



RAFAEL FERNANDO DIORIO

**IMPLEMENTAÇÃO E TESTES DE UM *GATEWAY*
MULTIMÍDIA BASEADO EM IP**

LIMEIRA, SP
2013



UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE TECNOLOGIA

Rafael Fernando Diorio

IMPLEMENTAÇÃO E TESTES DE UM *GATEWAY* MULTIMÍDIA BASEADO EM IP

Orientador: Prof. Dr. Varese Salvador Timóteo

Grupo de Óptica e Modelagem Numérica
GOMNI

Dissertação apresentada à Faculdade de Tecnologia da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Tecnologia, na área de Tecnologia e Inovação.

Este exemplar corresponde à versão final da dissertação defendida pelo aluno Rafael Fernando Diorio e orientada pelo Prof. Dr. Varese Salvador Timóteo.



Prof. Dr. Varese Salvador Timóteo

LIMEIRA, SP
2013

D623i Diorio, Rafael Fernando, 1983-
Implementação e testes de um *gateway* multimídia baseado em IP / Rafael
Fernando Diorio. – Limeira, SP : [s.n.], 2013.

Orientador: Varese Salvador Timóteo.
Dissertação (mestrado) – Universidade Estadual de Campinas, Faculdade de
Tecnologia.

1. TCP/IP. 2. Sistemas multimídia. 3. Software livre. 4. Modelagem de tráfego.
I. Timóteo, Varese Salvador. II. Universidade Estadual de Campinas. Faculdade
de Tecnologia. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Implementation and testing an IP-based multimedia gateway

Palavras-chave em inglês:

TCP/IP

Multimedia systems

Free software

Traffic modeling

Área de concentração: Tecnologia e Inovação

Titulação: Mestre em Tecnologia

Banca examinadora:

Varese Salvador Timóteo [Orientador]

Paulo Sérgio Martins Pedro

Luiz Henrique Bonani do Nascimento

Data de defesa: 06-12-2013

Programa de Pós-Graduação: Tecnologia

DISSERTAÇÃO DE MESTRADO EM TECNOLOGIA
ÁREA DE CONCENTRAÇÃO: TECNOLOGIA E INOVAÇÃO

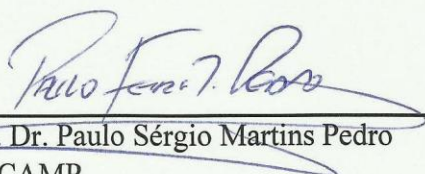
Implementação e testes de um Gateway Multimídia baseado em IP

Rafael Fernando Diorio

A Banca Examinadora composta pelos membros abaixo aprovou esta Dissertação:



Prof. Dr. Varese Salvador Timóteo
UNICAMP
Presidente



Prof. Dr. Paulo Sérgio Martins Pedro
UNICAMP



Prof. Dr. Luiz Henrique Bonani do Nascimento
UFABC

Resumo

A presente dissertação contempla a implementação e validação funcional de um *gateway* multimídia baseado em IP a partir da implementação de recursos para classificação, rotulação, identificação e encaminhamento de fluxos de tráfego distintos (elástico e *stream*), ambos com modelagem de tráfego pré-definida, a partir de informações constantes no cabeçalho dos pacotes IP (campos ToS do IPv4 e TC do IPv6, tidos como DSCP [RFC 2474] e ECN [RFC 3168]) para os serviços multimídia de áudio, voz, vídeo e dados fornecidos por um emulador de tráfego multimídia baseado em IP. De modo complementar a tais implementações, o *gateway* multimídia também objetiva o fornecimento de recursos de qualidade de serviço (QoS) aos serviços por ele intermediados e que necessitem de tais recursos, tais como serviços multimídia de voz e vídeo, por exemplo. Os testes funcionais e de desempenho com o *gateway* multimídia, realizados em ambiente cabeado e sem fio, demonstram que sua implementação é válida e que não influencia em modificações quanto ao perfil (características) dos tráfegos por ele intermediados, bem como à questões envolvendo erros, atrasos e variações de atrasos (*jitter*), dentre outras, demonstrando que sua implementação é transparente aos sistemas finais envolvidos no processo de comunicação intermediado por tal *gateway* multimídia. Seu ambiente de desenvolvimento e testes é baseado em soluções de *software* livre, fornecido, especialmente, pelo sistema operacional Linux e pela solução Netfilter/Iptables, disponibilizando uma plataforma aberta para o estudo e aprimoramento futuro quanto ao *gateway* multimídia. Por fim, espera-se que o *gateway* multimídia contribua como uma nova ferramenta para testes e análises de soluções voltadas às redes multimídia de modo geral.

Palavras chave: TCP/IP; Sistemas multimídia; *Software* livre; Modelagem de tráfego.

Abstract

This dissertation describes the implementation and functional validation of an IP-based multimedia gateway to the identification, classification and forwarding of different traffic flows (elastic and stream), both with pre-defined traffic profiles, from the ToS field of the IPv4 header and the TC field of the IPv6 header, taken as DSCP [RFC 2474] and ECN [RFC 3168]. The multimedia traffic corresponding to audio, voice, video and data services are provided by a multimedia traffic generator, which generates traffic according to given distributions. The multimedia gateway also aims at providing resources for quality of service (QoS) for services that require these resources, such as multimedia services for voice and video. The functional and performance testing with multimedia gateway, performed in a wired and wireless environment, demonstrates that its implementation is valid and not influence in changes in the traffic profile (characteristics) of the traffic intermediated by him, as well as issues involving errors, delays and variations in delay (jitter), among others, showing that its implementation is transparent to the end systems involved in the communication process intermediated by such multimedia gateway. It's development and testing environment is based on open source solutions, based on the Linux operating system and the Netfilter/Iptables solution, providing an open platform for future research and improvement of the multimedia gateway. Finally, it is expected that the multimedia gateway contributes as a new tool for testing and analysis of multimedia networks in general.

Keywords: TCP/IP; Multimedia systems; Free software; Traffic modeling.

Sumário

1 – Introdução.....	1
2 – Redes Multimídia	3
2.1 – Aplicações de Redes Multimídia.....	3
2.1.1 – Fluxo de áudio e vídeo armazenado	4
2.1.2 – Fluxo de áudio e vídeo ao vivo.....	4
2.1.3 – Fluxo de áudio e vídeo interativo de tempo real	5
2.2 – Protocolos de Redes Multimídia	5
2.2.1 – Protocolos TCP, UDP e IP	5
2.2.2 – Protocolos RTP, RTCP e RTSP	8
2.2.3 – Protocolo SIP	9
2.2.4 – Padrão H.323	9
2.3 – Acesso e distribuição de conteúdo <i>stream</i> na Internet	10
2.3.1 – Compressão de áudio e vídeo	13
2.3.2 – Serviço <i>best effort</i> da Internet.....	14
2.3.3 – Redes de distribuição de conteúdos.....	15
2.3.4 – Redes multicast.....	16
2.4 – Algumas considerações para o dimensionamento de redes multimídia	17
3 – Modelos para fontes de tráfego	19
3.1 – Categorias de tráfego	20
3.1.1 – Tráfego de bloco.....	20
3.1.2 – Tráfego de transição <i>on/off</i>	21
3.1.3 – Tráfego <i>stream</i>	21
3.1.4 – Tráfego fractal e multifractal.....	22
3.2 – Funções de distribuição	22
3.2.1 – Distribuição normal	23
3.2.2 – Distribuição exponencial	23
3.2.3 – Distribuição de Poisson (Discreta)	23
3.2.4 – Distribuição de Pareto	24
3.2.5 – Distribuição de Weibull.....	24
4 – Gateway multimídia	25
4.1 – Descrição geral	25
4.2 – Identificação e encaminhamento do tráfego multimídia	27
4.3 – Identificadores para o tráfego multimídia	31
4.4 – Qualidade de serviço (QoS).....	32

4.4.1 – Visão geral.....	32
4.4.2 – Mecanismos de escalonamento e regulação	33
4.4.3 – Algumas considerações	36
4.5 – Classificação e marcação de pacotes IP	37
4.6 – Ambiente e ferramentas de desenvolvimento.....	39
4.6.1 – Identificação e encaminhamento do tráfego multimídia	40
4.6.2 – Qualidade de serviço	41
4.6.3 – Gerador de tráfego multimídia	42
5 – Resultados e discussões	45
5.1 – Validação funcional.....	45
5.1.1 – Classificação e marcação de pacotes IP	45
5.1.2 – Identificação e encaminhamento do tráfego multimídia	61
5.1.3 – Qualidade de serviço	80
5.2 – Validação de desempenho	86
5.2.1 – Perfil de tráfego	86
5.2.2 – Erros, atrasos e variações de atrasos.....	91
5.2.3 – Recursos de rede.....	94
5.2.4 – Recursos de processamento, memória e processos	95
6 – Conclusões.....	99
Referências	101

Dedicatória

Dedico a presente dissertação, especialmente, à minha família, com ênfase à minha filha (Giovana), que representa meu amor incondicional; ao meu pai (Sergio), que me espelhou a ser o que sou e, infelizmente, nos deixou antes da finalização desta dissertação; à minha mãe (Elisie), que, junto de minha filha, é a mulher da minha vida; e, aos meus irmãos (Débora, Felipe e Luana), que não medem esforços para agradar nossa família.

Agradecimentos

Agradeço, especialmente, ao meu orientador (Prof. Varese), por toda sua contribuição, atenção e dedicação; à minha família, pelas condições dadas para que pudesse “chegar até aqui”; aos membros de minha banca de qualificação e defesa, pela atenção e ensinamentos quanto ao meu projeto de pesquisa; aos meus amigos de trabalho e convivência (que por serem vários, prefiro não nomeá-los para não “correr o risco” de deixar de citar alguém), pelo incentivo e momentos de alegria indispensáveis até a conclusão de tal dissertação; e, à UNICAMP, que possibilitou minha inserção em seu concorrido corpo de discentes, viabilizando a realização da presente dissertação de Mestrado.

Lista de Figuras

<i>Figura 1 – Arquitetura TCP/IP e o Modelo de Referência ISO/OSI</i>	6
<i>Figura 2 – Protocolos TCP, UDP e IP</i>	8
<i>Figura 3 – Modelo funcional geral do H.323 (Adaptado de [21, 22])</i>	10
<i>Figura 4 – Transmissão de fluxo de áudio e vídeo armazenado (1) (Fonte: Adaptado de [23])</i>	11
<i>Figura 5 – Transmissão de fluxo de áudio e vídeo armazenado (2) (Fonte: Adaptado de [23])</i>	11
<i>Figura 6 – Utilização de buffers para atenuação de atrasos (Adaptado de [23, 24])</i>	12
<i>Figura 7 – Controle de reprodução de conteúdo multimídia (stream) utilizando o protocolo RTSP (Fonte: Adaptado de [23])</i>	13
<i>Figura 8 – Redes de distribuição de conteúdos (CDNs) (Fonte: Adaptado de [23])</i>	16
<i>Figura 9 – Transmissões unicast (a) versus transmissões multicast (b)</i>	16
<i>Figura 10 – Algumas aplicações e seus tipos de tráfego</i>	19
<i>Figura 11 – Visão geral: Tráfego de bloco (Fonte: Adaptado de [28])</i>	20
<i>Figura 12 – Visão geral: Tráfego de transição on/off (Fonte: Adaptado de [28])</i>	21
<i>Figura 13 – Visão geral: Tráfego stream (Fonte: Adaptado de [28])</i>	21
<i>Figura 14 – Visão geral: Tráfego fractal (Fonte: [29])</i>	22
<i>Figura 15 – Gateway multimídia</i>	25
<i>Figura 16 – Sistemas transmissor e receptor dos serviços de áudio, voz, vídeo e dados (com gateway multimídia)</i>	26
<i>Figura 17 – Visão geral: Estrutura funcional do subsistema de comunicação do gateway multimídia</i>	27
<i>Figura 18 – Formato do datagrama IPv4 (Fonte: Adaptado de RFC 791)</i>	28
<i>Figura 19 – Formato do datagrama IPv6 (Fonte: Adaptado de RFC 2460)</i>	28
<i>Figura 20 – Estrutura dos campos DSCP e ECN no IPv4 e no IPv6 (Fonte: Adaptado dos RFCs 2474 e 3168)</i>	29
<i>Figura 21 – Antigo formato do campo ToS no IPv4 (Fonte: Adaptado de RFC 1349)</i>	29
<i>Figura 22 – Exemplo de cenário para marcação e classificação de pacotes IP</i>	30
<i>Figura 23 – Proposta de organização de bits para o campo DSCP</i>	31
<i>Figura 24 – Disciplina de escalonamento do tipo primeiro a entrar, primeiro a sair</i>	34
<i>Figura 25 – Disciplina de escalonamento do tipo enfileiramento prioritário</i>	34
<i>Figura 26 – Disciplina de escalonamento do tipo enfileiramento justo ponderado</i>	35
<i>Figura 27 – Regulação com leaky bucket algorithm</i>	35
<i>Figura 28 – Regulação com token bucket algorithm</i>	36
<i>Figura 29 – Sistemas transmissor e receptor do conteúdo multimídia (com adaptador de tráfego multimídia e o gateway multimídia)</i>	39

<i>Figura 30 – Estrutura funcional proposta em [21] para o gerador de tráfego multimídia. ...</i>	<i>43</i>
<i>Figura 31 – Interação entre os módulos do gerador de tráfego multimídia (Fonte: [21]).</i>	<i>44</i>
<i>Figura 32 – Ambiente (1) para validação e testes do adaptador de tráfego multimídia.</i>	<i>45</i>
<i>Figura 33 – Ambiente (2) para validação e testes do adaptador de tráfego multimídia.</i>	<i>46</i>
<i>Figura 34 – Endereçamento de rede do ambiente para validação e testes do adaptador de tráfego multimídia.</i>	<i>46</i>
<i>Figura 35 – Saltos (hops) IPv4 entre os hosts transmissor e receptor no ambiente para validação e testes do adaptador de tráfego multimídia.</i>	<i>47</i>
<i>Figura 36 – Saltos (hops) IPv6 entre os hosts transmissor e receptor no ambiente para validação e testes do adaptador de tráfego multimídia.</i>	<i>47</i>
<i>Figura 37 – Definições de DSCP no adaptador de tráfego multimídia para o IPv4 (1).</i>	<i>48</i>
<i>Figura 38 – Definições de DSCP no adaptador de tráfego multimídia para o IPv6 (1).</i>	<i>49</i>
<i>Figura 39 – Tráfego de dados, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>49</i>
<i>Figura 40 – Tráfego de dados, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>50</i>
<i>Figura 41 – Tráfego de áudio, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>51</i>
<i>Figura 42 – Tráfego de áudio, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>51</i>
<i>Figura 43 – Tráfego de voz, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>52</i>
<i>Figura 44 – Tráfego de voz, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>52</i>
<i>Figura 45 – Tráfego de vídeo, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>53</i>
<i>Figura 46 – Tráfego de vídeo, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>54</i>
<i>Figura 47 – Definições de DSCP no adaptador de tráfego multimídia para o IPv4 (2)</i>	<i>55</i>
<i>Figura 48 – Definições de DSCP no adaptador de tráfego multimídia para o IPv6 (2).</i>	<i>55</i>
<i>Figura 49 – Tráfego de dados (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>56</i>
<i>Figura 50 – Tráfego de dados (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>56</i>
<i>Figura 51 – Tráfego de áudio (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>57</i>
<i>Figura 52 – Tráfego de áudio (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>58</i>
<i>Figura 53 – Tráfego de voz (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>59</i>

<i>Figura 54 – Tráfego de voz (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>59</i>
<i>Figura 55 – Tráfego de vídeo (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>60</i>
<i>Figura 56 – Tráfego de vídeo (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.</i>	<i>61</i>
<i>Figura 57 – Ambiente (1) para validação e testes de identificação e encaminhamento de pacotes IP (via DSCP) pelo gateway multimídia.</i>	<i>62</i>
<i>Figura 58 – Ambiente (2) para validação e testes de identificação e encaminhamento de pacotes IP (via DSCP) pelo gateway multimídia.</i>	<i>62</i>
<i>Figura 59 – Endereçamento de rede do ambiente para validação e testes com o gateway multimídia.</i>	<i>63</i>
<i>Figura 60 – Saltos (hops) IPv4 entre os hosts transmissor e receptor no ambiente para validação e testes do gateway multimídia.</i>	<i>64</i>
<i>Figura 61 – Saltos (hops) IPv6 entre os hosts transmissor e receptor no ambiente para validação e testes do gateway multimídia.</i>	<i>64</i>
<i>Figura 62 – Encaminhamento de pacotes IPv4 com base no DSCP pelo gateway multimídia (1).</i>	<i>65</i>
<i>Figura 63 – Encaminhamento de pacotes IPv6 com base no DSCP pelo gateway multimídia (1).</i>	<i>66</i>
<i>Figura 64 – Encaminhamento de pacotes IPv4 (a) e IPv6(b) do tráfego de dados com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>66</i>
<i>Figura 65 – Tráfego de dados entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	<i>67</i>
<i>Figura 66 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de áudio com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>68</i>
<i>Figura 67 – Tráfego de áudio entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	<i>69</i>
<i>Figura 68 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de voz com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>69</i>
<i>Figura 69 – Tráfego de voz entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	<i>70</i>
<i>Figura 70 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de vídeo com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>71</i>
<i>Figura 71 – Tráfego de vídeo entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	<i>72</i>
<i>Figura 72 – Encaminhamento de pacotes IPv4 com base no DSCP pelo gateway multimídia (2).</i>	<i>73</i>
<i>Figura 73 – Encaminhamento de pacotes IPv6 com base no DSCP pelo gateway multimídia (2).</i>	<i>73</i>
<i>Figura 74 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de dados (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>74</i>
<i>Figura 75 – Tráfego de dados (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	<i>75</i>
<i>Figura 76 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de áudio (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	<i>76</i>

<i>Figura 77 – Tráfego de áudio (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	77
<i>Figura 78 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de voz (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	77
<i>Figura 79 – Tráfego de voz (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	78
<i>Figura 80 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de vídeo (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.</i>	79
<i>Figura 81 – Tráfego de vídeo (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).</i>	80
<i>Figura 82 – Ambiente para validação e testes quanto à qualidade de serviço pelo gateway multimídia.</i>	81
<i>Figura 83 – Tráfego elástico (de navegação web) entrante ao gateway multimídia utilizando IPv4 (a) e IPv6 (b).</i>	82
<i>Figura 84 – Tráfego stream (de streaming de vídeo) entrante ao gateway multimídia utilizando IPv4 (a) e IPv6 (b).</i>	82
<i>Figura 85 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede utilizando de mecanismos de qualidade de serviço (1).</i>	83
<i>Figura 86 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede sem a utilização de mecanismos de qualidade de serviço.</i>	84
<i>Figura 87 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede utilizando de mecanismos de qualidade de serviço (2).</i>	85
<i>Figura 88 – Histograma pertinente aos tráfegos elástico de dados e stream de áudio, vídeo e voz, em ambiente cabeado, não intermediado (a) e intermediado (b) pelo gateway multimídia.</i>	87
<i>Figura 89 – Histograma pertinente aos tráfegos elástico de dados e stream de áudio, vídeo e voz, em ambiente sem fio, não intermediado (a) e intermediado (b) pelo gateway multimídia.</i>	88
<i>Figura 90 – Histograma pertinente aos tráfegos stream de voz intermediados pelo gateway multimídia em ambiente cabeado (testes de 30 minutos e de 2 horas).</i>	89
<i>Figura 91 – Histograma pertinente aos tráfegos stream de voz intermediados pelo gateway multimídia em ambiente cabeado (testes de 12 horas e de 24 horas).</i>	90
<i>Figura 92 – Estatísticas de transmissão da interface de rede cabeada do gateway multimídia.</i>	94
<i>Figura 93 – Estatísticas de transmissão da interface de rede sem fio do gateway multimídia.</i>	95
<i>Figura 94 – Estatísticas de utilização de processamento pelo gateway multimídia.</i>	96
<i>Figura 95 – Estatísticas de utilização de memória pelo gateway multimídia.</i>	97
<i>Figura 96 – Estatísticas de processos do gateway multimídia.</i>	97

Lista de Tabelas

<i>Tabela 1 – Requisitos de algumas aplicações de rede (Fonte: [23]).</i>	3
<i>Tabela 2 – Breve comparativo dos protocolos TCP e UDP.</i>	7
<i>Tabela 3 – Breve comparativo dos protocolos IPv4 e IPv6.</i>	7
<i>Tabela 4 – ToS's definidos pelo RFC 1349 (obsoletos pelo RFC 2474).</i>	29
<i>Tabela 5 – Identificadores para os serviços de dados, áudio, voz e vídeo e seus fluxos (canais) de transmissão.</i>	31
<i>Tabela 6 – Algumas aplicações e seus requisitos de QoS. (Fonte: [24]).</i>	32
<i>Tabela 7 – Endereçamento IPv4 e IPv6 dos hosts do ambiente para validação e testes do adaptador de tráfego multimídia.</i>	47
<i>Tabela 8 – Definições de DSCP no adaptador de tráfego multimídia (I).</i>	48
<i>Tabela 9 – Definições de DSCP no adaptador de tráfego multimídia (II).</i>	55
<i>Tabela 10 – Endereçamento IPv4 e IPv6 dos hosts do ambiente para validação e testes com o gateway multimídia.</i>	63
<i>Tabela 11 – Portas de envio e escuta/recebimento nos módulos transmissor e receptor do gerador de tráfego multimídia (I).</i>	65
<i>Tabela 12 – Portas de envio e escuta/recebimento nos módulos transmissor e receptor do gerador de tráfego multimídia (II).</i>	73
<i>Tabela 13 – Percentuais de datagramas perdidos com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente cabeado.</i>	91
<i>Tabela 14 – Tempos de transmissão com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente cabeado.</i>	91
<i>Tabela 15 – Variações de atrasos (jitter) com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente cabeado.</i>	92
<i>Tabela 16 – Percentuais de datagramas perdidos com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.</i>	92
<i>Tabela 17 – Tempos de transmissão com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.</i>	93
<i>Tabela 18 – Variações de atrasos (jitter) com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.</i>	93

Lista de abreviaturas e siglas

CDN	=	Content Distribution Networks
CoS	=	Class of Service
DVMRP	=	Distance Vector Multicast Routing Protocol
DNS	=	Domain Name System
DS	=	Differentiated Services
DSCP	=	Differentiated Services Codepoint
ECN	=	Explicit Congestion Notification
FIFO	=	First In First Out
FCFS	=	First Come First Served
FTP	=	File Transfer Protocol
HTTP	=	Hypertext Transfer Protocol
IETF	=	Internet Engineering Task Force
IGMP	=	Internet Group Management Protocol
IP	=	Internet Protocol
IPTV	=	Internet Protocol Television
IPv4	=	Internet Protocol (versão 4)
IPv6	=	Internet Protocol (versão 6)
IPSec	=	Internet Protocol Security
ISO	=	International Organization for Standardization
ISP	=	Internet Service Provider
ITU	=	International Telecommunication Union
Kbps	=	Kilobits por segundo
Mbps	=	Megabits por segundo
MBone	=	Multicast Backbone
MOSPF	=	Multicast Open Shortest Path First
NAT	=	Network Address Translation
OSI	=	Open Systems Interconnection
PIM	=	Protocol Independent Multicast
QoS	=	Quality of Service
RFC	=	Request for Comments
RTP	=	Real-Time Transport Protocol
RTCP	=	Real-Time Transport Control Protocol
RTSP	=	Real Time Streaming Protocol
SIP	=	Session Initiation Protocol

Tbps	=	Terabits por segundo
TCP	=	Transmission Control Protocol
TFTP	=	Trivial File Transfer Protocol
ToS	=	Type of Service
URL	=	Uniform Resource Locator
UDP	=	User Datagram Protocol
VoIP	=	Voice over Internet Protocol
WFQ	=	Weighted Fair Queueing

1 – Introdução

A evolução dos sistemas de comunicação e a popularização do acesso residencial de banda larga contribuíram de modo significativo para que os usuários da rede (Internet) explorassem os diversos serviços e aplicações por ela oferecidos. Dentre esses serviços e aplicações, aquelas voltadas ao conteúdo multimídia, tal como o acesso e compartilhamento de recursos de áudio e vídeo em portais de entretenimento e notícias e a realização de telefonia e videoconferência pela Internet, dentre outras, tornaram-se extremamente populares. Como exemplo, de acordo com estatísticas de acesso fornecidas pelo portal de compartilhamento de vídeos Youtube [1], mais de 4 bilhões de vídeos são assistidos por dia, totalizando cerca de 3 bilhões de horas assistidas por mês por mais de 800 milhões de usuários que, mensalmente, acessam seus conteúdos. Quanto ao envio de informações ao seu portal, o Youtube relata que recebe cerca de 60 horas de vídeos por minuto, totalizando, em um mês, mais que o total de vídeos produzidos pelas 3 principais emissoras de TV dos Estados Unidos em 60 anos. O portal também relata que no ano de 2011 teve mais de 1 trilhão de visualizações (das quais cerca de 70% do tráfego vêm de fora dos Estados Unidos), fazendo uma comparação de 140 visualizações por cada pessoa existente na Terra. Outro exemplo que impressiona refere-se aos recursos de telefonia pela Internet fornecidos pelo Skype que, de acordo com [2], apenas no primeiro trimestre de 2012 totalizou mais de 115 bilhões de minutos em chamadas telefônicas com pico recorde de cerca de 32 milhões de usuários acessando seus serviços simultaneamente (em março de 2012).

Por outro lado esses novos serviços e aplicações tornaram o fluxo de tráfego de rede mais detalhado e complexo, exigindo a utilização de abordagens específicas para, por exemplo, a modelagem de tráfego, bem como para a identificação e atendimento aos requisitos de certas aplicações quanto ao tráfego gerado por elas perante a rede. Como exemplo, alguns trabalhos recentes abordam estudos voltados ao entendimento e análise de tráfego de rede [3, 4], a partir de abordagens matemáticas e comportamentais, bem como de novas propostas acadêmicas para esse propósito. De modo similar, outros trabalhos recentes abordam questões voltadas à simulação e modelagem de tráfego para, principalmente, as aplicações multimídia, com estudos voltados à utilização de funções de distribuição e algoritmos de compressão [5, 6, 7, 8], para comunicação sem fio [9, 10, 11, 12], para customização de distribuição de conteúdos [13, 14, 15, 16] e em estudos voltados à temporização e qualidade de serviço [17, 18, 19, 20], dentre outros.

Nesse contexto, o presente projeto de pesquisa contempla a implementação e validação funcional de um *gateway* multimídia baseado em IP a partir da implementação de recursos para classificação, rotulação, identificação e encaminhamento de fluxos de tráfego distintos (elástico e *stream*), ambos com modelagem de tráfego pré-definida, a partir de informações constantes no cabeçalho dos pacotes IP associados aos diferentes fluxos de tráfegos para os serviços multimídia de áudio, voz, vídeo e dados fornecidos por um gerador de tráfego multimídia baseado em IP, desenvolvido em outro projeto de pesquisa junto à própria Faculdade de Tecnologia (FT) da Universidade Estadual de Campinas (UNICAMP) [21, 22].

No que se refere aos requisitos associados à sua implementação, além de estar embasado no protocolo IP, o *gateway* multimídia deve ser transparente aos sistemas finais e aplicações transmissora e receptora do conteúdo multimídia e ele não deve influenciar em questões quanto ao perfil (características) de tráfego gerado por tais aplicações e sistemas finais, bem como não deve favorecer ou induzir na ocorrência de erros de transmissão e em atrasos que inviabilizem ou prejudiquem tais transmissões, por exemplo. De modo complementar a tais

implementações, o *gateway* multimídia também deve contemplar o fornecimento de recursos de qualidade de serviço (QoS) aos serviços por ele intermediados e que necessitem de tais recursos, tais como serviços multimídia de voz e vídeo, por exemplo.

Quanto às principais características do presente projeto quando comparado a outros projetos de pesquisa, em vez de utilizar de recursos e mecanismos adicionais quanto ao tráfego intermediado pelo *gateway* multimídia, tais como, por exemplo, abordagens matemáticas para realizar a distinção dos vários tipos de tráfegos entrantes ao *gateway* multimídia, essa separação é realizada a partir de informações constantes nos campos ToS (*Type of Service*) do protocolo IPv4 e TC (*Traffic Class*) do protocolo IPv6, ambos com 8 bits de comprimento, hoje tidos (reformulados) como DSCP (*Differentiated Services Codepoint*) [RFC 2474], com 6 bits de comprimento, e ECN (*Explicit Congestion Notification*) [RFC 3168] com 2 bits de comprimento. Outra questão se deve ao ambiente de desenvolvimento e testes do *gateway* multimídia, o qual é baseado em soluções de *software* livre, fornecido, especialmente, pelo sistema operacional Linux e pela solução Netfilter/Iptables, disponibilizando uma plataforma aberta para o estudo e aprimoramento futuro de tal *gateway* multimídia.

No que se refere aos testes funcionais e de desempenho, estes são realizados em ambientes cabeado e sem fio, abordando questões envolvendo, por exemplo, à transparência do *gateway* multimídia quanto ao perfil (características) dos tráfegos por ele intermediados, bem como à questões envolvendo erros, atrasos e variações de atrasos (*jitter*) e à seu mecanismo de qualidade de serviço, dentre outras, demonstrando que sua implementação é viável e atende aos requisitos descritos anteriormente.

Para tal, quanto à organização desta dissertação, os conceitos básicos associados às redes multimídia e aos modelos para fontes de tráfego utilizados nos testes quanto ao *gateway* multimídia são descritos nos Capítulos 2 e 3, respectivamente; as características, recursos e funcionalidades do *gateway* multimídia, bem como os resultados pertinentes à sua implementação são descritos nos Capítulos 4 e 5, respectivamente; e, por fim, no Capítulo 6, uma conclusão quanto ao presente projeto de pesquisa é apresentada ao leitor.

Desta forma, espera-se, de modo resumido, que o *gateway* multimídia contribua como uma nova ferramenta para testes e análises de soluções voltadas às redes multimídia de modo geral.

2 – Redes Multimídia

2.1 – Aplicações de Redes Multimídia

De modo geral, pode-se dizer que as aplicações representam a razão de ser das redes de computadores [23]. São as grandes responsáveis por impulsionar o desenvolvimento de novos dispositivos, protocolos e tecnologias que objetivam e viabilizam sua implementação e utilização num contexto global, exigindo das redes (Internet) uma alta capacidade de se renovar e se reinventar (evoluir) para suportar tais aplicações.

Grande parte dessa necessidade de constante renovação (evolução) das redes para dar suporte às suas aplicações está associada aos requisitos impostos por tais aplicações para que estas sejam efetivamente executadas e utilizadas, em que os requisitos impostos pelas aplicações *stream* são extremamente distintos dos requisitos impostos pelas demais aplicações da rede [24]. Como exemplo, algumas aplicações típicas no contexto Internet, tais como transferência de arquivos ou correio eletrônico, não exigem, de modo geral, alta largura de banda para funcionarem de modo aceitável aos clientes que as utilizam, sendo essas tolerantes a atrasos e sensíveis a perdas de dados. Essas características são extremamente opostas aos requisitos exigidos pelas aplicações *stream* que, de modo geral, necessitam de alta largura de banda para serem efetivamente funcionais aos clientes que as utilizam, sendo sensíveis a atrasos, porém tolerantes a eventuais perdas de dados.

De acordo com [23], as exigências de funcionamento das aplicações multimídia (aplicações *stream*) divergem significativamente daquelas tradicionais aplicações elásticas, como *e-mails*, navegação na *web*, *login* remoto e *download* e compartilhamento de arquivos. Em particular, diferentemente das aplicações elásticas, as aplicações multimídia são muito mais sensíveis a atrasos ponto a ponto e a variações de atrasos, mas podem tolerar casuais perdas de informações. Como exemplo, a Tabela 1 descreve os requisitos que algumas aplicações exigem da rede quanto à perda de dados, largura de banda e sensibilidade ao atraso:

Aplicação	Perda de dados	Largura de banda	Sensibilidade ao atraso
Transferência de arquivos	Sem perda	Elástica	Não
<i>E-mail</i>	Sem perda	Elástica	Não
Documentos <i>web</i>	Sem perda	Elástica	Não
Telefonia via Internet/ videoconferência	Tolerante à perda	Áudio: alguns Kbps – 1 Mbps Vídeo: 10 Kbps – 5 Mbps	Sim: décimos de segundo
Áudio/vídeo armazenado	Tolerante à perda	Igual ao acima	Sim: alguns segundos
Jogos interativos	Tolerante à perda	Alguns Kbps – 10 Mbps	Sim: décimos de segundo
Mensagem instantânea	Sem perda	Elástica	Sim e não

Tabela 1 – Requisitos de algumas aplicações de rede (Fonte: [23]).

No que se refere à taxonomia das aplicações *stream*, é possível classificá-las em três categorias distintas:

- Fluxo de áudio e vídeo armazenado;

- Fluxo de áudio e vídeo ao vivo;
- Fluxo de áudio e vídeo interativo de tempo real.

De modo geral, a partir dessas classificações é possível identificar que cada uma dessas categorias de aplicativos tem um conjunto específico de exigências de funcionamento para a rede, demonstrando que, além de empolgantes, essas aplicações merecem atenção especial daqueles que desejam distribuir conteúdos multimídia na Internet ou apenas viabilizar que sua infraestrutura de rede dê suporte para que seus clientes desfrutem de tais aplicações. As seções seguintes descrevem as principais características das classificações de aplicações *stream* descritas anteriormente.

2.1.1 – Fluxo de áudio e vídeo armazenado

Aplicações *stream* pertencentes a essa categoria são aquelas que possibilitam que seus clientes requisitem, sob demanda, os conteúdos multimídia armazenados em servidores espalhados pela rede (Internet) [24]. Diversos sites na Internet fornecem esse recurso, sendo um desses sites o Youtube [1]. Através de sua página, seus clientes podem assistir a seus vídeos favoritos quando quiserem e com variado controle sobre os mesmos, podendo, por exemplo, pausá-los, avançá-los ou retrocedê-los.

Quanto às principais características dessa categoria de aplicativos, tem-se:

- O armazenamento prévio do conteúdo de áudio e vídeo em um determinado servidor da rede;
- O fluxo e reprodução contínua de tais conteúdos disponibilizados ao cliente, que inicia sua reprodução alguns segundos após iniciar o *download* do mesmo (sem a necessidade de baixar todo o arquivo antes de iniciar sua reprodução, porém dependente de que os dados disponíveis no servidor sejam baixados a tempo de serem exibidos ao cliente).

2.1.2 – Fluxo de áudio e vídeo ao vivo

Clientes de aplicações *stream* dessa categoria podem reproduzir conteúdos de áudio e vídeo “ao mesmo tempo” (com atrasos típicos de alguns segundos) com a qual esse conteúdo foi criado [23]. Aplicações típicas pertencentes a essa categoria estão associadas aos canais de rádio e TV pela Internet (IPTV). A partir dessas aplicações, de modo contrário às aplicações de fluxo de áudio e vídeo armazenado, seus clientes não podem adiantar o conteúdo de áudio e vídeo, uma vez que tal conteúdo ainda não foi gerado pelo sistema transmissor. Contudo, de modo similar às aplicações de fluxo de áudio e vídeo armazenado, após receber (e armazenar) o conteúdo multimídia, é possível pausá-lo ou retrocedê-lo.

Quanto às principais características dessa categoria de aplicativos, tem-se:

- A interatividade em tempo real para conteúdos de áudio e vídeo;
- A sensibilidade ao atraso superior às aplicações de fluxo de áudio e vídeo armazenado;

- O fluxo e reprodução contínua do conteúdo multimídia (conforme descrito nas aplicações *stream* de fluxo de áudio e vídeo armazenado).

2.1.3 – Fluxo de áudio e vídeo interativo de tempo real

Aplicações *stream* dessa categoria possibilitam que seus clientes se comuniquem a partir de conteúdos de áudio e vídeo em tempo real. Aplicações típicas pertencentes a essa categoria estão associadas à telefonia pela Internet (VoIP) e à videoconferência pela Internet. De modo geral, como o objetivo principal dessas aplicações é viabilizar a comunicação entre duas ou mais pessoas, atrasos superiores a alguns milissegundos podem tornar a “conversa” extremamente frustrante, a ponto de inviabilizá-la. Nesse caso, a sensibilidade ao atraso torna-se um requisito ainda mais importante para essa categoria de aplicações e um desafio tecnicamente ainda mais difícil para aqueles que irão viabilizar a utilização de tais aplicações pela rede [23, 24].

Quanto às principais características dessa categoria de aplicativos, tem-se:

- A reprodução do conteúdo multimídia tão logo ele foi gerado (com atrasos típicos de alguns milissegundos);
- A alta sensibilidade à atrasos (superior às duas outras categorias de aplicações *stream* descritas anteriormente);
- A possibilidade de armazenar o conteúdo multimídia recebido, podendo pausá-lo ou retrocedê-lo;
- O fluxo e reprodução contínua do conteúdo multimídia (conforme descrito nas aplicações *stream* de fluxo de áudio e vídeo armazenado).

2.2 – Protocolos de Redes Multimídia

Para viabilizar e controlar a comunicação entre os diversos dispositivos que compõem a rede, uma grande quantidade de protocolos, para os mais variados fins e objetivos, podem ser utilizados. Esses protocolos implementam, de modo geral, um conjunto padrão de regras e procedimentos capazes de viabilizar a troca de mensagens entre os mais variados dispositivos (aplicações em execução nesses dispositivos) conectados à rede [24].

Pelo fato do conteúdo multimídia ser acessado e disponibilizado, especialmente, num contexto Internet, seus protocolos estão embasados na arquitetura de protocolos TCP/IP, tidos como a “espinha dorsal” da Internet. Dependendo do tipo da aplicação multimídia, bem como de sua interatividade, um ou outro protocolo pode ser utilizado, sendo comum a utilização de protocolos como RTP, RTCP, RTSP e SIP, dentre outros, executando sobre UDP (ou TCP) e IP. Esses protocolos são descritos nas seções seguintes.

2.2.1 – Protocolos TCP, UDP e IP

Conforme descrito em [23, 24, 25], a Internet está fundamentada na arquitetura de protocolos TCP/IP, a qual foi desenvolvida na década de 70 pelo departamento de defesa americano e, desde então, vem sendo utilizada para atender os requisitos da rede daquele momento, bem como aos requisitos da rede para os dias de hoje. Pelo fato dessa arquitetura ser padrão na

Internet, as diversas redes que a compõem também utilizam o TCP/IP (em toda a rede ou, no mínimo, no elo dessas redes com a Internet) como protocolos de sua infraestrutura básica de comunicação. Logo, todas as aplicações de rede executadas no contexto Internet (aplicações multimídia ou não) utilizam protocolos dessa arquitetura para viabilizarem a comunicação entre seus pares transmissor e receptor.

No que se refere à sua nomenclatura, os termos TCP e IP referem-se a dois dos principais protocolos dessa arquitetura: o protocolo TCP (*Transmission Control Protocol*) e protocolo IP (*Internet Protocol*). Nos dias de hoje, mesmo ainda tendo seu nome referenciado ao TCP e ao IP, essa arquitetura é composta por uma infinidade de outros protocolos, para os mais variados fins e objetivos.

Estruturalmente, para facilitar e simplificar sua organização, bem como dar flexibilidade ao seu modelo funcional, que desde a década de 70 vem se adaptando aos “antigos” e “novos” requisitos e desafios impostos à rede (Internet), a arquitetura de protocolos TCP/IP está organizada em 4 camadas, conforme ilustra a Figura 1, a qual também permite compará-la ao Modelo de Referência OSI (*Open Systems Interconnection*) da ISO (*International Organization for Standardization*):

TCP/IP		ISO/OSI	
Aplicação		Aplicação	Camada 7
		Apresentação	Camada 6
		Sessão	Camada 5
Transporte		Transporte	Camada 4
Internet (ou Inter-rede)		Rede	Camada 3
Física (acesso à rede)		Enlace	Camada 2
		Física	Camada 1

Figura 1 – Arquitetura TCP/IP e o Modelo de Referência ISO/OSI.

No que se refere ao transporte das informações pela rede, a arquitetura TCP/IP especifica dois protocolos em sua camada de transporte: o protocolo TCP e o protocolo UDP (*User Datagram Protocol*). O primeiro, TCP, é o principal protocolo de transporte utilizado pelas aplicações disponíveis na rede (tais como navegação *web*, correio eletrônico e transferência de arquivos, dentre outras) tendo como uma de suas principais características a confiabilidade em suas transmissões (fornecida a partir de sua orientação à conexão, com confirmações de recebimento de mensagens, bem como retransmissão de eventuais mensagens “perdidas” na rede), porém tendo um custo de processamento associado a essa confiabilidade inerente aos controles que a viabilizam. O segundo, UDP, é um protocolo minimalista, não orientado à conexão (sem qualquer tipo de confirmação de recebimento de mensagens, bem como retransmissão de eventuais conteúdos perdidos), porém extremamente leve e rápido, adequado para aplicações que exigem velocidade e que são tolerantes a eventuais perdas de informações, como as aplicações *stream* de modo geral [23, 24, 25].

Nesse contexto, embora inicialmente desfavorável quando comparado ao TCP, o protocolo UDP é tido como o mais indicado para o transporte de conteúdos multimídia de tráfego *stream* pela rede, uma vez que, por ser leve e rápido, contribui significativamente para dois dos principais requisitos dessas aplicações: sensibilidade a atrasos e variações de atraso. Ainda nesse contexto, a ausência de confiabilidade (confirmações e retransmissões) também não afeta a transmissão de conteúdos *stream* pela rede, uma vez que essas aplicações toleram eventuais perdas de informações. Por esse motivo, grande parte das aplicações *stream* utilizam o protocolo UDP para o transporte de suas informações pela rede. Vale ressaltar que outras aplicações e serviços (como o serviço de resolução de nomes da Internet, DNS, e a transferência de arquivos via TFTP, por exemplo) também utilizam o protocolo UDP, de tal forma que ele não está restrito somente às aplicações *stream*. A Tabela 2 descreve e compara as principais características dos protocolos TCP e UDP:

TCP	UDP
É orientado para conexão	Não é orientado para conexão
Possui confiabilidade em suas transmissões	Sem confiabilidade em suas transmissões
Possui controle de fluxo	Sem controle de fluxo
Possui controle de congestionamento	Sem controle de congestionamento
Maior <i>overhead</i> de processamento	Menor <i>overhead</i> de processamento

Tabela 2 – Breve comparativo dos protocolos TCP e UDP.

No que se refere à movimentação dos datagramas pela rede, a arquitetura TCP/IP define o protocolo IP, além de também definir diversos outros protocolos para roteamento e envio de mensagens de controle pela rede, dentre outros. Atualmente, há duas versões do protocolo IP em execução na Internet: a versão 4 (IPv4) e a versão 6 (IPv6). Dessas versões, o IPv4, com um espaço de endereçamento de 32 bits, é o mais utilizado. Por sua vez, o IPv6, substituto natural do IPv4, com espaço de endereçamento de 128 bits e diversas melhorias quando comparado ao IPv4 (vide Tabela 3 e [23, 24, 25]), deve se solidificar como um dos principais protocolos para a Internet de próxima geração. Ainda no que se refere à utilização de ambos, como o IPv4 não é naturalmente compatível com o IPv6 e pelo fato do IPv4 ainda atender às demandas de grande parte das redes que compõem a Internet, o IPv6 ainda é tido como uma promessa futura para grande parte dessas redes, sendo pouco utilizado quando comparado ao seu antecessor. Vale ressaltar que estudos voltados à coexistência do IPv4 e do IPv6, bem como estratégias de migração de um para outro, por exemplo, já fizeram parte de muitas pesquisas voltadas às redes de computadores, as quais não serão abordadas neste documento por não estarem necessariamente adequadas ao presente projeto de pesquisa. Para maiores informações sobre algumas dessas abordagens e estratégias, vide referências [23, 24, 25].

IPv4	IPv6
Espaço de endereçamento de 32 bits	Espaço de endereçamento de 128 bits
Cabeçalho pouco otimizado, com alguns campos não utilizados	Cabeçalho aprimorado, mais simples e versátil
Segurança fragilizada (ex.: IPSec opcional)	Segurança aprimorada (ex.: IPSec obrigatório)
Difícil suporte à QoS	Melhor suporte à QoS
É comum a utilização de NAT	Não requer uso de NAT

Tabela 3 – Breve comparativo dos protocolos IPv4 e IPv6.

Nesse contexto, e de modo resumido, grande parte das aplicações *stream* disponíveis na Internet executam tipicamente sobre os protocolos UDP e IP ou TCP e IP. A Figura 2 ilustra o posicionamento dos protocolos TCP, UDP e IP na arquitetura de protocolos TCP/IP:

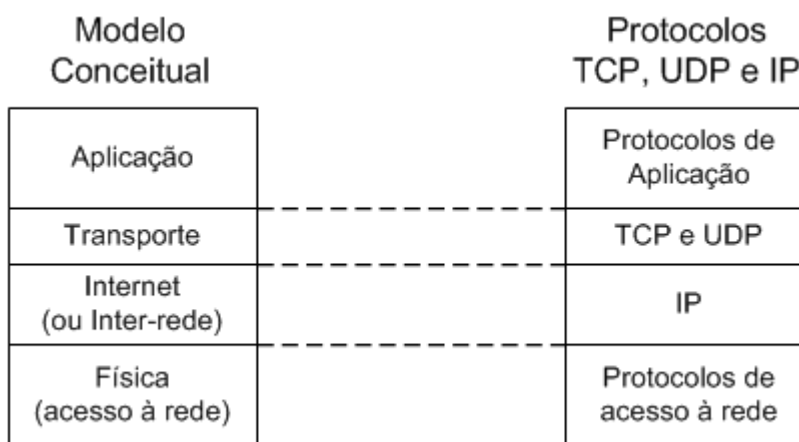


Figura 2 – Protocolos TCP, UDP e IP.

Vale ressaltar que, acima desses protocolos, no nível de aplicação e num nível intermediário entra as camadas de aplicação e transporte, é comum a utilização de protocolos multimídia específicos, tais como RTP, RTCP, RTSP e SIP, dentre outros, os quais são brevemente descritos nas seções seguintes.

Para maiores informações a respeito da arquitetura de protocolos TCP/IP, sugere-se a leitura de suas RFCs e das referências [23, 24, 25].

2.2.2 – Protocolos RTP, RTCP e RTSP

Aplicações *stream* de tempo real utilizam, comumente, os protocolos RTP (*Real-Time Transport Protocol*), RTCP (*Real-Time Transport Control Protocol*) e RTSP (*Real Time Streaming Protocol*), ambos projetados pelo IETF, sobre os protocolos de transporte UDP e de rede IP (descritos na Seção 2.2.1). A filosofia básica de ambos é fornecer mecanismos para a estruturação, diagnóstico e controle do conteúdo de tempo real transmitido na rede.

De acordo com [23], a partir dos recursos e funcionalidades do RTP é possível adicionar certos controles estruturais quanto ao conteúdo multimídia (*stream*) que será transportado na rede, tais como número de sequência e marcas de tempo dentre outros (visto que esse conteúdo será tipicamente transportado sobre UDP que, conforme descrito na Seção 2.2.1, é extremamente minimalista). Essas estruturas fazem parte do pacote RTP que será encapsulado, comumente, sobre UDP e, em seguida, sobre o IP para, posteriormente, serem transmitidos à rede.

Quanto ao *feedback* sobre o conteúdo transportado, bem como informações de sincronização e/ou informações específicas que podem ser exibidas ao usuário, utiliza-se o RTCP [24], o qual possibilita, nesse contexto, a obtenção de informações quanto a atrasos, variações de atrasos e pacotes enviados e perdidos, dentre outros. A partir dessas informações, o desenvolvedor da aplicação *stream* pode tomar certas ações sobre como se dará a transmissão de dados sobre a rede, tais como modificações nas taxas de transmissão ou eventuais diagnósticos sobre o processo de transmissão [23], ou exibir estatísticas aos usuários das aplicações, dentre outros.

Por sua vez, o controle de reprodução do conteúdo multimídia no cliente, tais como pausa, avanço ou retrocesso da mídia, é de responsabilidade do protocolo RTSP que, em linhas gerais, proporciona ao cliente *stream* os controles inerentes a assistir a um DVD, por exemplo [23, 24].

Para maiores informações a respeito de ambos os protocolos, sugere-se a leitura de suas RFCs e das referências [23, 24].

2.2.3 – Protocolo SIP

O protocolo SIP (*Session Initiation Protocol*), projetado pelo IETF, é um protocolo em nível de aplicação utilizado para estabelecer, gerenciar e encerrar sessões de chamadas multimídia (telefonia, videoconferência ou outra) em redes IP [23, 24]. Pode utilizar os protocolos RTP e RTCP para o transporte dos dados multimídia e executar sobre UDP ou TCP. Também pode realizar chamadas de redes IP para redes de telefonia caso exista um *gateway* entre ambas.

De acordo com [24], o SIP é um protocolo leve, modular e flexível que foi projetado de modo à interoperar bem com as aplicações e protocolos típicos da Internet. Também é similar ao HTTP no que se refere ao seu modelo cliente-servidor e à sua sintaxe, com números telefônicos representados como URLs (do tipo sip:rafael@diorio.com.br) que, em um clique, podem iniciar uma chamada VoIP a partir de páginas *web*, por exemplo.

