----------|-----------------------------|-----------------|
|--------|-----------------|----------|-----------------------------|-----------------|

<sup>39</sup> Sítio do QuickTime: <http://www.apple.com/quicktime>

|                             |                                                                                                                  |                                                       |                                                                                                                                         |                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b>Windows Media Player</b> | Todas as versões do Windows, Mac OS 8.1/9.x, Mac OSX, Pocket PC, Solaris, HP HandHeld, Casio Palm, Compact Palm. | WMV, WMA, WAV, AVI, MPEG-1, MPEG-2, MPEG-4, MP3.      | Internet Explorer 5.0 +, Netscape 4 + (necessário <i>plug-in</i> adicional), Mozilla (com o mesmo <i>plug-in</i> utilizado no Netscape) | Gratuito.                |
| <b>Real Media Player</b>    | Todas as versões do Windows, Linux, Mac OSX, Pocket PC, Solaris.                                                 | RealPix, RealText, MPEG-1, MPEG-2, MPEG-4, AVI, SMIL. | Internet Explorer, Netscape, Mozilla, Opera, + vários browsers do Linux.                                                                | Gratuito em versão demo. |
| <b>QuickTime</b>            | Todas as versões Windows e Macintosh.                                                                            | MOV, MPEG-1, MPEG-2, AVI, SMIL, + outros.             | Internet Explorer, Netscape, Mozilla.                                                                                                   | Gratuito em versão demo. |

Tabela 0-2. Diferenças entre *players* de vídeo.

#### 1.1.1.34 Flash player<sup>40</sup>



O mundo do *streaming* tem sido dominado maioritariamente pelos três sistemas que acabamos de referir. No então tal domínio não durará para sempre.

Com a nova versão “Flash Player 7”, a “Macromedia Flash” tem ganho cada vez mais presença na área do *streaming* de vídeo. Apesar de toda a sua difícil utilização, o “Flash” tem sido cada vez mais utilizado na criação de conteúdos multimédia. Tem as desvantagens de ser caro e de não ser fácil de utilizar. No entanto, quem dedicar muitas horas a aprender tudo sobre o seu funcionamento, irá certamente descobrir que o “Flash” proporciona uma enorme flexibilidade capaz de produzir conteúdos de multimédia que vão para além dos sonhos. Menus criativos, integração dinâmica em páginas *Web*, vídeos e animações interactivas, são só algumas das potencialidades que o “Flash” permite.

<sup>40</sup> Sítio do Flash Player: <http://www.macromedia.com/software/flashplayer>



## Protocolos envolvidos

Desenvolver um protocolo de transporte para fins de *streaming* é um grande desafio, especialmente pela sensibilidade dos dados de vídeo ou áudio.

Os protocolos de transporte mais conhecidos, como o UDP, permitem enviar os dados de multimédia em forma de pequenos pacotes. Esta é uma técnica simples e eficiente, mas que pode originar muitas perdas. Contudo, os clientes de streaming utilizam, normalmente, técnicas de detecção e correcção de erros.

Já os protocolos RTP, RTCP e RTSP foram especialmente desenhados para efeitos de *streaming* através da rede e todos eles são encapsulados no UDP.

Os protocolos seguros, tal como o TCP, garantem a entrega de cada um dos bits que constituem a informação enviada. Tal garantia é conseguida através de mecanismos de retransmissão, os quais são complexos de implementar e provocam algum atraso indesejável em sistemas de *streaming*.

Os protocolos *unicast* enviam uma cópia dos dados, do servidor para o cliente. Esta técnica é simples mas pode originar uma duplicação massiva da informação na rede. Os protocolos *multicast* comprometem-se a enviar para a rede apenas uma cópia da informação, isto é, nas ligações entre os *routers* não circula informação redundante. Esta é uma forma de gerir a rede eficientemente, mas requer muita complexidade na implementação.

Os protocolos P2P são preparados para troca de informação entre dois clientes. Ou seja, quando um cliente pretende determinada informação não necessita de aceder ao servidor, mas em vez disso acede a outro cliente que já tenha a informação pretendida. A utilização deste tipo de protocolos permite reduzir o congestionamento nas ligações com os servidores.

Concluimos assim que, nas comunicações de *streaming* podemos utilizar vários protocolos, sendo que a escolha dos mesmos depende essencialmente das nossas necessidades.

## Passos básicos para efectuar streaming de vídeo

Existem quatro passos fundamentais para disponibilizar ficheiros de vídeo através de uma rede. Cada um deles poderá ser mais ou menos complexo de acordo com a qualidade que pretendemos alcançar.

**Gravação:** os conteúdos de vídeo podem ser captados através dos meios tradicionais, tal como as câmaras de vídeo ou os gravadores VCR. Contudo, a qualidade do equipamento ou a técnica de filmagem poderá influenciar a qualidade final do vídeo. **Error! Reference source not found.**

**Digitalização:** o vídeo resultante da gravação tem de ser digitalizado. Normalmente utiliza-se um cabo S-video (*Separated video*) para ligar o equipamento de gravação ao computador e software de edição de vídeo como o *Adobe Premier Plus*<sup>41</sup>. Actualmente já existem alguns equipamentos que capturam o vídeo e convertem-no imediatamente para formato digital. Nesse caso este passo é omitido.