Quanto às suas funcionalidades e recursos, o SIP possibilita o estabelecimento de sessões de áudio, vídeo ou dados entre duas ou mais partes (para chamadas telefônicas convencionais ou conferências entre múltiplos usuários, por exemplo), tratando de questões voltadas à localização de usuários, da identificação dos recursos da chamada (transferências de chamadas, videoconferência, etc.), da forma como a chamada será realizada (entre dois ou mais usuários, por exemplo), da participação de novos usuários às chamadas (triagens, lista de espera, etc.), bem como do estabelecimento, gerenciamento e encerramento da mesma, dentre outros.

Conforme descrito em [23], como o SIP é um protocolo de sinalização para inicializar e encerrar chamadas em geral, ele pode ser utilizado desde aplicações de telefonia e videoconferência pela Internet até para transmissões de dados e textos em redes multimídia, tais como conteúdos multimídia de aplicações de mensagens instantâneas ou dados de jogos *online*, por exemplo. Para outras informações a respeito do protocolo SIP, sugere-se a leitura de suas RFCs e das referências [23, 24].

2.2.4 – Padrão H.323

O padrão H.323, projetado pela ITU (*International Telecommunication Union*), representa um conjunto de recomendações (protocolos) para sistemas de comunicações multimídia em redes baseadas em pacotes (como a Internet). É tido como bem definido estruturalmente (organizado em camadas com protocolos com funções específicas), porém é grande, complexo e pouco flexível, típico da indústria de telefonia [23, 24].

De acordo com [24], a recomendação H.323 é mais uma avaliação da arquitetura de telefonia da Internet que um protocolo específico, fazendo referência a um grande número de protocolos específicos para codificação de voz, configuração de chamadas, sinalização e

transporte de dados, dentre outros, em vez de especificar propriamente cada um desses elementos.

Seu modelo funcional é representado, tipicamente, por terminais H.323 e um dispositivo responsável por gerenciar as chamadas (denominado *gatekeeper*). Quanto a sua comunicação com a rede de telefonia, pode-se utilizar um *gateway* responsável pela interoperação da rede telefônica com a Internet (Figura 3).

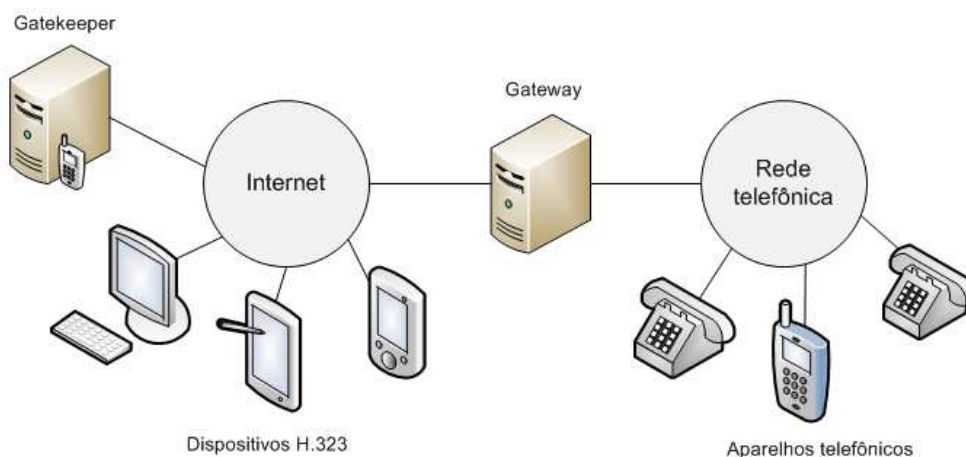


Figura 3 – Modelo funcional geral do H.323 (Adaptado de [21, 22]).

Para mais informações a respeito do H.323, sugere-se as referências [23, 24].

2.3 – Acesso e distribuição de conteúdo *stream* na Internet

Grande parte do conteúdo *stream* distribuído na Internet consiste de fluxo de áudio e vídeo armazenado em servidores *web* [23, 24]. Nesse caso, a maior parte dos acessos a esses conteúdos ocorre diretamente pelo *browser* do cliente, a partir de requisições HTTP (*Hypertext Transfer Protocol*) e utilizando o protocolo da camada de transporte TCP. No lado cliente, além do *browser*, é comum a presença de um transdutor (uma aplicação auxiliar, como o MS Windows Media Player, o SMPlayer ou um transdutor *Flash*, por exemplo) responsável por reproduzir e controlar o arquivo de áudio e vídeo, além de descomprimir e eliminar a variação do atraso de tais conteúdos, dentre outros. Nesse caso, o cliente (*browser*) requisita o conteúdo *stream* diretamente ao servidor *web* a partir de requisições HTTP. Ao clicar no *link* do conteúdo desejado, o cliente (*browser*) recebe um metarquivo contendo a URL de tal conteúdo no servidor *web*. Após processar o metarquivo, o *browser* “contata” o transdutor associado, que estabelece uma conexão TCP junto ao servidor *web* requisitando tal conteúdo que é, então, exibido ao usuário.

Como exemplo, a Figura 4 ilustra a interação entre os lados cliente e servidor para uma transmissão de fluxo de áudio e vídeo armazenado em servidores *web*:

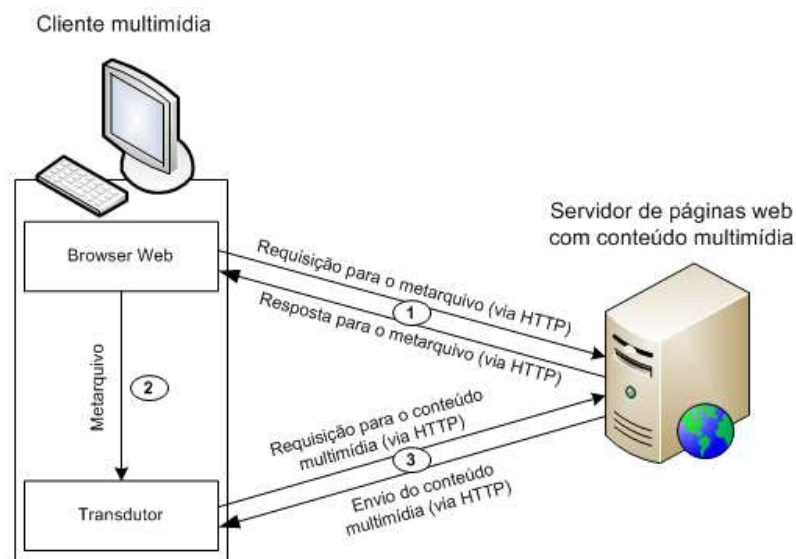


Figura 4 – Transmissão de fluxo de áudio e vídeo armazenado (1) (Fonte: Adaptado de [23]).

No caso de um servidor de fluxo contínuo (*streaming*), em vez do TCP, é comum a utilização do protocolo UDP como protocolo de transporte. Nesse caso, o lado servidor é tipicamente composto por dois servidores: um servidor *web* e um servidor de fluxo contínuo. O cliente (*browser*) requisita as páginas do servidor *web* e seu transdutor requisita o conteúdo *stream* diretamente do servidor de fluxo contínuo. Nesse caso, dependendo da tecnologia utilizada no transdutor do cliente e no servidor de fluxo contínuo, ambos podem utilizar protocolos específicos (protocolos proprietários, por exemplo) para realizar a transferência de tais conteúdos. A Figura 5 ilustra a interação entre os lados cliente e servidor para uma transmissão de fluxo de áudio e vídeo armazenado em servidores de fluxo contínuo:

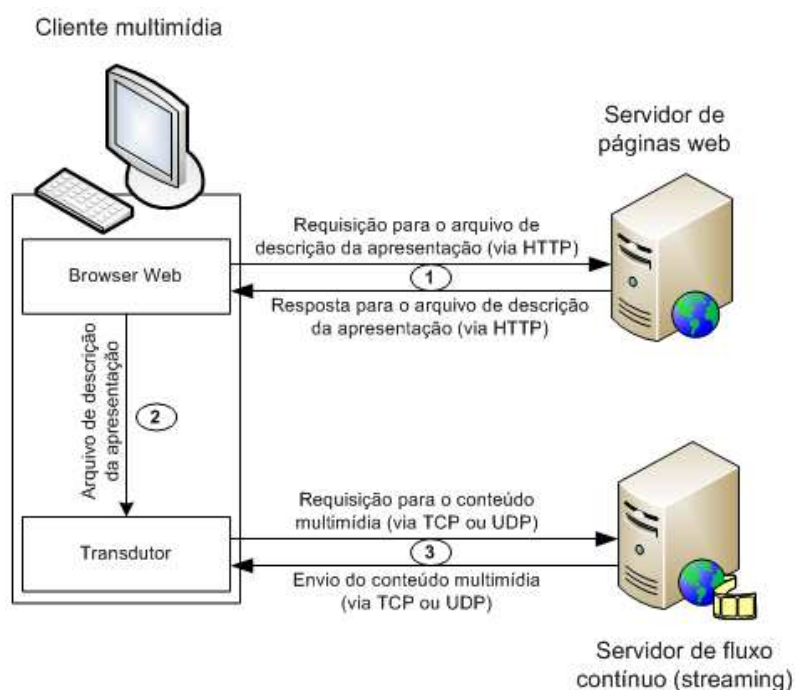


Figura 5 – Transmissão de fluxo de áudio e vídeo armazenado (2) (Fonte: Adaptado de [23]).

Em ambos os casos, para atenuar a variação do atraso (inerentes ao serviço *best effort*, de melhor esforço, da Internet), é comum que o transdutor do cliente retarde (em alguns segundos) o início da reprodução do conteúdo *stream*. Faz isso armazenando o conteúdo recebido do servidor em um *buffer* e, posteriormente, repassando esse conteúdo de seu *buffer* ao cliente.

Como exemplo, a Figura 6 ilustra esse processo de “*bufferização*” do conteúdo multimídia pelo cliente multimídia (aplicação *stream*) de modo a atenuar os efeitos indesejados, especialmente ao usuário final, quanto a variação do atraso associada ao serviço *best effort* da Internet durante a exibição de tal conteúdo:



Figura 6 – Utilização de buffers para atenuação de atrasos (Adaptado de [23, 24]).

Para realizar controles sobre a reprodução do conteúdo multimídia (*stream*) entre o transdutor e o servidor de fluxo contínuo, é comum a utilização de protocolos específicos no nível de aplicação, como, por exemplo, o protocolo RTSP (descrito na Seção 2.2.2).

Em linhas gerais, o RTSP apenas controla a transmissão do conteúdo *stream*, possibilitando que o cliente pause, retroceda ou avance tal conteúdo. Nesse caso, a interação entre cliente e servidor é similar à descrita anteriormente, porém utilizando o protocolo RTSP para o controle da transmissão de tal conteúdo. O cliente (*browser*) requisita as páginas do servidor *web* e seu transdutor requisita o conteúdo *stream* do servidor de fluxo contínuo. Ao clicar no *link* do conteúdo desejado junto ao servidor *web*, o cliente (*browser*) recebe um arquivo de descrição da apresentação contendo a “URL RTSP” de tal conteúdo junto ao servidor de fluxo contínuo. Após processar o arquivo de descrição da apresentação, o *browser* contata o transdutor associado que troca uma série de mensagens RTSP com o servidor de fluxo contínuo, possibilitando o controle da transmissão do conteúdo multimídia (*stream*).

Como exemplo, a Figura 7 ilustra a interação entre os lados cliente e servidor utilizando o protocolo RTSP:

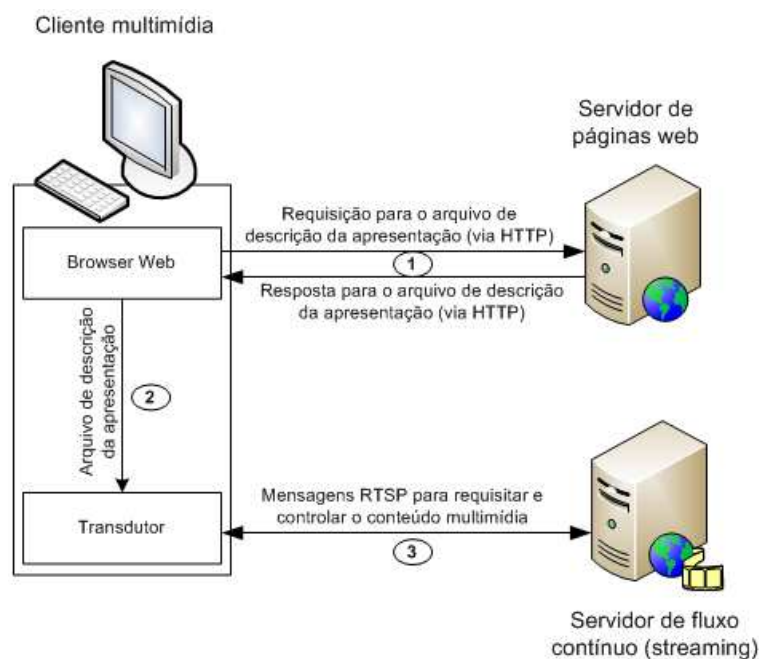


Figura 7 – Controle de reprodução de conteúdo multimídia (stream) utilizando o protocolo RTSP (Fonte: Adaptado de [23]).

2.3.1 – Compressão de áudio e vídeo

Transmissões de áudio e vídeo exigem e consomem altas larguras de banda, além de também exigirem altas capacidades de armazenamento nos *hosts* que hospedam tais conteúdos [23, 24]. Para atenuar tais exigências, depois de digitalizados, os sinais de áudio e vídeo passam por uma compressão antes de serem transmitidos pela rede. Como exemplo, de acordo com [23], sem compressão, uma única imagem constituída de 1024 pixels (com cada pixel codificado em 24 bits – 8 bits para cada uma das cores vermelha, verde e azul), exige 3 Mbytes de armazenamento. Levaria 7 minutos para enviar essa imagem por um enlace de 64 kbps. Por outro lado, se a imagem for comprimida na modesta razão de compressão de 10:1, a necessidade de armazenamento será reduzida para 300 kbytes e o tempo de transmissão também diminuirá por um fator de 10.

Quanto às técnicas e padrões de compressão de áudio e vídeo, conforme descrito em [23, 24], existem diversas disponíveis para utilização. No contexto Internet, dentre as mais populares para compressão de áudio estão a GSM, a G.729, a G.723.3, a MPEG-1 e a PCM, além de diversas outras técnicas e padrões proprietários. Para compressão de vídeo, as mais utilizadas são a MPEG-1, a MPEG-2, a MPEG-4 e os padrões H.261, além de diversos outros padrões e técnicas proprietárias.

Vale ressaltar que, apenas como exemplo, algumas universidades dedicam disciplinas específicas inteiras para tratar desse assunto, demonstrando o quão vasta é essa “área”. Dessa forma, para maiores informações a respeito desse assunto, sugere-se a leitura das referências [23, 24].

2.3.2 – Serviço *best effort* da Internet

Conforme descrito anteriormente, a Internet está fundamentada na arquitetura de protocolos TCP/IP. Como característica, disponibiliza um serviço de melhor esforço para todos os datagramas IP enviados entre cada par transmissor/receptor. Como resultado, esse serviço de melhor esforço, embora extremamente funcional, pode acarretar perda de pacotes, atrasos fim a fim relativamente longos (denominado “latência”) e variações aleatórias de atrasos (denominado “*jitter*”), influenciando e dificultando de forma significativa no projeto e distribuição de novas aplicações multimídia, as quais são diretamente afetadas e prejudicadas por tais características, além de exigirem altas larguras de banda para viabilizar sua utilização, dentre outros.

De modo geral, conforme descrito em [23], o serviço de melhor esforço da Internet faz o possível para transportar cada datagrama da origem ao destino o mais rápido possível. Porém, esse serviço não promete nada quanto à dimensão do atraso fim a fim para um pacote individual ou quanto à dimensão da variação do atraso ou da perda de pacotes de modo global.

Nesse contexto, o serviço de melhor esforço da Internet representa um dos principais desafios para a distribuição de conteúdos multimídia na rede (nesse caso, com referência especial aos conteúdos *stream*), tendo no atraso fim a fim, na variação do atraso e na perda de pacotes, alguns dos principais desafios quanto ao projeto e utilização de novas aplicações *stream*. Outro fator que dificulta a distribuição de novas aplicações *stream* está associado às exigências de altas larguras de banda que tais aplicações necessitam [24]. Em diversos casos, mesmo com altos investimentos de provedores de serviços de Internet (ISPs) e a crescente popularização do acesso residencial de banda larga, ainda existe uma grande dificuldade no dimensionamento dos enlaces dos servidores multimídia da rede para atender à demanda dos “clientes multimídia”. Como exemplo (descrito em [23]), se um determinado provedor de IPTV desejasse transmitir um grande evento esportivo (como uma final de Copa do Mundo) para cerca de 100 milhões de clientes com uma velocidade de 1 Mbps, o enlace do servidor deveria ser de 1 Tbps, requisito que inviabilizaria tal transmissão.

Nesse cenário, para contornar essas limitações do serviço de melhor esforço da Internet e para atender aos requisitos impostos pelas diversas aplicações *stream* disponíveis na rede (Internet), algumas estratégias e recursos podem ser utilizados pelos projetistas de tais aplicações [23, 24] como, por exemplo:

- Utilização do protocolo UDP, mais simples e com menos controles que o TCP, como protocolo de transporte para conteúdos de áudio e vídeo;
- Adição de atrasos (retardos) propositais para reprodução do conteúdo *stream* no receptor para reduzir os efeitos da variação do atraso induzidos pela rede;
- Envio de informações redundantes do transmissor para o receptor para reduzir o efeito de perda de pacotes;
- *Download* antecipado dos conteúdos *stream* do cliente para o servidor quando houver largura de banda disponível (para áudio e vídeo armazenados), dentre outros.

Outras abordagens comuns, nesse caso com ênfase na distribuição do conteúdo *stream* e não no projeto de suas aplicações, estão associadas ao super dimensionamento de velocidades de enlaces do sistema transmissor multimídia e na utilização de recursos e estratégias que simplifiquem e aproximem esse conteúdo aos clientes da rede (Internet) como, por exemplo, a utilização de redes de distribuição de conteúdos [23, 26], descritas na seção seguinte.

2.3.3 – Redes de distribuição de conteúdos

De acordo com [23], com taxas de vídeo em fluxo contínuo na faixa de centenas de Kbps para vídeos de baixa resolução e até vários Mbps para vídeos com qualidade de DVD, a tarefa de transmitir um vídeo armazenado em fluxo contínuo, sob demanda, a um grande número de usuários geograficamente distribuídos é um grande desafio. A abordagem mais simples seria armazenar o vídeo em um único servidor e simplesmente transmiti-lo de um servidor de vídeo (ou de um *server farm*) a um cliente, porém essa abordagem tem dois problemas óbvios: em primeiro lugar, como um cliente pode estar muito distante do servidor, os pacotes do servidor para o cliente podem passar por muitos ISPs, aumentando a probabilidade de atrasos e perdas de pacotes e, em segundo lugar, se o vídeo for muito popular, provavelmente será enviado muitas vezes através dos mesmos ISPs (e pelos mesmos enlaces de comunicação), consumindo alta largura de banda.

Nesse contexto, a filosofia básica das redes de distribuição de conteúdos (*CDNs – Content Distribution Networks*) é a de distribuir (replicar) o conteúdo multimídia, antes armazenado em um local centralizado, em diversos pontos estratégicos da rede (Internet) aproximando-o dos clientes que requisitam e acessam tais conteúdos [26]. Faz isso replicando (duplicando), a partir de um nó de distribuição, o conteúdo multimídia de seus clientes em ISPs de níveis mais baixos (mais próximos dos usuários da rede).

Quanto ao acesso pelos clientes da rede, as CDNs utilizam de resoluções DNS para redirecionar as requisições desses clientes ao servidor CDN mais próximo [23, 26]. Nesse caso, conforme descrito em [23], quando o *browser* do cliente requisita algum objeto do servidor *web* que possui conteúdos distribuídos em CDNs, essa requisição tem o endereço da CDN na URL requisitada (por exemplo, cliente requisita “http://www.diorio.com.br/video”. Essa URL aponta para “http://www.cdn.com.br/www.diorio.com.br/video”). Com base na URL de retorno, o cliente realiza uma consulta DNS para o domínio da CDN que o direciona para o servidor mais próximo desse cliente. Ao final, o cliente vai até o servidor da CDN para obter o vídeo requisitado.

A Figura 8 ilustra o modelo organizacional típico de uma CDN, bem como o processo de requisição e acesso aos conteúdos multimídia distribuídos em CDNs:

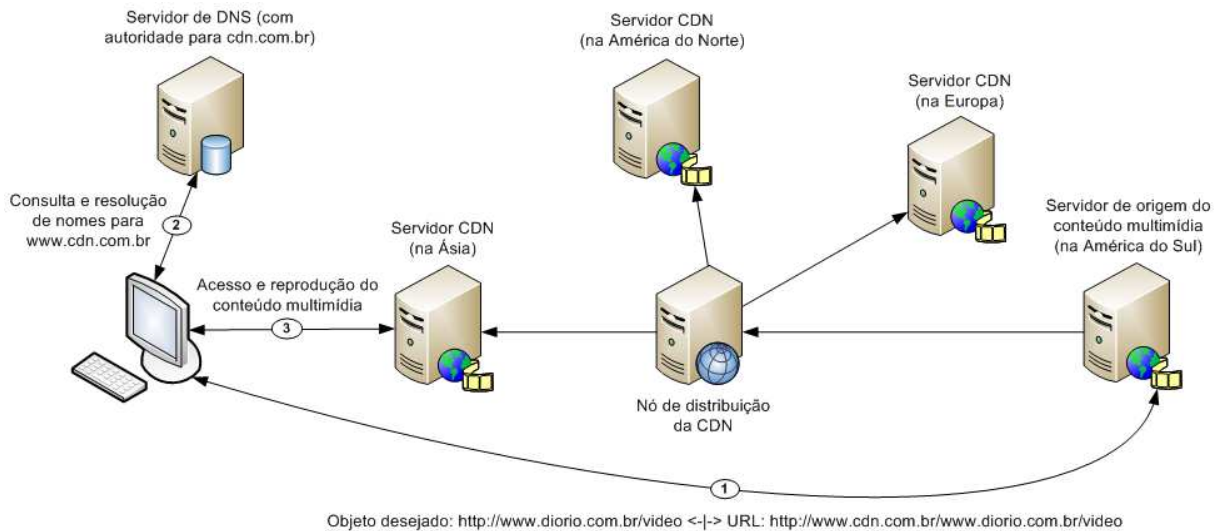


Figura 8 – Redes de distribuição de conteúdos (CDNs) (Fonte: Adaptado de [23]).

Dessa forma a CDN determina qual é o melhor servidor para atender a requisição solicitada pelo cliente *web* com base em sua localização, reduzindo a distância entre o usuário e o servidor multimídia (e os eventuais atrasos e perdas de pacotes associados a essa distância) e, também, as altas demandas de largura de banda nos ISPs de níveis mais altos para atender múltiplas requisições ao conteúdo multimídia requisitado (especialmente quando o conteúdo requisitado torna-se popular no contexto Internet).

2.3.4 – Redes multicast

De modo complementar às CDNs, redes com transmissões multicast também podem ser utilizadas para reduzir o tráfego de rede na distribuição de grandes volumes de dados na Internet. Nesse caso, em vez de efetuar transmissões individuais entre o transmissor e cada receptor de modo individualizado, essa transmissão é realizada de um transmissor para um grupo de receptores (grupo multicast), reduzindo o volume de tráfego na rede de modo significativo (Figura 9).

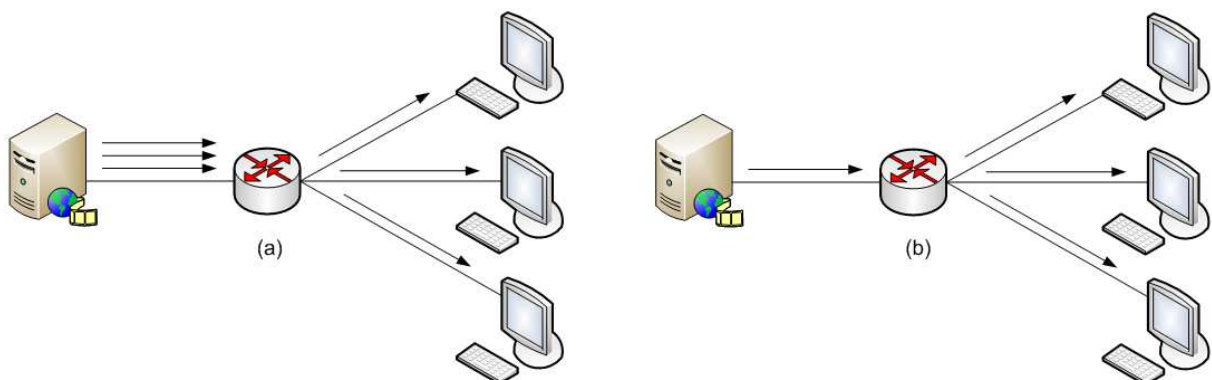


Figura 9 – Transmissões unicast (a) versus transmissões multicast (b).

De acordo com [23], exemplos de aplicações que podem se beneficiar desse tipo de transmissão incluem aquelas voltadas à transferência de dados de modo constante e/ou em grandes volumes (como atualizações de *softwares* ou aplicações de cotações, dentre outras) e

aplicações multimídia de modo geral (para distribuição de áudio, vídeo e dados, como palestras, filmes e jogos *online*, dentre outras).

Conforme descrito em [24], um exemplo desse tipo de rede é a MBone (*Multicast Backbone*), que é uma rede *overlay* formada sobre a Internet e que está em operação desde 1992. Dentre os conteúdos transmitidos na MBone estão conferências e eventos científicos (tipicamente do IETF) até experiências com *shows* e festivais de cinema, dentre outros.

Quanto aos seus protocolos, esse tipo de rede tem suas exigências próprias quanto ao gerenciamento de grupos multicast, bem como ao processo de roteamento de seu conteúdo, dentre outros, sendo comum os protocolos IGMP (*Internet Group Management Protocol*), MOSPF (*Multicast Open Shortest Path First*), DVMRP (*Distance Vector Multicast Routing Protocol*) e PIM (*Protocol Independent Multicast*), dentre outros [23, 24]. Para outras informações a respeito de transmissões multicast, sugerem-se as referências [23, 24]. Para o MBone em específico, sugere-se a referência [24].

2.4 – Algumas considerações para o dimensionamento de redes multimídia

Conforme descrito anteriormente, as principais dificuldades associadas às aplicações multimídia estão voltadas aos requisitos impostos por elas para a rede (especialmente quanto à temporização e largura de banda). Nesse contexto, de acordo com [23], uma possível forma de minimizar essas dificuldades seria, por exemplo, implementar enlaces de altas velocidades em toda à Internet e dar um tratamento diferenciado para tais aplicações num contexto fim a fim. Porém, tendo em vista toda a heterogeneidade da rede, tanto quanto às questões técnicas quanto às questões organizacionais e comerciais, isso é uma tarefa extremamente complexa, praticamente impossível de ser realizada.

Dessa forma, percebe-se que realizar o dimensionamento de uma rede multimídia, bem como o provisionamento de banda necessário para dar suporte às suas aplicações é uma tarefa extremamente complexa [23, 24]. Para contornar essas dificuldades, no lado “desenvolvedor”, os projetistas das aplicações multimídia se desdobram utilizando técnicas e recursos para atenuar os requisitos impostos por suas aplicações junto ao serviço de melhor esforço da Internet (conforme descrito na Seção 2.3.2). No lado “rede”, os provedores investem, isoladamente, em dispositivos de rede mais eficientes e em enlaces mais rápidos. E, ainda assim, a Internet de hoje precisa evoluir de modo significativamente grande para suportar, com qualidade, as atuais e futuras demandas por conteúdos multimídia [23, 24].

Nesse contexto, além das soluções e procedimentos anteriormente descritos, uma possível forma de se maximizar os recursos da rede para atender as demandas das aplicações multimídia está associada à implementação de modelos de tráfego específicos para tais aplicações, de modo a definir, por exemplo, o comportamento dessas aplicações perante a rede, bem como de tratá-las de modo diferenciado (a partir de classificações e marcações nos cabeçalhos IP, por exemplo). Para tal, os próximos capítulos descrevem as características e procedimentos que podem ser utilizados para viabilizar tais recursos.

3 – Modelos para fontes de tráfego

Com a evolução das redes de computadores e a popularização do acesso residencial de banda larga, o perfil de tráfego de rede gerado pelas diversas aplicações em execução nos sistemas finais da Internet também vem evoluindo e se tornando mais complexo [3, 4, 27].

Inicialmente, nos primórdios da Internet, o tráfego de rede era tipicamente gerado por aplicações de acesso *web*, correio eletrônico e transferência de arquivos [25], dentre outras, as quais têm seu perfil de tráfego tipicamente associado à alta sensibilidade quanto à perda de pacotes, porém pequena sensibilidade quanto à atrasos e variações de atrasos, tendo como protocolo de transporte, comumente, o protocolo TCP, que tem como uma de suas filosofias, a confiabilidade na entrega de seus segmentos (conforme descrito na Seção 2.2.1). Nesse caso, diz-se que o tráfego gerado por tais aplicações é elástico (não impõe exigências temporais em sua transmissão, porém exige confiabilidade na entrega de suas informações).

Por outro lado, nos dias de hoje, além das aplicações citadas anteriormente, é comum a utilização de diversas aplicações *stream*, tais como aplicações para acesso e distribuição de áudio e vídeo pela Internet, além de diversas aplicações para telefonia e videoconferência, também, pela Internet, dentre outras [23, 24]. Nesse caso, o perfil de tráfego dessas aplicações é completamente distinto do perfil de tráfego das demais aplicações da rede, exigindo, por exemplo, pequeno atraso fim a fim e pequena variação de atraso como alguns de seus requisitos funcionais perante a rede, tendo como protocolo de transporte, comumente, o protocolo UDP, que tem como uma de suas filosofias a alta velocidade na entrega de seus segmentos, porém sem a confiabilidade fornecida pelo TCP (conforme descrito na Seção 2.2.1), dentre outras características. Nesse caso, diz-se que o tráfego gerado por tais aplicações é *stream* (ou inelástico – não exige confiabilidade na entrega de suas informações, porém impõe exigências temporais em sua transmissão).

A Figura 10 ilustra algumas aplicações e seus tipos de tráfego:

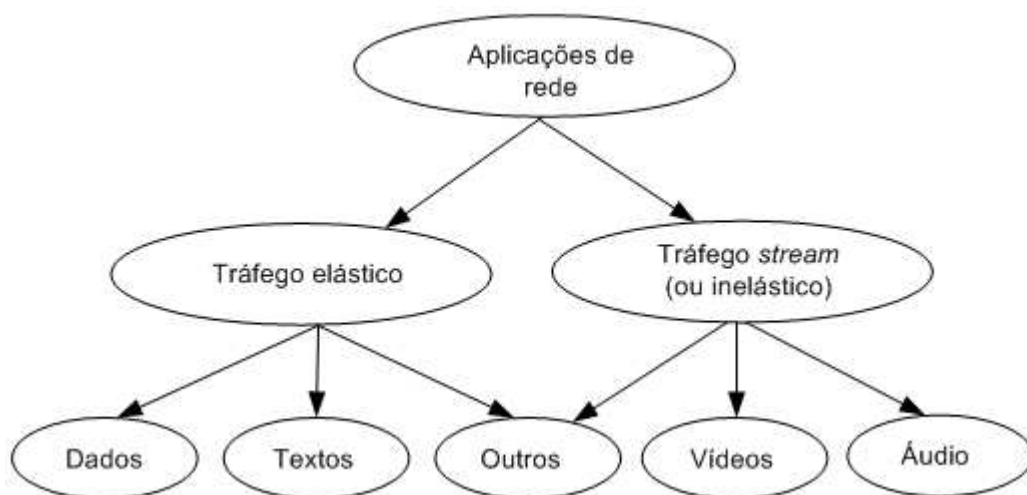


Figura 10 – Algumas aplicações e seus tipos de tráfego.

De modo macro, a principal distinção entre o perfil de tráfego dessas aplicações está associada às suas exigências temporais, bem como ao comportamento de ambas quanto às condições da rede durante seu processo de transmissão (congestionamento, largura de banda,

etc.). Esse comportamento se deve, especialmente, ao serviço de melhor esforço da Internet (conforme descrito na Seção 2.3.2), do protocolo de transporte utilizado para o transporte das informações pela rede (TCP ou UDP, conforme descrito na Seção 2.2.1) e dos eventuais controles realizados no nível de aplicação para adicionar novas funcionalidades e recursos a essas aplicações como, por exemplo, adição de marcas de tempo para execução de conteúdos multimídia em momentos específicos ou definição de uma taxa de transmissão específica em aplicações que executam sobre UDP, dentre outras [23].

Nesse contexto, os modelos para fontes de tráfego podem ser utilizados para definir o comportamento das aplicações perante a rede, tratando de questões voltadas, por exemplo, da quantidade de *bits* que será transmitida a cada momento, de como se dará a transmissão em situações de congestionamento ou ociosidade da rede, do tamanho dos dados a serem enviados e do atendimento às novas requisições, dentre outros [5, 6, 9, 11, 12]. Para tal, a modelagem de tráfego está fortemente associada à forma com a qual os dados serão enviados à rede (tipo de tráfego), bem como na utilização de algoritmos e funções de distribuição para fornecer os procedimentos para a geração do tráfego desejado [7, 8, 10], conforme descrito nas seções seguintes.

3.1 – Categorias de tráfego

Uma aplicação pode enviar suas informações à rede utilizando diversos tipos de tráfego, sendo mais comuns os tráfegos elásticos de bloco e de transição *on/off* e o tráfego *stream*, os quais são descritos nas seções seguintes.

3.1.1 – Tráfego de bloco

De acordo com [28], no tráfego de bloco, o transmissor envia uma quantidade específica de dados (blocos de dados) por sessão ao seu destinatário. Esses blocos de dados possuem limitações rígidas de tamanho (quantidade de blocos transmitidos) e de tempo (intervalo) de envio (periodicidade de transmissão dos blocos de dados) ao seu receptor, conforme ilustra a Figura 11:

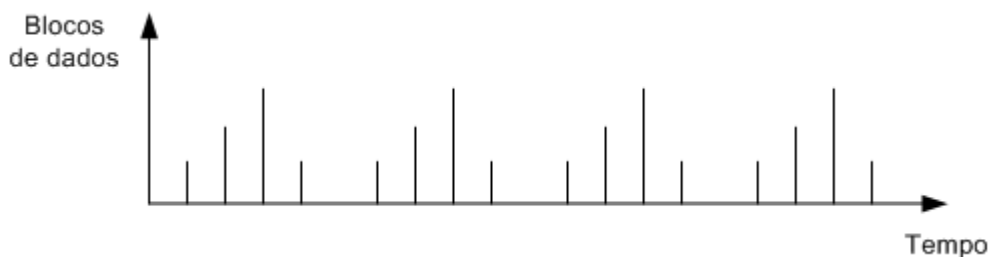


Figura 11 – Visão geral: Tráfego de bloco (Fonte: Adaptado de [28]).

Nesse caso, a modelagem de fontes de tráfego baseadas em blocos de dados consiste, basicamente, na definição de variáveis associadas (I) à quantidade (taxa) de blocos a serem enviados por sessão, (II) ao tamanho de cada bloco de dados e (III) à temporização (intervalo) que será utilizada para o envio de cada bloco de dados, bem como na utilização de funções de distribuição (como Poisson, por exemplo) para a geração do tráfego propriamente dito.

3.1.2 – Tráfego de transição *on/off*

Conforme descrito em [28], no tráfego de transição *on/off*, o envio de dados do transmissor para o receptor ocorre alternando entre períodos de atividade (*on*) e inatividade (*off*). Durante o período de atividade é comum que o transmissor envie rajadas de dados a uma taxa constante para o receptor. Por sua vez, durante o período de inatividade, não há geração de pacotes do transmissor para o receptor [28]. A Figura 12 ilustra o envio de dados utilizando o tráfego de transição *on/off*:

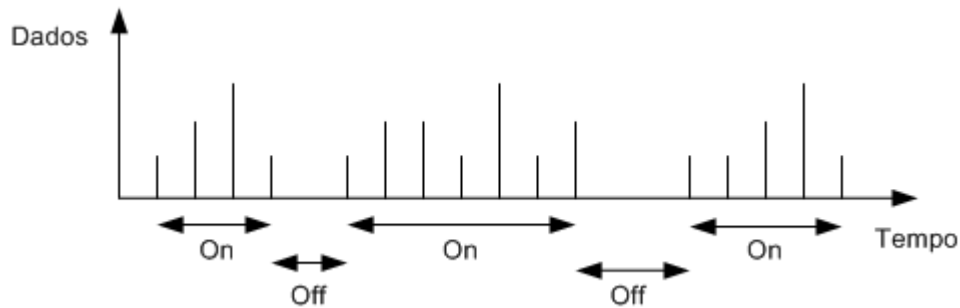


Figura 12 – Visão geral: Tráfego de transição *on/off* (Fonte: Adaptado de [28]).

Nesse caso, a modelagem de fontes de tráfego baseadas em transições *on/off* consiste, basicamente, na definição de variáveis associadas (I) à duração dos períodos “*on*” e “*off*”, (II) à quantidade (taxa) de dados a serem enviados durante o período “*on*”, (III) ao tamanho dos dados que serão enviados e (IV) ao intervalo para o envio desses dados, bem como na utilização de funções de distribuição (como Pareto, por exemplo) para a geração do tráfego propriamente dito.

3.1.3 – Tráfego *stream*

No tráfego *stream*, é comum que a fonte geradora de tráfego emita rajadas de dados distintas em diferentes escalas de tempo aproveitando-se, especialmente, dos períodos de inatividade da rede [28]. Nesse caso, as rajadas de dados têm como base a largura de banda da rede num determinado período de tempo. Quanto maior a largura de banda disponível, maior será a rajada de dados. Por outro lado, à medida que outros tráfegos de dados são gerados na rede, as rajadas do tráfego *stream* são reduzidas. A Figura 13 ilustra o perfil típico de um tráfego *stream*:

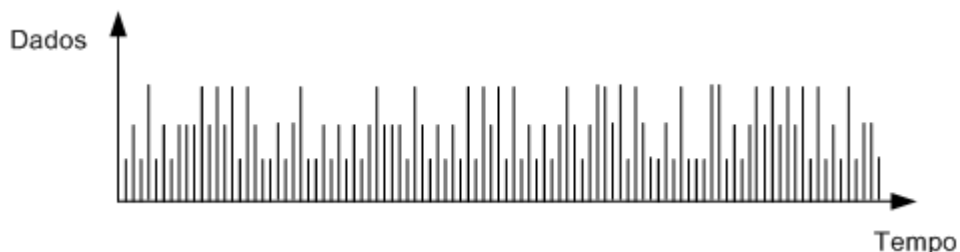


Figura 13 – Visão geral: Tráfego *stream* (Fonte: Adaptado de [28]).

Nesse caso, a modelagem de fontes de tráfego do tipo *stream* consiste, basicamente, na definição da taxa de dados que será enviada do transmissor ao receptor, a qual pode ser fixa ou variável (utilizando o modelo *Wavelet*, por exemplo).

3.1.4 – Tráfego fractal e multifractal

De acordo com [29], o termo fractal foi proposto em 1975 por Benoit B. Mandelbrot para designar objetos matemáticos que possuem uma estrutura rica em detalhes ao longo de muitas escalas de observação, tendo como principal característica os padrões de auto-similaridade entre esses objetos, em que um objeto é tido como auto-similar quando contém réplicas menores de si mesmo em todas as suas proporções de escala. Dessa forma, o termo fractal não está restrito à área computacional e pode ser utilizado em diversas outras áreas, tais como físicas e humanas para identificar padrões de auto-similaridade entre os vários objetos analisados. Quanto ao termo multifractal, ele é uma generalização do termo fractal.

No que se refere à modelagem de tráfego, a partir de análises no tráfego de rede e utilizando, por exemplo, a distribuição de Poisson (brevemente descrita na Seção 3.2.3), pode-se modelar, por exemplo, tráfegos multimídia a partir de processos fractais que identificam a auto-similaridade do tráfego analisado.

Como exemplo, de acordo com [29], a Figura 14 ilustra padrões de auto-similaridade em 4 momentos distintos (instantes 10 milissegundos, 100 milissegundos, 1 segundo e 10 segundos) em umas das redes FastEthernet da Universidade de Drexel:

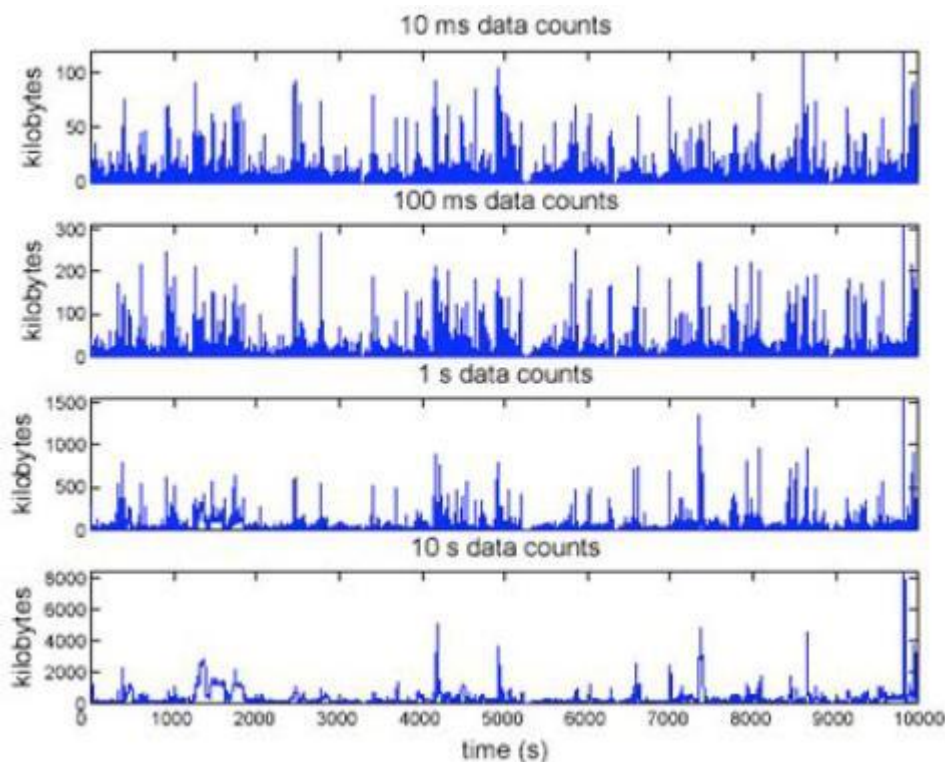


Figura 14 – Visão geral: Tráfego fractal (Fonte: [29]).

3.2 – Funções de distribuição

As funções de distribuição são utilizadas para fornecer os parâmetros desejados para a geração do tráfego multimídia. Dentre as funções de distribuição mais utilizadas, destacam-se a distribuição normal e a distribuição exponencial. Outras distribuições que podem ser utilizadas na modelagem de tráfego multimídia são as distribuições de Poisson, de Pareto e de Weibull, dentre outras, as quais são brevemente descritas nas seções seguintes.

3.2.1 – Distribuição normal

De acordo com [30], é a mais importante distribuição de probabilidade, sendo aplicada em inúmeros fenômenos e utilizada para o desenvolvimento teórico da estatística. Também é conhecida como distribuição de Gauss ou distribuição gaussiana, sendo descrita por seus parâmetros de média (μ) e desvio padrão (σ) e tendo a seguinte função densidade de probabilidade:

$$f(x; \mu, \sigma^2) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \quad (1)$$

Quanto à sua utilização, é comumente empregada em fenômenos físicos e financeiros e na estatística inferencial (estimação estatística), servindo de referência para outras distribuições. Exemplos típicos de utilização estão associados à análise de erros, estimativas de falhas, estimativas de reparo e retornos financeiros, dentre outros.

3.2.2 – Distribuição exponencial

De acordo com [30], a distribuição de probabilidade do intervalo x entre dois sucessos consecutivos de uma lei de Poisson é a distribuição exponencial. Sua função densidade de probabilidade é dada por:

$$f(x; \lambda) = \begin{cases} 0 & x < 0 \\ \lambda e^{-\lambda x} & x \geq 0 \end{cases} \quad (2)$$

Quanto à sua utilização, é comumente empregada em estatísticas de vida útil de equipamentos diversos ou no intervalo de tempo entre eventos que ocorrem aleatoriamente como, por exemplo, demandas de serviços por computador, de chamadas telefônicas e de pesquisas em sites de busca, dentre outros.

3.2.3 – Distribuição de Poisson (Discreta)

A distribuição de Poisson (ou distribuição discreta) é utilizada para expressar a quantidade de eventos num determinado período de tempo e/ou espaço [31]. Esses eventos devem ocorrer a uma taxa média conhecida e de modo independente (aleatório) ao tempo do último evento. Sua função densidade de probabilidade é dada por:

$$P(x, t) = \frac{(\lambda t)^x}{x!} e^{-\lambda t} \quad (3)$$

Quanto à sua utilização, é comumente empregada em estatísticas de chamadas telefônicas por unidade de tempo, de chegada de clientes por unidade de tempo e de acidentes por unidade de tempo, dentre outros. Como exemplo, de acordo com [30], em muitos casos, conhece-se o número de sucessos, porém se torna difícil, às vezes, sem sentido, determinar o número de fracassos ou o número total de provas. Por exemplo: Automóveis que passam numa esquina. Pode-se, num determinado intervalo de tempo, anotar o número de carros que passaram, porém, o número de carros que deixaram de passar pela esquina não poderá ser determinado. Da mesma forma, o número de emendas num rolo de fita colante. Pode-se determinar quantas emendas existem, porém não é possível contar quantas emendas não ocorreram. Para tal, a distribuição de Poisson pode ser utilizada.

3.2.4 – Distribuição de Pareto

É uma distribuição utilizada para modelar diversos fatos observáveis em diversas áreas, tais como áreas social, econômica, científica e industrial, dentre outras [29]. Sua função densidade de probabilidade é dada por:

$$f(x) = \begin{cases} \alpha \frac{x_m^\alpha}{x^{\alpha+1}} & x \geq x_m \\ 0 & x < x_m \end{cases} \quad (4)$$

Quanto à sua utilização, é comumente empregada em estatísticas de renda e riqueza e em comparações que demonstram equilíbrio do “grande” com o “pequeno” como, por exemplo, o tamanho dos centros urbanos quando comparados ao número de vilarejos/aldeias, o tamanho dos arquivos enviados à rede utilizando um ou outro protocolo de rede, o número de conexões por serviços de rede, as unidades de CPU por processos, etc.

3.2.5 – Distribuição de Weibull

A distribuição de Weibull é uma distribuição estatística utilizada para modelar, comumente, falhas em equipamentos [31]. Está relacionada com outras distribuições estatísticas como, por exemplo, com a distribuição exponencial (brevemente descrita na Seção 3.2.2). Sua função densidade de probabilidade é dada por:

$$f(x; k, \lambda) = \frac{k}{\lambda} \left(\frac{x}{\lambda}\right)^{k-1} e^{-(x/\lambda)^k} \quad (5)$$

Em que $x \geq 0$ e $k > 0$, e k é o parâmetro de tamanho, e $\lambda > 0$ é o parâmetro de escala da distribuição.

Quanto à sua utilização, assim como a distribuição exponencial, é comumente empregada em estatísticas de vida útil de equipamentos diversos e, também, para a determinação de falhas em tais equipamentos, conforme descrito anteriormente.

4 – Gateway multimídia

4.1 – Descrição geral

Um *gateway* multimídia é um elemento de rede capaz de distinguir e encaminhar tráfegos associados a serviços multimídia, tais como áudio, vídeo e voz, por exemplo, à sua respectiva aplicação receptora. Essa identificação/distinção de tráfego e seu encaminhamento à sua aplicação receptora devem ser realizados em tempo real, considerando o tipo de tráfego em questão (*stream* ou elástico, associados aos serviços de áudio, voz, vídeo ou dados, por exemplo), bem como o ambiente de rede ao qual esse tráfego está sendo gerado e consumido (ambiente com um ou vários transmissores e receptores, utilizando meio físico guiado ou não guiado, etc.). A Figura 15 ilustra, de modo macro, a distinção e o encaminhamento de tráfegos associados aos serviços de áudio, voz, vídeo e dados para suas respectivas aplicações receptoras através de um *gateway* multimídia:

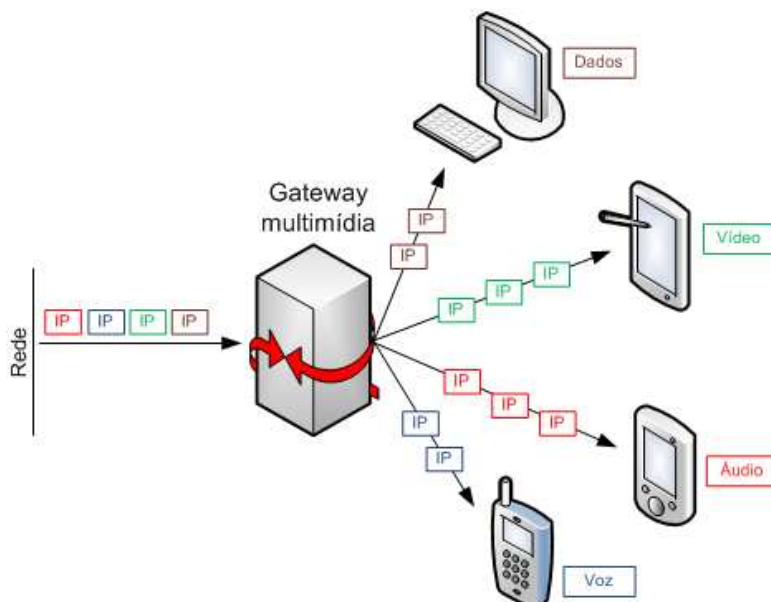


Figura 15 – Gateway multimídia.

Em tal ambiente, múltiplas aplicações multimídia geram tráfego tipicamente *stream* na rede, os quais são intermediados pelo *gateway* multimídia e direcionados à sua respectiva aplicação receptora. Essa intermediação ocorre de modo transparente às aplicações transmissora e receptora do conteúdo multimídia (assim como em uma transmissão fim a fim na Internet, por exemplo, em que os comutadores e roteadores ao longo desse caminho fim a fim são transparentes às aplicações transmissora e receptora), tornando sua implementação neutra quanto aos *hosts* e aplicações da rede.

Para tal, o *gateway* multimídia é tido como *gateway* de acesso à rede do *host* que executa as aplicações multimídia (e eventuais outras aplicações de rede) objetos de seu mecanismo funcional, posicionado (implementado) como um componente intermediário a tal *host*, nesse caso como um “elemento terciário” a tal *host*, de modo a se portar como um “módulo complementar” ao processo de comunicação entre aplicações multimídia variadas (em execução ao longo da rede), agregando e fornecendo recursos que viabilizem, por exemplo, a identificação, priorização e tratamento diferenciado quanto aos tráfegos *stream* gerado por

aplicações de áudio, vídeo ou voz, por exemplo, quando comparado ao tráfego elástico gerado por outras aplicações de rede.

Nessa estrutura, por meio dessa abordagem “modular”, assim como na abordagem em camadas do Modelo de Referência ISO/OSI ou da própria Arquitetura de Protocolos TCP/IP, por exemplo, a implementação desse novo componente de rede (*gateway* multimídia) torna-se, além de menos complexa, objetiva quanto às suas funcionalidades, bem como independente quanto aos demais componentes da rede, porém utilizando e fornecendo serviços específicos às aplicações multimídia de tais componentes, tais como utilização do tráfego *stream* gerado por aplicações multimídia de áudio, vídeo ou voz, dentre outras, para o fornecimento de serviços de identificação e priorização de tais tráfegos quando comparado a tráfegos elásticos gerado por outras aplicações da rede, bem como da adição de mecanismos de qualidade de serviço aos tráfegos que necessitem de maior prioridade quanto aos demais tráfegos da rede, por exemplo.

Vale ressaltar que, funcionalmente, o *gateway* multimídia é tido como componente intermediário aos sistemas transmissor e receptor do conteúdo multimídia, atuando como um “módulo” externo ao(s) *host(s)* executando tais aplicações, conforme ilustra a Figura 16:

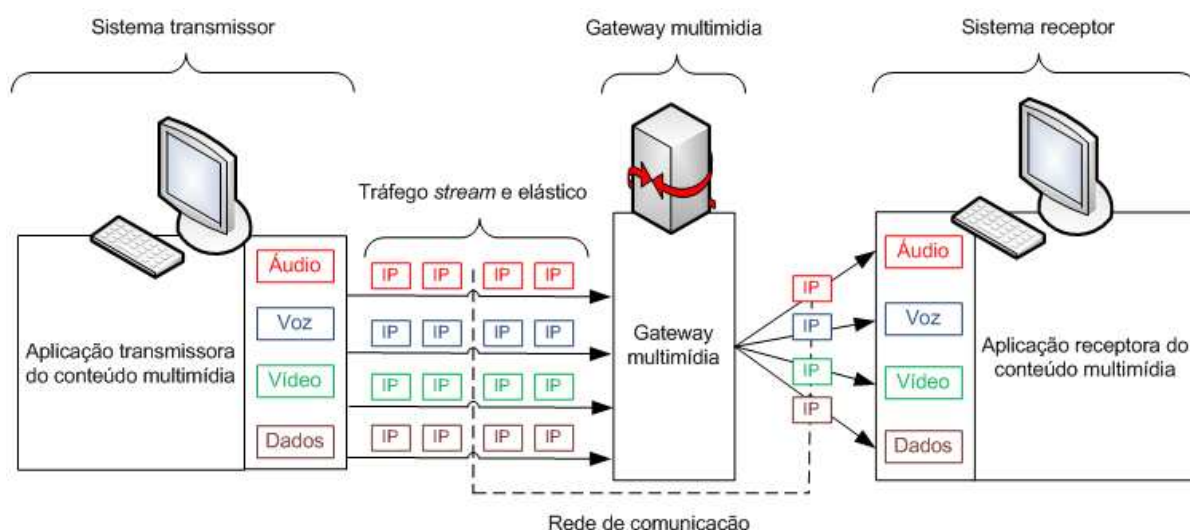


Figura 16 – Sistemas transmissor e receptor dos serviços de áudio, voz, vídeo e dados (com gateway multimídia).

Em tal ambiente, cabe ao *gateway* multimídia direcionar, especialmente, o tráfego *stream* pertinente aos serviços multimídia de áudio, vídeo ou voz, por exemplo, ou até mesmo elástico, pertinente a serviços de dados, por exemplo, entrantes às suas interfaces de rede para suas respectivas aplicações receptoras no(s) *host(s)* que as executa(m), nesse caso utilizando de identificadores distintos quanto a tais tráfegos a partir de valores armazenados no cabeçalho do protocolo IP dos pacotes IP de tais tráfegos, bem como de mecanismos de qualidade de serviço (QoS) que objetivem a priorização e tratamento diferenciado entre um e outro tipo de tráfego, de modo a disponibilizar, por exemplo, maior taxa de transmissão para aplicações que necessitem de tal recurso quando comparado a outras aplicações de rede que não necessitem de tal recurso.

Pelo fato do *gateway* multimídia ser posicionado como *gateway* de acesso do(s) *host(s)* da rede, ele pode receber pacotes IP pertinentes a outros tipos de tráfegos, tais como navegação

web, transferência de arquivos ou acesso a *e-mail*, dentre outros, os quais podem, por exemplo, ser descartados ou transmitidos à sua aplicação receptora utilizando de mecanismos que disponibilizem, por exemplo, pequena ou alta taxa de transmissão a tais tipos de tráfegos, dentre outros.

Para tal, a estrutura funcional do *gateway* multimídia se deve, especialmente, pela utilização de identificadores quanto aos tráfegos intermediados por ele, bem como na utilização do protocolo IP, responsável, nesse caso, por armazenar tais identificadores em seus datagramas e viabilizar sua estrutura funcional. A partir de tais identificadores, o *gateway* multimídia, além de direcionar o tráfego em questão à sua respectiva aplicação receptora, pode classificar esse tráfego conforme seu tipo de serviço (áudio, voz, vídeo ou dados, por exemplo), bem como adicionar mecanismos que objetivem garantir qualidade de serviço a um ou outro tipo de tráfego ou serviço multimídia, dentre outros.

Nesse contexto, a Figura 17 ilustra, de modo geral, a estrutura funcional quanto ao subsistema de comunicação do *gateway* multimídia:

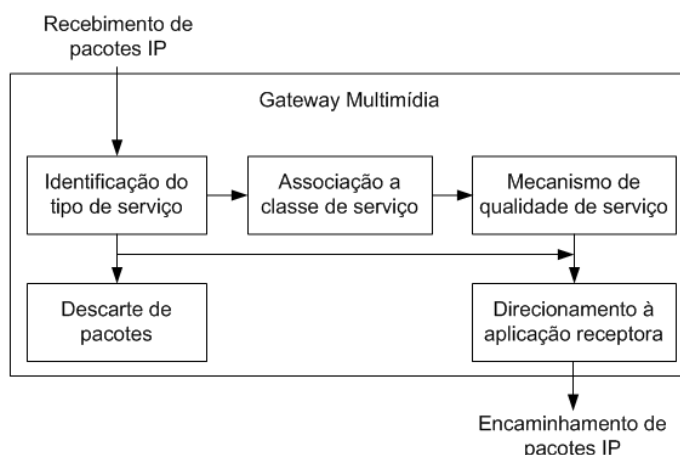


Figura 17 – Visão geral: Estrutura funcional do subsistema de comunicação do *gateway* multimídia.

De modo complementar a essa macro-descrição quanto ao *gateway* multimídia, as seções seguintes descrevem os conceitos e técnicas que viabilizam a identificação de tipos de tráfegos distintos com base em identificadores presentes no cabeçalho do protocolo IP, bem como da utilização de tais identificadores para criar múltiplas classes de serviço (CoS) na rede e da utilização de tais classes de serviço para implementar mecanismos para ao fornecimento de qualidade serviço (QoS) aos tráfegos de maior prioridade quando comparado aos demais tráfegos de menor prioridade ao longo da rede.

4.2 – Identificação e encaminhamento do tráfego multimídia

Para distinguir e encaminhar tráfegos *stream* e/ou elástico pertinentes aos serviços multimídia de áudio, voz, vídeo ou dados, por exemplo, à sua respectiva aplicação receptora, bem como do tratamento diferenciado de tais tráfegos, é necessária a utilização de mecanismos que, inicialmente, identifiquem e classifiquem tais tráfegos conforme seu tipo de serviço multimídia.

Nesse contexto, uma possível forma de se distinguir o tráfego das diversas aplicações elásticas ou *stream* para, por exemplo, dar um tratamento diferenciado a uma ou outra aplicação está associado ao fornecimento de múltiplas classes de serviço (CoS) na rede. A partir dessas múltiplas classes de serviço é possível, por exemplo, realizar certas reservas de recursos, bem como dar certas prioridades a uma ou outra aplicação de modo isolado das demais aplicações da rede. Para tal, pode-se, por exemplo, associar as aplicações a uma ou a outra classe de serviço a partir de seu protocolo de nível de aplicação ou transporte ou do endereço (IP) do transmissor ou do receptor (ou, ainda, do endereço de rede de ambos). Como exemplo, essa abordagem de classificação de serviços é a mesma utilizada pelo padrão atual de fornecimento de serviços diferenciados da Internet, denominado Diffserv [RFC 2475].

Em tal ambiente, para viabilizar o fornecimento de múltiplas classes de serviço na rede, deve-se utilizar algum mecanismo para marcação e identificação de quais pacotes pertencem a qual classe de serviço. No contexto IP, no protocolo IPv4, isso se dá pelo campo ToS (*Type of Service*) e no protocolo IPv6 pelo campo TC (*Traffic Class*), ambos com 8 bits de comprimento, hoje tidos (reformulados) como DSCP (*Differentiated Services Codepoint*) [RFC 2474], com 6 bits de comprimento, e ECN (*Explicit Congestion Notification*) [RFC 3168] com 2 bits de comprimento.

Como exemplo, as Figuras 18 e 19 ilustram, respectivamente, o formato dos datagramas IPv4 e IPv6 em suas especificações iniciais, bem como a estrutura dos novos campos DSCP e ECN no cabeçalho de ambos (Figura 20):

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

Figura 18 – Formato do datagrama IPv4 (Fonte: Adaptado de RFC 791).

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
Source Address				
Destination Address				

Figura 19 – Formato do datagrama IPv6 (Fonte: Adaptado de RFC 2460).

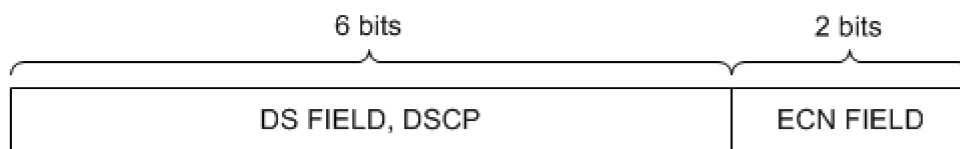


Figura 20 – Estrutura dos campos DSCP e ECN no IPv4 e no IPv6 (Fonte: Adaptado dos RFCs 2474 e 3168).

Vale ressaltar que, nos datagramas IPv4, as definições originais quanto ao ToS (como as definidas no RFC 1349, por exemplo – Tabela 4) são incompatíveis com as definições do DSCP (RFC 2474). Apenas como exemplo, a Figura 21 ilustra o antigo formato organizacional do campo ToS nos datagramas IPv4. De modo similar, a Tabela 4 descreve alguns valores de ToS definidos pelo RFC 1349 (obsoletos pelo RFC 2474):

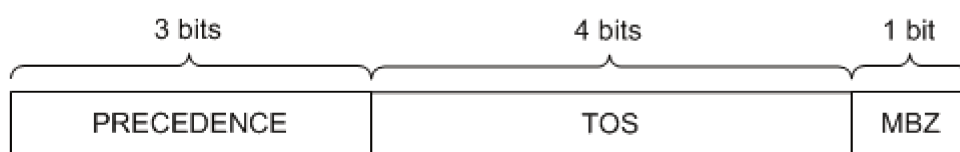


Figura 21 – Antigo formato do campo ToS no IPv4 (Fonte: Adaptado de RFC 1349).

ToS	Descrição
000-0000-0 (0)	Normal service (ToS padrão)
000-0001-0 (2)	Minimize monetary cost
000-0010-0 (4)	Maximize reliability
000-0100-0 (8)	Maximize throughput
000-1000-0 (16)	Minimize delay

Tabela 4 – ToS's definidos pelo RFC 1349 (obsoletos pelo RFC 2474).

Nessa nova estrutura, o DSCP possibilita a definição de até 64 (2^6) classes de tráfegos distintas, associadas a um determinado tipo (grupo) de comportamento de tráfego como, por exemplo:

- BE (*Best Effort*) ou DF (*Default Forwarding*): para tráfegos de melhor esforço (sem a necessidade de tratamentos específicos perante à rede);
- EF (*Expedited Forwarding*), RFC 3246: para tráfegos sensíveis a perdas, atrasos e variações de atrasos;
- AF (*Assured Forwarding*), RFC 2597: para tráfegos com garantias de taxas de transmissão com bases em condições previamente definidas. Esse grupo está organizado em quatro classes com três níveis de prioridade (alto, médio e baixo) em cada uma dessas classes;
- CS (*Class Selector*): para manter a compatibilidade com tráfegos que utilizam os valores de precedência do ToS do IPv4.

Quanto à marcação dos pacotes IP propriamente ditos, em linhas gerais, ela pode ocorrer assim que eles são gerados, diretamente por seu transmissor, ou por seu roteador de ingresso à

rede. A Figura 22 ilustra um possível cenário para classificação e marcação de pacotes IP com o intuito de se distinguir, por exemplo, o tráfego gerado por uma aplicação de videoconferência pela Internet do tráfego gerado pelas demais aplicações da rede (acesso *web*, por exemplo):

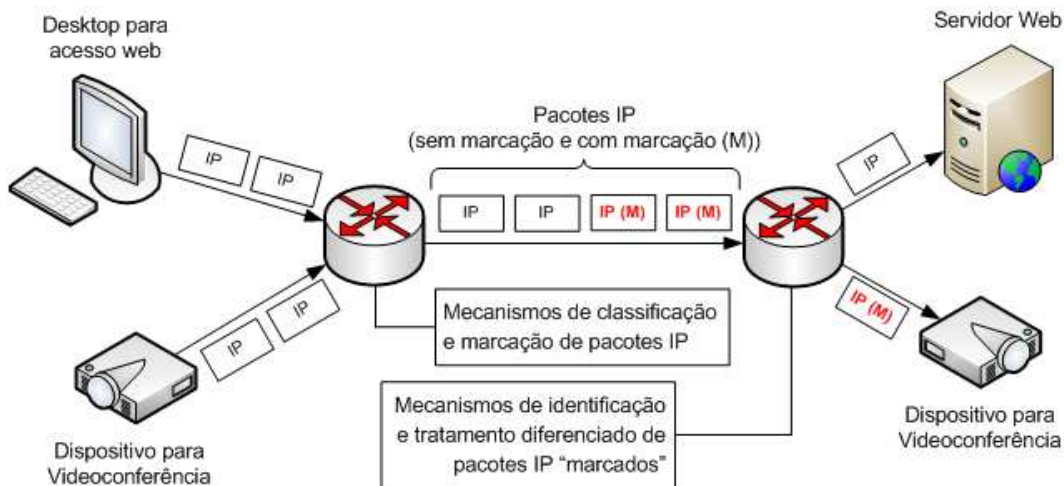


Figura 22 – Exemplo de cenário para marcação e classificação de pacotes IP.

Dessa forma, depois de marcado, o pacote IP poderá receber um tratamento diferenciado com base em sua respectiva marcação como, por exemplo, eventuais reservas de recursos, limitações ou garantias de taxas de transmissão e tratamento diferenciado pelo sistema receptor desse pacote, dentre outros. Vale ressaltar que o fato de marcar o pacote não significa, necessariamente, que ele terá tratamento diferenciado, mas sim que essa marcação poderá ser utilizada para esse propósito.

Nesse contexto, o presente projeto de pesquisa propõe que a identificação, classificação e priorização quanto aos tráfegos, especialmente *stream*, entrantes ao *gateway* multimídia ocorram em nível de rede (assim como no processo de roteamento de pacotes IP ao longo da rede, por exemplo), de modo transparente (e independente) ao *host* e à aplicação receptora (inclusive quanto à sua arquitetura funcional e de desenvolvimento) a partir da utilização dos campos ToS (*Type of Service*) e TC (*Traffic Class*) do protocolo IP (versões 4 e 6, respectivamente), nesse caso fazendo referência aos campos DSCP (*Differentiated Services Codepoint*) e ECN (*Explicit Congestion Notification*).

Essa proposta tem como base principal, além da motivação acadêmica e científica quanto ao presente projeto de pesquisa, a viabilidade de sua implantação a partir da utilização de campos já presentes no cabeçalho do protocolo IP, de modo que nenhuma mudança arquitetural é necessária para dar suporte à sua implementação nas redes IP (como na Internet e em todas as redes que a compõe), bem como nos sistemas finais que fazem parte de tais redes e em suas respectivas (e diversificadas) aplicações multimídia.

Vale ressaltar que para tal, é necessário que o tráfego intermediado pelo *gateway* multimídia possua identificadores que viabilizem sua distinção, os quais devem ser previamente definidos e sincronizados tanto no sistema transmissor quanto no *gateway* multimídia, de modo que o encaminhamento do tráfego seja realizado corretamente (nesse caso, sem erros de dissociação) à sua respectiva aplicação receptora.

4.3 – Identificadores para o tráfego multimídia

Quanto ao cabeçalho do protocolo IP, utilizando-se apenas do campo DSCP, de 6 bits de comprimento (uma vez que o campo ECN, de 2 bits de comprimento, refere-se a notificações de congestionamento), é possível realizar a distinção de 64 (2^6) tipos de tráfego, nesse caso tráfegos *stream* ou elástico pertinente às aplicações de rede, distintos a partir de tal campo. Considerando apenas os serviços de dados, áudio, voz e vídeo (utilizados para validar e testar o *gateway* multimídia), apenas 2 desses 6 bits seriam necessários para identificar os tráfegos associados aos mesmos, em que os demais 4 bits restantes podem ser utilizados para, por exemplo, identificar fluxos (canais) de transmissão distintos para cada um desses 4 serviços. Essa abordagem, além de explorar de uma melhor maneira o campo DSCP (evitando, por exemplo, o desperdício de utilização de seus bits), possibilita, no protocolo IPv4, a pseudo implementação do campo “*Flow Label*” presente no cabeçalho do protocolo IPv6, viabilizando a identificação de fluxos (canais) distintos para variados tipos de tráfego *stream* ou elástico através de tal campo (sem a necessidade de utilização de outros campos do cabeçalho do protocolo IP, inexistentes para esse propósito no IPv4).

Para tal, considerando-se os 6 bits disponíveis no campo DSCP, propõe-se, na Figura 23, a utilização dos 2 primeiros bits para identificação dos serviços multimídia de dados, áudio, voz e vídeo e os 4 bits seguintes para identificação dos fluxos (canais) de transmissão quanto à tais serviços:

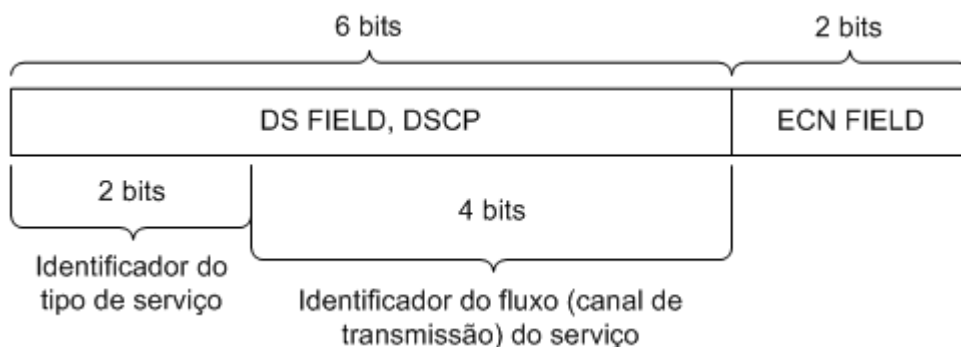


Figura 23 – Proposta de organização de bits para o campo DSCP.

De modo complementar a tal organização, propõem-se os seguintes identificadores para os serviços de dados, áudio, voz e vídeo e seus respectivos fluxos (canais) de transmissão (Tabela 5):

Tipo de serviço	Identificador do serviço	Identificador do Fluxo (canal) do Serviço
Dados	00	de “0000” até “1111” (16, 2^4 , canais)
Áudio	01	
Voz	10	
Vídeo	11	

Tabela 5 – Identificadores para os serviços de dados, áudio, voz e vídeo e seus fluxos (canais) de transmissão.

Vale ressaltar que tal abordagem (organização de bits) pode ser facilmente adequada para suportar mais ou menos serviços, aumentando-se ou diminuindo-se os bits utilizados para a identificação do serviço e/ou os bits utilizados para identificação do fluxo (canal) associado ao respectivo serviço (respeitando-se o limite de 6 bits disponível em tal campo, DSCP, do cabeçalho do protocolo IP).

4.4 – Qualidade de serviço (QoS)

4.4.1 – Visão geral

Conforme descrito na Seção 2.3.2, no atual modelo de serviço de rede utilizado na Internet (serviço de melhor esforço), as informações enviadas à rede não possuem qualquer garantia quanto à entrega de pacotes, nem quanto ao atraso fim a fim e à variação desse atraso. Além disso, pelo fato de não haver tratamento diferenciado para as diversas aplicações disponíveis na rede, uma aplicação multimídia de tempo real, tal como telefonia pela Internet, teria, por exemplo, o mesmo tratamento que uma aplicação para acesso ao serviço de *e-mail* ou navegação *web*, dentre outras. Nesse caso, como o tratamento é o mesmo, em uma situação de congestionamento os pacotes de ambas as aplicações teriam a mesma chance de serem descartados ou sujeitos aos atrasos oriundos de tal congestionamento. Porém, esse efeito seria mais negativo à aplicação multimídia de tempo real (extremamente sensível ao atraso) do que à aplicação de *e-mail* ou acesso *web* (tolerantes ao atraso).

Nesse contexto, para minimizar a ocorrência desse tipo de problema, pode-se utilizar de mecanismos que objetivem a garantia da qualidade de serviço (QoS) às aplicações que necessitem de tratamento diferenciado perante a rede, os quais consistem, basicamente, na diferenciação entre um e outro serviço, no isolamento do fluxo de tráfego desses serviços e na reserva de certos recursos de rede (como largura de banda e *buffers*, por exemplo) aos serviços que exigem tratamento diferenciado, os quais podem ser realizados, por exemplo, a partir de mecanismos para marcação, identificação e classificação de pacotes IP, dentre outros.

Quanto à qualidade de serviço propriamente dita, de acordo com [24], os principais parâmetros que a definem são: confiabilidade, retardo, flutuação e largura de banda. Esses parâmetros estão associados aos fluxos de tráfego gerados pelas diversas aplicações da rede, de modo que os parâmetros que atendam aos requisitos de qualidade de serviço de uma determinada aplicação não serão necessariamente os mesmos que atendam os requisitos de outra aplicação. A Tabela 6 descreve algumas aplicações de rede típicas e seus requisitos de qualidade de serviço:

Aplicação	Confiabilidade	Retardo	Flutuação	Largura de banda
Correio eletrônico	Alta	Baixo	Baixa	Baixa
Transferência de arquivos	Alta	Baixo	Baixa	Média
Acesso à <i>web</i>	Alta	Médio	Baixa	Média
Áudio por demanda	Baixa	Baixo	Alta	Média
Vídeo por demanda	Baixa	Baixo	Alta	Alta
Telefonia	Baixa	Alto	Alta	Baixa
Videoconferência	Baixa	Alto	Alta	Alta

Tabela 6 – Algumas aplicações e seus requisitos de QoS. (Fonte: [24]).

Dessa forma, percebe-se que mesmo em execução numa mesma rede, algumas aplicações possuem requisitos diferenciados das demais aplicações. Aplicações de transferência de arquivos exigem alta confiabilidade na entrega de suas informações, enquanto aplicações multimídia não. Algumas aplicações possuem baixa sensibilidade a atrasos (na Tabela 6, tido como retardo), enquanto outras são extremamente sensíveis ao atraso. Algumas aplicações possuem baixa sensibilidade para a entrega de pacotes em intervalos irregulares de tempo entre si (na Tabela 6, tido como flutuação), enquanto outras possuem alta sensibilidade quanto a essa flutuação de tempo. Por fim, algumas aplicações necessitam de baixa largura de banda para desempenharem suas funções com qualidade, enquanto outras necessitam de alta largura de banda para desempenhar suas funções.

Nesse contexto, o presente projeto de pesquisa propõe que, além da identificação e classificação do tráfego entrante ao *gateway* multimídia, tal *gateway* disponibilize mecanismos de qualidade de serviço quanto aos tráfegos gerados, especialmente, pelas aplicações multimídia da rede, realizando, também, um tratamento diferenciado quanto ao tráfego de tais aplicações quando em conjunto de outros tráfegos entrantes ao mesmo. Para tal, tem-se como base os identificadores descritos na Tabela 5 quanto aos campos ToS e TC do protocolo IP (versões 4 e 6, respectivamente), nesse caso fazendo referência aos campos DSCP e ECN de seu cabeçalho.

4.4.2 – Mecanismos de escalonamento e regulação

Conforme descrito em [23], uma possível forma para se alcançar a qualidade de serviço está associada à implementação de mecanismos de escalonamento e regulação na rede. Nesse caso, os mecanismos de escalonamento estão associados aos critérios de seleção de quais pacotes serão transmitidos à rede a partir de uma determinada fila de transmissão de um roteador ou do *buffer* de um *gateway* multimídia, por exemplo. Por sua vez, os mecanismos de regulação estão associados à regulação da taxa e do volume de transmissão de uma determinada aplicação ou rede, por exemplo.

Quanto aos mecanismos de escalonamento, dentre os mais comuns, destacam-se:

- Primeiro a entrar, primeiro a sair (*First In First Out*, FIFO ou *First Come First Served*, FCFS): seleciona os pacotes para transmissão com base em sua ordem de chegada à fila de transmissão. O primeiro pacote a chegar será o primeiro da fila e, conseqüentemente, o primeiro a ser transmitido; o segundo pacote a chegar será o segundo da fila e, por sua vez, transmitido logo após o primeiro e assim por diante. Não há tratamento diferenciado quanto ao tipo de pacote presente na fila, ambos têm a mesma prioridade e apenas diferem pela ordem de chegada na fila de transmissão. A Figura 24 ilustra, de modo geral, uma disciplina de escalonamento do tipo primeiro a entrar, primeiro a sair (FIFO):

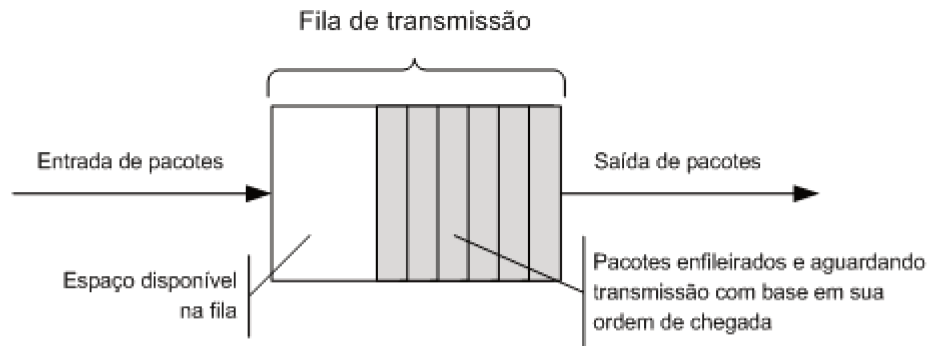


Figura 24 – Disciplina de escalonamento do tipo primeiro a entrar, primeiro a sair.

- Enfileiramento prioritário: seleciona os pacotes para transmissão com base em filas de prioridade. Ao chegar, os pacotes são classificados (com base em seu tipo de serviço) e enfileirados em filas de prioridade distintas (de alta ou baixa prioridade, por exemplo). Durante o processo de transmissão, os pacotes das filas de alta prioridade têm preferência (são transmitidos primeiro) sobre os de filas de baixa prioridade. Dessa forma, enquanto existirem pacotes de alta prioridade para serem transmitidos, os pacotes de baixa prioridade devem aguardar por sua transmissão, o que pode ser ruim para as aplicações de baixa prioridade que, provavelmente, terão um alto atraso quando comparado as aplicações de alta prioridade (enquanto houver tráfego dessas aplicações para serem enviados à rede). Quanto à organização dos pacotes de mesma prioridade nessas filas de prioridade distintas, é comum a utilização de disciplinas FIFO. A Figura 25 ilustra, de modo geral, tal disciplina de escalonamento:

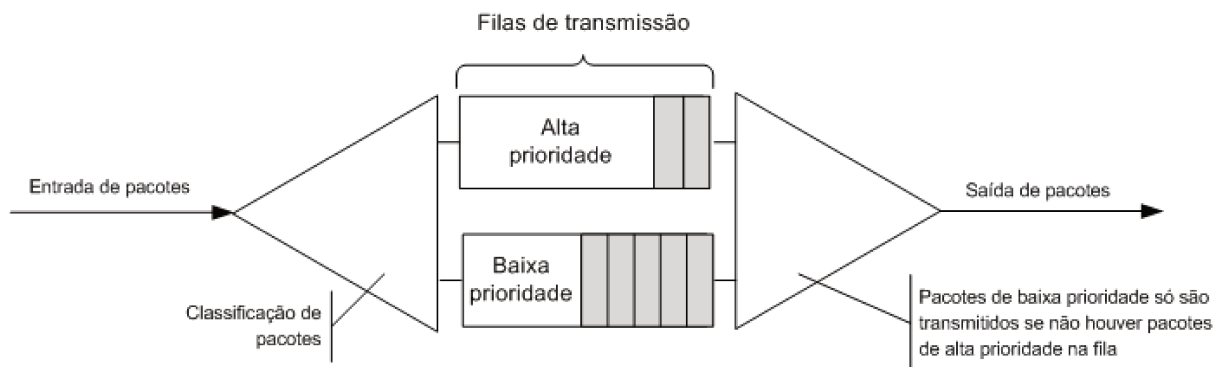


Figura 25 – Disciplina de escalonamento do tipo enfileiramento prioritário.

- Enfileiramento justo ponderado (*Weighted Fair Queueing*, WFQ): de forma similar ao enfileiramento prioritário, os pacotes também são classificados com base em sua prioridade, porém, durante o processo de transmissão, é realizado um “rodízio” entre as diversas filas de prioridade, de modo que todos os pacotes sejam transmitidos sem ter que aguardar, necessariamente, os pacotes de filas de maior prioridade. Nesse caso, a fração de banda de rede destinada aos pacotes de filas de alta prioridade é maior que os pacotes de filas de menor prioridade, mas ainda assim todos serão transmitidos de modo intercalado. A Figura 26 ilustra, de modo geral, tal disciplina de escalonamento:

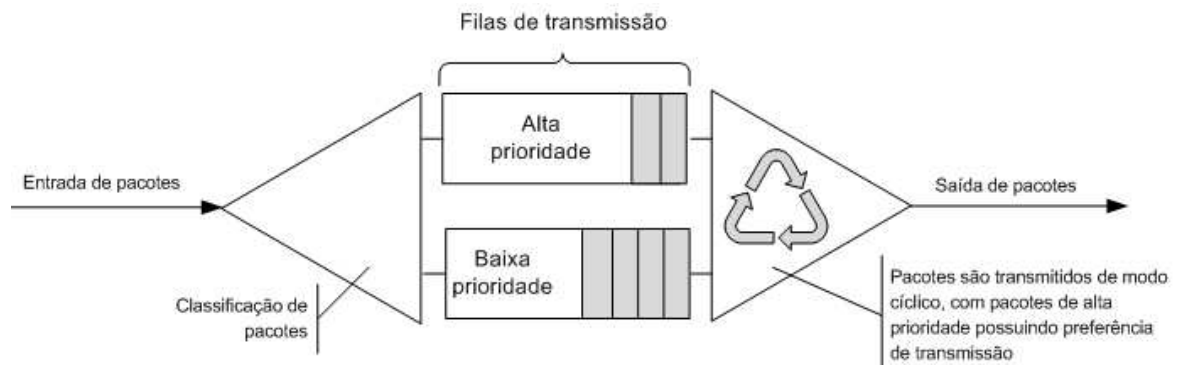


Figura 26 – Disciplina de escalonamento do tipo enfileiramento justo ponderado.

Quanto aos mecanismos de regulação, os mais comuns são o *leaky bucket* (ou algoritmo de balde furado) e o *token bucket* (ou algoritmo de balde de símbolos).

De acordo com [23], o mecanismo *leaky bucket* é uma abstração que pode ser usada para caracterizar os limites da regulação para transmissão de pacotes à rede (taxa média, taxa de pico e tamanho da rajada). É representado por um balde furado que contém b permissões. Dependendo de sua capacidade, novas permissões podem ser adicionadas (se ele não estiver cheio) ou retiradas (se ele não estiver vazio) do balde. Os pacotes só podem ser transmitidos à rede se houver permissões disponíveis, caso contrário devem aguardar a chegada de novas permissões ou, então, serem descartados pelo algoritmo do *leaky bucket* (Figura 27).

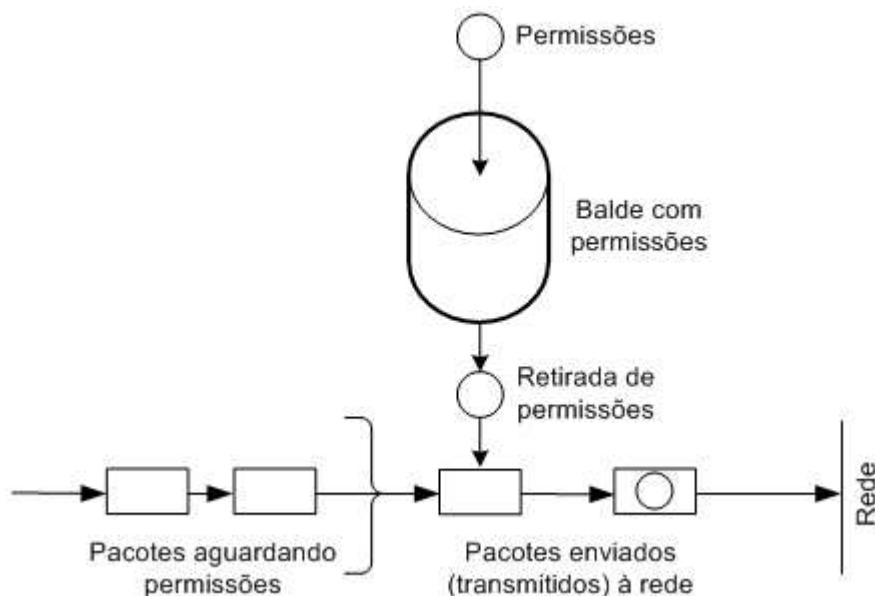


Figura 27 – Regulação com *leaky bucket algorithm*.

Por outro lado, conforme descrito em [24], em alguns casos pode ser interessante dar flexibilidade de transmissão para aplicações que necessitem de rajadas maiores (de modo não tão rígido como o aplicado pelo *leaky bucket algorithm*). Para tal, pode-se utilizar o algoritmo de balde de símbolos (*token bucket algorithm*) que, de modo similar ao *leaky bucket*, utiliza um balde furado para reter símbolos (ou *tokens*) gerados por um temporizador na velocidade de um símbolo a cada T segundos. Contudo, a partir desse algoritmo, *hosts* inativos podem poupar suas permissões (até o tamanho máximo do balde) para poderem

enviar rajadas maiores posteriormente (o que não ocorre no *leaky bucket*), dando mais flexibilidade de transmissão às aplicações da rede. A Figura 28 ilustra a implementação de mecanismos de regulação com o *token bucket algorithm*:

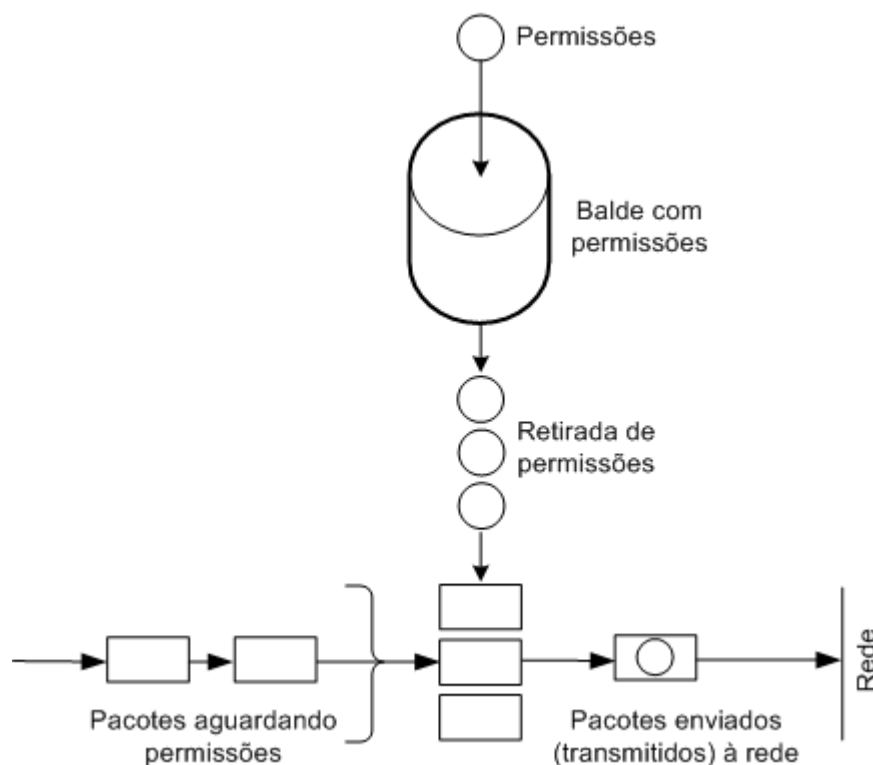


Figura 28 – Regulação com *token bucket algorithm*.

Nesse contexto, propõe-se que o *gateway* multimídia utilize do mecanismo de escalonamento fornecido pela disciplina WFQ quanto às suas filas de transmissão, priorizando o tráfego *stream* pertinente às aplicações multimídia, porém viabilizando, com menor prioridade, a transmissão de eventuais outros tipos de tráfego entrantes ao mesmo (de modo cíclico), e do mecanismo de regulação fornecido pelo *token bucket algorithm*, viabilizando transmissões em rajadas, bem como dando mais flexibilidade às aplicações da rede quanto ao seu tipo de tráfego, ambos tendo como base, novamente, os identificadores descritos na Tabela 5 quanto aos campos ToS e TC do protocolo IP (versões 4 e 6, respectivamente), nesse caso fazendo referência aos campos DSCP e ECN de seu cabeçalho.

4.4.3 – Algumas considerações

A proposta de adição de mecanismos de qualidade de serviço ao *gateway* multimídia objetiva que, no presente projeto de pesquisa, aplicações multimídia (nesse caso, referindo-se aos tráfegos *stream* dessas aplicações) tenham certa prioridade quanto às demais aplicações da rede, considerando-se que tal mecanismo de QoS tem como base o tráfego entrante ao *gateway* multimídia. Contudo, num contexto fim a fim (Internet, por exemplo), tal *gateway* está posicionado nas extremidades (bordas) da rede, de modo que nenhuma garantia de QoS pode ser realizada por ele quanto aos elementos intermediários ao longo da aplicação transmissora até suas interfaces de rede, bem como dele para eventuais outras redes até a aplicação receptora. Em linhas gerais, é objetivo do *gateway* multimídia priorizar certos tipos de tráfego (nesse caso, tráfego *stream*), porém essa priorização apenas será perceptível se os

hosts/aplicações receptoras de tais tráfegos estiverem, especialmente, no mesmo segmento de rede do *gateway*. Caso estejam em redes ou segmentos distintos, essa priorização poderá ser desrespeitada de acordo com as configurações desse outro ambiente ou rede (em que um administrador poderia, por exemplo, deixar de priorizar os tráfegos do tipo *stream* para priorizar outros tipos de tráfego, dentre outros). Além disso, no contexto Internet, todas as aplicações são executadas sobre seu serviço de melhor esforço (conforme descrito na Seção 2.3.2), o qual não fornece nenhuma garantia quanto à temporização (atrasos, variações de atrasos, etc.), entrega ordenada de pacotes e, se quer, quanto à entrega de tais pacotes.

Para tal, num contexto mais amplo, diversas propostas vêm sendo discutidas a respeito de como a Internet deveria evoluir para dar um melhor suporte às aplicações multimídia. Parte dessas propostas argumentam que a arquitetura Internet atual pode evoluir sem modificações em seu serviço de melhor esforço. Essas propostas sugerem, dentre outras, uma reestruturação dos Provedores de Serviços de Internet (ISPs) de modo que tenham condições de atender a demanda (largura de banda) dos serviços requisitados pelos usuários da rede (como em [23]); a instalação de redes de distribuição de conteúdos (CDNs, conforme descrito na Seção 2.3.3) para aproximar os recursos multimídia dos clientes da rede (como em [24]) e a partir da disponibilização de redes *overlay* para tráfego multimídia (como em [16]) em tempo real em toda a estrutura dos Provedores de Serviços Internet, algo similar ao *multicast* IP (em [24]), porém controlado pela camada de aplicação em vez de pelos roteadores IP. Outras propostas, como na arquitetura de serviços diferenciados (Diffserv), sugerem, por exemplo, pequenas mudanças na camada de rede da Internet, com adição de classes de tráfego (CoS) a partir de identificadores previamente definidos nos cabeçalhos dos protocolos IPv4 e IPv6 para as aplicações da rede na interface entre o usuário e seu Provedor de Serviços de Internet, ou seja, na borda da rede. A partir dessas classes, as aplicações podem ser distinguidas, tratadas e até cobradas de modo distinto aos demais tráfegos da rede (como em [RFC 2475] e [32]). Por fim, abordagens mais extremas, como na arquitetura de serviços integrados (Intserv), sugerem grandes modificações na atual arquitetura Internet, tal que as aplicações utilizadas na rede sejam capazes de realizar reservas explícitas de largura de banda fim a fim, com adição de protocolos de sinalização/reserva de recursos, alteração nas filas de escalonamento dos roteadores, adição de mecanismos de inspeção de tráfego e reserva dos recursos solicitados, dentre outros (como em [RFC 2215] e [RFC 2210]).

Dessa forma, percebe-se que os conceitos voltados à qualidade de serviço são extremamente amplos, de tal modo que a priorização de certos tipos de tráfego no *gateway* multimídia representa uma pequena e importante parte de sua estrutura funcional, mas, por si só, não é a solução inovadora que resolverá as exigências de rede requisitadas pelas aplicações multimídia, ainda sendo necessário, por exemplo, a utilização de outras estratégias para garantir certa qualidade de serviço para transmissões realizadas sobre o serviço de melhor esforço da Internet, tais como utilização do protocolo UDP em vez do TCP, configurações de retardos de reprodução no receptor, adição de marcas de tempo nos pacotes enviados pelo remetente e aquisição de dados antecipadamente para reprodução, dentre outros (conforme descrito na Seção 2.3.2).

4.5 – Classificação e marcação de pacotes IP

Conforme descrito nas seções 4.2 e 4.3, em linhas gerais, o *gateway* multimídia utiliza de identificadores presentes no cabeçalho do protocolo IP (especialmente no campo DSCP, presente na atual reformulação dos campos ToS e TC do IPv4 e do IPv6, respectivamente) para identificar e encaminhar o tráfego entrante ao mesmo à sua respectiva aplicação

receptora. Esses mesmos identificadores também são utilizados para priorizar certos tipos de tráfego (nesse caso, tráfego *stream*, gerado pelas aplicações multimídia de áudio, voz e vídeo) quanto à qualidade de serviço atribuída às suas respectivas aplicações transmissoras (nesse caso, referindo-se ao tráfego gerado por tais aplicações).

Para tal, é necessário que esse tráfego possua identificadores que viabilizem sua distinção (identificação) e tratamento junto ao *gateway* multimídia, os quais podem ser definidos, preferencialmente, pela própria aplicação transmissora ou por um elemento intermediário a tais aplicações. Independentemente do método utilizado deve-se ter uma coerência entre os identificadores presentes nos tráfegos propriamente ditos e no *gateway* multimídia, uma vez que uma “interpretação incorreta”, oriunda de uma definição distinta de identificadores nas aplicações e no *gateway* multimídia podem, por exemplo, inviabilizar as transmissões intermediadas por tal *gateway*.

Nesse contexto, dada a importância de tais identificadores (nesse caso do processo de classificação e marcação de pacotes IP), bem como na impossibilidade de defini-los diretamente nas ferramentas utilizadas para validar e testar o *gateway* multimídia (seja por não se ter acesso aos fontes de tais aplicações ou, nesse momento, não serem objetivos do presente projeto de pesquisa, mas sim um meio para validar a solução proposta no mesmo), optou-se pela implementação de um elemento classificador e marcador de pacotes IP, nomeado de “adaptador de tráfego multimídia”, para classificar e “rotular” os pacotes IP pertinentes aos serviços de áudio, voz, vídeo e dados utilizados para validar e testar o *gateway* multimídia.

Em linhas gerais, assim como o *gateway* multimídia, esse adaptador de tráfego multimídia é transparente às aplicações transmissora e receptora do conteúdo multimídia de áudio, vídeo, voz e dados, atuando como um “módulo externo” ao *host* que executa a aplicação transmissora de tais conteúdos, de modo a rotular os pacotes IP conforme seu respectivo serviço e viabilizar, posteriormente, a identificação e tratamento diferenciado de tais pacotes IP pelo *gateway* multimídia.

Conforme descrito anteriormente, por meio dessa abordagem “modular”, a implementação desses novos componentes de rede (nesse caso, referindo-se ao adaptador de tráfego multimídia e ao *gateway* multimídia) torna-se, além de menos complexa, objetiva quanto a funcionalidade de ambos, bem como independente quanto aos demais componentes da rede, porém utilizando e fornecendo serviços (nesse caso, serviços para classificação, marcação e identificação de pacotes IP, bem como de priorização de tráfegos multimídia, *stream*, na rede) a tais componentes.

Para tal, quanto ao *host* transmissor dos conteúdos de áudio, voz, vídeo e dados, o adaptador de tráfego multimídia é tido como seu *gateway* de acesso à rede, de modo que todo o tráfego gerado pelo *host* transmissor seja direcionado ao adaptador de tráfego multimídia antes de chegar ao *host* que executa sua respectiva aplicação receptora. Dessa forma, é possível classificar e marcar o tráfego *stream* e elástico gerado pelas aplicações transmissoras antes que tais tráfegos cheguem ao sistema receptor, em que o *gateway* multimídia é tido como componente intermediário aos sistemas transmissor e receptor.