**Compressão e codificação:** o vídeo resultante é, normalmente, demasiado grande para ser transmitido através de uma rede, por isso o ficheiro deve ser alterado para reduzir o seu tamanho. Assim, é necessário utilizar um software de compressão de vídeo, mas apenas depois de se decidir qual a norma de compressão a utilizar (MPEG-2, MPEG-4, H264, entre outros). Este passo é omitido se os equipamentos de captura também comprimirem o vídeo. **Error! Reference source not found.**

**Streaming:** após a digitalização e compressão do ficheiro de vídeo, este deverá ser colocado num servidor de *streaming* para assim poder ser distribuído pela rede.

---

<sup>41</sup> Sítio do Adobe Premier Plus: <http://www.adobe.com/products/premiere>

## Streaming em redes sem fios

As ligações sem fios são bastante diferentes das convencionais com fios, especialmente pelas limitações de largura de banda e dos terminais móveis. Por isso o *Streaming* em redes *wireless* é um grande desafio, tanto para conseguir uma boa ligação entre o emissor e o receptor, como para escolher o método de compressão mais adequado, nomeadamente quando as redes oferecem pouca largura de banda. A norma de compressão MPEG-4 promete tornar-se o líder no que diz respeito ao envio de áudio e vídeo para os terminais móveis, tais como telemóveis e PDAs (*Personal Digital Assistants*). A versão 2 do “NetShow”<sup>42</sup>, o “Windows Media Player”, “RealSystem”<sup>43</sup> e “PacketVideo”<sup>44</sup> funcionam já com suporte para MPEG-4. Mas melhor que tudo, esta norma permite a criação de conteúdos que podem ser usados em todo o tipo de equipamentos e sistemas operativos. As tecnologias de vídeo prometem invadir cada vez mais as redes sem fios. As redes de telemóveis 3G foram já projectadas no sentido de levar o *streaming* de vídeo até aos equipamentos móveis.

Muitas das entidades envolvidas no desenvolvimento de tecnologias de streaming (*ActiveSky*, *Emblaze Research*, *Philips Digital Networks*, *RealNetworks*, *Toshiba*, entre outros) estão a levar avante a possibilidade de tornar as suas aplicações executáveis na maioria dos equipamentos móveis. Algumas utilizam algoritmos proprietários baseados em *Java applets*, outras efectuam o *streaming* imediatamente após a compressão dos conteúdos em MPEG-4.

É fundamental a existência de uma forte relação entre os mais populares *softwares* de *streaming* e as características dos equipamentos móveis. Este tipo de aplicações exige muito do hardware dos equipamentos e requer funcionalidades de áudio e vídeo, que até há bem pouco tempo não existiam nos terminais. Assim o sucesso de qualquer dispositivo móvel na reprodução de multimédia passa pelo acréscimo de melhorias no seu hardware: processador mais rápido, mais memória e um monitor a cores. Mas esta não é uma tarefa fácil porque os dispositivos, como funcionam com baterias, têm que utilizar mecanismos de poupança de energia que passam pela redução da potência dispendida no processamento de dados, por isso a codificação do áudio e vídeo deve ser bastante simples para que o decodificador funcione sem problemas nesta condições.

A melhoria da qualidade dos equipamentos móveis e o aumento das velocidades de transmissão levam a que as redes sem fios sejam cada vez mais atractivas pela possibilidade de se aceder a conteúdos multimédia a partir de qualquer lugar. Mas obviamente a dimensão dos equipamentos móveis será sempre uma limitação que não poderá ser ultrapassada. Não faz sentido considerar móvel algo que, apesar de não ter fios, é demasiado grande para transportar.

## Internet Streaming Media Alliance (ISMA)<sup>45</sup>

ISMA constitui uma série de especificações para o *streaming* sobre a Internet. De entre essas especificações destacamos a escolha do MPEG-4 (nomeadamente os *profiles* de áudio e vídeo) como norma de codificação e do RTP como protocolo de *streaming*.

## 3rd Generation Partnership Project (3GPP and 3GPP2)<sup>46</sup>

Estes projectos definem normas para a 3ª geração de redes e serviços móveis e para sistemas baseados em GSM (*Global System for Mobile communications*). Ambos dedicam especial atenção às transmissões multimédia nos sistemas sem fios. Nas suas especificações para redes *wireless*, os

---

<sup>42</sup> Sistema desenvolvido pela Microsoft para *streaming* multimédia através da Internet.

<sup>43</sup> Conjunto de ferramentas para *streaming* multimédia.

<sup>44</sup> Software para *streaming* multimédia em dispositivos móveis.

<sup>45</sup> Sítio do ISMA: <http://www.isma.tv>

<sup>46</sup> Sítio do 3GPP: <http://www.3gpp.org>

projectos 3GPP e 3GPP2, usam o formato MPEG-4 como norma de compressão e os protocolos RTP e RTSP para efectuar o *streaming* dos dados multimédia.

## **Conclusões**

O streaming de multimédia, em especial vídeo e áudio, através das redes de computadores é uma tecnologia que atrai cada vez mais pessoas. Isso é evidenciado pela grande quantidade de organizações e entidades comerciais envolvidas de várias formas na tecnologia. O aspecto chave que origina a existência de um vasto leque de produtos comerciais ou gratuitos diferentes na área do *streaming* é a grande diversidade de infra-estruturas, redes, protocolos e técnicas de compressão.

Cada um dos produtos de *streaming* implementa os seus próprios formatos de vídeo e áudio, sendo que alguns deles podem também utilizar os formatos já normalizados, como o MPEG. A compatibilidade entre os vários produtos torna-se difícil precisamente devido à existência dos formatos proprietários. Mas actualmente, já é usual desenvolver sistemas que permitem a fácil incorporação de *codecs* afim de poderem funcionar com outros formatos de codificação.