Nesse contexto, a Figura 29 ilustra os sistemas transmissor e receptor do conteúdo multimídia com o adaptador de tráfego multimídia e com o *gateway* multimídia (além das aplicações transmissora e receptora de tais conteúdos):

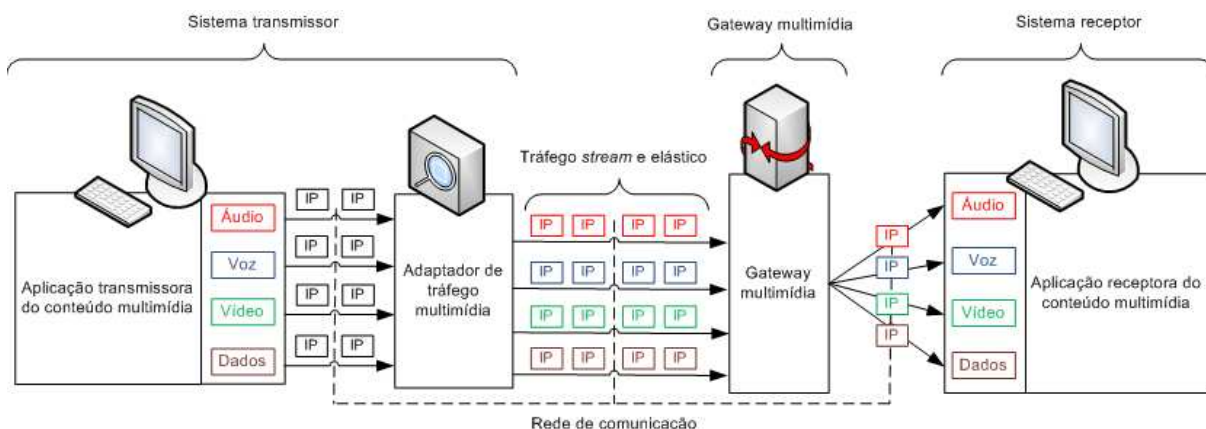


Figura 29 – Sistemas transmissor e receptor do conteúdo multimídia (com adaptador de tráfego multimídia e o gateway multimídia).

Quanto à classificação, para posterior marcação, dos tráfegos *stream* e elástico associados a uma determinada aplicação transmissora, no presente projeto de pesquisa esta se dá a partir dos identificadores de conexão no nível de transporte utilizados por tais aplicações, nesse caso referindo-se as portas de comunicação utilizadas por tais aplicações quanto aos protocolos TCP ou UDP. Esse processo mostra-se viável pelo fato de que na Arquitetura de Protocolos TCP/IP toda aplicação de rede necessita de uma interface de acesso à rede fornecida por meio de *sockets*, os quais utilizam, além dos endereços (IP) da origem e do destino, de números de portas (de origem e de destino) específicos da camada de transporte para viabilizar a multiplexação e demultiplexação dos dados de seus segmentos para suas respectivas aplicações receptoras.

Nesse caso, em que aplicações de rede utilizam de números de portas específicos para viabilizarem sua transmissão na rede, pode-se utilizar de tais números para, também, classificar os tráfegos destinados a tais aplicações. Como exemplo, se uma determinada aplicação de rede, que utiliza a porta 1001/UDP para receber os tráfegos pertinentes ao seu serviço de áudio, a porta 1002/UDP para receber os tráfegos pertinentes ao seu serviço de vídeo e a porta 1003/UDP para receber os tráfegos pertinentes ao seu serviço de voz, pode-se utilizar de tais números de portas para classificar tais tráfegos e, posteriormente, rotulá-los (marcá-los) com identificadores únicos e exclusivos pertinentes a tais serviços. Por outro lado, se todos os tráfegos pertinentes aos serviços de áudio, vídeo e voz dessa aplicação de exemplo fossem destinados a uma única porta no sistema receptor, essa abordagem necessitaria de outros fatores como, por exemplo, da identificação do tipo de tráfego com base em seu conteúdo no nível de aplicação ou, preferencialmente, que esse tráfego já fosse gerado com seus respectivos identificadores de tipo de serviço por seu sistema transmissor, dentre outros.

4.6 – Ambiente e ferramentas de desenvolvimento

Objetivando maior flexibilidade quanto ao ambiente de implementação e desenvolvimento do *gateway* multimídia, em que essa flexibilidade refere-se, especialmente, ao acesso aos códigos-fonte de tal componente, bem como da liberdade de sua utilização e modificação sem a necessidade da aquisição de eventuais licenças quanto ao mesmo, dentre outros, optou-se pela utilização do Sistema Operacional Linux, das ferramentas Netfilter/iptables e iproute2, bem como do compilador C/C++ GCC, fornecendo recursos aderentes a tais requisitos e contribuindo de modo facilitado para a continuidade do presente projeto de pesquisa.

Nesse contexto, as seções seguintes descrevem, de modo resumido e objetivo quanto às particularidades do *gateway* multimídia, as ferramentas Netfilter/iptables e iproute2, utilizadas para identificação e encaminhamento do tráfego multimídia, bem como para o fornecimento de recursos de qualidade de serviço a um ou outro tipo de tráfego em específico.

4.6.1 – Identificação e encaminhamento do tráfego multimídia

Quanto à ferramenta utilizada para identificar e encaminhar o tráfego pertinente aos serviços multimídia de áudio, voz, vídeo e dados pelo *gateway* multimídia, nesse caso tendo como base a utilização de pacotes IP associados a tais tráfegos e utilizando os identificadores descritos na Tabela 5 quanto ao campo DSCP do protocolo IP, utilizou-se o Netfilter/iptables [33] do Linux. Essa mesma ferramenta também foi utilizada para classificar e marcar (rotular) os pacotes IP gerados pelo sistema transmissor de tais conteúdos, nesse caso pelo adaptador de tráfego multimídia (também tendo como base os identificadores descritos na Tabela 5 quanto ao campo DSCP do protocolo IP).

Conceitualmente, o Netfilter/iptables é uma solução de *software* (de código aberto) implementada em nível de Kernel (na forma de módulos) e administrada via linha de comandos de modo a disponibilizar mecanismos para filtragem de pacotes em sistemas Linux. É amplamente utilizado para a implementação de *firewalls*, compartilhamento de acessos à Internet (via *Network Address Translation* - NAT) e redirecionamento de portas, dentre outros.

Funcionalmente, suas regras de filtragem são escritas e organizadas em tabelas específicas, as quais tem propósitos distintos umas das outras como, por exemplo, realizar ou não o aceite de um pacote no sistema ou manipular o conteúdo desse pacote durante sua “passagem” pelo *host* Linux em questão. Como exemplo, de acordo com as páginas de manual do Netfilter/iptables no Linux, as seguintes tabelas estão pré-definidas no sistema:

- Tabela *filter*: é a tabela de filtragem padrão do Netfilter/iptables, utilizada para realizar ou não o aceite de pacotes pelo *host* Linux em questão;
- Tabela *nat*: é a tabela de filtragem utilizada para definição de regras para compartilhamento de acesso à Internet via NAT (*Network Address Translation*) e para redirecionamento de portas, dentre outros;
- Tabela *mangle*: é a tabela de filtragem utilizada para manipular o conteúdo (cabeçalho) dos pacotes IP, tais como os campos DSCP e ECN (descritos anteriormente);
- Tabela *raw*: é a tabela utilizada, especialmente, para definição de exceções quanto às regras de filtragem do sistema, sendo processada antes das demais tabelas de filtragem do Netfilter/iptables;
- Tabela *security*: é a tabela utilizada para definições de regras MAC (*Mandatory Access Control*) implementadas pelo módulo SELinux (*Security Enhanced Linux*) do Linux.

Por sua vez, nas tabelas de filtragem, as regras de filtragem devem estar embasadas em uma determinada cadeia/corrente (*chain*) para manipulação de pacotes, tratando-os, por exemplo,

assim que chegarem, passarem ou saírem do *host* Linux, dentre outros. Para tal, cada tabela possui suas próprias *chains*, com destaque para as *chains*:

- *INPUT*, que trata de pacotes IP destinados ao *host* Linux;
- *FORWARD*, que trata de pacotes IP que passam pelo *host* Linux;
- *OUTPUT*, que trata de pacotes IP gerados pelo *host* Linux, dentre outras.

Ao final, pode-se, por exemplo, liberar, rejeitar ou registrar (em arquivos de *log*) os pacotes aderentes às regras de filtragem a partir de diversas informações, tais como portas de origem e/ou destino de uma determinada conexão, protocolo de transporte (TCP ou UDP) e endereço (IP) de rede/*host* de origem e/ou destino, dentre outros.

Nesse contexto, o presente projeto de pesquisa contempla a utilização do Netfilter/iptables como mecanismo central ao processo de identificação e encaminhamento dos tráfegos pertinentes aos serviços multimídia de áudio, vídeo e voz e de dados pelo *gateway* multimídia (assim como pelo adaptador de tráfego multimídia), tendo como base sua capacidade funcional quanto ao protocolo IP, bem como aos protocolos de transporte TCP e UDP e, até mesmo, quanto às mensagens trocadas em nível de aplicação ao longo da rede. Além disso, por ser uma ferramenta livre e também distribuída a partir de seu código fonte, ela pode ser modificada e customizada (além de estudada e implementada) conforme as necessidades de seu utilizador.

4.6.2 – Qualidade de serviço

Quanto à ferramenta utilizada para a implementação de mecanismos voltados à qualidade de serviço (QoS) no *gateway* multimídia, nesse caso priorizando os tráfegos *stream* gerados pelas aplicações multimídia de áudio, voz ou vídeo ao longo da rede, utilizou-se o *iproute2* [34]. Os principais objetivos associados à utilização dessa ferramenta se devem, especialmente, ao seu suporte nativo ao ambiente de desenvolvimento do *gateway* multimídia (ambiente Linux), bem como de sua integração com o Netfilter/Iptables.

Conceitualmente, o *iproute2* (ou simplesmente *iproute*) é uma solução de *software* (de código aberto) que corresponde a uma coleção de utilitários de linha de comando utilizados, especialmente, para o gerenciamento de parâmetros de rede e para a implementação de mecanismos para qualidade de serviço em ambientes Linux. É tipicamente utilizado para implementações de soluções para balanceamento de carga e alta disponibilidade envolvendo múltiplos *links* Internet em um mesmo *host* Linux e para controlar as taxas de *download* e/ou *upload* em servidores de acesso à Internet e/ou de hospedagem *web* (tais como servidores FTP, dentre outros).

Funcionalmente, no que se refere ao seu recurso para qualidade de serviço, possui suporte a vários mecanismos de escalonamento e regulação, tais como o *Token Bucket* e as disciplinas FIFO e WFQ (conforme descritas na Seção 4.4.2), dentre outras. Destas, algumas disciplinas, como a FIFO, por exemplo, são tidas como *classless*, enquanto outras, como o *Hierarchical Token Bucket (HTB)*, por exemplo, são tidas como *classful*. Quanto ao mecanismo funcional de ambas, hierarquicamente, disciplinas do tipo *classful* suportam a definição de outros componentes internos, tais como classes e filtros, utilizados para a criação de múltiplas classes de serviços (CoS) na rede, bem como do tratamento diferenciado dos tráfegos

associados a tais classes de serviço quanto ao mecanismo de qualidade de serviço, enquanto as disciplinas do tipo *classless* não possibilitam essa hierarquização interna, tratando o tráfego de todas as aplicações da rede como “sinônimos” quanto ao seu mecanismo funcional. Outro recurso funcional presente nas disciplinas do tipo *classful* está associado à priorização de certos tipos de tráfegos (como os tráfegos *stream*, por exemplo) e ao empréstimo de recursos (taxa de transmissão) entre as múltiplas classes de serviço caso tal classe não o esteja utilizando ao máximo, possibilitando, por exemplo, que a reserva e regulação da taxa de transmissão alocada para um determinado tipo de tráfego ou aplicação, por exemplo, ajuste-se dinamicamente conforme sua utilização atual, de modo a não desperdiçar recursos de banda passante a partir da reserva de recursos para tráfegos inexistentes num dado momento.

Quanto à associação dos tipos de tráfego à sua respectiva classe de serviço (nas disciplinas *classful*), pelo fato do *iproute2* (nesse caso, referindo-se ao utilitário “*tc*”, responsável, na linha de comando do Linux, pela definição das regras de qualidade de serviço do *iproute2*) se integrar ao *Netfilter/iptables*, é possível utilizar dos recursos de ambos para, dado um determinado pacote IP marcado como prioritário (nesse caso por transportar um determinado tráfego *stream*) pelo próprio *Netfilter/iptables* (ou por sua própria aplicação transmissora), associá-lo a uma classe de serviço prioritária (que exija, por exemplo, maior banda passante para transmissão de suas informações), sem a necessidade de utilização de outras ferramentas e mecanismos externos ao ambiente de implementação e desenvolvimento do *gateway* multimídia (ambiente Linux).

Nesse contexto, o presente projeto de pesquisa contempla a utilização do *iproute2* como mecanismo central ao processo de adição de mecanismos de qualidade de serviço junto ao *gateway* multimídia quanto aos tráfegos, especialmente, *stream* pertinentes às aplicações multimídia de áudio, voz e vídeo em execução ao longo da rede, tendo como base sua capacidade funcional quanto ao protocolo IP, bem como de sua integração ao *Netfilter/iptables*. Além disso, por ser uma ferramenta livre e também distribuída a partir de seu código fonte, ela pode ser modificada e customizada (além de estudada e implementada) conforme as necessidades de seu utilizador.

4.6.3 – Gerador de tráfego multimídia

Mesmo não sendo um componente específico do *gateway* multimídia, um gerador (ou emulador) de tráfego multimídia é um componente importante quanto ao seu ambiente de desenvolvimento, bem como ao seu processo de validação e testes, uma vez que por meio dessa ferramenta pode-se, por exemplo, testar o *gateway* multimídia, bem como validar seu mecanismo funcional e comparar os resultados de sua intervenção com os resultados sem tal intervenção, de modo a verificar, por exemplo, se tal *gateway* se comportou, também, de modo neutro ao perfil de tráfego gerado pelas aplicações transmissoras do conteúdo multimídia, dentre outros.

Funcionalmente, em linhas gerais, o principal objetivo de um gerador de tráfego multimídia é emular tráfego multimídia na rede (e não simular a geração desse tráfego) de modo a representar esse tráfego em situações reais (utilizando transmissões em meios físicos guiados e não guiados, por exemplo, com *hosts* clientes acessando outros serviços de rede, tais como navegação *web* ou transferência de arquivos, dentre outros). Dessa forma, tanto o envio quanto à análise de dados pode ser realizada em um ambiente real, que pode ser mais ou menos complexo dependendo da quantidade de variáveis utilizadas durante o processo de geração do tráfego à rede, dentre outros.

Nesse contexto, como principal ferramenta utilizada para testar e validar o *gateway* multimídia utilizou-se o gerador de tráfego multimídia proposto em [21, 22], implementado e validado na própria FT/UNICAMP nos anos de 2010 e 2011. Nessa mesma referência, a partir de vários ambientes de emulação e simulação, o autor compara os resultados obtidos a partir de seu gerador com os resultados obtidos com o *software* de simulação de eventos discretos de propósitos gerais Arena [35], demonstrando que tais resultados foram estatisticamente os mesmos entre o gerador e o simulador, possibilitando sua utilização em cenários reais. O autor também propõe melhorias futuras para contribuir com o aprimoramento do gerador de tráfego multimídia, como a implementação de mecanismos para classificação e marcação de pacotes IP e para a regulação do tráfego emulado por seu gerador, dentre outros, os quais foram implementados de forma modular à sua ferramenta (como um elemento externo e complementar ao gerador de tráfego multimídia).

Quanto à arquitetura de aplicação de tal gerador de tráfego multimídia, ele está implementado no modelo cliente-servidor, em que o cliente é o gerador de tráfego multimídia propriamente dito e o servidor é o receptor do tráfego gerado por seu respectivo cliente (Figura 30).

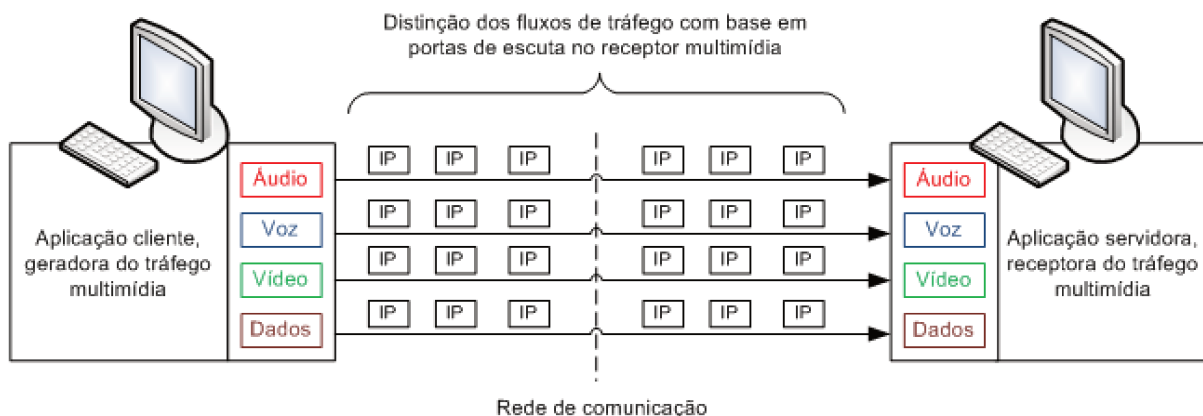


Figura 30 – Estrutura funcional proposta em [21] para o gerador de tráfego multimídia.

Funcionalmente todo seu fluxo de tráfego está embasado no protocolo de rede IP e nos protocolos de transporte UDP e TCP, em que a distinção entre os diferentes fluxos de tráfego *stream* e elástico pertinente às suas respectivas aplicações transmissoras, nesse caso para os serviços de áudio, voz, vídeo e dados, se dá por meio de números de portas de escuta na aplicação servidora (receptora) do conteúdo multimídia, definidos na aplicação cliente durante o processo de geração do tráfego na rede e utilizados no receptor para viabilizar o encaminhamento de tais fluxos à sua correta aplicação receptora.

Internamente, quanto ao mecanismo responsável pela geração do tráfego pertinente aos serviços de áudio, voz, vídeo e dados na rede, ele está organizado em módulos distintos que se interagem entre si. Esses módulos são os seguintes:

- Seletor de serviço: é o módulo que contém as informações a respeito dos serviços disponíveis no gerador de tráfego multimídia que, nesse caso, são representados por áudio, voz, vídeo e dados. A partir de suas informações, o serviço poderá ser criado em momentos específicos (pré-definidos) e, com base em funções de probabilidade, admitido ou não à rede a partir de controles de admissão que objetivam determinar o número máximo de serviços suportado pela rede;

- Perfilador de tráfego: é o módulo que contém as informações sobre o tipo de tráfego que será gerado para cada serviço desejado. A partir do serviço selecionado e de suas respectivas características (que são distintas entre um e outro serviço), o perfilador de tráfego identificará, a partir de funções de probabilidade, a duração e o tamanho dos pacotes para cada serviço em questão. Dessa forma, esse módulo influenciará na geração dos pacotes associados ao serviço desejado, indicando a periodicidade e o tamanho com que eles devem ser criados;
- Gerador de pacotes: é o módulo responsável por gerar os pacotes associados ao serviço desejado com base nas informações armazenadas no perfilador de tráfego. Para que os pacotes possam ser mais facilmente analisados, todo tráfego gerado possui informações pertinentes ao tipo de serviço gerado (áudio, voz, vídeo e dados), à identificação (numeração) desse serviço e à temporização desse serviço (momento em que foi gerado e enviado à rede, tempo de geração e duração do serviço).

A interação entre esses módulos pode ser observada na Figura 31:

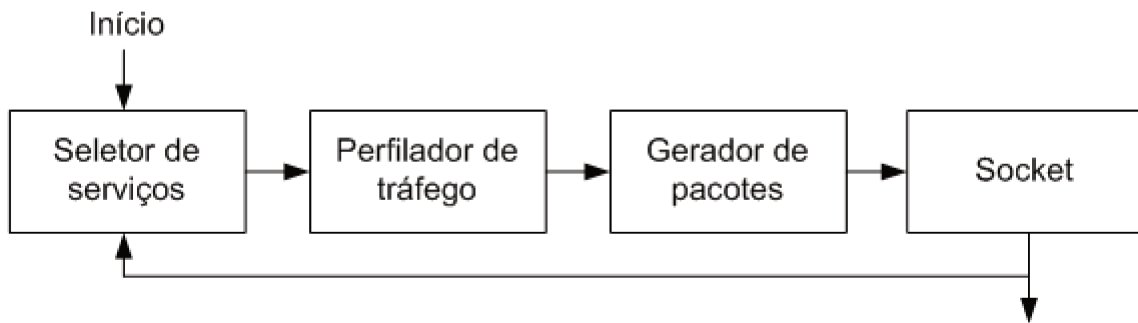


Figura 31 – Interação entre os módulos do gerador de tráfego multimídia (Fonte: [21]).

Nesse contexto, o presente projeto de pesquisa contempla a utilização do gerador de tráfego multimídia proposto em [21, 22] como principal ferramenta utilizada para testar e validar o *gateway* multimídia, tendo como base sua capacidade funcional quanto à geração de tráfegos *stream* e elástico pertinentes aos serviços de áudio, voz, vídeo e dados na rede, bem como por ser uma ferramenta implementada e testada na própria FT/UNICAMP. Além de sua comprovação funcional, outros fatores que motivaram sua escolha quanto aos testes e validações com o *gateway* multimídia se devem, especialmente, ao acesso aos seus fontes (código fonte) e ao seu ambiente de desenvolvimento, sendo codificado na linguagem de programação C++ e projetado para ser executado em ambientes Unix, tais como em sistemas Linux (ambiente do *gateway* multimídia) e Mac OS, com a possibilidade de também estar acessível a outros sistemas operacionais, como em sistemas Microsoft Windows, por exemplo.

5 – Resultados e discussões

As seções seguintes descrevem os procedimentos utilizados para validar e testar os mecanismos funcionais do *gateway* multimídia e, também, do adaptador de tráfego multimídia, conforme descrito no capítulo 4.

5.1 – Validação funcional

Esta seção descreve os ambientes utilizados para validar o funcionamento do adaptador de tráfego multimídia e do *gateway* multimídia.

5.1.1 – Classificação e marcação de pacotes IP

Dois ambientes são propostos para validar e testar o adaptador de tráfego multimídia:

- Um ambiente com uma única instância das aplicações transmissoras e receptoras dos tráfegos pertinentes aos serviços de áudio, voz, vídeo e dados, em que há apenas um fluxo (canal) de transmissão associado a tais serviços (Figura 32);

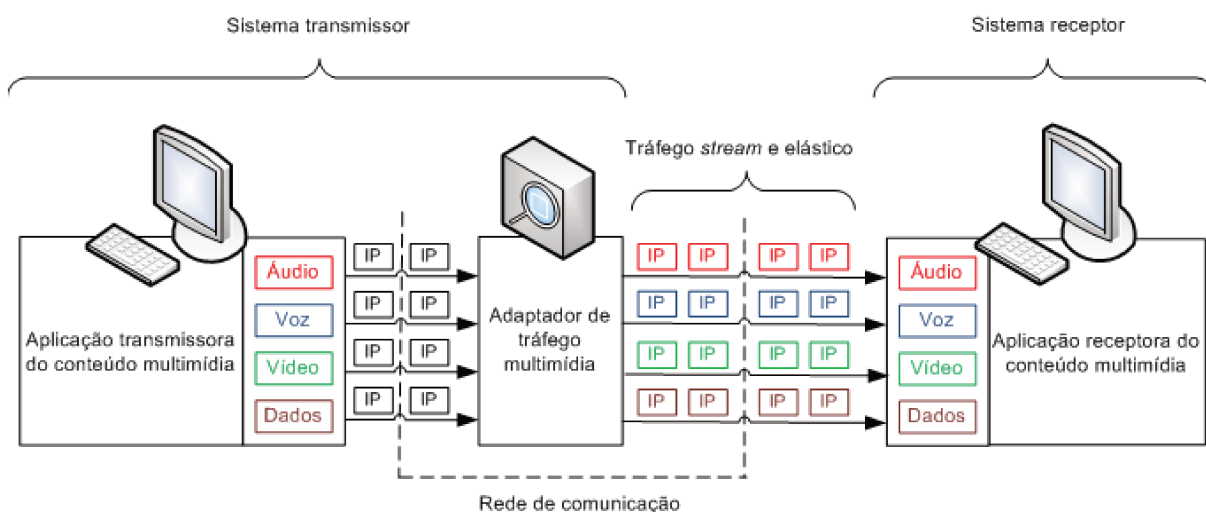


Figura 32 – Ambiente (1) para validação e testes do adaptador de tráfego multimídia.

- Um ambiente com múltiplas instâncias (2 instâncias) das aplicações transmissoras e receptoras dos tráfegos pertinentes aos serviços de áudio, voz, vídeo e dados, em que há múltiplos fluxos (2 canais) de transmissão associados a tais serviços (Figura 33).

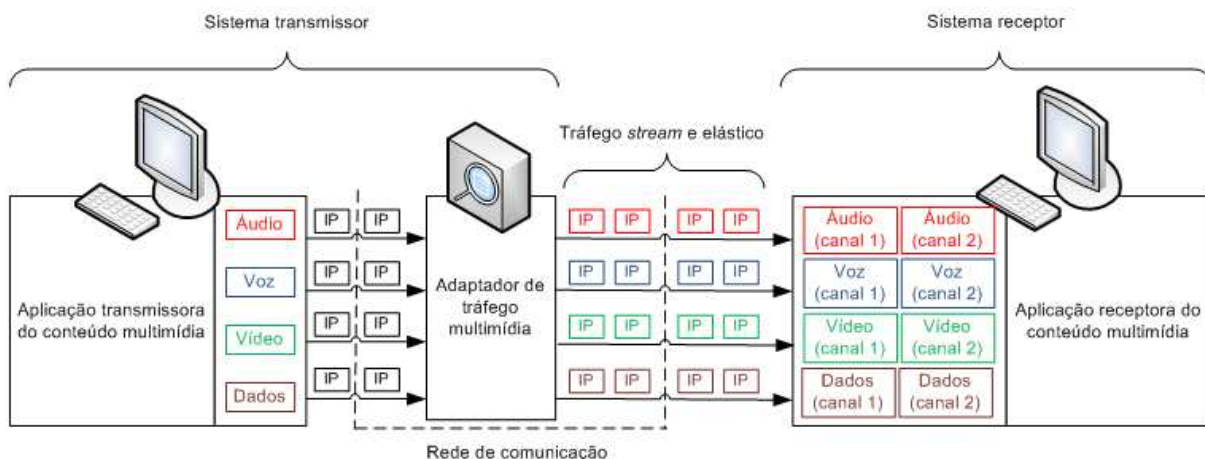


Figura 33 – Ambiente (2) para validação e testes do adaptador de tráfego multimídia.

Em ambos os ambientes, o adaptador de tráfego multimídia é tido como “módulo complementar”, na forma de *gateway* de acesso à rede, de um determinado sistema transmissor de conteúdos de áudio, voz, vídeo e dados (nesse caso, de um sistema transmissor que executa a aplicação geradora de tais conteúdos quanto ao gerador de tráfego multimídia descrito na Seção 4.6.3), sendo o responsável por classificar e “rotular” os tráfegos associados a tais serviços conforme seu respectivo tipo de serviço (áudio, voz, vídeo ou dados). Dessa forma, todo tráfego gerado pelo *host* transmissor, inicialmente sem qualquer identificação quanto ao seu tipo de serviço (de áudio, voz, vídeo ou dados) nos cabeçalhos do protocolo IP, é intermediado pelo adaptador de tráfego multimídia e devidamente classificado/marcado com base em seu tipo de serviço (no campo DSCP do cabeçalho do protocolo IP). Após essa “rotulação” de pacotes IP, eles são enviados à rede para que cheguem às suas respectivas aplicações receptoras.

Para tal, os *hosts* transmissor e receptor estão logicamente organizados em redes distintas, de modo que seu elo de comunicação seja embasado pelo adaptador de tráfego multimídia, conforme descrito anteriormente, tido como *gateway* de acesso à rede do *host* transmissor dos conteúdos de áudio, voz, vídeo e dados, conforme ilustra a Figura 34:

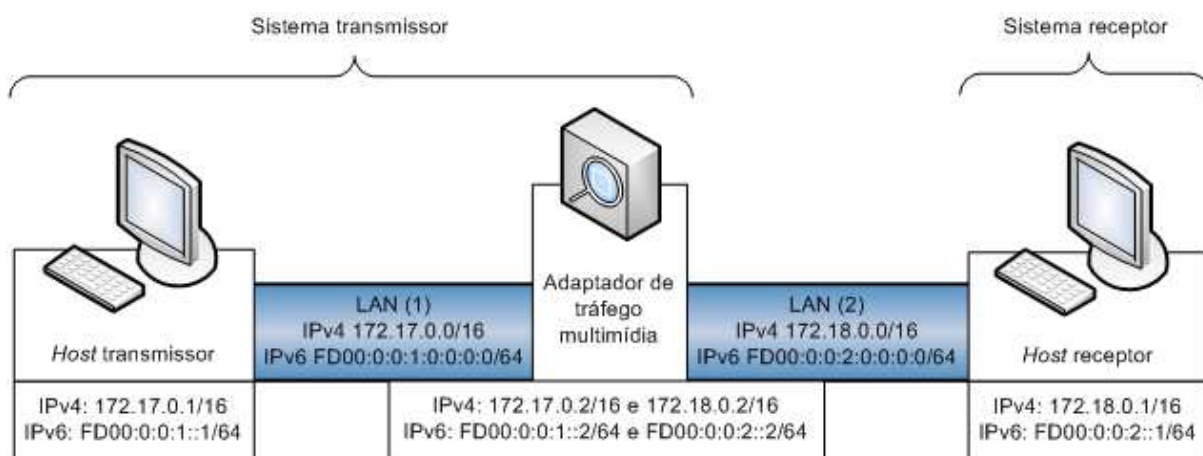


Figura 34 – Endereçamento de rede do ambiente para validação e testes do adaptador de tráfego multimídia.

Em tal ambiente, o adaptador de tráfego multimídia possui quatro endereços de rede (dois endereços IPv4 e dois endereços IPv6), enquanto os *hosts* transmissor e receptor possuem dois endereços de rede cada (um endereço IPv4 e um endereço IPv6), conforme descrito na Tabela 7:

<i>Host</i>	Endereço IPv4	Endereço IPv6
Transmissor	172.17.0.1/16	FD00:0:0:1::1/64
Adaptador de tráfego multimídia	172.17.0.2/16 172.18.0.2/16	FD00:0:0:1::2/64 FD00:0:0:2::2/64
Receptor	172.18.0.1/16	FD00:0:0:2::1/64

Tabela 7 – Endereçamento IPv4 e IPv6 dos hosts do ambiente para validação e testes do adaptador de tráfego multimídia.

A partir de tais configurações, o adaptador de tráfego multimídia (com um endereço IPv4/IPv6 na rede do *host* transmissor e outro endereço IPv4/IPv6 na rede do *host* receptor) é tido como elo de comunicação entre tais *hosts*, de modo que todo o fluxo de comunicação entre ambos seja intermediado por tal adaptador de tráfego multimídia. Como exemplo, as Figuras 35 e 36 ilustram, respectivamente, os saltos (*hops*) IPv4 e IPv6 entre os *hosts* transmissor e receptor, em que o adaptador de tráfego multimídia é intermediário a tais *hosts*:

```
aluno@transmissor:~$ traceroute receptor.diorio.corp.br
traceroute to receptor.diorio.corp.br (172.18.0.1), 30 hops max, 60 byte packets
 1 marcador.diorio.corp.br (172.17.0.2)  0.865 ms  0.547 ms  0.332 ms
 2 receptor.diorio.corp.br (172.18.0.1)  2.670 ms  4.483 ms  4.347 ms
```

Figura 35 – Saltos (hops) IPv4 entre os hosts transmissor e receptor no ambiente para validação e testes do adaptador de tráfego multimídia.

```
aluno@transmissor:~$ traceroute6 receptor.diorio.corp.br
traceroute to receptor.diorio.corp.br (fd00:0:0:2::1) from fd00:0:0:1::1, 30 hops
max, 16 byte packets
 1 marcador.diorio.corp.br (fd00:0:0:1::2)  0.717 ms  0.491 ms  0.62 ms
 2 receptor.diorio.corp.br (fd00:0:0:2::1)  1.328 ms  1.052 ms  1.527 ms
```

Figura 36 – Saltos (hops) IPv6 entre os hosts transmissor e receptor no ambiente para validação e testes do adaptador de tráfego multimídia.

A partir de tais listagens de saltos (*hops*), pode-se observar que o adaptador de tráfego multimídia é o *host* intermediário entre o *host* transmissor e o *host* receptor, sendo o primeiro (e único) salto entre tais *hosts* (salto de número 1 antes de alcançar o *host* receptor, de número 2, nas Figuras 35 e 36 exibidas anteriormente), tanto no IPv4, quanto no IPv6.

Quanto às aplicações transmissora e receptora do gerador de tráfego multimídia em execução nos *hosts* transmissor e receptor, todo tráfego gerado pela aplicação transmissora é destinado à portas de escuta específicas para a aplicação receptora de tais tráfegos (há servidores para os serviços de áudio, voz, vídeo e dados em execução em portas distintas para cada um desses serviços no *host* receptor de tais conteúdos), de modo que o processo de classificação e marcação dos pacotes IP associados a tais tráfegos está embasado nas portas de escuta de sua respectiva aplicação receptora (os pacotes IP destinados à aplicação receptora de áudio são classificados/marcados como áudio com base na porta de escuta de tal aplicação receptora de áudio; os pacotes IP destinados à aplicação receptora de vídeo são classificados/marcados

como vídeo com base na porta de escuta de tal aplicação receptora de vídeo; os pacotes IP destinados à aplicação receptora de voz são classificados/marcados como voz com base na porta de escuta de tal aplicação receptora de voz; e, os pacotes IP destinados à aplicação receptora de dados são classificados/marcados como dados com base na porta de escuta de tal aplicação receptora de dados). Dessa forma, a partir desse arranjo topológico e funcional, todos os pacotes IP enviados à rede pelo sistema transmissor do gerador de tráfego multimídia devem chegar ao seu respectivo sistema receptor devidamente identificados (no campo DSCP do cabeçalho do protocolo IP) quanto aos seus serviços de áudio, voz, vídeo e dados.

Vale ressaltar que, nesse momento, o objetivo de tais testes é apenas “rotular” os pacotes IP (mediante a classificação e posterior marcação de tais pacotes) conforme seu tipo de serviço (áudio, voz, vídeo ou dados), não utilizando, no sistema receptor, tais “rótulos” para distinguir esses pacotes entre si, porém disponibilizando um meio para que isso seja possível (nesse caso, a partir de identificadores armazenados no campo DSCP do cabeçalho do protocolo IP).

Teste I

No primeiro teste (ambiente descrito na Figura 32), os tráfegos associados ao serviço de dados são destinados à aplicação receptora na porta 6001/TCP, os tráfegos associados ao serviço de áudio são destinados à aplicação receptora na porta 7001/UDP, os tráfegos associados ao serviço de voz são destinados à aplicação receptora na porta 8001/UDP e os tráfegos associados ao serviço de vídeo são destinados à aplicação receptora na porta 9001/UDP.

Dado tal ambiente, a Tabela 8 descreve os DSCP's que devem ser atribuídos aos tráfegos elástico e *stream* pertinente às aplicações de dados, áudio, voz e vídeo conforme suas respectivas portas de destino no *host* receptor (aplicação receptora):

Aplicação	Porta de Destino	DSCP
Dados	6001/TCP	000000 (0x00)
Áudio	7001/UDP	010000 (0x10)
Voz	8001/UDP	100000 (0x20)
Vídeo	9001/UDP	110000 (0x30)

Tabela 8 – Definições de DSCP no adaptador de tráfego multimídia (1).

Internamente ao adaptador de tráfego multimídia, as Figuras 37 e 38 ilustram tais definições de DSCP's para os protocolos IPv4 e IPv6, respectivamente:

```
aluno@marcador:~$ sudo iptables -L -n -t mangle -Z FORWARD
Chain FORWARD (policy ACCEPT)
target      prot opt source                destination
DSCP        tcp  --  0.0.0.0/0              172.18.0.1             tcp dpt:6001 DSCP set 0x00
DSCP        udp  --  0.0.0.0/0              172.18.0.1             udp dpt:7001 DSCP set 0x10
DSCP        udp  --  0.0.0.0/0              172.18.0.1             udp dpt:8001 DSCP set 0x20
DSCP        udp  --  0.0.0.0/0              172.18.0.1             udp dpt:9001 DSCP set 0x30
```

Figura 37 – Definições de DSCP no adaptador de tráfego multimídia para o IPv4 (1).


```

aluno@marcador:~$ sudo iptables -L -n -t mangle -Z FORWARD
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DSCP      tcp  :/:0 fd00:0:0:2::1/128      tcp dpt:6001 DSCP set 0x00
DSCP      udp  :/:0 fd00:0:0:2::1/128      udp dpt:7001 DSCP set 0x10
DSCP      udp  :/:0 fd00:0:0:2::1/128      udp dpt:8001 DSCP set 0x20
DSCP      udp  :/:0 fd00:0:0:2::1/128      udp dpt:9001 DSCP set 0x30

```

Figura 38 – Definições de DSCP no adaptador de tráfego multimídia para o IPv6 (1).

A partir de tais configurações, todo fluxo de tráfego gerado pelo sistema transmissor (inicialmente sem qualquer identificação quanto ao seu tipo de serviço junto ao campo DSCP do cabeçalho do protocolo IP), destinado ao *host* receptor (de endereço IPv4 “172.18.0.1” e IPv6 “FD00:0:0:2::1”) nas portas TCP e UDP utilizadas pelas aplicações de dados (6001/TCP), áudio (7001/UDP), voz (8001/UDP) e vídeo (9001/UDP), com tráfego intermediado pelo adaptador de tráfego multimídia (tido como *gateway* de acesso à rede de tal *host* transmissor) é devidamente classificado (com base nas portas de destino de tais aplicações) e “rotulado” quanto aos seus fluxos de tráfego de dados (“000000”, “0x00”), áudio (“010000”, “0x10”), voz (“100000”, “0x20”) ou vídeo (“110000”, “0x30”) no campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) conforme definições da Tabela 8.

Nesse contexto, quanto ao serviço de dados, as Figuras 39 e 40 ilustram os tráfegos associados a tal serviço (destinados à porta 6001/TCP do *host* receptor de endereço IPv4 “172.18.0.1” e IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” (no campo DSCP do cabeçalho do protocolo IP) pelo adaptador de tráfego multimídia para os protocolos IPv4 e IPv6, respectivamente:

No.	Source	Destination	Protocol	Info
9	172.17.0.1	172.18.0.1	TCP	33305 > 6001 [SYN] Seq=0
13	172.17.0.1	172.18.0.1	TCP	33305 > 6001 [ACK] Seq=1
17	172.17.0.1	172.18.0.1	TCP	[TCP segment of a reassem
26	172.17.0.1	172.18.0.1	TCP	[TCP segment of a reassem

▶ Frame 17: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

▶ Ethernet II, Src: 00:0c:29:6f:e7:b7 (00:0c:29:6f:e7:b7), Dst: 00:0c:29:78:0d:57 (00:0c:29:78:0d:57)

▼ Internet Protocol Version 4, Src: 172.17.0.1 (172.17.0.1), Dst: 172.18.0.1 (172.18.0.1)

Version: 4
Header length: 20 bytes

▼ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT-0))

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)

(a)

No.	Source	Destination	Protocol	Info
5	172.18.0.2	172.18.0.1	TCP	33305 > 6001 [SYN] Seq=0 Win=14600 Len=0 MSS=1460
7	172.18.0.2	172.18.0.1	TCP	33305 > 6001 [ACK] Seq=1 Ack=1 Win=14600 Len=0
8	172.18.0.2	172.18.0.1	TCP	[TCP segment of a reassembled PDU]
13	172.18.0.2	172.18.0.1	TCP	[TCP segment of a reassembled PDU]

▶ Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

▶ Ethernet II, Src: 00:0c:29:78:0d:57 (00:0c:29:78:0d:57), Dst: 00:0c:29:7d:c7:10 (00:0c:29:7d:c7:10)

▼ Internet Protocol Version 4, Src: 172.18.0.2 (172.18.0.2), Dst: 172.18.0.1 (172.18.0.1)

Version: 4
Header length: 20 bytes

▼ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECT-0))

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport)

(b)

Figura 39 – Tráfego de dados, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

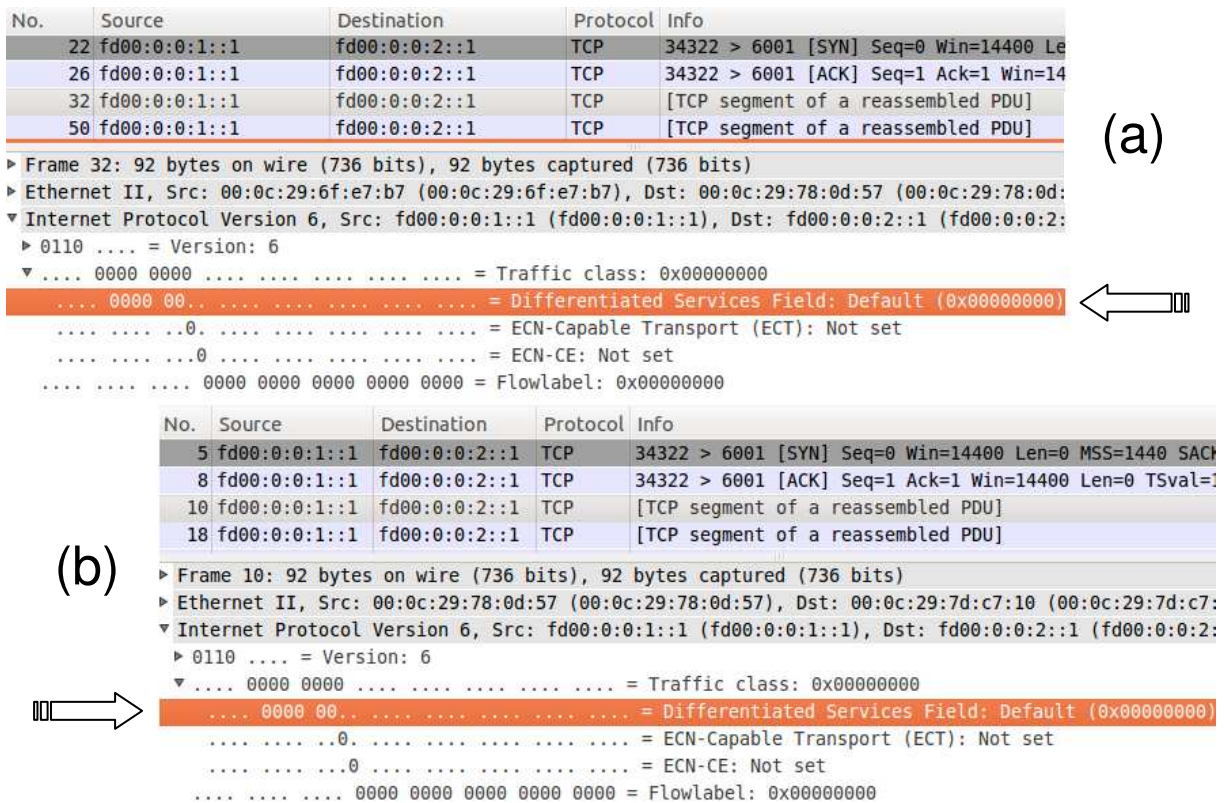


Figura 40 – Tráfego de dados, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que o DSCP associado ao serviço de dados (“sinalizado” por uma seta), após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (itens “(b)”, das Figuras 39 e 40), tanto no IPv4 quanto no IPv6, está devidamente definido como “000000” (0x00), conforme configurações do adaptador de tráfego multimídia descritas na Tabela 8.

Para esse exemplo em específico, vale ressaltar que pelo fato do DSCP padrão para todos os pacotes IP da rede ser definido como “000000” (0x00), num primeiro momento, parece não haver distinção dos tráfegos antes e após sua classificação pelo adaptador de tráfego multimídia, uma vez que tal DSCP é o mesmo dos demais pacotes IP da rede (pacotes IP sem qualquer tipo de identificação quanto ao campo DSCP), percepção distinta dos demais canais associados a tal tráfego de dados (conforme realizado no Teste II, descrito na sequência) ou dos demais tráfegos (de áudio, voz e vídeo) gerados pelo sistema transmissor do conteúdo multimídia (também, descritos na sequência).

Quanto aos demais serviços multimídia, de modo similar ao tráfego associado ao serviço de dados, as Figuras 41 e 42 ilustram os tráfegos associados ao serviço de áudio (destinados à porta 7001/UDP do *host* receptor de endereço IPv4 “172.18.0.1” e IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia para os protocolos IPv4 e IPv6, respectivamente:

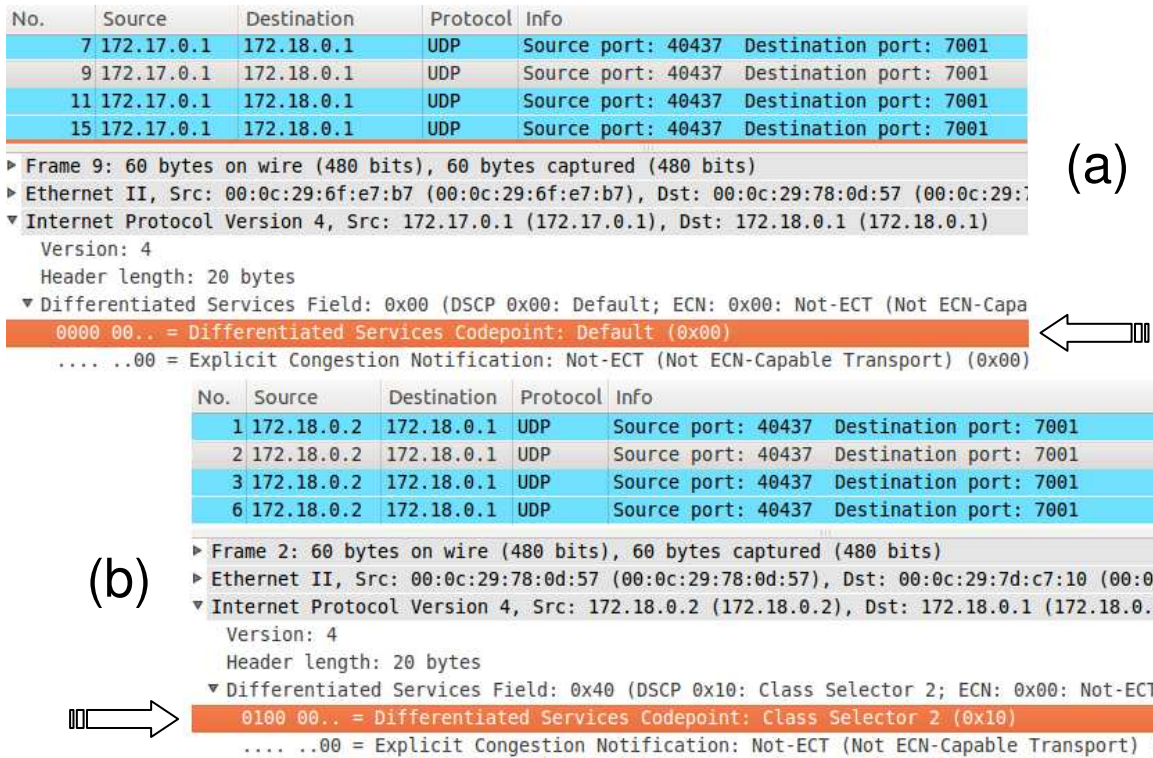


Figura 41 – Tráfego de áudio, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

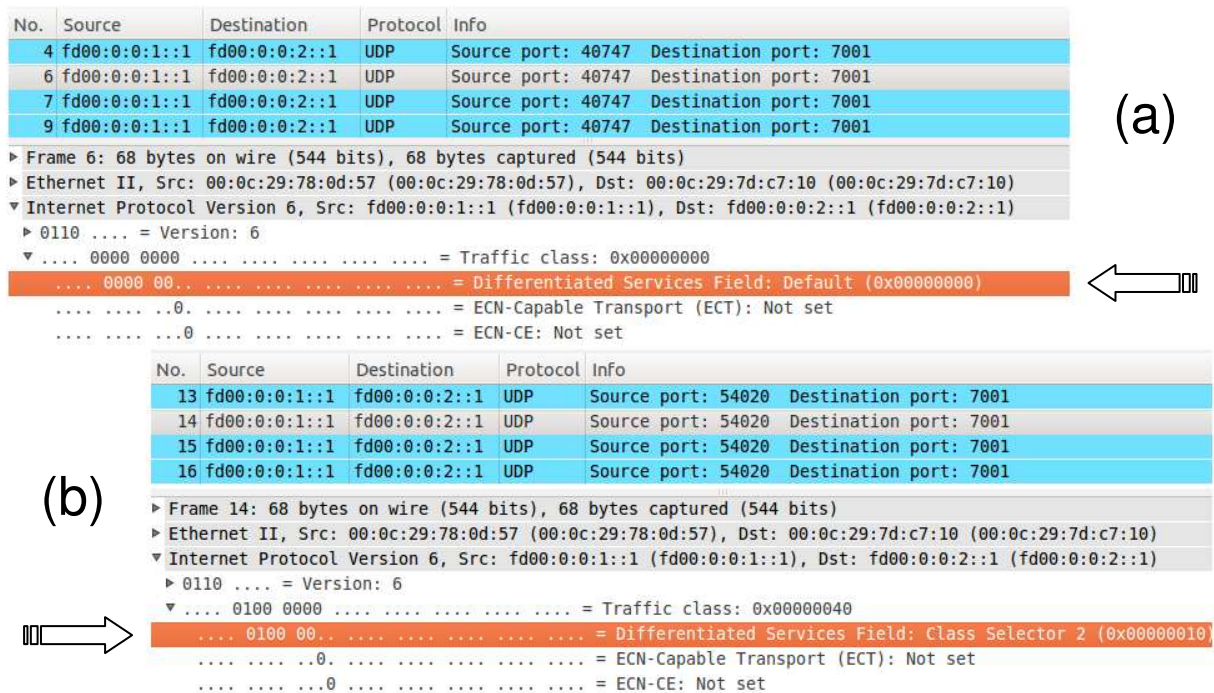


Figura 42 – Tráfego de áudio, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que antes da “rotulação” (itens “(a)” das Figuras 41 e 42), para o IPv4 e para o IPv6, o DSCP associado a tais tráfegos de áudio é definido como “000000” (0x00), valor padrão, e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (itens “(b)” das Figuras 41 e 42), o DSCP é definido como “010000” (0x10), ambos sinalizados por uma seta.

Na sequência, quanto ao serviço de voz, de modo similar aos exemplos anteriores, as Figuras 43 e 44 ilustram os tráfegos associados a tal serviço (destinados à porta 8001/UDP do *host* receptor de endereço IPv4 “172.18.0.1” e IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia para os protocolos IPv4 e IPv6, respectivamente:

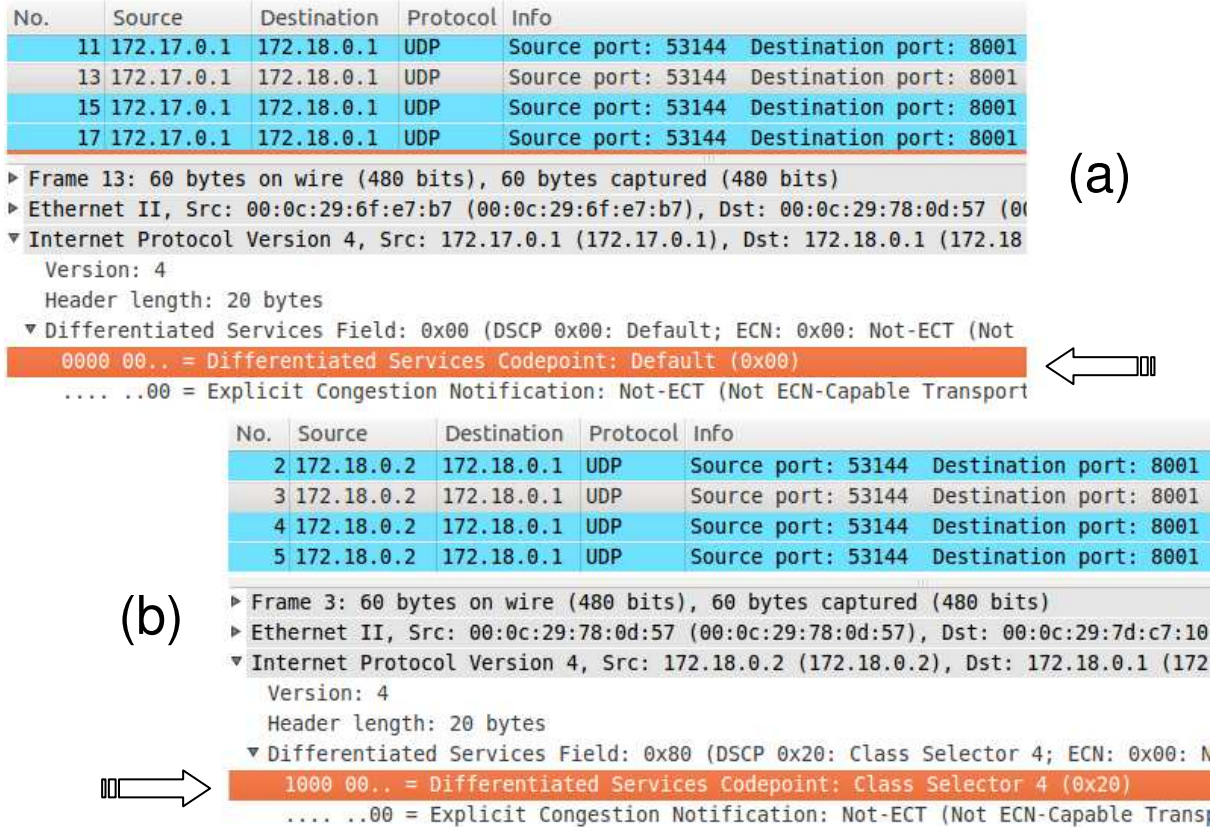


Figura 43 – Tráfego de voz, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

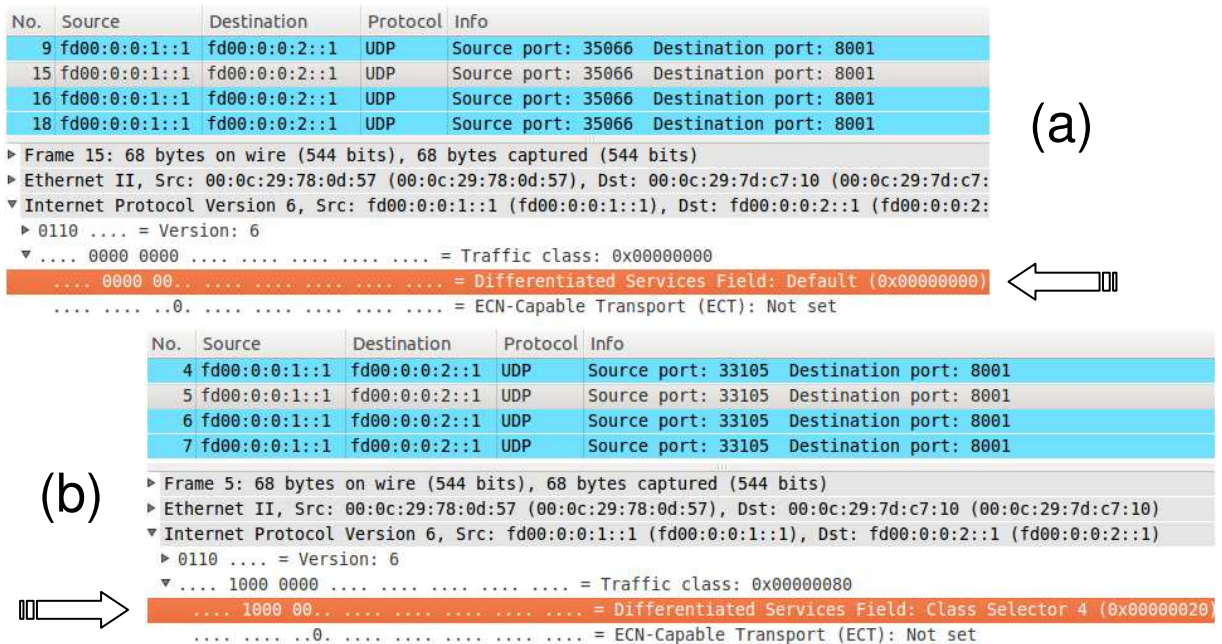


Figura 44 – Tráfego de voz, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que, assim como para os tráfegos de dados e áudio descritos anteriormente, antes da “rotulação” (itens “(a)” das Figuras 43 e 44), tanto para o protocolo IPv4, quanto para o protocolo IPv6, o DSCP associado a tais tráfegos de voz é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia, tal DSCP é definido como “100000” (0x20), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 8.

Por sua vez, a Figura 45 ilustra os tráfegos associados ao serviço de vídeo (destinados à porta 9001/UDP do *host* receptor de endereço “172.18.0.1”), nesse caso para o protocolo IPv4, antes e após sua “rotulação” pelo adaptador de tráfego multimídia:

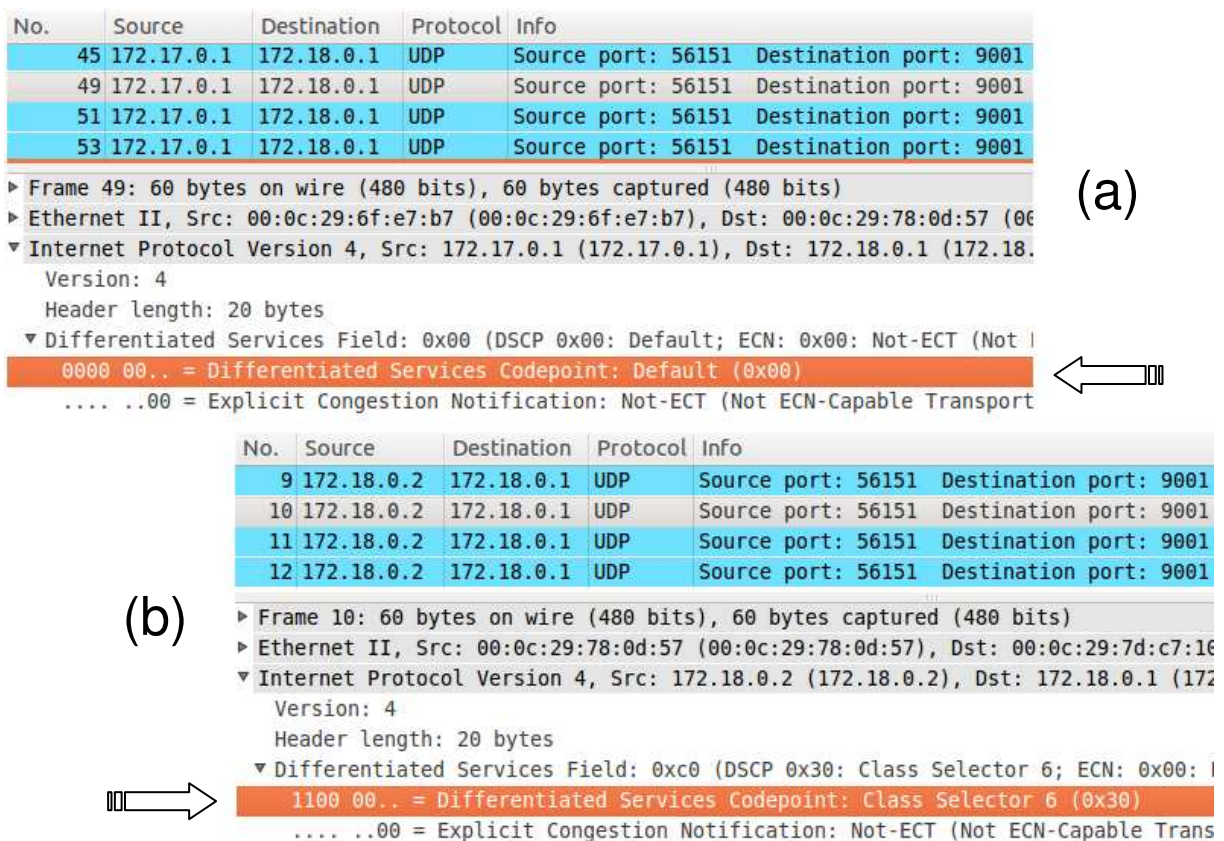


Figura 45 – Tráfego de vídeo, utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que antes da “rotulação”, o DSCP associado a tais tráfegos de vídeo é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia, tal DSCP é definido como “110000” (0x30), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 8.

Ainda quanto ao serviço de vídeo, nesse caso referindo-se ao protocolo IPv6, a Figura 46 ilustra os tráfegos associados a tal serviço (também destinados à porta 9001/UDP do *host* receptor, nesse caso de endereço IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia:

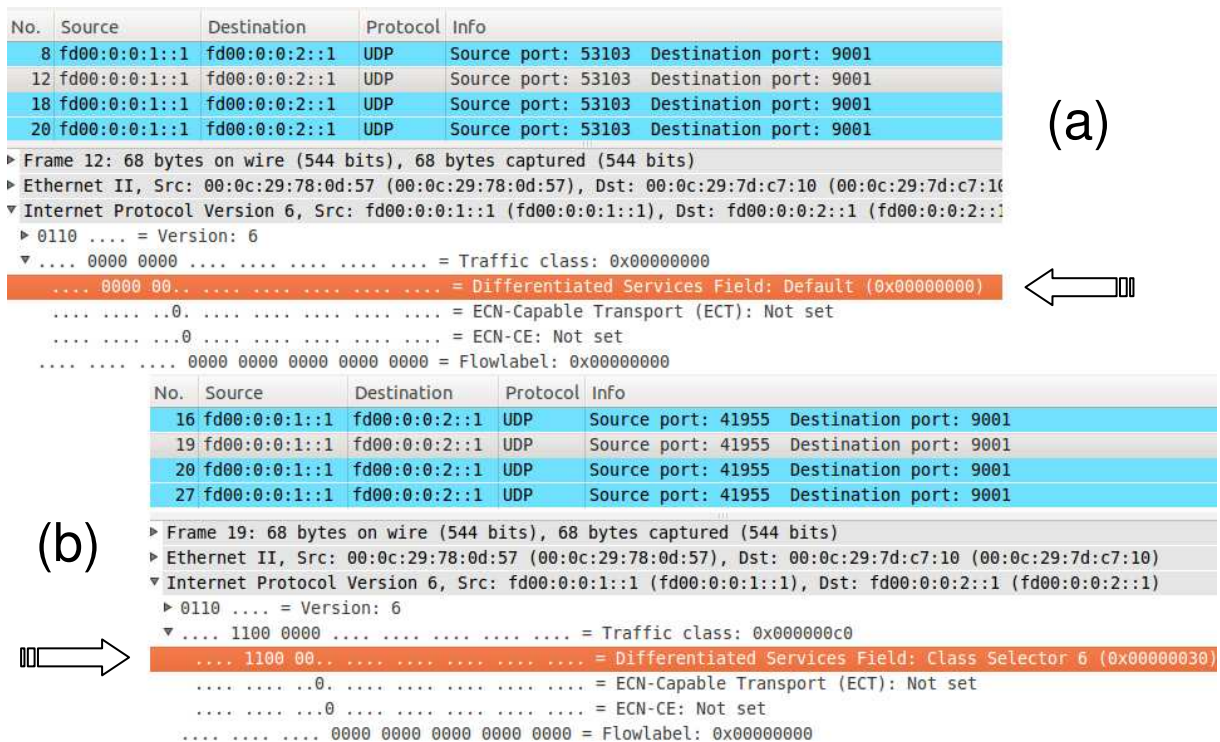


Figura 46 – Tráfego de vídeo, utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Assim como para o IPv4, observe que antes da “rotulação” pelo adaptador de tráfego multimídia, o DSCP associado a tais tráfegos de vídeo é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” tal DSCP é definido como “110000” (0x30), também “sinalizado” por uma seta.

Apenas como observação, note que para os tráfegos associados ao protocolo IPv4, após sua intermediação pelo adaptador de tráfego multimídia (itens “(b)” das Figuras 39, 41, 43 e 45), o endereço IP do *host* transmissor (nesse caso, “172.17.0.1”) é mascarado (via NAT) pelo endereço IP do adaptador de tráfego multimídia (nesse caso, “172.18.0.1” - endereço na rede do *host* receptor), o que não ocorre com os tráfegos associados ao protocolo IPv6, em que o endereço do *host* transmissor (nesse caso “FD00:0:0:1::1”) não é mascarado pelo endereço do adaptador de tráfego multimídia (nesse caso, “FD00:0:0:2::1” - endereço na rede do *host* receptor).

Teste II

O segundo teste é similar ao primeiro, porém com mais fluxos de transmissão (nesse caso, dois fluxos de transmissão) associados aos serviços de áudio, voz, vídeo e dados. Em tal teste (ambiente descrito na Figura 33), de modo complementar ao Teste I, há um segundo canal de comunicação associado aos serviços de dados (com tráfegos pertinentes a tal serviço também sendo enviados à porta 6002/TCP do *host* receptor), ao serviço de áudio (com tráfegos pertinentes a tal serviço também sendo enviados à porta 7002/UDP do *host* receptor), ao serviço de voz (com tráfegos pertinentes a tal serviço também sendo enviados à porta 8002/UDP do *host* receptor) e ao serviço de vídeo (com tráfegos pertinentes a tal serviço também sendo enviados à porta 9002/UDP do *host* receptor).

Dado tal ambiente, a Tabela 9 descreve os DSCP's que devem ser atribuídos aos tráfegos elástico e *stream* pertinente às aplicações de dados, áudio, voz e vídeo conforme suas respectivas portas de destino no *host* receptor (aplicação receptora):

Aplicação	Porta de Destino	DSCP
Dados	6001/TCP (canal 1)	000000 (0x00) (canal 1)
	6002/TCP (canal 2)	000000 (0x01) (canal 2)
Áudio	7001/UDP (canal 1)	010000 (0x10) (canal 1)
	7002/UDP (canal 2)	010001 (0x11) (canal 2)
Voz	8001/UDP (canal 1)	100000 (0x20) (canal 1)
	8002/UDP (canal 2)	100001 (0x21) (canal 2)
Vídeo	9001/UDP (canal 1)	110000 (0x30) (canal 1)
	9002/UDP (canal 2)	110001 (0x31) (canal 2)

Tabela 9 – Definições de DSCP no adaptador de tráfego multimídia (2).

Internamente ao adaptador de tráfego multimídia, as Figuras 47 e 48 ilustram tais definições de DSCP's para os protocolos IPv4 e IPv6, respectivamente:

```
aluno@marcador:~$ sudo iptables -L -n -t mangle -Z FORWARD
Chain FORWARD (policy ACCEPT)
target      prot opt source                destination
DSCP        tcp  --  0.0.0.0/0              172.18.0.1          tcp dpt:6001 DSCP set 0x00
DSCP        tcp  --  0.0.0.0/0              172.18.0.1          tcp dpt:6002 DSCP set 0x01
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:7001 DSCP set 0x10
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:7002 DSCP set 0x11
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:8001 DSCP set 0x20
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:8002 DSCP set 0x21
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:9001 DSCP set 0x30
DSCP        udp  --  0.0.0.0/0              172.18.0.1          udp dpt:9002 DSCP set 0x31
```

Figura 47 – Definições de DSCP no adaptador de tráfego multimídia para o IPv4 (2)

```
aluno@marcador:~$ sudo ip6tables -L -n -t mangle -Z FORWARD
Chain FORWARD (policy ACCEPT)
target      prot opt source                destination
DSCP        tcp  --  ::/0                   fd00:0:0:2::1/128  tcp dpt:6001 DSCP set 0x00
DSCP        tcp  --  ::/0                   fd00:0:0:2::1/128  tcp dpt:6002 DSCP set 0x01
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:7001 DSCP set 0x10
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:7002 DSCP set 0x11
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:8001 DSCP set 0x20
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:8002 DSCP set 0x21
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:9001 DSCP set 0x30
DSCP        udp  --  ::/0                   fd00:0:0:2::1/128  udp dpt:9002 DSCP set 0x31
```

Figura 48 – Definições de DSCP no adaptador de tráfego multimídia para o IPv6 (2).

A partir de tais configurações, todo fluxo de tráfego gerado pelo sistema transmissor (inicialmente sem qualquer identificação quanto ao seu tipo de serviço junto ao campo DSCP do cabeçalho do protocolo IP), destinado ao *host* receptor (de endereço IPv4 “172.18.0.1” e IPv6 “FD00:0:0:2::1”) nas portas TCP e UDP utilizadas pelo segundo canal de comunicação das aplicações de dados (6002/TCP), áudio (7002/UDP), voz (8002/UDP) e vídeo (9002/UDP), com tráfego intermediado pelo adaptador de tráfego multimídia (tido como *gateway* de acesso à rede de tal *host* transmissor) é devidamente classificado (com base nas portas de destino de tais aplicações) e “rotulado” quanto aos seus fluxos de tráfego de dados (“000001”, “0x01”), áudio (“010001”, “0x11”), voz (“100001”, “0x21”) ou vídeo (“110001”, “0x31”) no campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6).

Nesse contexto, quanto ao canal 2 do serviço de dados, as Figuras 49 e 50 ilustram os tráfegos associados a tal serviço (destinados à porta 6002/TCP do *host* receptor) antes e após sua “rotulação” (no campo DSCP do cabeçalho do protocolo IP) pelo adaptador de tráfego multimídia para os protocolos IPv4 e IPv6, respectivamente:

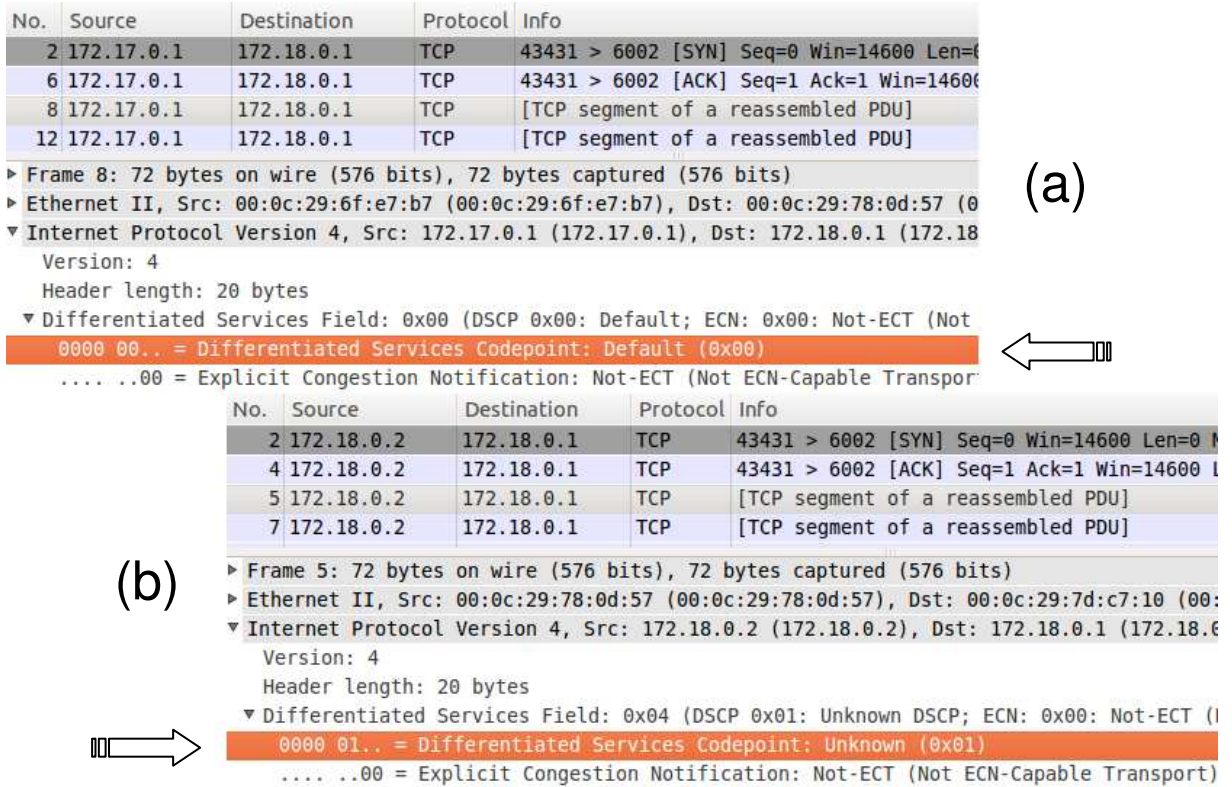


Figura 49 – Tráfego de dados (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

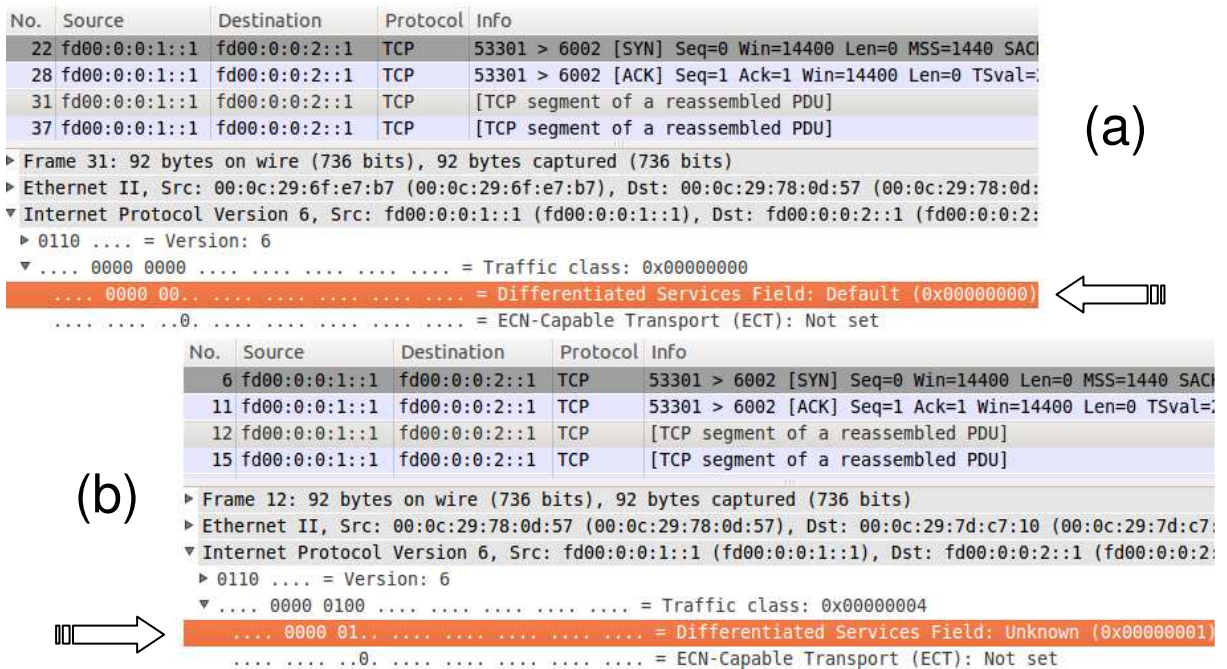


Figura 50 – Tráfego de dados (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que antes da “rotulação” (itens “(a)” das Figuras 49 e 50), tanto para o protocolo IPv4, quanto para o protocolo IPv6, o DSCP associado a tal tráfego de dados é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (itens “(b)” das Figuras 49 e 50), tal DSCP é definido como “000001” (0x01), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 9.

De modo similar ao tráfego associado ao canal 2 do serviço de dados, a Figura 51 ilustra os tráfegos associados ao canal 2 do serviço de áudio (destinados à porta 7002/UDP do *host* receptor de endereço IPv4 “172.18.0.1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia para o protocolo IPv4:

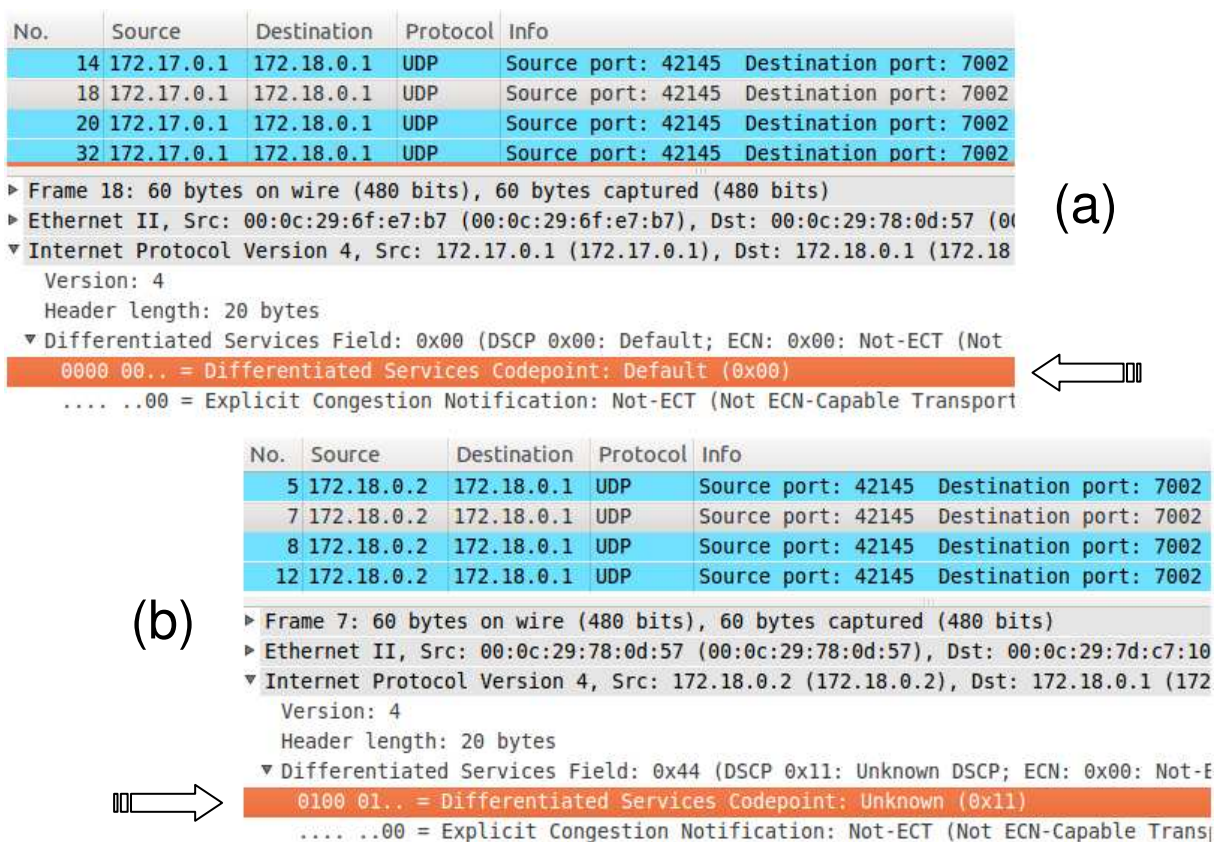


Figura 51 – Tráfego de áudio (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que antes da “rotulação” (item “(a)” da Figura 51), o DSCP associado a tais tráfegos de áudio é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (item “(b)” da Figura 51), tal DSCP é definido como “010001” (0x11), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 9.

Por sua vez, ainda quanto ao canal 2 do serviço de áudio, nesse caso referindo-se ao protocolo IPv6, a Figura 52 ilustra os tráfegos associados a tal serviço/canal (também destinados à porta 7002/UDP do *host* receptor, nesse caso de endereço IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia:

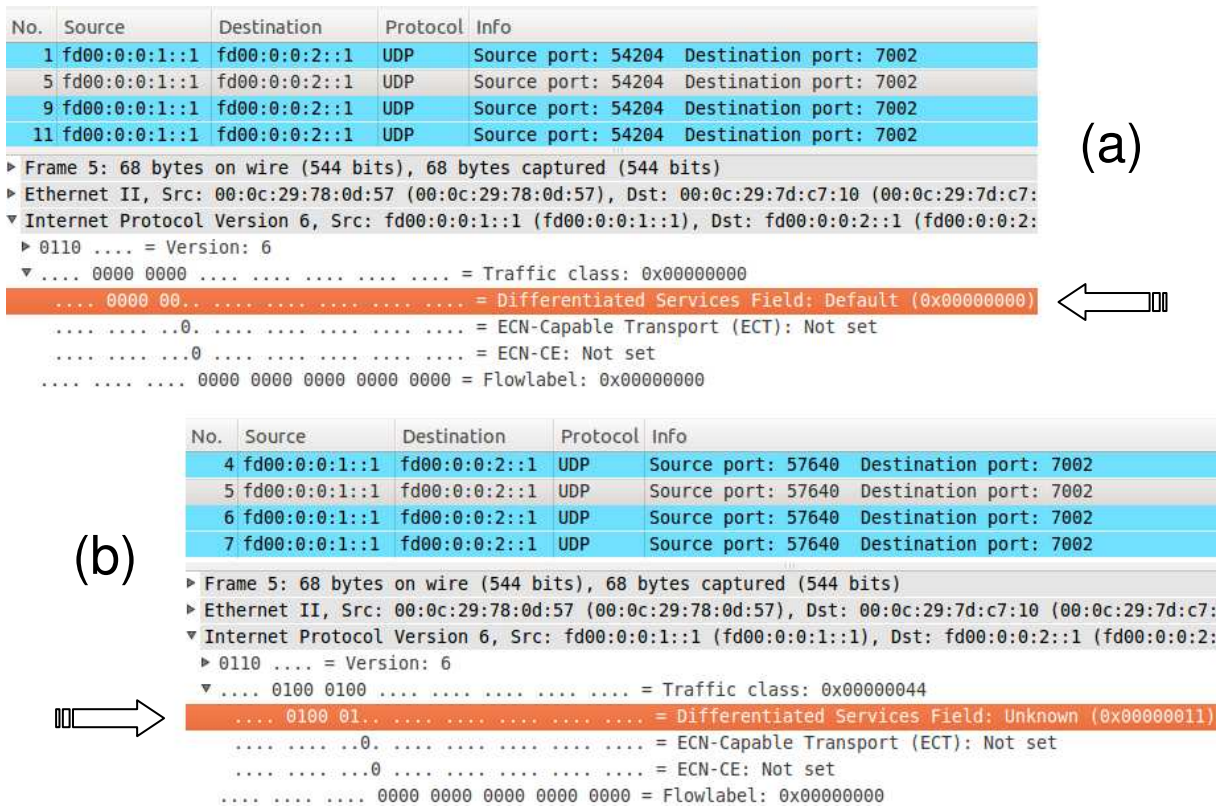


Figura 52 – Tráfego de áudio (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Assim como para o IPv4, observe que antes da “rotulação” pelo adaptador de tráfego multimídia (item “(a)” da Figura 52), o DSCP associado a tais tráfegos de áudio é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” por tal adaptador de tráfego multimídia (item “(b)” da Figura 52), o DSCP é definido como “010001” (0x11), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 9.

Na sequência, nesse caso quanto ao serviço de voz, as Figuras 53 e 54 ilustram os tráfegos associados ao canal 2 de tal serviço (nesse caso, destinados à porta 8002/UDP do *host* receptor de endereço IPv4 “172.18.0.1” e de endereço IPv6 “FD00:0:0:2::1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia para os protocolos IPv4 e IPv6, respectivamente:

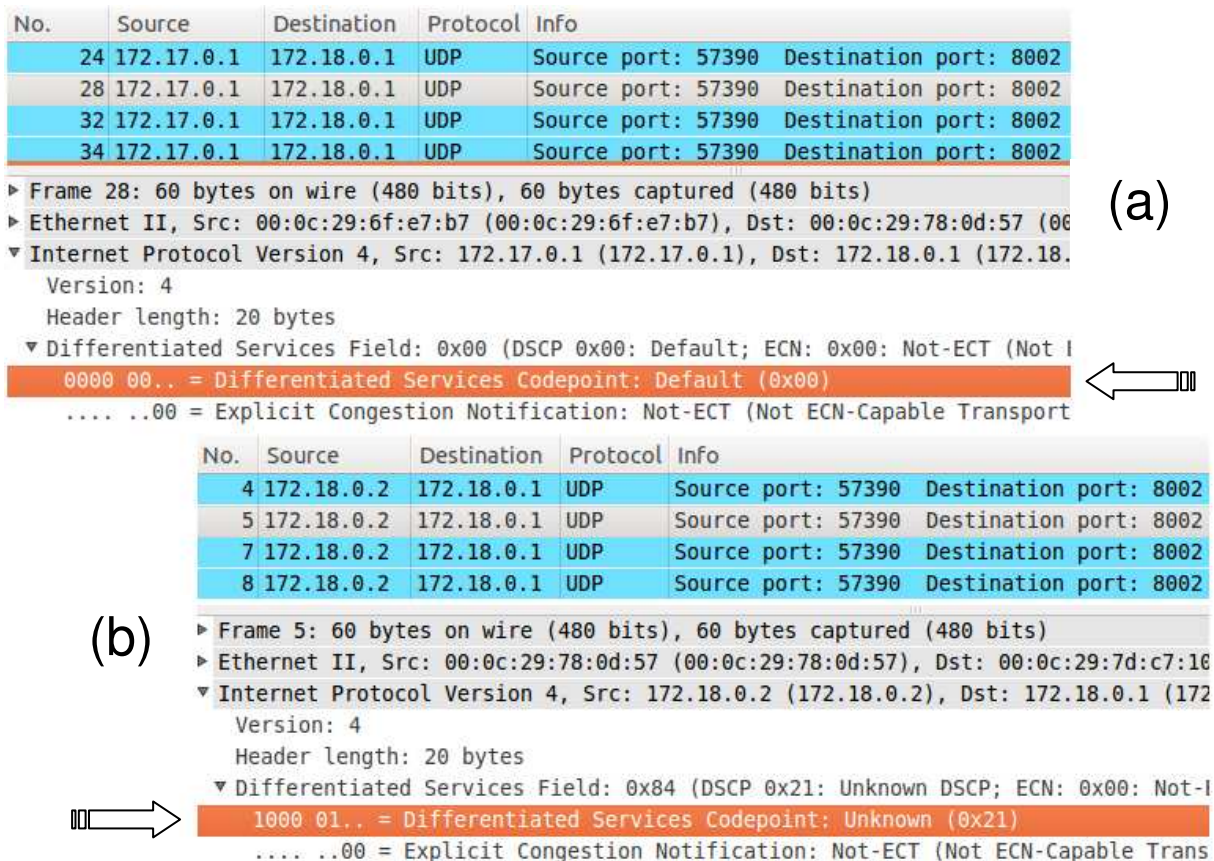


Figura 53 – Tráfego de voz (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

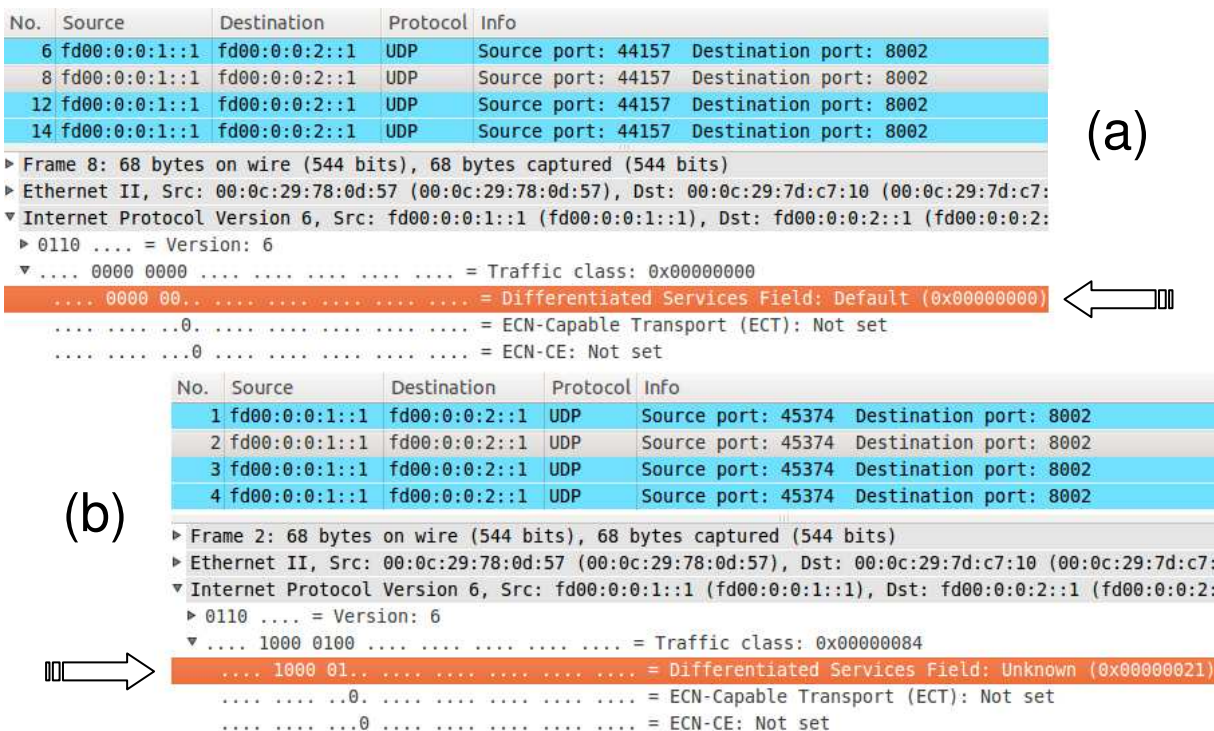


Figura 54 – Tráfego de voz (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que, assim como para os tráfegos do segundo canal de dados e do segundo canal de áudio descritos anteriormente, antes da “rotulação” (itens “(a)” das Figuras 53 e 54), tanto para o protocolo IPv4, quanto para o protocolo IPv6, o DSCP associado a tais tráfegos de voz (canal 2) é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (itens “(b)” das Figuras 53 e 54), tal DSCP é definido como “100001” (0x21), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 9.

Por sua vez, quanto ao serviço de vídeo, nesse caso referindo-se ao protocolo IPv4, a Figura 55 ilustra os tráfegos associados ao canal 2 de tal serviço (destinados à porta 9002/UDP do *host* receptor de endereço IPv4 “172.18.0.1”) antes e após sua “rotulação” pelo adaptador de tráfego multimídia:

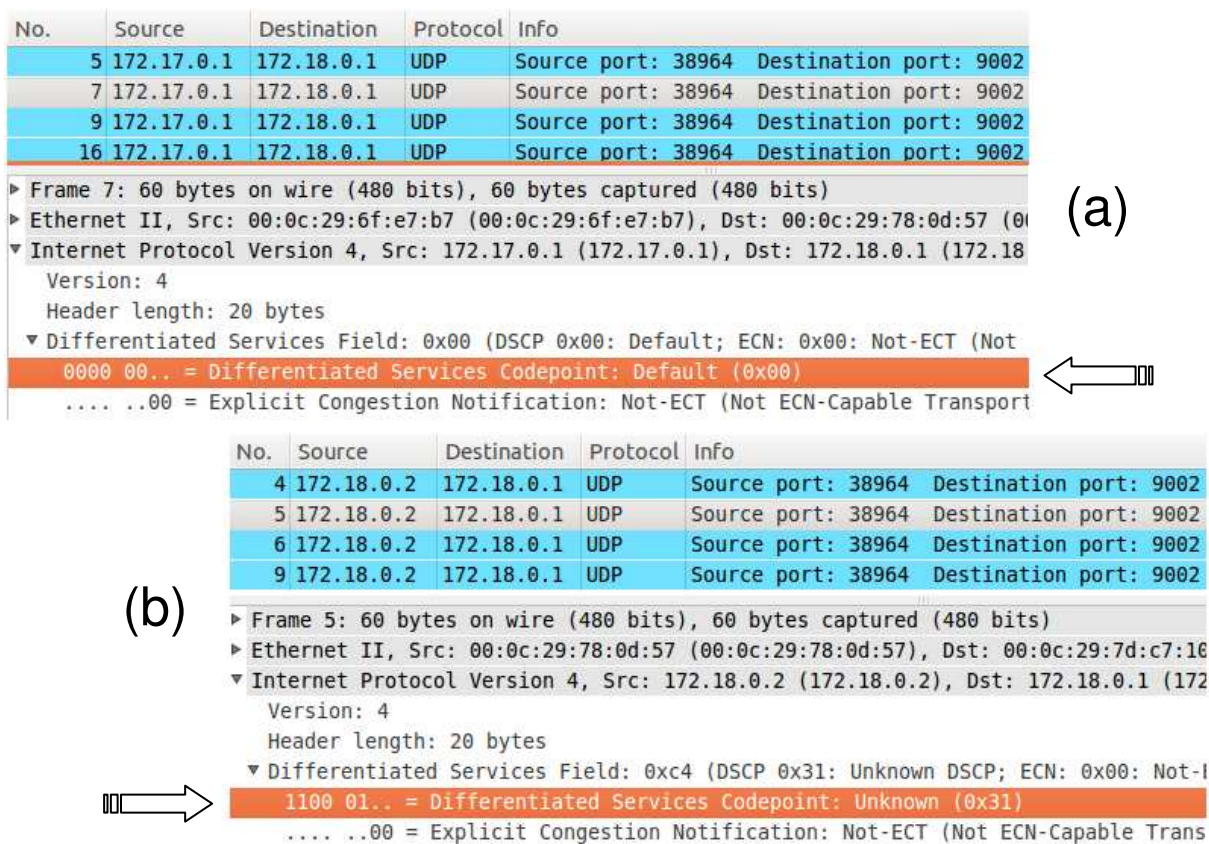


Figura 55 – Tráfego de vídeo (canal 2), utilizando IPv4, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que antes da “rotulação” (item “(a)” da Figura 55), o DSCP associado a tais tráfegos de vídeo (canal 2) é definido como “000000” (0x00), valor padrão (“sinalizado” por uma seta), e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia (item “(b)” da Figura 55), tal DSCP é definido como “110001” (0x31), também “sinalizado” por uma seta, conforme definido anteriormente na Tabela 9.

Ainda quanto ao segundo canal do serviço de vídeo, nesse caso referindo-se ao protocolo IPv6, a Figura 56 ilustra os tráfegos associados a tal serviço/canal (também destinados à porta 9002/UDP do *host* receptor, nesse caso de endereço IPv6 “FD00:0:0:2::1”) antes e após sua classificação e “rotulação” pelo adaptador de tráfego multimídia:

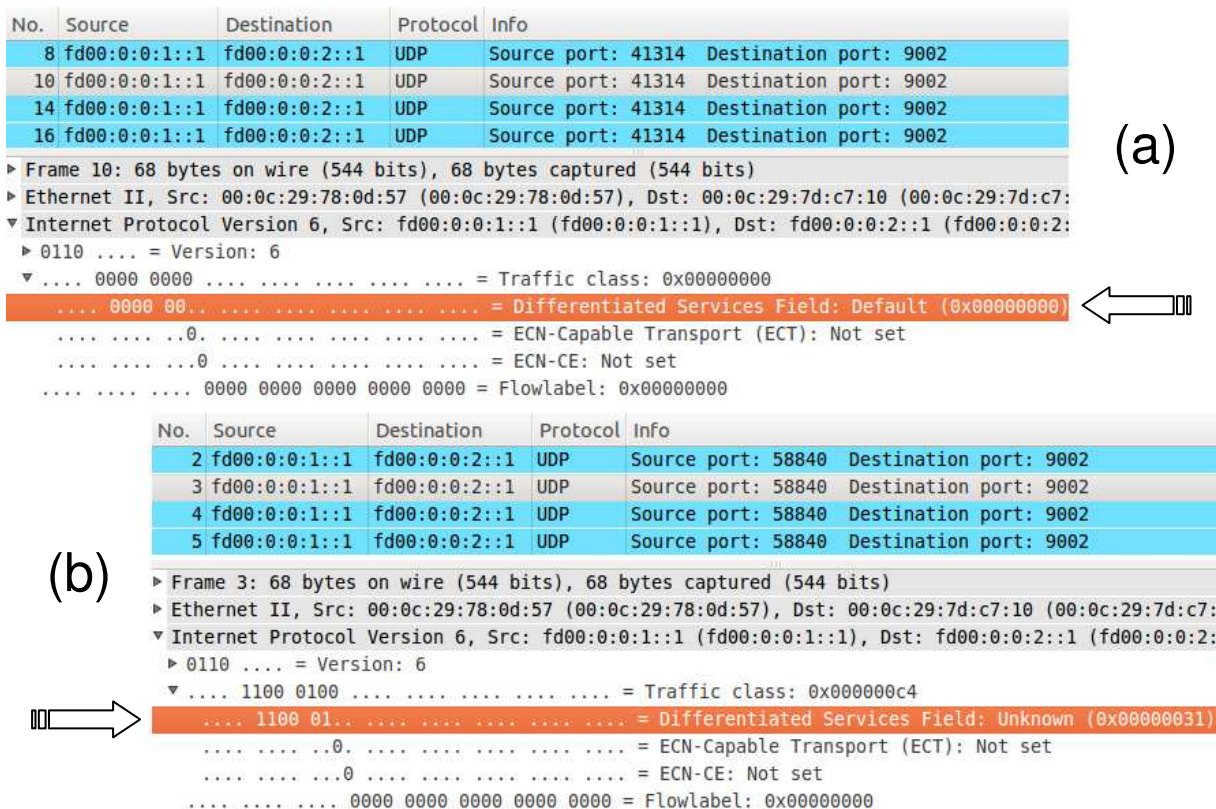


Figura 56 – Tráfego de vídeo (canal 2), utilizando IPv6, antes (a) e após (b) sua classificação e marcação pelo adaptador de tráfego multimídia.

Observe que assim como para o protocolo IPv4, antes da “rotulação” pelo adaptador de tráfego multimídia (item “(a)” da Figura 56), o DSCP associado a tais tráfegos de vídeo (canal 2) é definido como “000000” (0x00), valor padrão, e após sua classificação e “rotulação” por tal adaptador de tráfego multimídia (item “(b)” da Figura 56), o DSCP é definido como “110001” (0x31), ambos “sinalizados” por uma seta.

Sendo assim, quanto ao mecanismo para classificação e marcação de pacotes IP descrito e utilizado nos testes anteriores (Testes I e II), pode-se comprovar que ele é funcional e válido, podendo ser utilizado para “rotular” os pacotes IP (de versões 4 e 6) pertinentes aos diferentes serviços multimídia de áudio, voz, vídeo e de dados originados por seu respectivo sistema transmissor, de modo que os tráfegos *stream* e elástico associados a tais serviços possam ser identificados e tratados pelo *gateway* multimídia com base em seus respectivos identificadores, nesse caso utilizando dos valores que representam tais serviços junto ao campo DSCP do cabeçalho do protocolo IP de tais pacotes.

5.1.2 – Identificação e encaminhamento do tráfego multimídia

De modo similar ao realizado para o adaptador de tráfego multimídia, dois ambientes são propostos para validar e testar o *gateway* multimídia quanto a sua funcionalidade de identificação e encaminhamento de múltiplos tipos de serviços (tráfegos de áudio, voz, vídeo e dados) para sua correta aplicação receptora a partir de informações (identificadores específicos) armazenadas no cabeçalho do protocolo IP (no campo DSCP) pertinentes aos pacotes IP de tais tráfegos:

- Um ambiente com uma única instância das aplicações transmissoras e receptoras dos tráfegos pertinentes aos serviços de áudio, voz, vídeo e dados, em que há apenas um fluxo (canal) de transmissão associado a tais serviços (Figura 57);

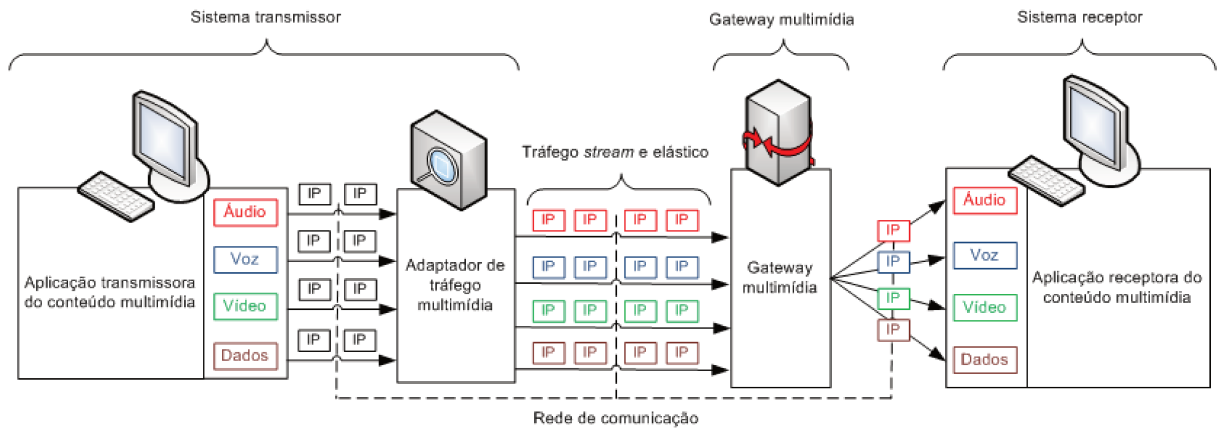


Figura 57 – Ambiente (1) para validação e testes de identificação e encaminhamento de pacotes IP (via DSCP) pelo gateway multimídia.

- Um ambiente com múltiplas instâncias (2 instâncias) das aplicações transmissoras e receptoras dos tráfegos pertinentes aos serviços de áudio, voz, vídeo e dados, em que há múltiplos fluxos (2 canais) de transmissão associados a tais serviços (Figura 58).

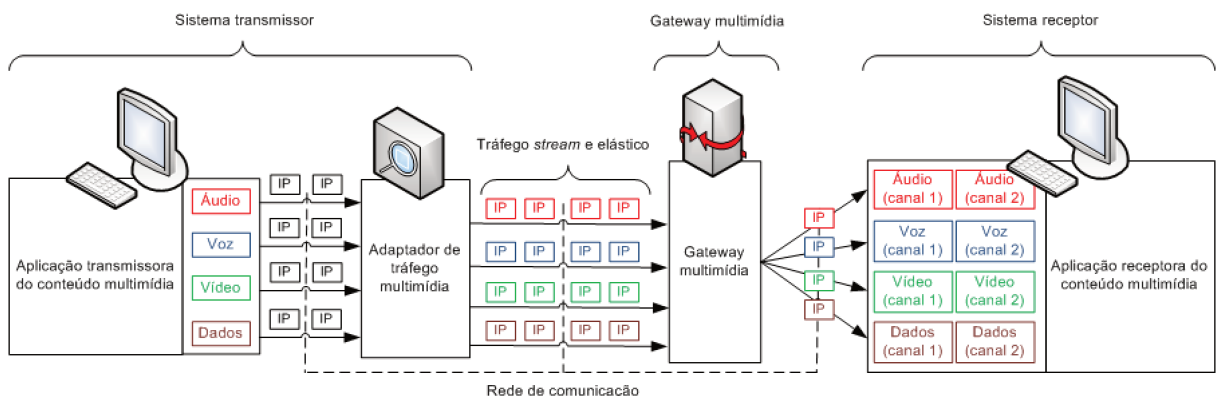


Figura 58 – Ambiente (2) para validação e testes de identificação e encaminhamento de pacotes IP (via DSCP) pelo gateway multimídia.

Em ambos os ambientes, o *gateway* multimídia é tido como “módulo complementar”, na forma de *gateway* de acesso à rede, de um determinado sistema receptor de conteúdos de áudio, voz, vídeo e dados (enviados a ele por um determinado sistema transmissor de tais conteúdos, nesse caso pelo gerador de tráfego multimídia descrito na Seção 4.6.3 com intermédio do adaptador de tráfego multimídia descrito na Seção 4.5), sendo o responsável por receber, identificar (distinguir) e encaminhar (direcionar) os tráfegos associados a tais conteúdos de áudio, voz, vídeo e dados para sua respectiva aplicação receptora no *host* que as executa ao longo da rede. Dessa forma, todo tráfego gerado pelo sistema transmissor às suas respectivas aplicações receptoras é intermediado pelo *gateway* multimídia e, conforme seus identificadores de tipo de serviço (de áudio, voz, vídeo ou dados, por exemplo) definidos no campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) pertinentes a tais tráfegos, encaminhado à sua correta aplicação receptora no *host* que as executa. Se, eventualmente,

pacotes IP não “rotulados” ou com identificadores desconhecidos pelo *gateway* multimídia forem intermediados por ele, tais pacotes podem ser descartados ou encaminhados à aplicação receptora conforme critérios próprios para esse propósito, cabendo ao administrador da rede definir tais critérios. Nesse contexto, em ambos os ambientes descritos anteriormente, parte-se do ponto que todos os pacotes IP intermediados pelo *gateway* multimídia estão devidamente rotulados (no campo DSCP do cabeçalho do protocolo IP) conforme seu tipo de serviço (de áudio, voz, vídeo ou dados), descritos na Tabela 5.

Para tal, assim como no ambiente de testes com o adaptador de tráfego multimídia, para validar o *gateway* multimídia, os *hosts* transmissor e receptor dos tráfegos associados aos serviços de dados, áudio, voz e vídeo estão logicamente organizados em redes distintas, em que o elo de comunicação de ambos com a rede se dá, respectivamente, pelo adaptador de tráfego multimídia (no sistema transmissor) e pelo *gateway* multimídia (no sistema receptor), conforme ilustra a Figura 59:

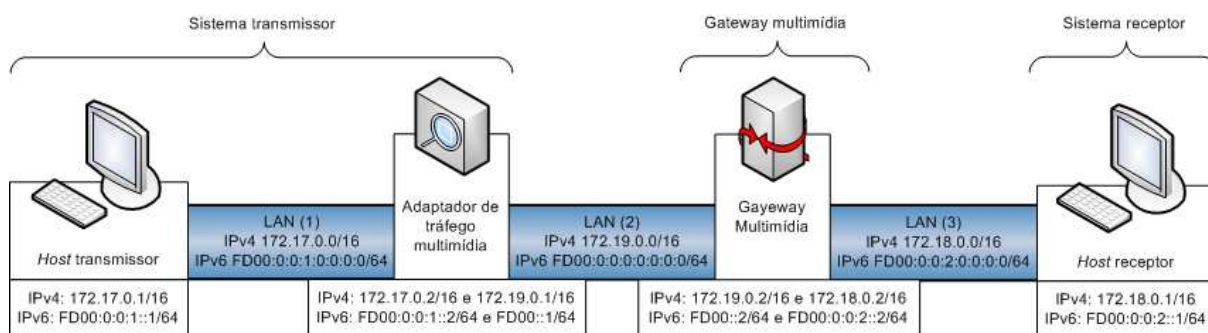


Figura 59 – Endereçamento de rede do ambiente para validação e testes com o *gateway* multimídia.

Em tal ambiente, o *gateway* multimídia, assim como o adaptador de tráfego multimídia, possui quatro endereços de rede (dois endereços IPv4 e dois endereços IPv6), enquanto os *hosts* transmissor e receptor do conteúdo multimídia possuem dois endereços de rede cada (um endereço IPv4 e um endereço IPv6), conforme descrito na Tabela 10:

<i>Host</i>	Endereço IPv4	Endereço IPv6
Transmissor	172.17.0.1/16	FD00:0:0:1::1/64
Adaptador de tráfego multimídia	172.17.0.2/16 172.19.0.1/16	FD00:0:0:1::2/64 FD00::1/64
<i>Gateway</i> multimídia	172.19.0.2/16 172.18.0.2/16	FD00::2/64 FD00:0:0:2::2/64
Receptor	172.18.0.1/16	FD00:0:0:2::1/64

Tabela 10 – Endereçamento IPv4 e IPv6 dos *hosts* do ambiente para validação e testes com o *gateway* multimídia.

A partir de tais configurações, o adaptador de tráfego multimídia (com um endereço IPv4/IPv6 na rede do *host* transmissor e outro endereço IPv4/IPv6 na rede do *gateway* multimídia) e o *gateway* multimídia (com um endereço IPv4/IPv6 na rede do *host* receptor e outro endereço IPv4/IPv6 na rede do adaptador de tráfego multimídia) representam o elo de comunicação entre tais *hosts*, de modo que todo fluxo de comunicação trocado entre ambos

sejam intermediados tanto pelo adaptador de tráfego multimídia quanto pelo *gateway* multimídia. Como exemplo, as Figuras 60 e 61 ilustram, respectivamente, os saltos (*hops*) IPv4 e IPv6 entre o *host* transmissor e o *host* receptor a partir de tais configurações de rede:

```
aluno@transmissor:~$ traceroute receptor.diorio.corp.br
traceroute to receptor.diorio.corp.br (172.18.0.1), 30 hops max, 60 byte packets
 1 marcador.diorio.corp.br (172.17.0.2)  0.672 ms  0.310 ms  0.903 ms
 2 gateway.diorio.corp.br (172.19.0.2)  0.736 ms  0.806 ms  0.644 ms
 3 receptor.diorio.corp.br (172.18.0.1)  1.588 ms  1.431 ms  1.253 ms
```

Figura 60 – Saltos (*hops*) IPv4 entre os *hosts* transmissor e receptor no ambiente para validação e testes do *gateway* multimídia.

```
aluno@transmissor:~$ traceroute6 receptor.diorio.corp.br
traceroute to receptor.diorio.corp.br (fd00:0:0:2::1) from fd00:0:0:1::1, 30 hops
max, 16 byte packets
 1 marcador.diorio.corp.br (fd00:0:0:1::2)  0.896 ms  0.477 ms  0.408 ms
 2 gateway.diorio.corp.br (fd00::2)  1.2 ms  1.022 ms  1.034 ms
 3 receptor.diorio.corp.br (fd00:0:0:2::1)  1.609 ms  1.276 ms  1.2 ms
```

Figura 61 – Saltos (*hops*) IPv6 entre os *hosts* transmissor e receptor no ambiente para validação e testes do *gateway* multimídia.

A partir de tais listagens de saltos (*hops*), pode-se observar que, no sistema transmissor, o adaptador de tráfego multimídia (salto de número 1, nas Figuras 60 e 61 exibidas anteriormente) é o *gateway* de acesso à rede do *host* transmissor e que, no sistema receptor, o *gateway* multimídia (salto de número 2, nas Figuras 60 e 61 exibidas anteriormente) é o *gateway* de acesso à rede do *host* receptor, tanto no IPv4, quanto no IPv6.

Quanto às aplicações transmissora e receptora do gerador de tráfego multimídia em execução nos *hosts* transmissor e receptor do conteúdo multimídia, para efetivamente validar a identificação e encaminhamento de pacotes IP com base no campo DSCP do cabeçalho do protocolo IP, ambos foram configurados de modo distinto quanto às suas portas de envio e recebimento de informações, de modo que os tráfegos associados aos serviços de áudio, voz, vídeo e dados fossem transmitidos ao *gateway* multimídia (e não diretamente ao *host* receptor) em “portas inválidas” e distintas quanto à aplicação receptora do tráfego pertinente a tais serviços (em execução no *host* receptor de tais conteúdos). Por exemplo, o tráfego de áudio foi enviado à porta “a/UDP” do *gateway* multimídia com aplicação receptora em execução na porta “b/UDP” do *host* receptor; o tráfego de vídeo foi enviado à porta “c/UDP” do *gateway* multimídia com aplicação receptora em execução na porta “d/UDP do *host* receptor”; e assim por diante.

Dessa forma, sem o intermédio do *gateway* multimídia, não há processo de comunicação entre as aplicações transmissora e receptora dos conteúdos de áudio, voz, vídeo e de dados, de modo que nenhum tráfego *stream* ou elástico pertinente a tais serviços será trocado entre os *hosts* transmissor e receptor caso o *gateway* multimídia não realize o direcionamento de tais tráfegos às suas respectivas aplicações receptoras (nesse caso, a partir de identificadores junto ao campo DSCP do cabeçalho do protocolo IP dos pacotes associados a tais tráfegos de áudio, voz, vídeo e dados).

Teste I

No primeiro teste (ambiente descrito na Figura 57), os tráfegos associados ao serviço de dados são identificados pelo DSCP “000000” e devem ser encaminhados à aplicação receptora na porta 6001/TCP do *host* receptor, os tráfegos associados ao serviço de áudio são identificados pelo DSCP “010000” e devem ser encaminhados à aplicação receptora na porta 7001/UDP do *host* receptor, os tráfegos associados ao serviço de voz são identificados pelo DSCP “100000” e devem ser encaminhados à aplicação receptora na porta 8001/UDP do *host* receptor e os tráfegos associados ao serviço de vídeo são identificados pelo DSCP “110000” e devem ser encaminhados à aplicação receptora na porta 9001/UDP do *host* receptor. Ambos os tráfegos são intermediados pelo *gateway* multimídia e direcionados ao *host* receptor (aplicação receptora) com base em seus respectivos identificadores quanto ao campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) dos pacotes pertinentes a tais tráfegos.

Em tal ambiente, conforme descrito anteriormente, quanto aos módulos transmissor e receptor do gerador de tráfego multimídia, para efetivamente validar a identificação e encaminhamento de pacotes IP com base no campo DSCP do cabeçalho do protocolo IP, ambos foram configurados de modo distinto quanto às suas portas de envio e recebimento de informações, de modo que os tráfegos associados aos serviços de áudio, voz, vídeo e dados fossem transmitidos ao *gateway* multimídia (e não diretamente ao *host* receptor) em “portas inválidas” e distintas quanto à aplicação receptora do tráfego pertinente a tais serviços (o tráfego de dados foi enviado à porta 6111/TCP do *gateway* multimídia com aplicação receptora em execução na porta 6001/TCP do *host* receptor; o tráfego de áudio foi enviado à porta 7111/UDP do *gateway* multimídia com aplicação receptora em execução na porta 7001/UDP do *host* receptor; o tráfego de voz foi enviado à porta 8111/UDP do *gateway* multimídia com aplicação receptora em execução na porta 8001/UDP do *host* receptor; e, o tráfego de vídeo foi enviado à porta 9111/UDP do *gateway* multimídia com aplicação receptora em execução na porta 9001/UDP do *host* receptor, conforme descrito na Tabela 11).

Aplicação	Porta de envio (do sistema transmissor ao <i>gateway</i> multimídia)	Porta de escuta/recebimento (no sistema receptor, direcionada pelo <i>gateway</i> multimídia)
Dados	6111/TCP	6001/TCP
Áudio	7111/UDP	7001/UDP
Voz	8111/UDP	8001/UDP
Vídeo	9111/UDP	9001/UDP

Tabela 11 – Portas de envio e escuta/recebimento nos módulos transmissor e receptor do gerador de tráfego multimídia (1).

Internamente ao *gateway* multimídia, as Figuras 62 e 63 ilustram as definições de encaminhamento de pacotes IP com base nos DSCP’s associados aos serviços de dados, áudio, voz e vídeo para os protocolos IPv4 e IPv6, respectivamente:

```
aluno@gateway:~$ sudo iptables -L -n -t nat -Z PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination           DSCP match
DNAT      tcp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x00 to:172.18.0.1:6001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x10 to:172.18.0.1:7001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x20 to:172.18.0.1:8001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x30 to:172.18.0.1:9001
```

Figura 62 – Encaminhamento de pacotes IPv4 com base no DSCP pelo *gateway* multimídia (1).

```

aluno@gateway:~$ sudo iptables -L -n -t mangle -Z PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
TPROXY    tcp  :/:0                  fd00:0:0:2::2/128    DSCP match 0x00 TPROXY redirect fd00:0:0:2::1:6001
TPROXY    udp  :/:0                  fd00:0:0:2::2/128    DSCP match 0x10 TPROXY redirect fd00:0:0:2::1:7001
TPROXY    udp  :/:0                  fd00:0:0:2::2/128    DSCP match 0x20 TPROXY redirect fd00:0:0:2::1:8001
TPROXY    udp  :/:0                  fd00:0:0:2::2/128    DSCP match 0x30 TPROXY redirect fd00:0:0:2::1:9001

```

Figura 63 – Encaminhamento de pacotes IPv6 com base no DSCP pelo gateway multimídia (1).

Observe que em ambos os casos (IPv4 e IPv6), todo pacote IP destinado ao *gateway* multimídia (nos endereços IPv4 “172.18.0.2” ou IPv6 “FD00:0:0:2::2”) será encaminhado ao *host* receptor (nos endereços IPv4 “172.18.0.1” ou IPv6 “FD00:0:0:2::1”) a partir de seus respectivos DSCP’s, cabendo a tal *gateway* multimídia realizar a distinção entre um e outro pacote, bem como o encaminhamento de tais pacotes ao *host* receptor (em ambos os casos, a partir do DSCP associado a tais pacotes IP). Vale ressaltar que, com base em tais definições, pacotes IP com DSCP “000000” (0x00) serão encaminhados à porta 6001/TCP do *host* receptor, pacotes IP com DSCP “010000” (0x10) serão encaminhados à porta 7001/UDP do *host* receptor, pacotes IP com DSCP “100000” (0x20) serão encaminhados à porta 8001/UDP do *host* receptor e pacotes IP com DSCP “110000” (0x30) serão encaminhados à porta 9001/UDP do *host* receptor.

Nesse contexto, quanto ao Teste I propriamente dito, nesse caso referindo-se ao serviço de dados, a Figura 64 ilustra os pacotes IPv4 e IPv6 enviados pelo sistema transmissor ao *gateway* multimídia (nesse caso, enviados pelo *host* transmissor, “rotulados” pelo adaptador de tráfego multimídia e destinados ao *gateway* multimídia) para que sejam encaminhados ao *host* receptor (aplicação receptora):

No.	Source	Destination	Protocol	Info
15	172.19.0.1	172.18.0.2	TCP	59190 > 6111 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK
16	172.18.0.2	172.18.0.1	TCP	59190 > 6001 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK
17	172.18.0.1	172.18.0.2	TCP	6001 > 59190 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MS
18	172.18.0.2	172.19.0.1	TCP	6111 > 59190 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MS
20	172.19.0.1	172.18.0.2	TCP	59190 > 6111 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4
21	172.18.0.2	172.18.0.1	TCP	59190 > 6001 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4

▶ Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: 00:0c:29:78:0d:57 (00:0c:29:78:0d:57), Dst: 00:0c:29:3f:95:af (00:0c:29:3f:95:af)
 ▼ Internet Protocol Version 4, Src: 172.19.0.1 (172.19.0.1), Dst: 172.18.0.2 (172.18.0.2)
 Version: 4
 Header length: 20 bytes
 ▼ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) (0x00)
 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)

(a) ←

No.	Source	Destination	Protocol	Info
2	fd00:0:0:1::1	fd00:0:0:2::2	TCP	36323 > 6111 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK
3	fd00:0:0:2::2	fd00:0:0:1::1	TCP	6111 > 36323 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 M
5	fd00:0:0:1::1	fd00:0:0:2::2	TCP	36323 > 6111 [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=
8	fd00:0:0:2::2	fd00:0:0:2::1	TCP	36142 > 6001 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK
9	fd00:0:0:2::1	fd00:0:0:2::2	TCP	6001 > 36142 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 M
10	fd00:0:0:2::2	fd00:0:0:2::1	TCP	36142 > 6001 [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=

▶ Frame 2: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
 ▶ Ethernet II, Src: 00:0c:29:78:0d:57 (00:0c:29:78:0d:57), Dst: 00:0c:29:3f:95:af (00:0c:29:3f:95:af)
 ▼ Internet Protocol Version 6, Src: fd00:0:0:1::1 (fd00:0:0:1::1), Dst: fd00:0:0:2::2 (fd00:0:0:2::2)
 ▶ 0110 = Version: 6
 ▼ 0000 0000 = Traffic class: 0x00000000
 0000 00.. = Differentiated Services Field: Default (0x00000000)
 0. = ECN-Capable Transport (ECT): Not set
 0. = ECN-CE: Not set

← (b)

Figura 64 – Encaminhamento de pacotes IPv4 (a) e IPv6(b) do tráfego de dados com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Observe, na Figura 64, que todo tráfego gerado pelo sistema transmissor é enviado ao *gateway* multimídia na porta 6111/TCP e direcionado por tal *gateway* ao *host* receptor na porta 6001/TCP. Como exemplo, no item “(a)” de tal figura, o pacote de número 15 demonstra o *host* transmissor (de endereço IPv4 “172.19.0.1”) enviando uma requisição TCP ao *gateway* multimídia (de endereço IPv4 “172.18.0.2”) na porta de destino de número 6111. Em seguida, no pacote de número 16, o *gateway* multimídia (com base no DSCP associado ao pacote IP em questão) o encaminha para o *host* receptor (de endereço IPv4 “172.18.0.1”) na porta TCP de número 6001. Por sua vez, no pacote de número 17, o *host* receptor confirma o recebimento do pacote IP ao *gateway* multimídia que, no pacote 19, confirma o recebimento do pacote ao *host* transmissor. Ao final, no pacote de número 20, o *host* transmissor confirma o estabelecimento da conexão TCP com o *gateway* multimídia (na porta 6111/TCP) que, no pacote de número 21, realiza o mesmo procedimento com o *host* receptor, confirmando o estabelecimento da conexão TCP na porta 6001 de tal *host* e viabilizando todo o processo de comunicação seguinte a tal estabelecimento de conexão TCP.

De modo similar ao IPv4, no item “(b)” da Figura 64, para o IPv6, nos pacotes de número 2, 3 e 5, há o estabelecimento da conexão TCP entre os *hosts* transmissor (de endereço IPv6 “FD00:0:0:1::1”) e o *gateway* multimídia (de endereço IPv6 “FD00:0:0:2::2”), tendo como base a porta 6111/TCP. Por sua vez, novamente com base no DSCP associado ao pacote IP em questão, nos pacotes de número 8, 9 e 10, o *gateway* multimídia o encaminha ao *host* receptor (de endereço IPv6 “FD00:0:0:2::1”), estabelecendo a conexão TCP junto a porta 6001 de tal *host*.

Quanto ao *host* receptor, para ele só há o estabelecimento de conexão partindo do *gateway* multimídia em sua porta 6001/TCP, em que todo tráfego entrante a tal porta é recebido pelo *gateway* multimídia do *host* transmissor e direcionado para tal *host* receptor de modo transparente a ele, conforme ilustra a Figura 65 para os protocolos IPv4 e IPv6, respectivamente:

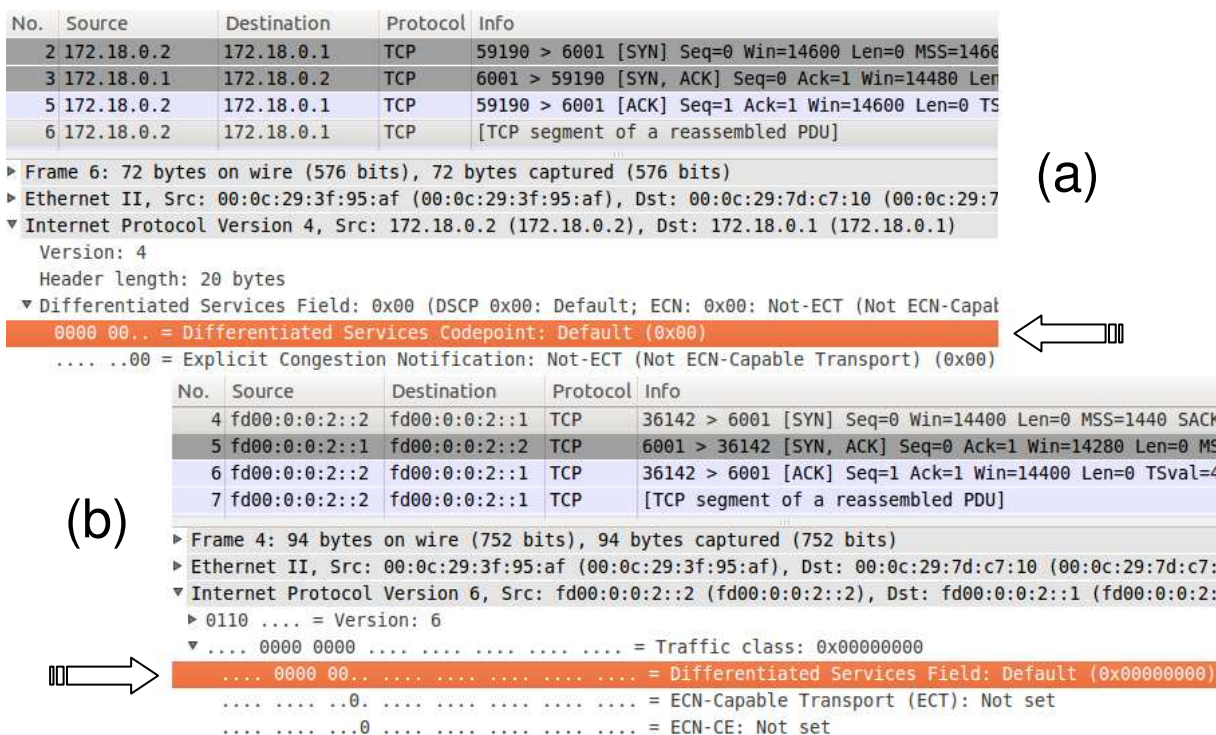


Figura 65 – Tráfego de dados entrante ao *host* receptor utilizando IPv4 (a) e IPv6 (b).

De modo similar ao serviço de dados, todo tráfego pertinente ao serviço de áudio também é destinado ao *gateway* multimídia que, por sua vez, o encaminha ao *host* receptor tendo como base o DSCP associado aos pacotes IP pertinentes a tal tráfego (nesse caso, DSCP “010000”, “0x10”), conforme ilustra a Figura 66:

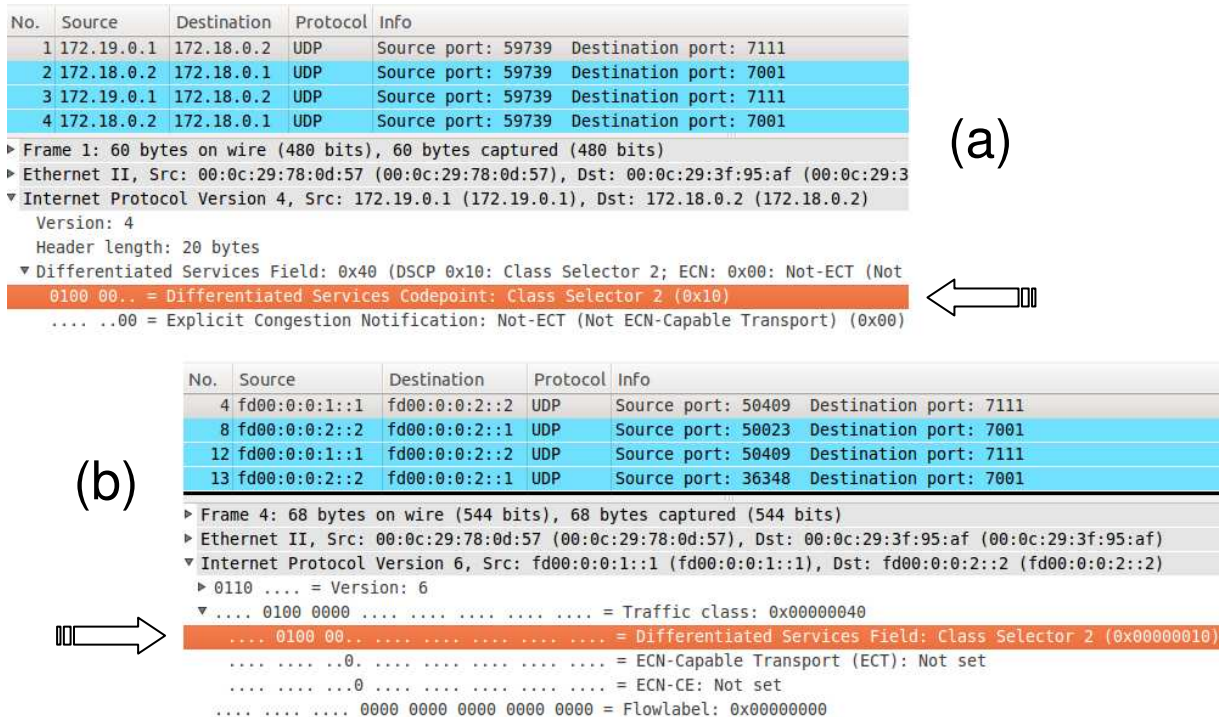


Figura 66 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de áudio com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações (Figura 66), pelo fato do tráfego associado ao serviço de áudio estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 7111/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 4 e 12 no item “(b)” de tal figura), devidamente “rotulados” quanto ao serviço de áudio no DSCP dos pacotes IP, são, na sequência, direcionados à porta 7001/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 8 e 13 no item “(b)” de tal figura).

Quanto ao *host* receptor, para ele todo tráfego de áudio é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 7001/UDP, conforme ilustra a Figura 67 para os protocolos IPv4 e IPv6, respectivamente:

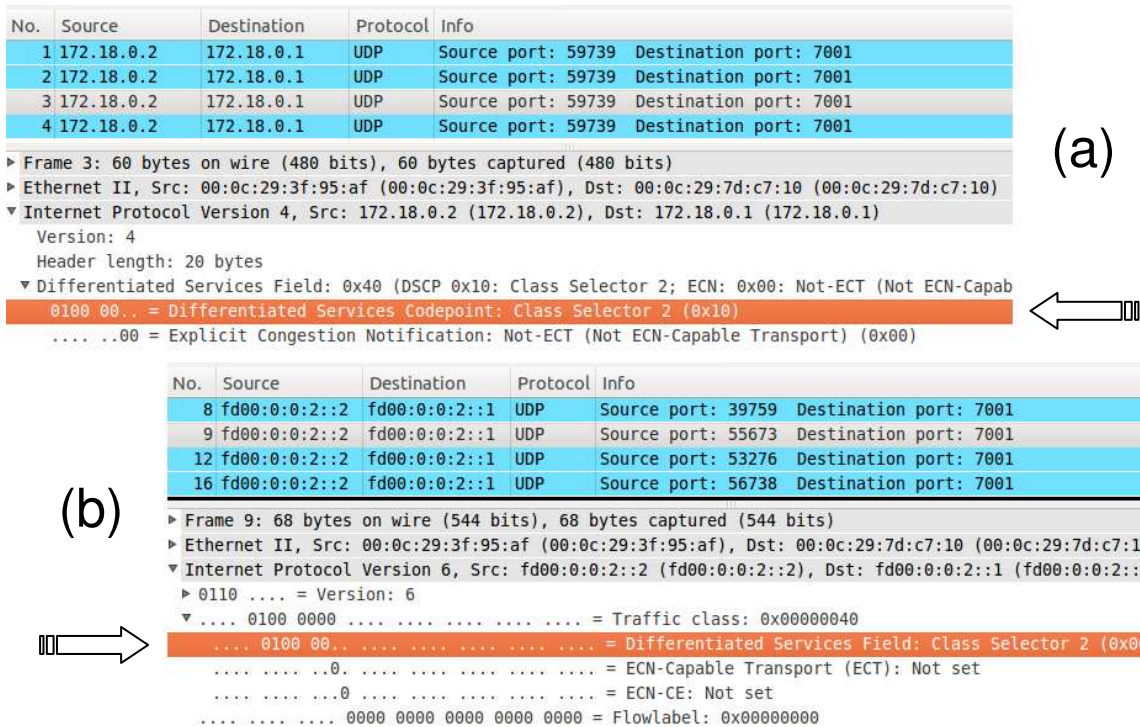


Figura 67 – Tráfego de áudio entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).

Na sequência, quanto ao serviço de voz, todo tráfego com DSCP “100000” (0x20) transmitido para o *gateway* multimídia, é direcionado por ele ao *host* receptor na porta de escuta de sua respectiva aplicação receptora (porta 8001/UDP), conforme ilustra a Figura 68:

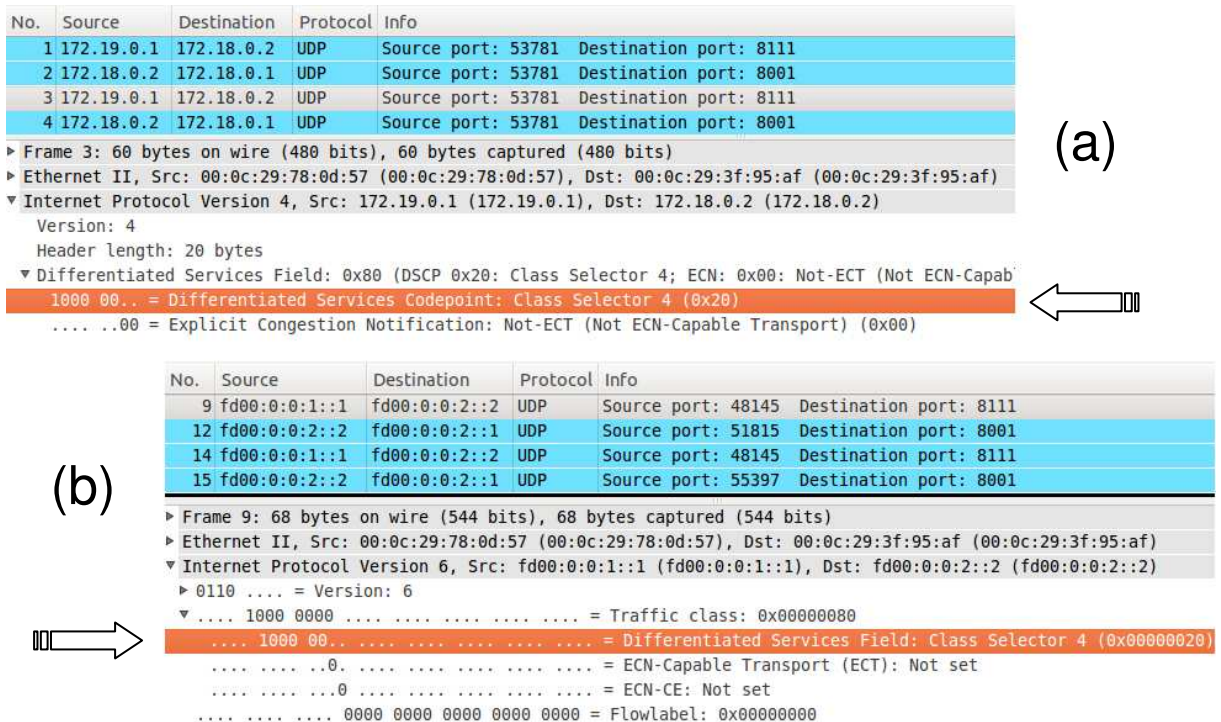


Figura 68 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de voz com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações, assim como no tráfego de áudio, pelo fato do tráfego associado a tal serviço de voz estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 8111/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 9 e 14 no item “(b)” da Figura 68), devidamente “rotulados” quanto ao serviço de voz no DSCP dos pacotes IP, são, na sequência, direcionados à porta 8001/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 12 e 15 no item “(b)” da Figura 68).

Quanto ao *host* receptor, para ele todo tráfego de voz é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 8001/UDP, conforme ilustra a Figura 69 para os protocolos IPv4 e IPv6, respectivamente:

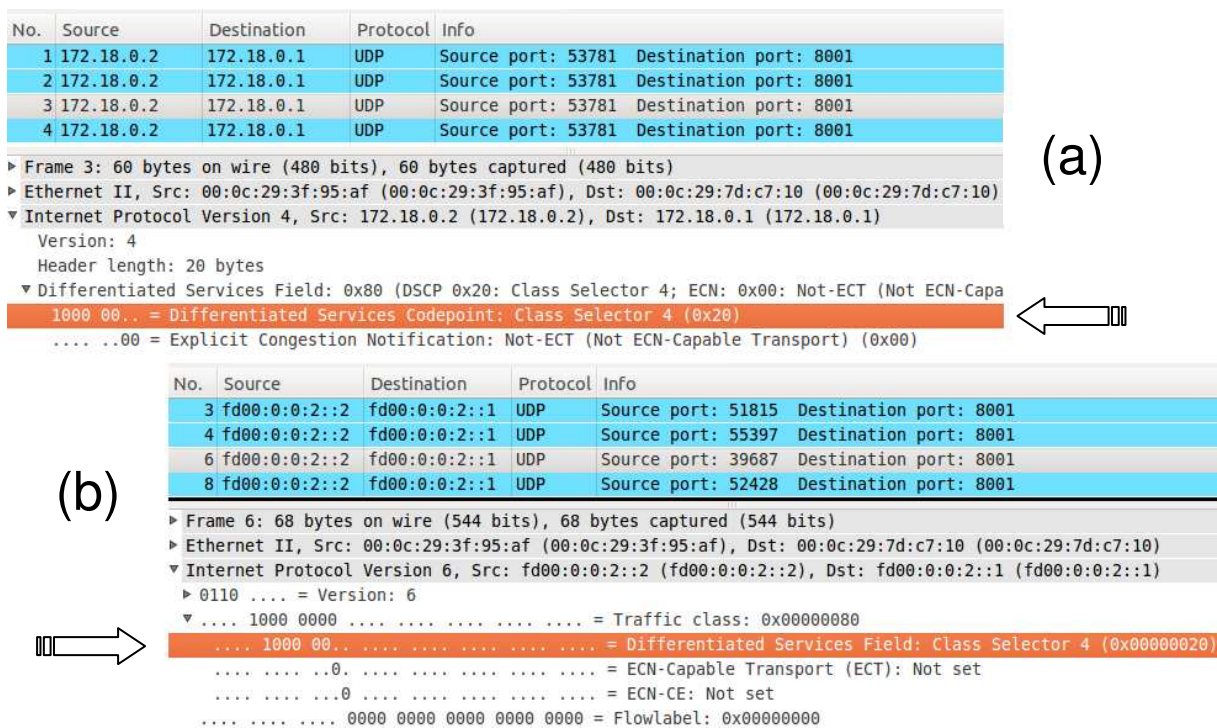


Figura 69 – Tráfego de voz entrante ao *host* receptor utilizando IPv4 (a) e IPv6 (b).

Por sua vez, quanto ao serviço de vídeo, todo tráfego gerado pelo sistema transmissor com DSCP “110000” (0x30), transmitido para o *gateway* multimídia, é direcionado por ele ao *host* receptor na porta de escuta de sua respectiva aplicação receptora (porta 9001/UDP), conforme ilustra a Figura 70:

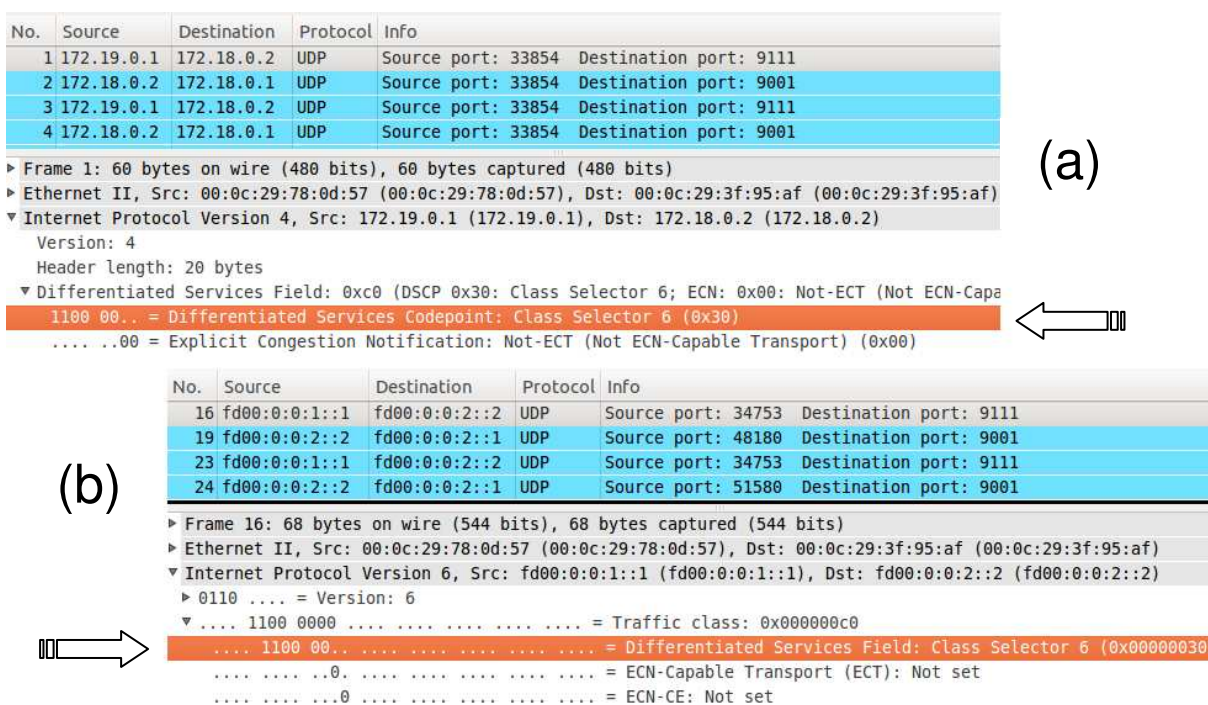


Figura 70 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de vídeo com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações, assim como nos tráfegos de áudio e de voz, pelo fato do tráfego associado a tal serviço de vídeo estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 9111/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 16 e 23 no item “(b)” da Figura 70), devidamente “rotulados” quanto ao serviço de vídeo no DSCP dos pacotes IP, são, na sequência, direcionados à porta 9001/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 19 e 24 no item “(b)” da Figura 70).

Assim como para os serviços de dados, áudio e voz descritos anteriormente, quanto ao *host* receptor, para ele todo tráfego de vídeo é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 9001/UDP, conforme ilustra a Figura 71 para os protocolos IPv4 e IPv6, respectivamente:

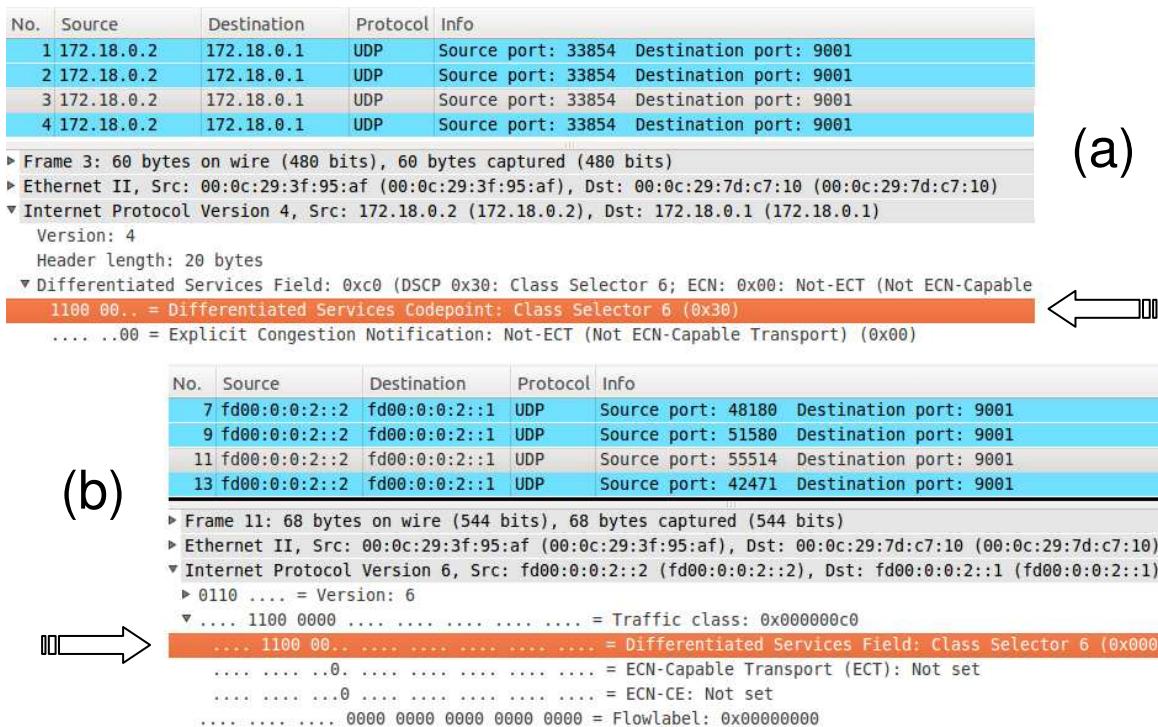


Figura 71 – Tráfego de vídeo entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).

Em ambos os casos, vale ressaltar que se o *gateway* multimídia for desligado ou tiver seu mecanismo funcional interrompido ou modificado quanto ao encaminhamento de pacotes IP com base no DSCP associado a tais pacotes IP, não há processo de comunicação entre as aplicações transmissora e receptora dos tráfegos de dados, áudio, voz e vídeo descritos anteriormente, validando, também, seu mecanismo funcional quanto à identificação e encaminhamento de pacotes IP com base em seu respectivo DSCP.

Teste II

O segundo teste é similar ao primeiro, porém com mais fluxos de transmissão (nesse caso, dois fluxos de transmissão) associados aos serviços de áudio, voz, vídeo e de dados. Em tal teste (ambiente descrito na Figura 58), de modo complementar ao Teste I, há um segundo canal de comunicação para aos serviços de dados, de áudio, de voz e de vídeo, em que os tráfegos associados ao segundo canal do serviço de dados são identificados pelo DSCP “000001” e devem ser encaminhados à aplicação receptora na porta 6002/TCP do *host* receptor; os tráfegos associados ao segundo canal do serviço de áudio são identificados pelo DSCP “010001” e devem ser encaminhados à aplicação receptora na porta 7002/UDP do *host* receptor; os tráfegos associados ao segundo canal do serviço de voz são identificados pelo DSCP “100001” e devem ser encaminhados à aplicação receptora na porta 8002/UDP do *host* receptor; e, os tráfegos associados ao segundo canal do serviço de vídeo são identificados pelo DSCP “110001” e devem ser encaminhados à aplicação receptora na porta 9002/UDP do *host* receptor.

Em tal ambiente, assim como realizado no Teste I, quanto aos módulos transmissor e receptor do gerador de tráfego multimídia, para efetivamente validar a identificação e encaminhamento de pacotes IP com base no campo DSCP do cabeçalho do protocolo IP para esse segundo canal quanto aos serviços de dados, áudio, voz e vídeo, ambos foram configurados de modo distinto quanto às suas portas de envio e recebimento de informações, de modo que os

tráfegos associados ao segundo canal de tais serviços também fossem transmitidos ao *gateway* multimídia (e não diretamente ao *host* receptor) e em “portas inválidas” e distintas quanto à aplicação receptora do tráfego pertinente a tais serviços (o tráfego de dados foi enviado às portas 6111/TCP e 6112/TCP do *gateway* multimídia com aplicação receptora em execução nas portas 6001/TCP e 6002/TCP do *host* receptor; o tráfego de áudio foi enviado às portas 7111/UDP e 7112/UDP do *gateway* multimídia com aplicação receptora em execução nas portas 7001/UDP e 7002/UDP do *host* receptor; o tráfego de voz foi enviado às portas 8111/UDP e 8112/UDP do *gateway* multimídia com aplicação receptora em execução nas portas 8001/UDP e 8002/UDP do *host* receptor; e, o tráfego de vídeo foi enviado às portas 9111/UDP e 9112/UDP do *gateway* multimídia com aplicação receptora em execução nas portas 9001/UDP e 9002/UDP do *host* receptor, conforme descrito na Tabela 12).

Aplicação	Porta de envio (do sistema transmissor ao <i>gateway</i> multimídia)	Porta de escuta/recebimento (no sistema receptor, direcionada pelo <i>gateway</i> multimídia)
Dados	6111/TCP (canal 1) 6112/TCP (canal 2)	6001/TCP (canal 1) 6002/TCP (canal 2)
Áudio	7111/UDP (canal 1) 7112/UDP (canal 2)	7001/UDP (cana 1) 7002/UDP (cana 2)
Voz	8111/UDP (canal 1) 8112/UDP (canal 2)	8001/UDP (canal 1) 8002/UDP (canal 2)
Vídeo	9111/UDP (canal 1) 9112/UDP (canal 2)	9001/UDP (canal 1) 9002/UDP (canal 2)

Tabela 12 – Portas de envio e escuta/recebimento nos módulos transmissor e receptor do gerador de tráfego multimídia (2).

Internamente ao *gateway* multimídia, as Figuras 72 e 73 ilustram as definições de encaminhamento de pacotes IP com base nos DSCP’s associados aos canais 1 e 2 dos serviços de dados, áudio, voz e vídeo para os protocolos IPv4 e IPv6, respectivamente:

```
aluno@gateway:~$ sudo iptables -L -n -t nat -Z PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT      tcp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x00 to:172.18.0.1:6001
DNAT      tcp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x01 to:172.18.0.1:6002
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x10 to:172.18.0.1:7001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x11 to:172.18.0.1:7002
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x20 to:172.18.0.1:8001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x21 to:172.18.0.1:8002
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x30 to:172.18.0.1:9001
DNAT      udp  --  0.0.0.0/0             172.18.0.2           DSCP match 0x31 to:172.18.0.1:9002
```

Figura 72 – Encaminhamento de pacotes IPv4 com base no DSCP pelo gateway multimídia (2).

```
aluno@gateway:~$ sudo ip6tables -L -n -t mangle -Z PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
TPROXY    tcp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x00 TPROXY redirect fd00:0:0:2::1:6001
TPROXY    tcp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x01 TPROXY redirect fd00:0:0:2::1:6002
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x10 TPROXY redirect fd00:0:0:2::1:7001
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x11 TPROXY redirect fd00:0:0:2::1:7002
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x20 TPROXY redirect fd00:0:0:2::1:8001
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x21 TPROXY redirect fd00:0:0:2::1:8002
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x30 TPROXY redirect fd00:0:0:2::1:9001
TPROXY    udp  --  ::/0                  fd00:0:0:2::2/128   DSCP match 0x31 TPROXY redirect fd00:0:0:2::1:9002
```

Figura 73 – Encaminhamento de pacotes IPv6 com base no DSCP pelo gateway multimídia (2).

Observe que em ambos os casos (IPv4 e IPv6), assim como no Teste I, todo pacote IP destinado ao *gateway* multimídia (nos endereços IPv4 “172.18.0.2” ou IPv6 “FD00:0:0:2::2”) será encaminhado ao *host* receptor (nos endereços IPv4 “172.18.0.1” ou IPv6 “FD00:0:0:2::1”) a partir de seus respectivos DSCP’s, cabendo a tal *gateway* multimídia realizar a distinção entre um e outro pacote, bem como ao canal de comunicação associado a tal pacote, além de realizar o encaminhamento de tais pacotes ao *host* receptor (em ambos os casos, a partir do DSCP associado a tais pacotes IP). Vale ressaltar que, com base em tais definições, pacotes IP com DSCP “000000” (0x00) serão encaminhados à porta 6001/TCP do *host* receptor, pacotes IP com DSCP “000001” (0x01) serão encaminhados à porta 6002/TCP do *host* receptor, pacotes IP com DSCP “010000” (0x10) serão encaminhados à porta 7001/UDP do *host* receptor, pacotes IP com DSCP “010001” (0x11) serão encaminhados à porta 7002/UDP do *host* receptor, pacotes IP com DSCP “100000” (0x20) serão encaminhados à porta 8001/UDP do *host* receptor, pacotes IP com DSCP “100001” (0x21) serão encaminhados à porta 8002/UDP do *host* receptor, pacotes IP com DSCP “110000” (0x30) serão encaminhados à porta 9001/UDP do *host* receptor e pacotes IP com DSCP “110001” (0x31) serão encaminhados à porta 9002/UDP do *host* receptor.

Nesse contexto, quanto ao Teste II propriamente dito, nesse caso referindo-se ao canal 2 do serviço de dados, a Figura 74 ilustra os pacotes IPv4 e IPv6 enviados pelo sistema transmissor (*host* transmissor e adaptador de tráfego multimídia) ao *gateway* multimídia para que sejam encaminhados ao *host* receptor (aplicação receptora):

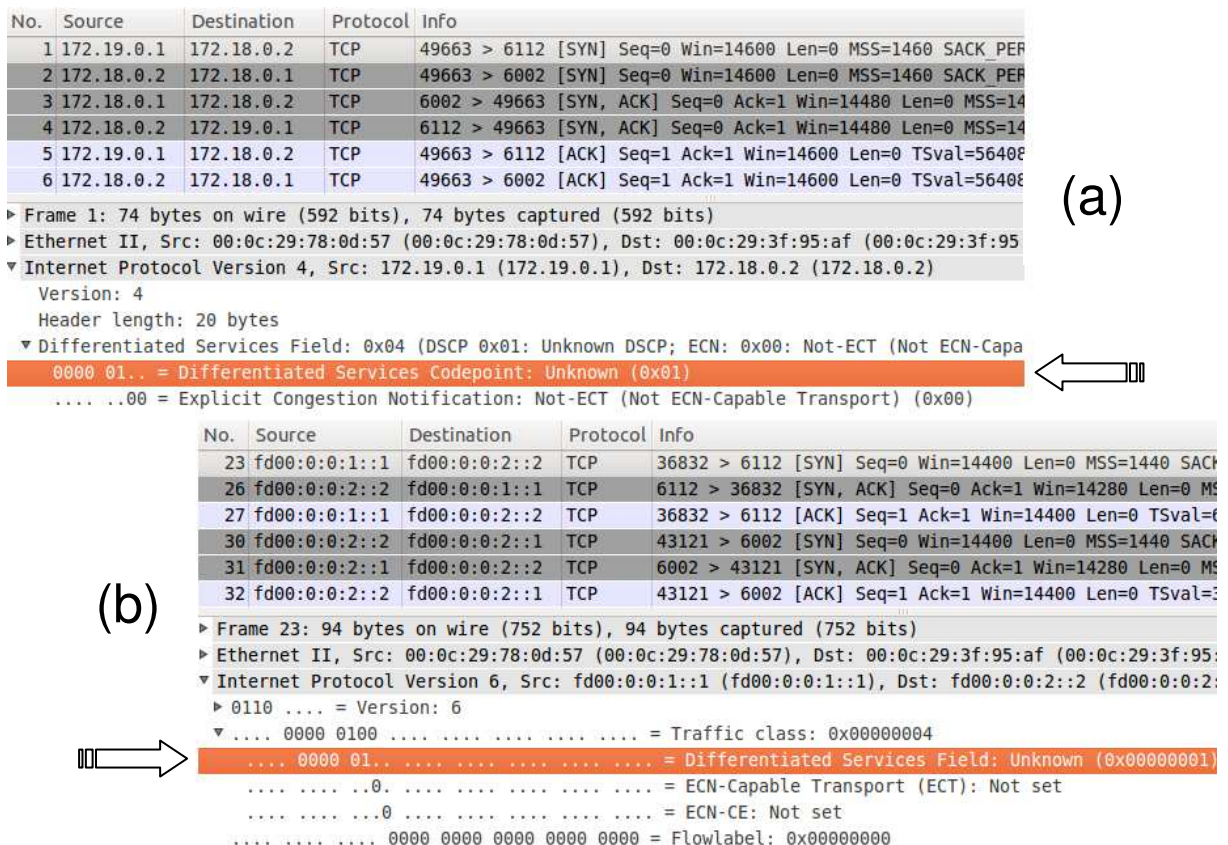


Figura 74 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de dados (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Quanto às informações descritas na Figura 74, observe que todo tráfego gerado pelo sistema transmissor para o canal 2 do serviço de dados, devidamente identificado com DSCP

“000001” (0x01), é enviado ao *gateway* multimídia na porta 6112/TCP e direcionado por tal *gateway* ao *host* receptor na porta 6002/TCP. Como exemplo, no item “(a)” da Figura 74, o pacote de número 1 demonstra o *host* transmissor (de endereço IPv4 “172.19.0.1”) enviando uma requisição TCP ao *gateway* multimídia (de endereço IPv4 “172.18.0.2”) na porta de destino de número 6112. Em seguida, no pacote de número 2, o *gateway* multimídia (com base no DSCP associado ao pacote IP em questão) o encaminha para o *host* receptor (de endereço IPv4 “172.18.0.1”) na porta TCP de número 6002. Por sua vez, no pacote de número 3, o *host* receptor confirma o recebimento do pacote IP ao *gateway* multimídia que, no pacote 4, confirma o recebimento do pacote ao *host* transmissor. Ao final, no pacote de número 5, o *host* transmissor confirma o estabelecimento da conexão TCP com o *gateway* multimídia (na porta 6112/TCP) que, no pacote de número 6, realiza o mesmo procedimento com o *host* receptor, confirmando o estabelecimento da conexão TCP na porta 6002 de tal *host* e viabilizando todo o processo de comunicação seguinte a tal estabelecimento de conexão TCP.

De modo similar ao IPv4, no item “(b)” da Figura 74, para o protocolo IPv6, nos pacotes de número 23, 26 e 27, há o estabelecimento da conexão TCP entre os *hosts* transmissor (de endereço IPv6 “FD00:0:0:1::1”) e o *gateway* multimídia (de endereço IPv6 “FD00:0:0:2::2”), tendo como base a porta 6112/TCP. Por sua vez, novamente com base no DSCP associado ao pacote IP em questão, nos pacotes de número 30, 31 e 32, o *gateway* multimídia o redireciona ao *host* receptor (de endereço IPv6 “FD00:0:0:2::1”), estabelecendo a conexão TCP junto a porta 6002 de tal *host*.

Quanto ao *host* receptor, para ele só há o estabelecimento de conexão no canal 2 de dados partindo do *gateway* multimídia em sua porta 6002/TCP, em que todo tráfego entrante a tal porta é recebido pelo *gateway* multimídia do *host* transmissor e direcionado para tal *host* receptor de modo transparente a ele, conforme ilustra a Figura 75 para os protocolos IPv4 e IPv6, respectivamente:

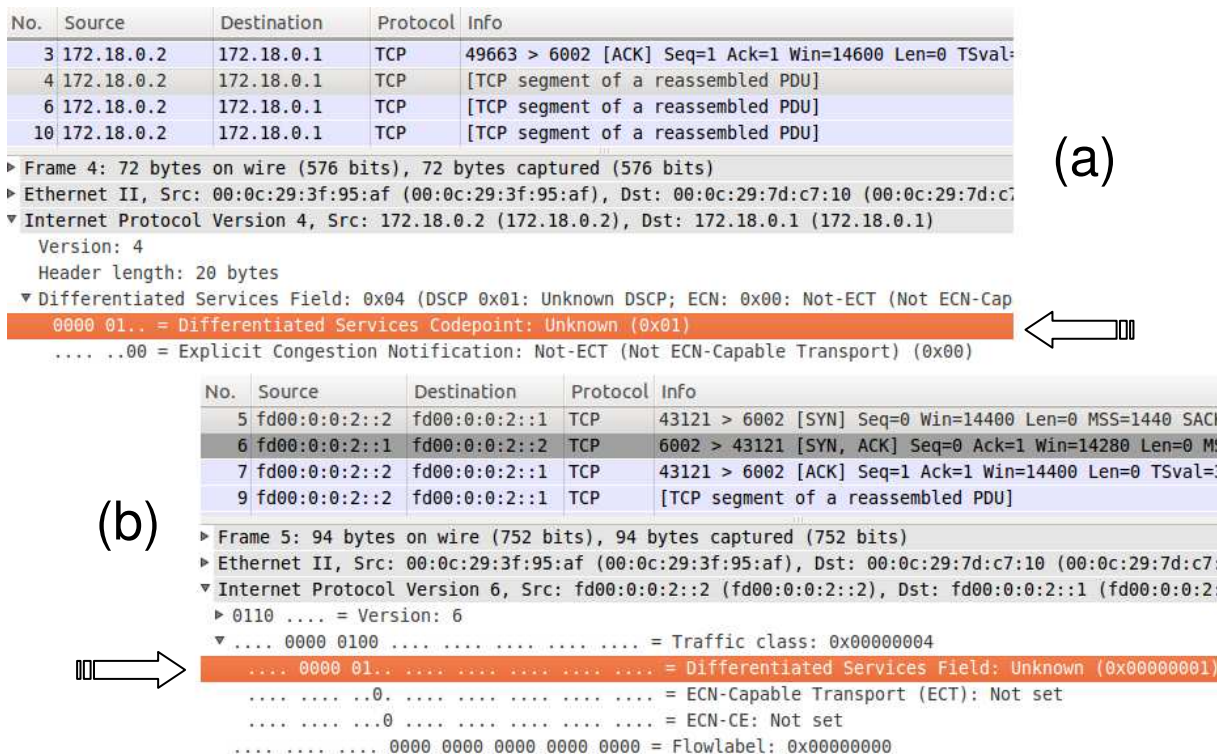


Figura 75 – Tráfego de dados (canal 2) entrante ao *host* receptor utilizando IPv4 (a) e IPv6 (b).

De modo similar ao serviço de dados, todo tráfego pertinente ao canal 2 do serviço de áudio também é destinado ao *gateway* multimídia que, por sua vez, o encaminha ao *host* receptor tendo como base o DSCP associado aos pacotes IP pertinentes a tal tráfego (nesse caso, DSCP “010001”), conforme ilustra a Figura 76:

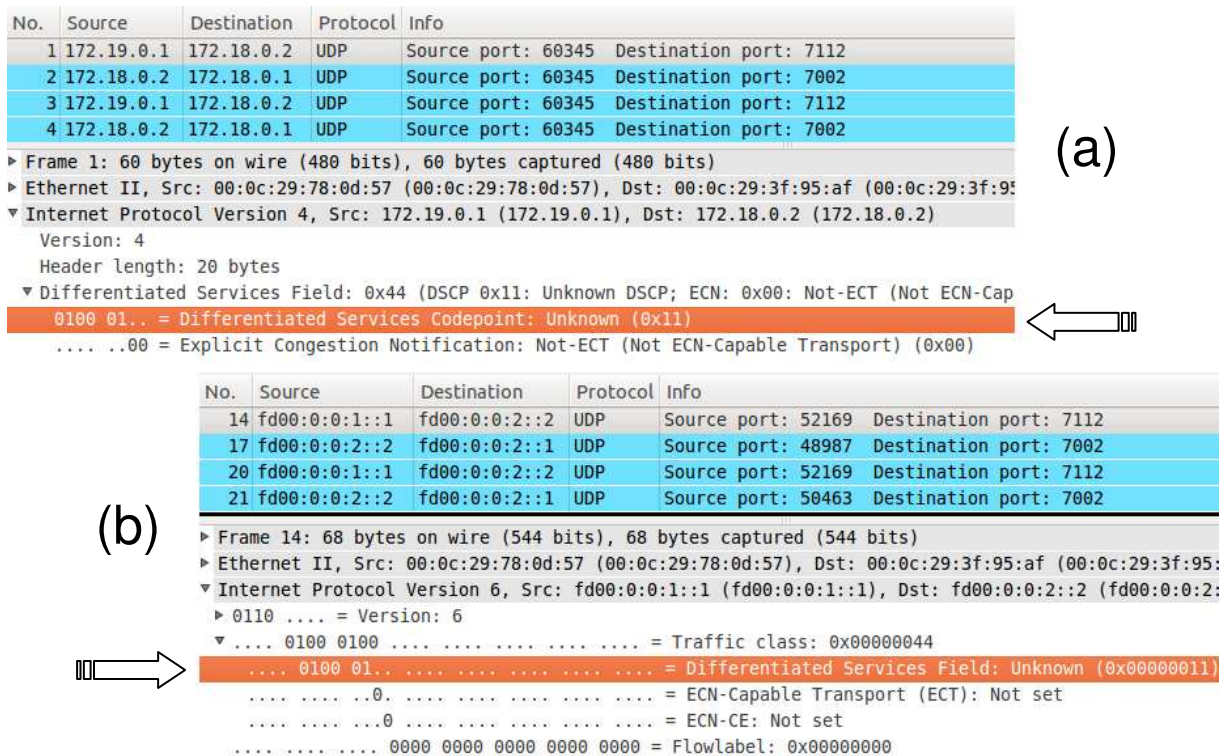


Figura 76 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de áudio (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações, pelo fato do tráfego associado a tal serviço de áudio estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 7112/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 14 e 20 no item “(b)” da Figura 76), devidamente “rotulados” quanto ao canal 2 do serviço de áudio no DSCP dos pacotes IP, são, na sequência, direcionados à porta 7002/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 17 e 21 no item “(b)” da Figura 76).

Quanto ao *host* receptor, para ele todo tráfego do canal 2 de áudio é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 7002/UDP, conforme ilustra a Figura 77 para os protocolos IPv4 e IPv6, respectivamente:

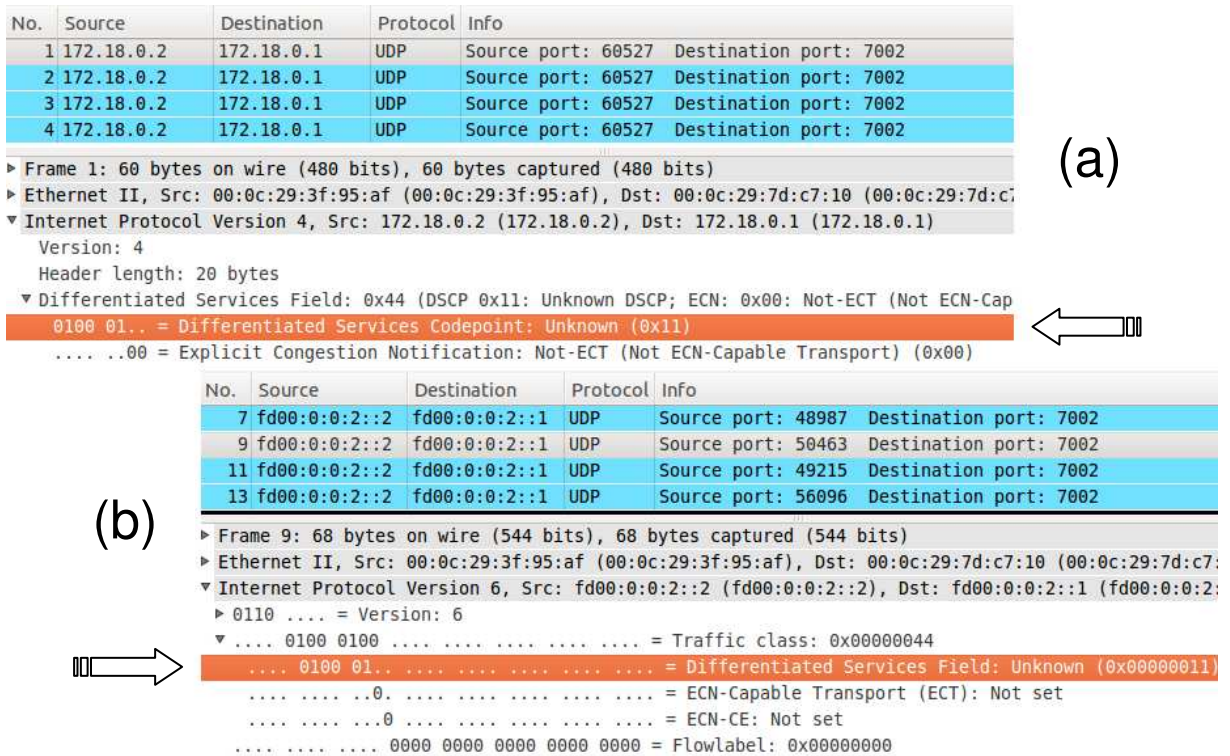


Figura 77 – Tráfego de áudio (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).

Quanto ao segundo canal do serviço de voz, todo tráfego com DSCP “100001” transmitido para o gateway multimídia, é direcionado por ele ao host receptor na porta de escuta de sua respectiva aplicação receptora (porta 8002/UDP), conforme ilustra a Figura 78:

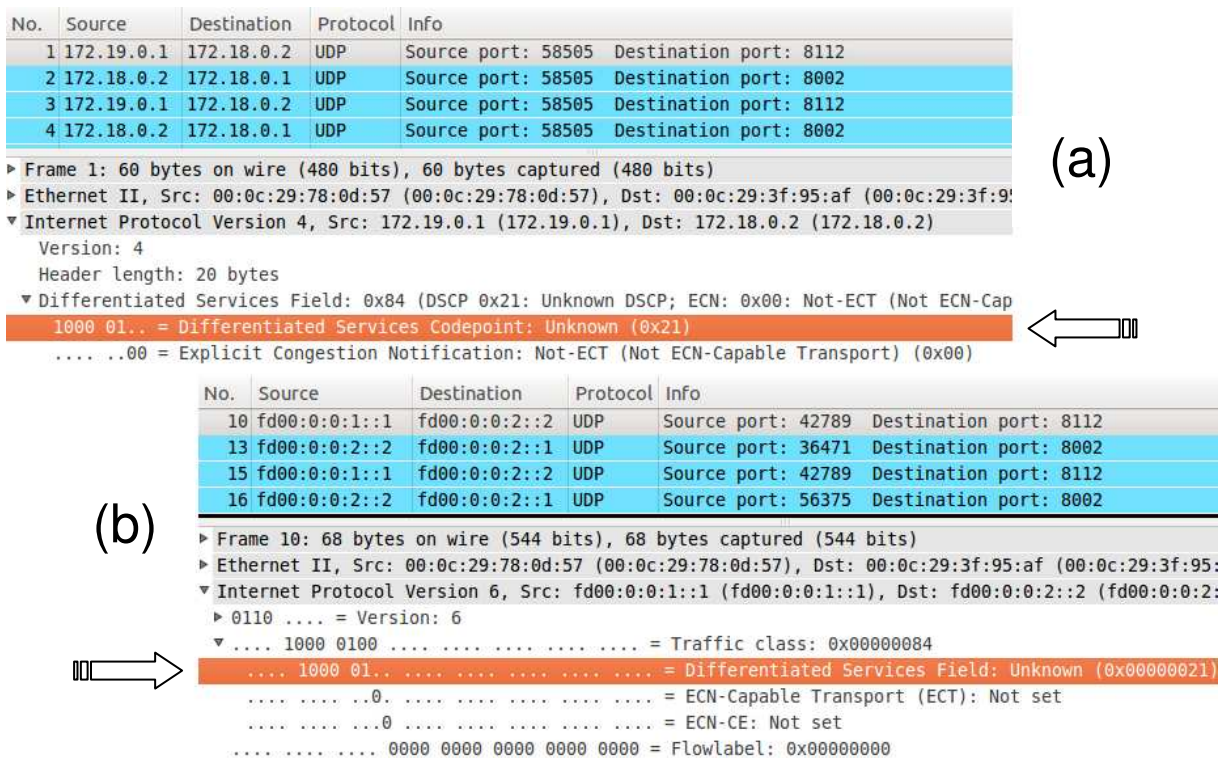


Figura 78 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de voz (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações, assim como no tráfego de áudio, pelo fato do tráfego associado a tal serviço de voz estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 8112/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 10 e 15 no item “(b)” da Figura 78), devidamente “rotulados” quanto ao segundo canal do serviço de voz no DSCP dos pacotes IP, são, na sequência, direcionados à porta 8002/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 13 e 16 no item “(b)” da Figura 78).

Quanto ao *host* receptor, para ele todo tráfego do segundo canal de voz é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 8002/UDP, conforme ilustra a Figura 79 para os protocolos IPv4 e IPv6, respectivamente:

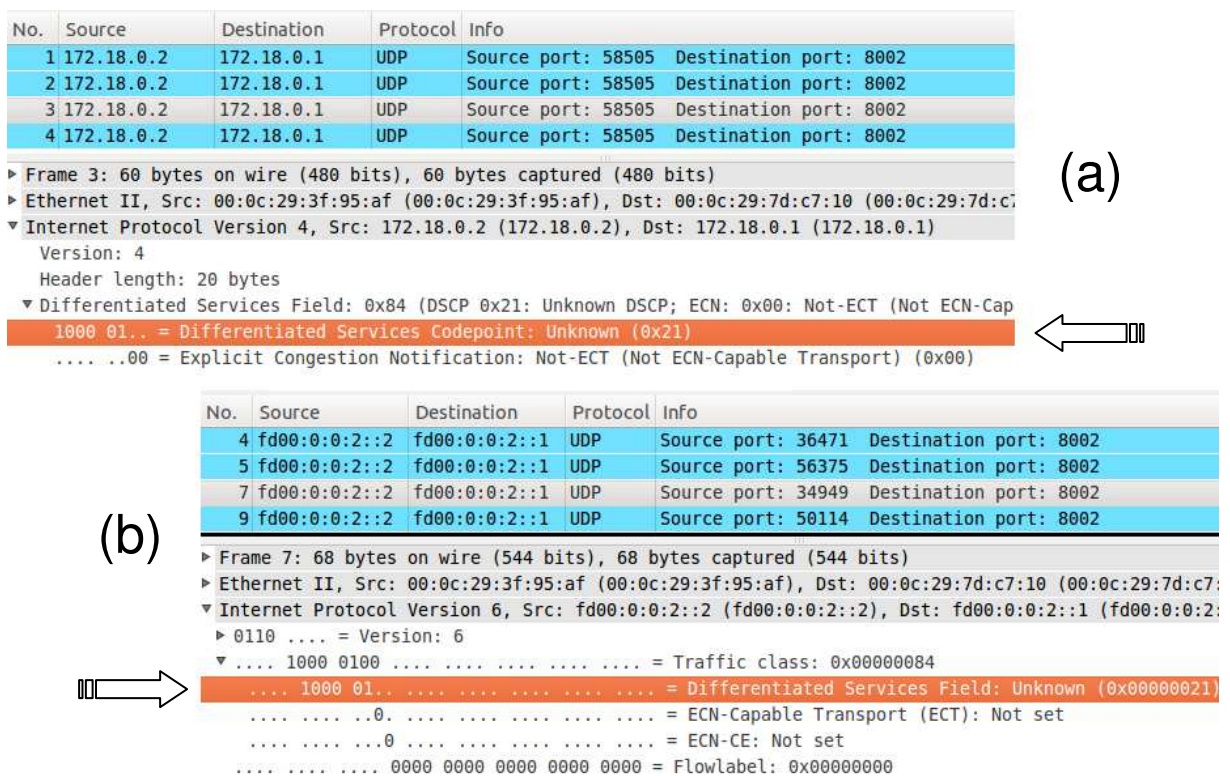


Figura 79 – Tráfego de voz (canal 2) entrante ao *host* receptor utilizando IPv4 (a) e IPv6 (b).

Por sua vez, quanto ao segundo canal do serviço de vídeo, todo tráfego com DSCP “110001” transmitido para o *gateway* multimídia, é direcionado por ele ao *host* receptor na porta de escuta de sua respectiva aplicação receptora (porta 9002/UDP), conforme ilustra a Figura 80:

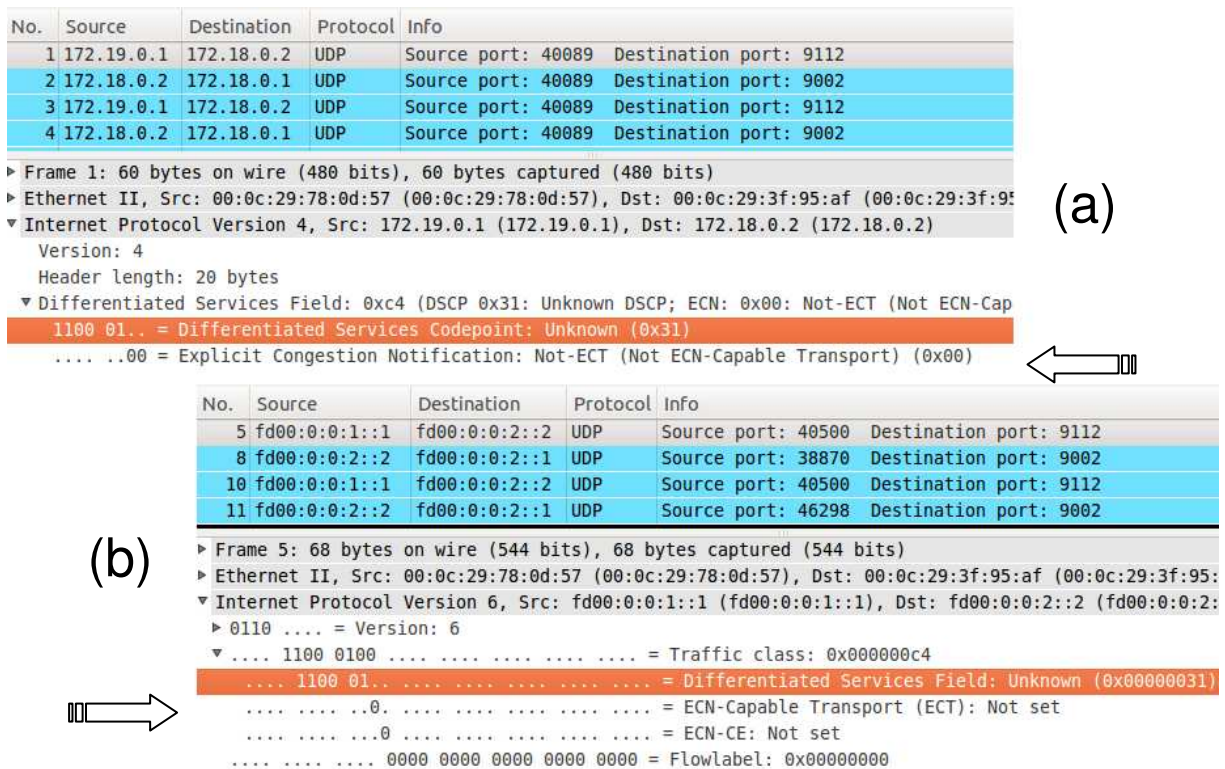


Figura 80 – Encaminhamento de pacotes IPv4 (a) e IPv6 (b) do tráfego de vídeo (canal 2) com base no campo DSCP do cabeçalho do protocolo IP pelo gateway multimídia.

Com base em tais informações, assim como nos tráfegos do segundo canal de áudio e de voz, pelo fato do tráfego associado a tal serviço de vídeo estar embasado no protocolo UDP, não há o estabelecimento de conexões entre os *hosts* envolvidos em tal processo de comunicação, de modo que os tráfegos destinados à porta 9112/UDP do *gateway* multimídia (pacotes de número 1 e 3 no item “(a)” e pacotes de número 5 e 10 no item “(b)” da Figura 80), devidamente “rotulados” quanto ao segundo canal do serviço de vídeo no DSCP dos pacotes IP, são, na sequência, direcionados à porta 9002/UDP do *host* receptor (pacotes de número 2 e 4 no item “(a)” e pacotes de número 8 e 11 no item “(b)” da Figura 80).

Assim como para os serviços de dados, áudio e voz descritos anteriormente, quanto ao *host* receptor, para ele todo tráfego do segundo canal de vídeo é entregue de modo transparente, nesse caso pelo *gateway* multimídia, em sua porta 9002/UDP, conforme ilustra a Figura 81 para os protocolos IPv4 e IPv6, respectivamente:

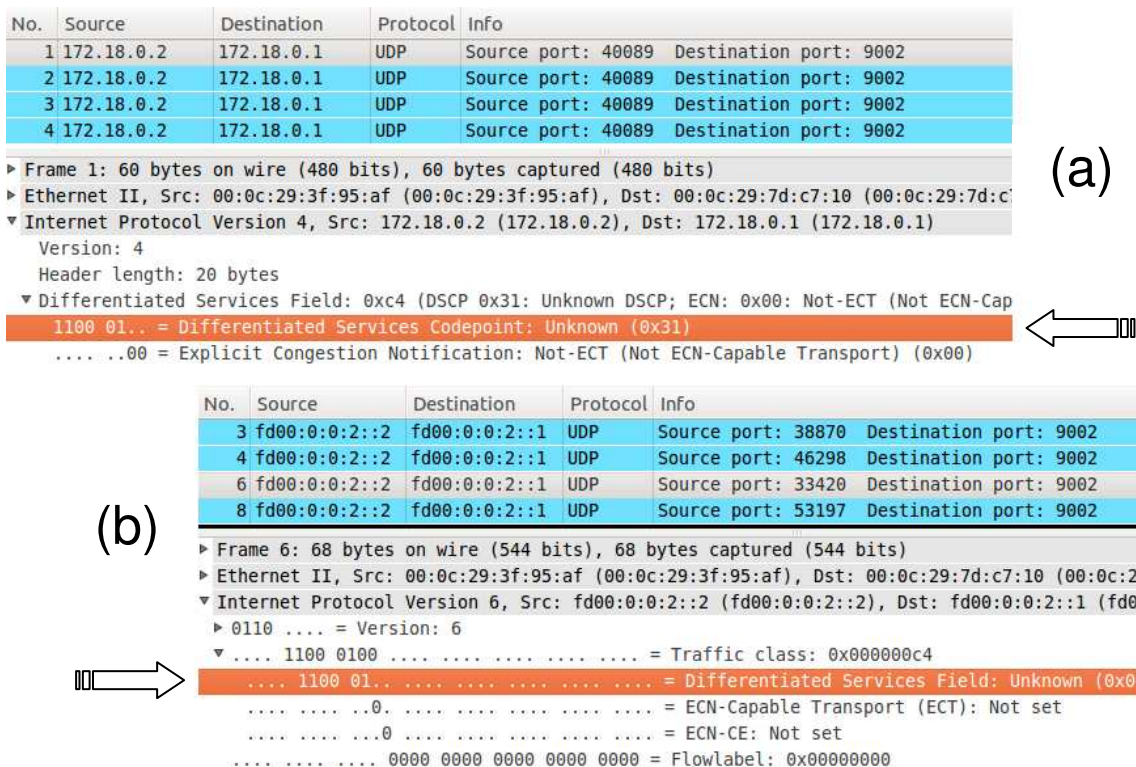


Figura 81 – Tráfego de vídeo (canal 2) entrante ao host receptor utilizando IPv4 (a) e IPv6 (b).

Assim como descrito no Teste I, vale ressaltar que se o *gateway* multimídia for desligado ou tiver seu mecanismo funcional interrompido ou modificado, não há processo de comunicação entre as aplicações transmissora e receptora dos tráfegos de dados, áudio, voz e vídeo descritos anteriormente, validando, também, seu mecanismo funcional quanto à identificação e encaminhamento de pacotes IP com base em seu respectivo DSCP.

Sendo assim, pode-se comprovar que a identificação e encaminhamento de pacotes IP com base em identificadores definidos junto ao campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) dos pacotes pertinentes ao tráfego entrante junto ao *gateway* multimídia, é válido e pode ser utilizado para identificar os diferentes tipos de tráfegos associados aos serviços de áudio, voz, vídeo e de dados intermediados por tal *gateway* multimídia, nesse caso tráfegos *stream* e elástico, bem como encaminhá-los à sua respectiva aplicação receptora.

5.1.3 – Qualidade de serviço

Para validar o mecanismo funcional quanto à qualidade de serviço utilizada para os tráfegos *stream* e elástico, nesse caso referindo-se à regulação da taxa máxima de transmissão à rede quanto a tais tráfegos, fornecido pelo *gateway* multimídia, tem-se como base o ambiente utilizado para validar o *gateway* multimídia descrito na seção anterior (Figura 59 e Tabela 10) e com a seguinte estrutura funcional quanto aos seus sistemas transmissor e receptor:

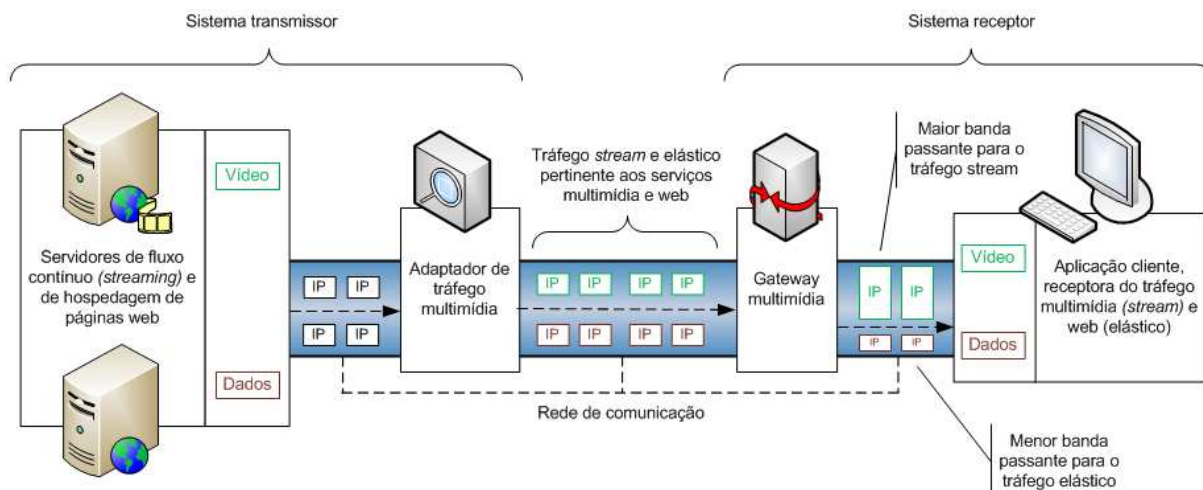


Figura 82 – Ambiente para validação e testes quanto à qualidade de serviço pelo gateway multimídia.

Em tal ambiente, dado dois tipos de tráfegos distintos, sendo um do tipo *stream* pertinente à transmissão de arquivos de vídeo (*streaming* de vídeo) e um elástico pertinente à acessos *web* (navegação Internet e transferência de arquivos), cabe ao *gateway* multimídia priorizar os tráfegos *stream* quanto aos tráfegos elásticos, reservando maior taxa de transmissão para, nesse caso, o conteúdo multimídia de vídeo do que ao conteúdo *web*, de modo geral.

Para tal, a identificação entre um e outro tipo de tráfego está embasada em identificadores definidos junto ao campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) dos pacotes pertinentes aos seus respectivos serviços multimídia e dados, sendo que os pacotes IP pertinentes ao tráfego *stream* de vídeo são identificados pelo DSCP “110000” e os pacotes IP pertinentes ao tráfego elástico de dados são identificados pelo DSCP “000000”, conforme definidos nas Tabelas 8 e 9 (para o canal 1 de tais serviços de dados e de vídeo) descritas anteriormente.

Nesse contexto, a partir de tais identificadores, foram criadas duas classes de serviços distintas junto ao *gateway* multimídia, uma classe de serviço referente ao tráfego de vídeo, nesse caso com taxa de transmissão de até 2 Mbps, e outra classe de serviço referente ao serviço de dados, nesse caso com taxa de transmissão de até 200 Kbps. Quanto à definição de tais taxas de transmissão, elas foram definidas aleatoriamente, apenas para efeito de testes, podendo ser modificadas para qualquer outro valor (limitado a taxa máxima de transmissão das interfaces de rede do *gateway* multimídia).

A partir de tais configurações, todos os pacotes IP (de versões 4 e 6) transmitidos pelos servidores *web* e de *streaming* de vídeo às aplicações receptoras de tais conteúdos são devidamente “rotulados” pelo adaptador de tráfego multimídia e chegam ao *gateway* multimídia devidamente identificados, conforme ilustram as Figuras 83 e 84:

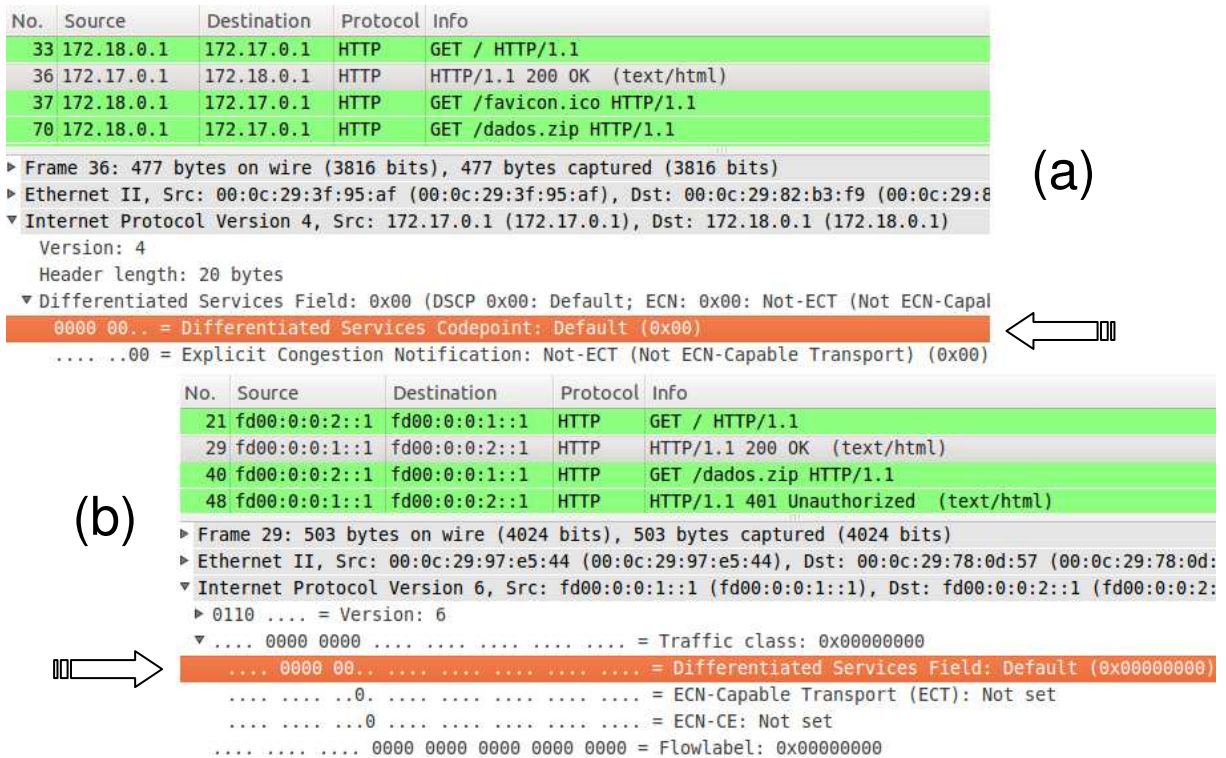


Figura 83 – Tráfego elástico (de navegação web) entrante ao gateway multimídia utilizando IPv4 (a) e IPv6 (b).

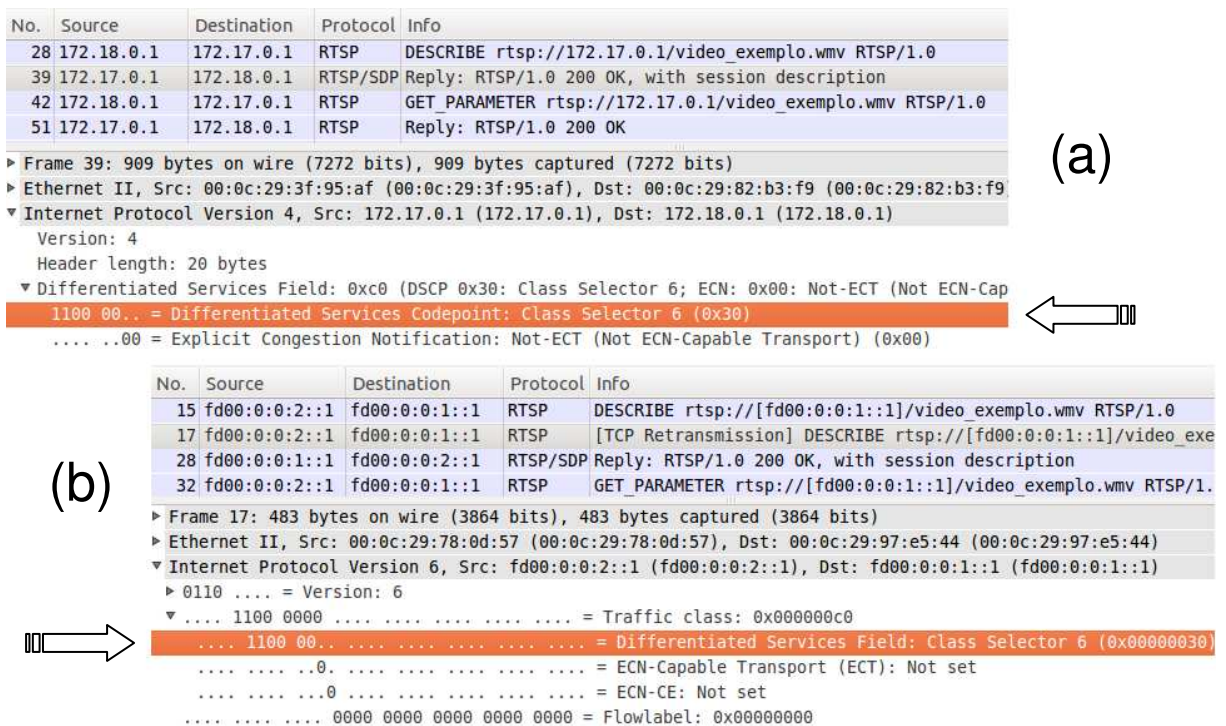


Figura 84 – Tráfego stream (de streaming de vídeo) entrante ao gateway multimídia utilizando IPv4 (a) e IPv6 (b).

Observe que os tráfegos pertinentes ao serviço de dados, ilustrados na Figura 83, possuem identificador “000000” (0x00), “sinalizados” por uma seta, enquanto os tráfegos associados ao serviço de vídeo, ilustrados na Figura 84, possuem identificador “110000” (0x30), também

“sinalizados” por uma seta, tanto no IPv4, quanto no IPv6, conforme definidos nas Tabelas 8 e 9 (para o canal 1 de tais serviços de dados e de vídeo) descritas anteriormente.

Por meio de tais DSCP's, os pacotes IP são identificados e classificados quanto à sua classe de serviço (classes de dados ou de vídeo) e, utilizando dos mecanismos de escalonamento e regulação fornecidos pelo HTB (*Hierarchical Token Bucket*), enviados à rede conforme as definições de qualidade de serviço a eles associados, nesse caso utilizando, no máximo, 2 Mbps como taxa de transmissão para o tráfego *stream* pertinente à classe de serviço de vídeo e 200 Kbps como taxa de transmissão para o tráfego elástico pertinente a classe de serviço de dados, de modo que a transmissão de tais tráfegos seja regulada pelo *gateway* multimídia e torne-se perceptível quanto às suas velocidades de acesso por sua respectiva aplicação receptora, conforme ilustra a Figura 85:

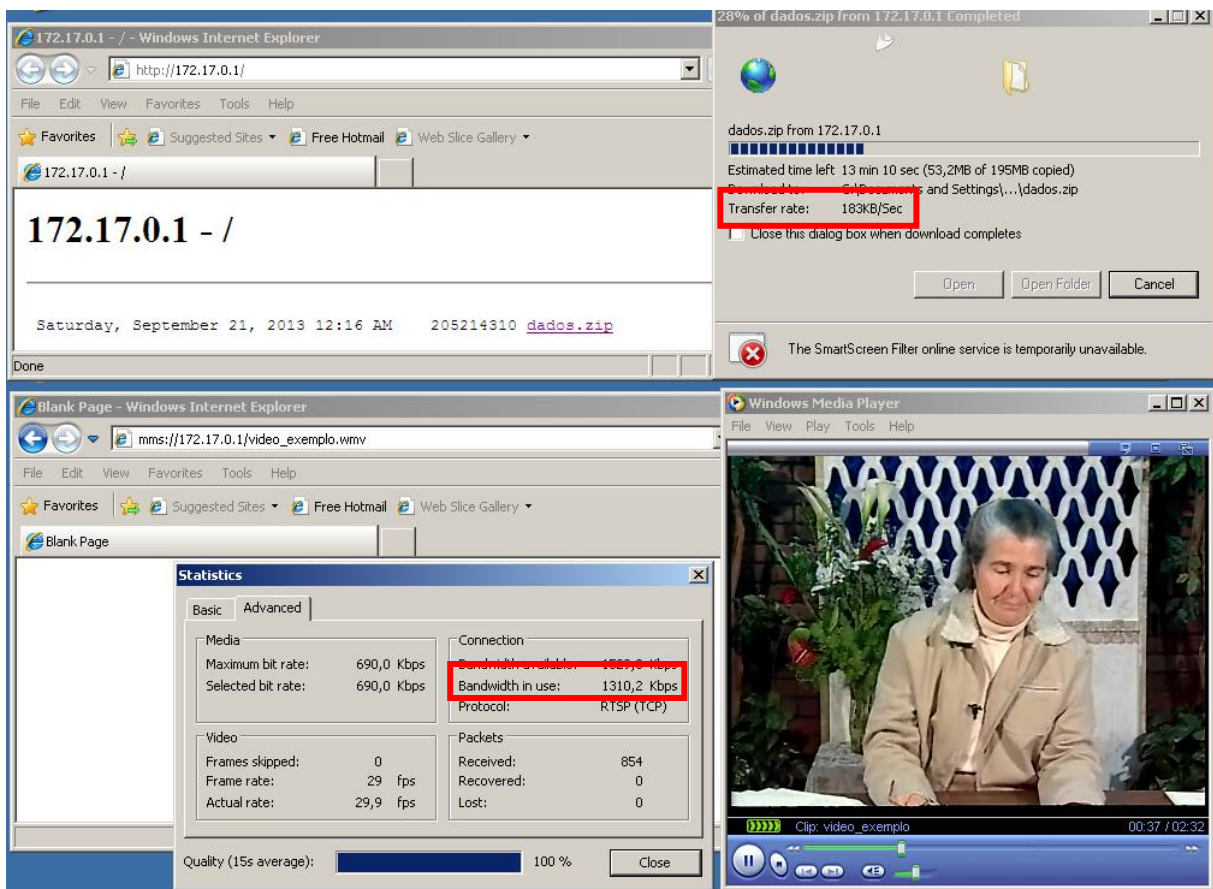


Figura 85 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede utilizando de mecanismos de qualidade de serviço (1).

Observe que as velocidades de acesso às aplicações *web* e de *streaming* de vídeo são distintas no *host* receptor, em que o *download* do arquivo de exemplo via *web* possui taxa de transmissão em torno de 200 Kbps (na Figura 85, taxa de 183 Kbps) e o arquivo de exemplo de vídeo possui taxa de transmissão em torno de 2 Mbps (na Figura 85, taxa de 1,3 Mbps), conforme as classes de serviços definidas anteriormente.

Como exemplo, caso o mecanismo de qualidade de serviço seja “desligado” junto ao *gateway* multimídia, a taxa de transmissão de tais tráfegos é “auto-regulada pela rede” e o cliente percebe, instantaneamente, os efeitos quanto às velocidades de acesso por suas respectivas aplicações receptoras do tráfego de dados (*web*) e de vídeo (*streaming* de vídeo), em que o

tráfego elástico é melhorado e o *stream* mantém-se aparentemente inalterado (com pequena variação quando comparado com a utilização do mecanismo de qualidade de serviço), conforme ilustra a Figura 86:

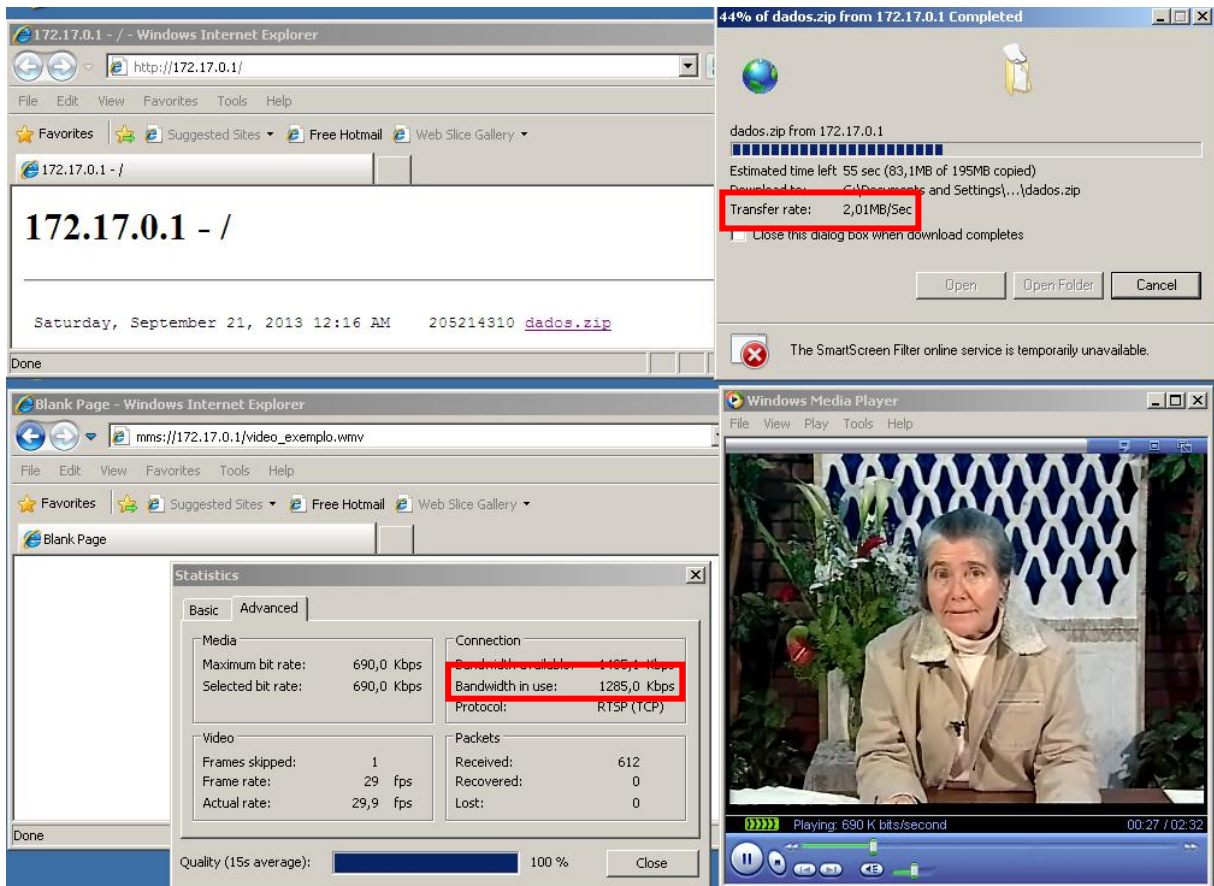


Figura 86 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede sem a utilização de mecanismos de qualidade de serviço.

Observe que sem o mecanismo de qualidade de serviço, o *download* do arquivo de exemplo via *web* não é mais regulado por sua classe de serviço de 200 Kbps e possui taxa de transmissão cerca de dez vezes superior a tal limitação de velocidade (na Figura 86, taxa de 2,01 Mbps). Nesse mesmo exemplo, a taxa de *download* do *streaming* de vídeo, sem a reserva de 2 Mbps pertinentes a sua classe de serviço, mantém-se em torno de 1,2 Mbps.

Nesse mesmo contexto, apenas para efeito comparativo e complementar aos testes anteriores, caso as velocidades de ambas as classes de serviço sejam invertidas para os tráfegos *stream* e elástico, em que no máximo 200 Kbps sejam reservados para o tráfego pertinente ao *streaming* de vídeo e no máximo 2 Mbps sejam reservados para o tráfego pertinente aos dados *web*, os efeitos quanto à velocidade de acesso por suas respectivas aplicações receptoras, mais uma vez, são instantâneos, em que a percepção de velocidade de acesso da aplicação que utiliza (consome) o tráfego elástico é extremamente melhor que a aplicação que utiliza (consome) o tráfego *stream*, conforme ilustra a Figura 87:

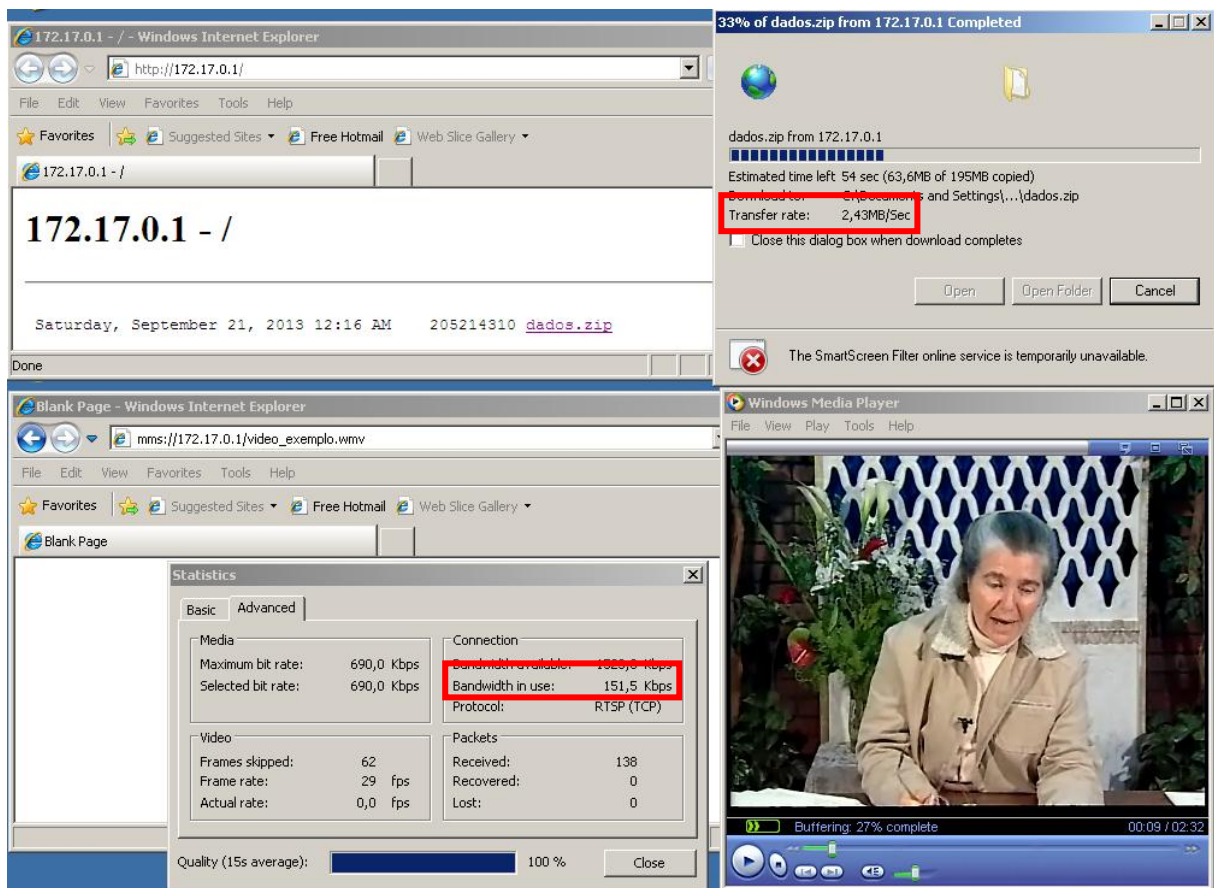


Figura 87 – Percepção da velocidade de download do tráfego elástico e stream pelo cliente da rede utilizando de mecanismos de qualidade de serviço (2).

Observe que, nesse exemplo, a velocidade de acesso ao *streaming* de vídeo é reduzida para cerca de 200 Kbps (na Figura 87, taxa de 151,5 Kbps) e o *download web* para cerca de 2 Mbps (na Figura 87, taxa de 2,43 Mbps), conforme as classes de serviços definidas anteriormente.

Vale ressaltar que quanto aos exemplos anteriores, pelo fato da percepção de velocidade ilustrado nas Figuras 85, 86 e 87 serem as mesmas quanto ao IPv4 e ao IPv6, optou-se por utilizar apenas uma figura para ilustrar tais percepções, nesse caso ilustrando acessos a partir do IPv4, os quais seriam similares no IPv6, distinguindo-se apenas pela escrita que especifica o endereço do servidor pertinente aos acessos *web* (nesse caso, “http://[fd00:0:0:1::1]” no IPv6, em vez de “http://172.17.0.1” no IPv4) e de *streaming* de vídeo (nesse caso, “mms://[fd00:0:0:1::1]/video_exemplo.wmv” no IPv6, em vez de “mms://172.17.0.1/video_exemplo.wmv” no IPv4).

Sendo assim, pode-se comprovar que o mecanismo funcional quanto ao fornecimento de recursos voltados à qualidade de serviço pelo *gateway* multimídia é válido e pode ser utilizado para regular a taxa de transmissão de diferentes tipos de tráfegos para seus respectivos clientes, priorizando a transmissão de tráfegos *stream* quando comparado a tráfegos elásticos (ou vice-versa, se assim for necessário) e utilizando dos identificadores definidos junto ao campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) como base para a distinção entre um e outro tipo de tráfego, bem como de sua associação (classificação) às classes utilizadas para reservar e regular a taxa de transmissão de tais tráfegos à rede.

5.2 – Validação de desempenho

Após validar os mecanismos funcionais do *gateway* multimídia (bem como do adaptador de tráfego multimídia), deve-se validar seu desempenho quanto às características da rede com sua utilização e sem sua utilização, de modo a verificar se há ou não modificações, por exemplo, quanto ao perfil de tráfego por ele intermediado e se há ou não influências quanto à perda de pacotes e eventuais contribuições para adição de atrasos ao longo da rede a partir de sua utilização, dentre outros.

Nesse contexto, questões referentes à sua transparência quanto às características dos tráfegos por ele intermediados, bem como pertinentes a erros e atrasos de transmissão, assim como utilização de seus recursos de processamento, memória e rede são analisados de modo a viabilizar (ou não) sua implementação ao longo da rede, as quais são descritas e analisadas nas seções seguintes.

5.2.1 – Perfil de tráfego

Conforme descrito na Seção 4.1, o *gateway* multimídia deve ser transparente às aplicações transmissoras e receptoras dos tráfegos por ele intermediados, de modo que ele não deve influenciar no perfil de tráfego utilizado por tais aplicações ao longo da rede, se portando apenas como *gateway* de acesso à rede ao *host* receptor de tais tráfegos e não realizando qualquer modificação quanto às características de tais tráfegos, tais como influência quanto ao tipo de tráfego ou às funções utilizadas na modelagem dos mesmos, dentre outros.

Nesse contexto, de modo a validar tal “transparência”, a partir do gerador de tráfego multimídia descrito na Seção 4.6.3, pode-se comparar o tráfego recebido pela aplicação receptora de tais tráfegos sem a utilização do *gateway* multimídia (com transmissão direta entre as aplicações transmissora e receptora) e com a utilização do *gateway* multimídia (com transmissão intermediada por ele), de modo a confrontar os resultados obtidos em ambas as situações e comprovar (ou não) tal “transparência” do *gateway* multimídia.

Dessa forma, utilizando o ambiente de validação funcional do *gateway* multimídia (ilustrado anteriormente nas Figuras 57 e 58) e considerando um período de transmissão simultâneo de 1 hora para os meios físicos guiado (transmissão cabeada) e não-guiado (transmissão sem fio) e de modo isolado entre ambos (transmissão 100% cabeada e 100% sem fio, durante 1 hora cada), como exemplo, as Figuras 88 e 89 ilustram os histogramas pertinentes aos tráfegos elástico e *stream* quanto aos serviços multimídia de dados, áudio, vídeo e voz (a partir do gerador de tráfego multimídia descrito na Seção 4.6.3) sem a intermediação do *gateway* multimídia, bem como com sua intermediação, em ambiente cabeado e sem fio, respectivamente:

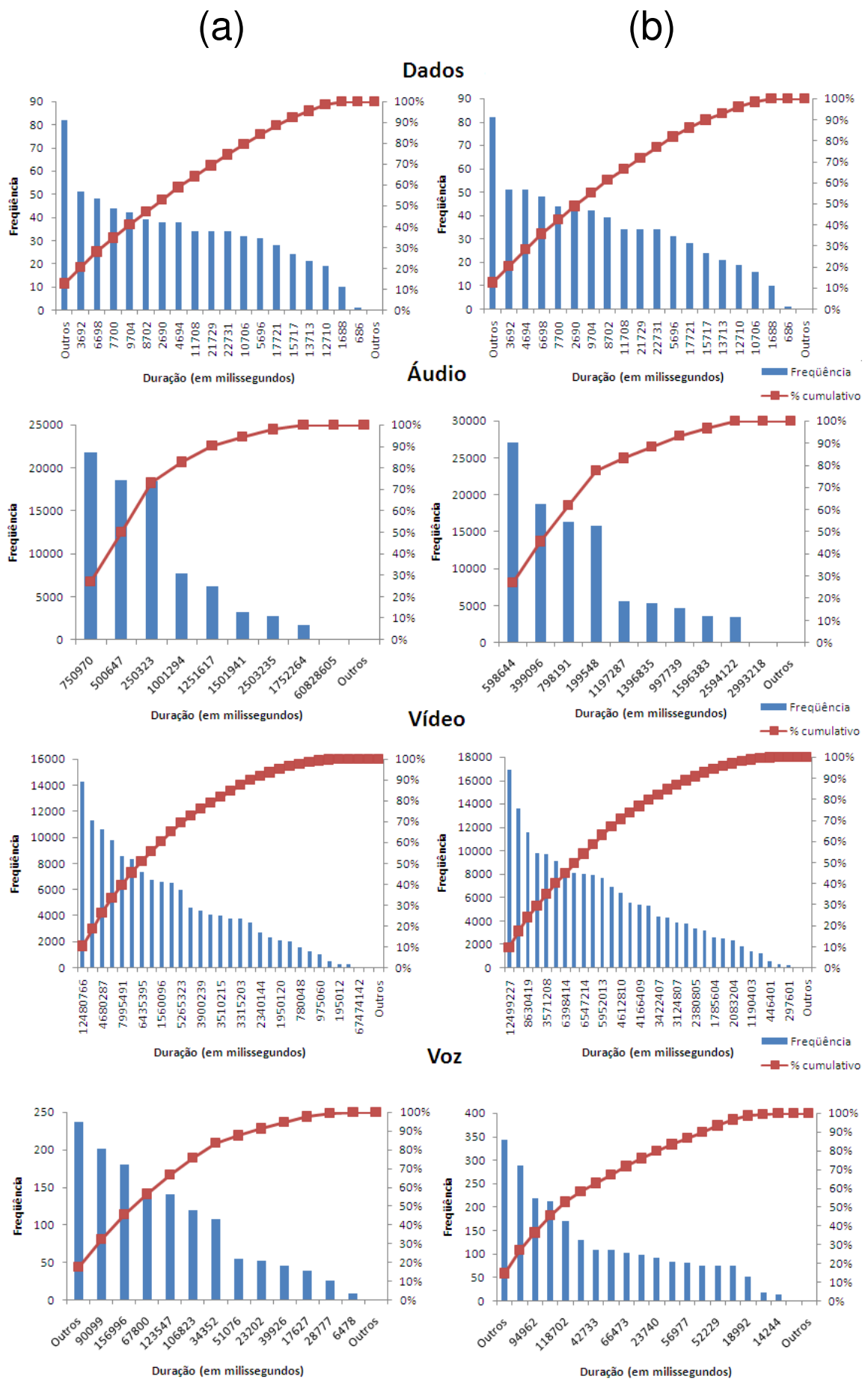


Figura 88 – Histograma pertinente aos tráfegos elástico de dados e stream de áudio, vídeo e voz, em ambiente cabeado, não intermediado (a) e intermediado (b) pelo gateway multimídia.

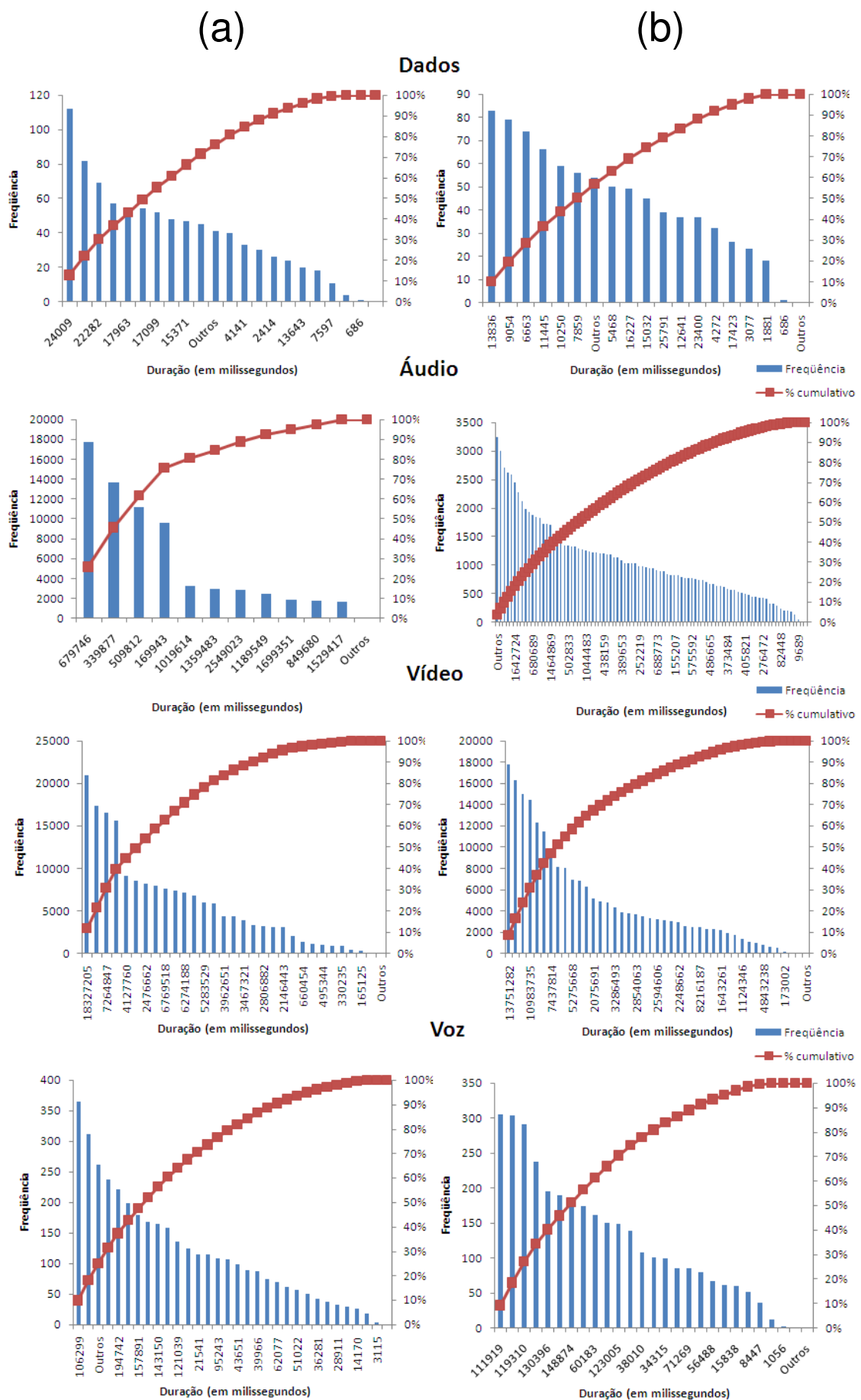


Figura 89 – Histograma pertinente aos tráfegos elástico de dados e stream de áudio, vídeo e voz, em ambiente sem fio, não intermediado (a) e intermediado (b) pelo gateway multimídia.

Quanto às Figuras 88 e 89, pode-se perceber que tanto no ambiente cabeado (Figura 88), quanto no ambiente sem fio (Figura 89), seja sem a intermediação do *gateway* multimídia (itens “(a)” de ambas as figuras) ou com sua intermediação (itens “(b)” de ambas as figuras), as características quanto ao perfil de tráfego para os serviços multimídia de dados, áudio, vídeo e voz (a partir do gerador de tráfego multimídia descrito na Seção 4.6.3) não são alteradas, preservando e mantendo extrema similaridade quanto as funções de distribuição utilizadas para a geração dos tráfegos *stream* e elástico de ambos os serviços à rede (nesse caso, distribuição exponencial, relativamente fácil de ser observada se “traçarmos uma linha” sobre as “barras azuis” de ambos os gráficos), bem como quanto ao percentual cumulativo de tal função de distribuição (CDF, *Cumulative Distribute Functions*, em vermelho em ambos os gráficos) em ambos os casos.

De modo complementar aos histogramas anteriores, quanto à duração dos testes, se seu período for reduzido para 30 minutos ou estendido para 2 horas, tanto no ambiente cabeado, quanto no ambiente sem fio, por exemplo, não há modificações quanto ao perfil de tráfego de ambos os serviços de dados, áudio, vídeo e voz. Como exemplo, a Figura 90 ilustra os histogramas pertinentes ao serviço de voz, nesse caso em ambiente cabeado e intermediados pelo *gateway* multimídia, em testes com duração de 30 minutos e de 2 horas, respectivamente:

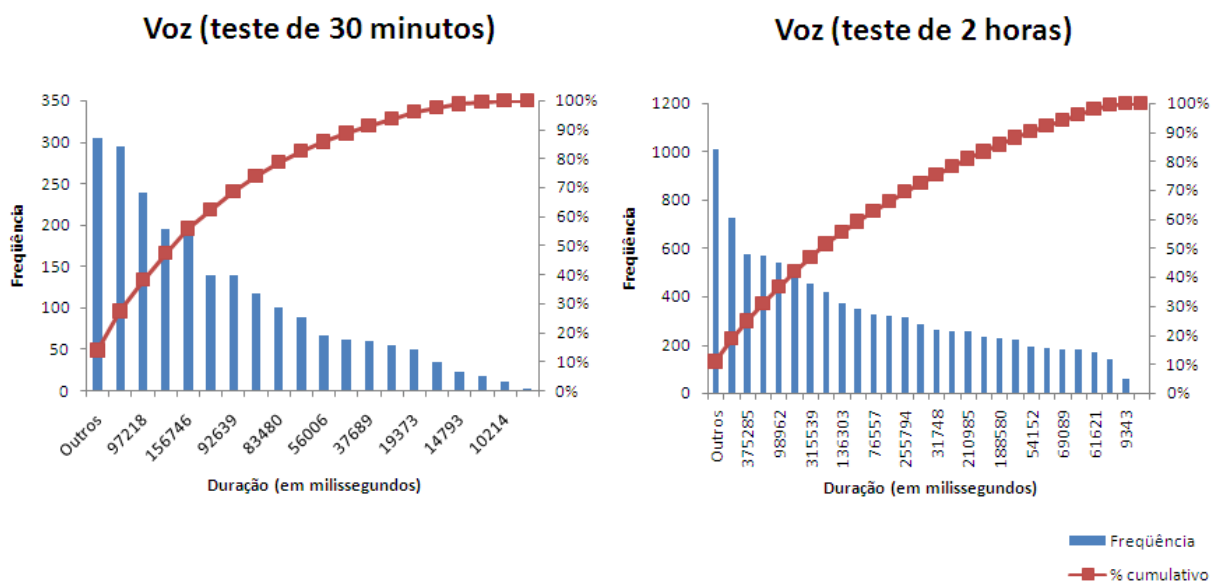


Figura 90 – Histograma pertinente aos tráfegos *stream* de voz intermediados pelo *gateway* multimídia em ambiente cabeado (testes de 30 minutos e de 2 horas).

Observe que mesmo com durações distintas, nesse caso durações reativamente pequenas, não há modificações quanto ao perfil de tais tráfegos, o que também ocorre em testes com durações superiores, como ilustra a Figura 91 para testes com durações de 12 e de 24 horas, respectivamente, também utilizando o serviço de voz como exemplo (nesse caso, também, em ambiente cabeado e com intermediação do *gateway* multimídia).

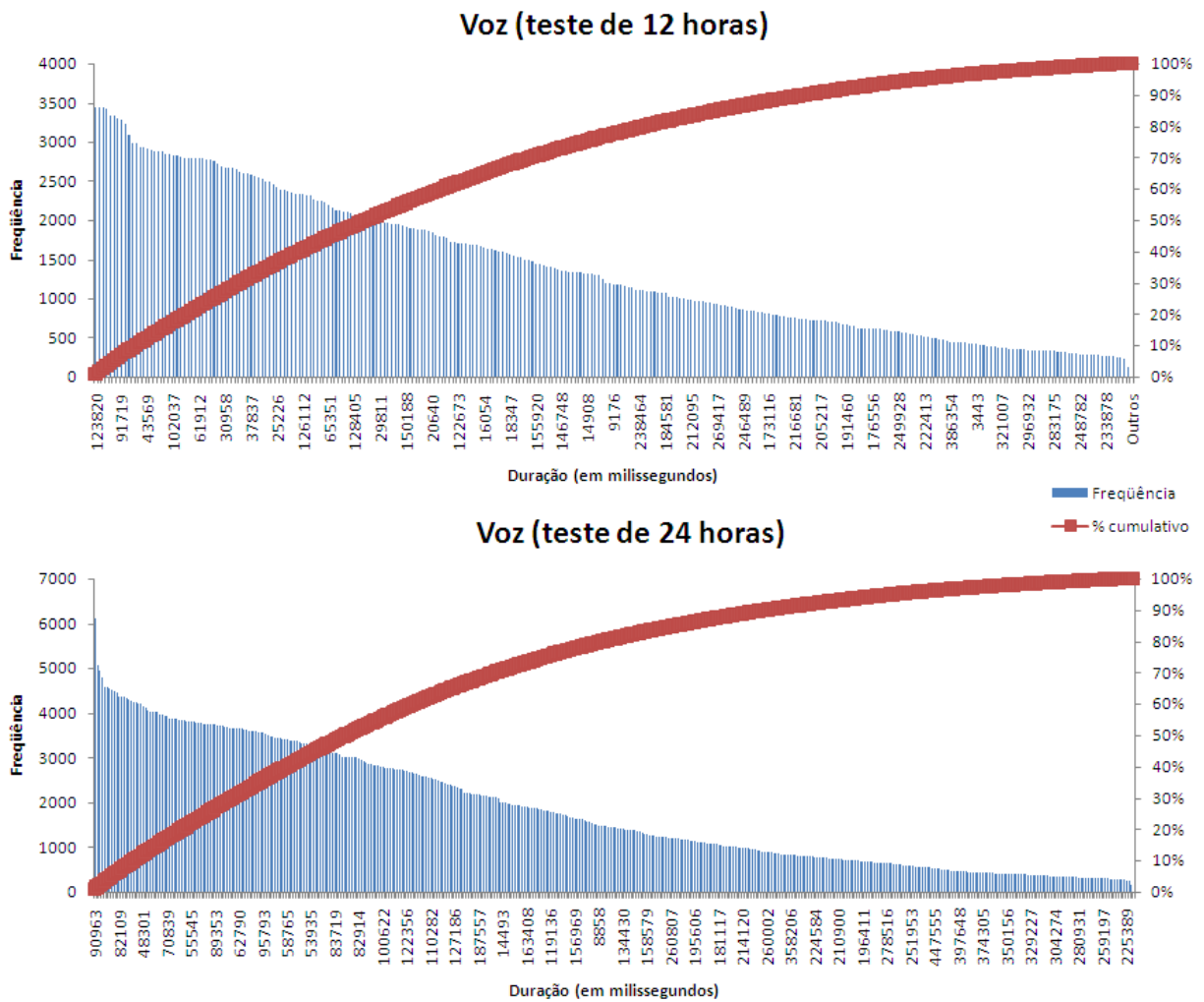


Figura 91 – Histograma pertinente aos tráfegos stream de voz intermediados pelo gateway multimídia em ambiente cabeado (testes de 12 horas e de 24 horas).

Novamente, pode-se perceber que as características do tráfego de voz em ambas as durações são extremamente similares nos testes de 12 e de 24 horas, assim como nos testes de 1 hora ilustrados nas Figuras 88 e 89, bem como nos testes de 30 minutos e de 2 horas ilustrados na Figura 90.

Sendo assim, confrontando-se os resultados obtidos em ambas as situações (sem a utilização e com a utilização do gateway multimídia), pode-se perceber que as características de tráfego em ambos os casos não são modificadas, preservando sua modelagem e similaridade em transmissões de curta, média ou longa duração, tanto no ambiente cabeado, quanto no ambiente sem fio e comprovando que tal gateway, efetivamente, portou-se de modo “transparente” aos tráfegos trocados entre suas aplicações transmissoras e receptoras.

Vale ressaltar que tais observações também foram extremamente importantes para definição dos tempos quanto aos testes com o gateway multimídia, em que, inicialmente, não se tinha um “balizador” quanto a tais tempos, de modo que diversos testes foram realizados com tempos extremamente distintos, ambos com o intuito de se obter uma amostragem de dados suficiente para identificar se houve ou não alterações quanto às características dos tráfegos intermediados pelo gateway multimídia, os quais não importando as durações (em que a duração mínima testada foi de 30 minutos e a máxima foi de 24 horas), mantiveram-se com as

mesmas características, comprovando a transparência do *gateway* multimídia em ambos os casos.

5.2.2 – Erros, atrasos e variações de atrasos

No que se refere a erros provenientes a perda de pacotes, bem como a atrasos quanto às transmissões não intermediadas *versus* as transmissões intermediadas pelo *gateway* multimídia, de modo complementar ao gerador de tráfego multimídia descrito na seção 4.6.3, utilizou-se a ferramenta Iperf [36], um gerador de tráfego de código aberto, implementado no modelo cliente-servidor, amplamente utilizado para análises de desempenho quanto ao *throughput* de rede, bem como para questões envolvendo lentidões na rede, de modo geral.

Em linhas gerais, a partir do Iperf é possível identificar facilmente os totais de datagramas trocados entre suas aplicações transmissora e receptora, bem como os totais de datagramas eventualmente perdidos e os tempos de transmissão e de sua variação de atraso (*jitter*), informações não disponíveis no gerador de tráfego multimídia descrito anteriormente.

Nesse contexto, pode-se comparar os resultados obtidos com o Iperf sem a utilização do *gateway* multimídia (com transmissão direta entre suas aplicações transmissora e receptora) e com a utilização do *gateway* multimídia (com transmissão intermediada pelo *gateway* multimídia), de modo a confrontar os resultados obtidos em ambas as situações e verificar se o *gateway* multimídia influencia (ou não) em tais transmissões (nesse caso, em especial quanto à perda de pacotes transmitidos, bem como quanto à atrasos e variações de atrasos).

Para tal, a partir de 5 testes distintos (T1 à T5) para tráfegos de 10 Mb, 100 Mb e 1 Gb utilizando o Iperf, nesse caso emulando tráfegos *stream* sobre o protocolo UDP em ambiente cabeado, pode-se comparar os percentuais de cada teste e a média dos 5 testes quanto ao percentual de datagramas perdidos (Tabela 13), tempos de transmissão (Tabela 14) e variações de atraso (Tabela 15) para tráfegos intermediados e não intermediados pelo *gateway* multimídia:

Tráfego stream de	Percentual de datagramas perdidos											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	4,3%	4,3%	4,4%	4,3%	4,3%	4,3%	4,3%	4,3%	4,3%	4,3%	4,3%	4,3%
100 Mb	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%	4,7%
1 Gb	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%	4,8%

Tabela 13 – Percentuais de datagramas perdidos com tráfegos não intermediados e intermediados pelo *gateway* multimídia em ambiente cabeado.

Tráfego stream de	Tempo de transmissão (em segundos)											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80	2,70	0,80	1,18
100 Mb	8,30	8,40	8,40	8,40	8,30	8,36	8,30	8,40	8,40	8,40	8,40	8,38
1 Gb	85,50	85,50	85,50	85,50	85,50	85,50	85,50	85,50	85,50	85,50	85,50	85,50

Tabela 14 – Tempos de transmissão com tráfegos não intermediados e intermediados pelo *gateway* multimídia em ambiente cabeado.

Tráfego stream de	Jitter (em milissegundos)											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	0,024	0,010	0,010	0,011	0,012	0,0134	0,012	0,013	0,010	0,012	0,011	0,0116
100 Mb	0,013	0,008	0,010	0,012	0,014	0,0114	0,013	0,011	0,009	0,011	0,012	0,0112
1 Gb	0,011	0,009	0,010	15,381	0,010	3,0842	0,010	0,009	0,009	0,016	0,014	0,0116

Tabela 15 – Variações de atrasos (jitter) com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente cabeado.

A partir de tais informações, nesse caso quanto ao ambiente cabeado, percebe-se extrema similaridade quanto às transmissões intermediadas ou não pelo *gateway* multimídia. Observe que quanto aos pacotes perdidos (Tabela 13), nos testes de 10 Mb, 100 Mb e 1 Gb, as médias totais são exatamente as mesmas utilizando ou não o *gateway* multimídia, inclusive com extrema similaridade quanto aos totais de pacotes perdidos individualmente em cada um dos 5 testes, em que só há distinção no teste T3 de 10 Mb sem a utilização do *gateway* multimídia (com 4,4% de pacotes perdidos) quando comparado ao teste de mesmo número com a utilização do *gateway* multimídia (com 4,3% de pacotes perdidos), nesse caso 0,1% menor quando comparado a não utilização do *gateway* multimídia.

Ainda no que se refere aos testes no ambiente cabeado, quanto aos tempos de transmissão descritos na Tabela 14, observe que só a distinção de tempos nos testes T4 de 10 Mb e T5 de 100 Mb ao compararmos os tráfegos intermediados e não intermediados pelo *gateway* multimídia, em que todos os demais testes individuais resultaram exatamente nos mesmos tempos de transmissão para tais tráfegos de 10 Mb, 100 Mb e 1 Gb. Quanto aos tempos pertinentes às variações de atrasos (*jitter*) descritas na Tabela 15, observe que, na média, os tráfegos intermediados pelo *gateway* multimídia tiveram menor *jitter* quando comparado aos tráfegos não intermediados por tal *gateway*, com extrema similaridade nos testes individuais em ambos os casos.

De modo similar ao ambiente cabeado, nesse caso quanto ao ambiente sem fio, a partir de 5 testes distintos (T1 à T5) para tráfegos de 10 Mb, 100 Mb e 1 Gb utilizando o Iperf, também emulando tráfegos *stream* sobre o protocolo UDP, pode-se comparar os percentuais de cada teste e a média dos 5 testes quanto ao percentual de datagramas perdidos (Tabela 16), tempos de transmissão (Tabela 17) e variações de atraso (Tabela 18) para tráfegos intermediados e não intermediados pelo *gateway* multimídia:

Tráfego stream de	Percentual de datagramas perdidos											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	1,5%	1,5%	7,9%	0,0%	3,4%	1,5%	0,0%	3,3%	8,7%	6,1%	0,1%	3,3%
100 Mb	8,9%	10,0%	18,0%	8,5%	11,0%	10,0%	4,7%	14,0%	9,8%	22,0%	7,9%	9,8%
1 Gb	8,0%	11,0%	10,0%	14,0%	12,0%	11,0%	11,0%	11,0%	13,0%	13,0%	10,0%	11,0%

Tabela 16 – Percentuais de datagramas perdidos com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.

Tráfego stream de	Tempo de transmissão (em segundos)											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	2,30	2,40	2,30	2,40	2,30	2,34	2,40	2,40	2,80	2,20	2,50	2,46
100 Mb	24,40	23,50	22,70	24,00	25,70	24,06	25,60	24,40	25,30	22,00	23,60	24,18
1 Gb	244,40	244,30	254,80	238,50	234,00	243,20	240,40	241,60	236,80	240,10	242,80	240,34

Tabela 17 – Tempos de transmissão com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.

Tráfego stream de	Jitter (em milissegundos)											
	Sem o Gateway Multimídia						Com o Gateway Multimídia					
	T1	T2	T3	T4	T5	Média	T1	T2	T3	T4	T5	Média
10 Mb	0,208	1,217	0,469	0,239	0,779	0,5824	0,719	0,691	0,376	0,352	0,186	0,4648
100 Mb	0,197	0,420	0,402	0,353	0,584	0,3912	0,317	0,358	0,308	0,559	0,473	0,403
1 Gb	0,335	1,313	1,014	0,929	1,387	0,9956	0,517	0,365	0,479	0,809	0,222	0,4784

Tabela 18 – Variações de atrasos (jitter) com tráfegos não intermediados e intermediados pelo gateway multimídia em ambiente sem fio.

Quanto ao ambiente sem fio, observe que os resultados obtidos também demonstram extrema similaridade nos tráfegos intermediados e não intermediados pelo *gateway* multimídia. Como exemplo, quanto aos pacotes perdidos (Tabela 16), nos testes de 10 Mb, a média dos resultados demonstra que o ambiente sem o *gateway* multimídia teve menor perda de pacotes (com 1,5% de perda) quando comparado ao mesmo ambiente com o *gateway* multimídia (com 3,3% de perda), o que não ocorre nos testes de 100 Mb, em que o percentual de pacotes perdidos utilizando o *gateway* multimídia (com 9,8% de perda) foi inferior ao mesmo ambiente sem sua utilização (com 10% de perda), bem como nos testes de 1 Gb, em que o percentual de perda foi o mesmo (11% de perda) em ambos os casos (com utilização do *gateway* multimídia e sem sua utilização).

Por sua vez, quanto aos tempos de transmissão descritos na Tabela 17, observe que os resultados também são extremamente similares, com transmissões mais rápidas na ordem de milissegundos nos testes de 10 Mb e 100 Mb no ambiente sem o *gateway* multimídia, porém mais rápidas com a utilização do *gateway* multimídia nos testes de 1 Gb. Ainda quanto a tempos, nesse caso quanto aos tempos pertinentes às variações de atrasos (*jitter*) descritas na Tabela 18, observe que com exceção à média dos testes de 100 Mb, o ambiente com utilização do *gateway* multimídia para os testes de 10 Mb e de 1 Gb se portou melhor que esses mesmos ambientes sem sua utilização, demonstrando, novamente, extrema similaridade em ambos os casos, em que, de modo geral, as distinções entre um e outro cenário diferem-se, na maior parte dos casos, em frações na ordem de alguns milissegundos.

Sendo assim, confrontando os resultados obtidos em ambas as situações (sem a utilização do *gateway* multimídia e com sua utilização), pode-se verificar que não há influências do *gateway* multimídia com as questões voltadas a erros (perda de pacotes), atrasos (quanto aos tempos de transmissão) e variações de atrasos (*jitter*) tanto no ambiente cabeado, quanto no ambiente sem fio. Como exemplo, considerando as 18 médias descritas nas Tabelas de número 13 ao número 18, 5 são exatamente iguais para os ambientes sem a utilização do *gateway* multimídia e com sua utilização, 7 são melhores nos ambientes intermediados pelo

gateway multimídia e 6 são melhores nos ambientes não intermediados por tal *gateway* multimídia, em que esse “melhor” quanto aos tempos está associado, em grande parte dos casos, em frações na ordem de milissegundos distribuídas em todos os testes realizados, não sendo concentradas num determinado ambiente ou numa determinada quantidade de tráfego em específico, demonstrando, novamente, extrema similaridade em ambos os casos e comprovando a transparência do *gateway* multimídia quanto aos tráfegos por ele intermediados quando comparados aos resultados obtidos sem a intermediação de tal *gateway* multimídia quanto a tais tráfegos.

5.2.3 – Recursos de rede

Quanto aos recursos de rede, nesse caso referindo-se às taxas de transmissão associadas ao intermédio de tráfegos pelo *gateway* multimídia quanto ao gerador de tráfego multimídia descrito na seção 4.6.3, os valores máximos pertinentes ao *gateway* estão associados, especialmente, às limitações de velocidade de suas interfaces de rede, além de limitações impostas pelo sistema de cabeamento e/ou pelos dispositivos de interconexão utilizados ao longo da rede, dentre outros, nesse caso de 100 Mbps para as transmissões cabeadas e de 54 Mbps para as transmissões sem fio.

A partir de tais informações, bem como de informações referentes às taxas de transmissão quanto ao tráfego intermediado pelo *gateway* multimídia, nesse caso obtidas a partir dos testes realizados quanto à análise do perfil de tráfego na Seção 5.2.1, pode-se identificar eventuais limitações e gargalos de transmissão que, de alguma maneira, possam contribuir negativamente quanto a utilização do *gateway* multimídia ao longo da rede, bem como quanto aos testes realizados anteriormente.

Nesse contexto, as Figuras 92 e 93 contemplam, especialmente, informações quanto às taxas média e máxima de transmissão, além de outras, durante os testes referentes ao perfil de tráfego da Seção 5.2.1 para os ambientes cabeado e sem fio, respectivamente:

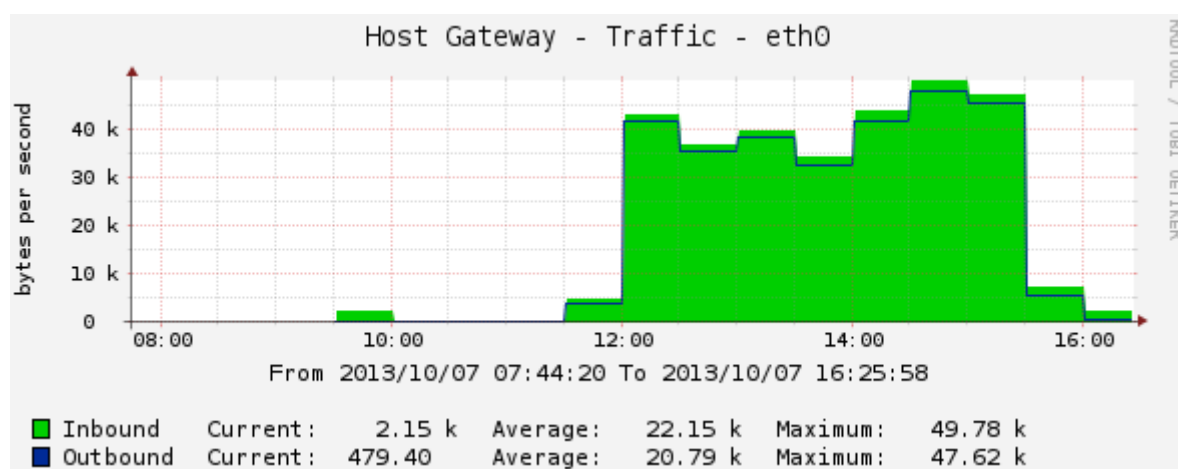


Figura 92 – Estatísticas de transmissão da interface de rede cabeada do gateway multimídia.

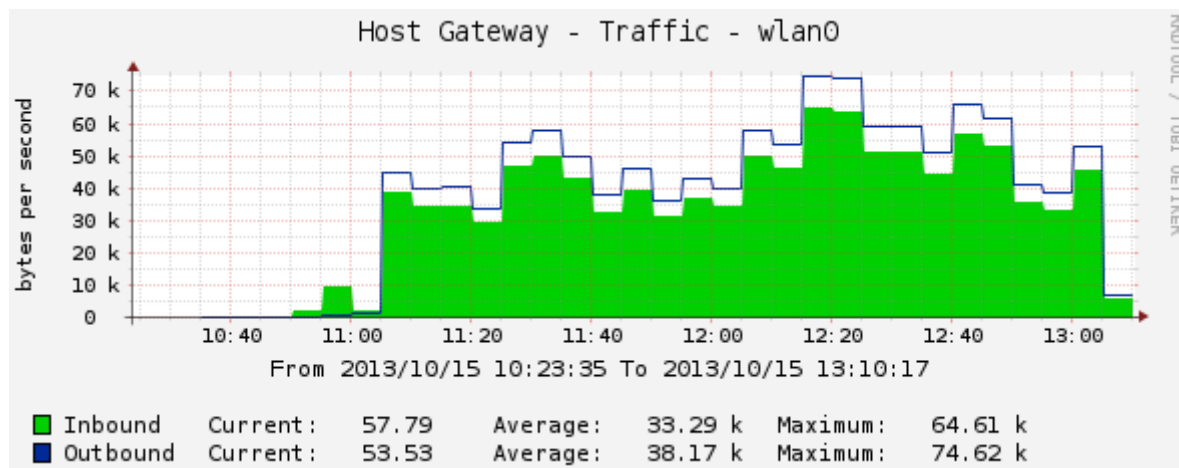


Figura 93 – Estatísticas de transmissão da interface de rede sem fio do gateway multimídia.

A partir de tais informações, pode-se observar que em ambos os casos (transmissão cabeada e transmissão sem fio), não há picos excessivos quanto às suas taxas de transmissão, com testes iniciados por volta das 12hs no ambiente cabeada e por volta das 11hs no ambiente sem fio (em dias distintos). Observe, também, que o tráfego de entrada (*Inbound*) e de saída (*Outbound*) ao *gateway* multimídia não chegou a cerca de 0,5% de sua taxa nominal máxima para a interface de rede cabeada, nesse caso com picos de 49,78 Kbps para o tráfego de entrada e de 47,62 Kbps para o tráfego de saída de tal interface, e a cerca de 1% de sua taxa nominal máxima para a interface de rede sem fio, nesse caso com picos de 64,61 Kbps para o tráfego de entrada e de 74,62 Kbps para o tráfego de saída de tal interface, com taxa média de 22,15 Kbps e 33,29 Kbps para os tráfegos de entrada às interfaces de cabeada e sem fio, respectivamente, e de 20,79 Kbps e 38,17 Kbps para os tráfegos de saída de tais interfaces.

Nesse contexto, a partir de tais informações é possível, por exemplo, contabilizar a utilização das interfaces de rede do *gateway* multimídia, bem como mensurar a utilização dos *links* de transmissão conectados em tais interfaces, de modo a contribuir para o dimensionamento da rede e de seus componentes de modo geral, bem como para identificação de eventuais gargalos, lentidões, atrasos e perdas de pacotes ao longo da rede, dentre outros.

Vale ressaltar que, quanto ao ambiente de rede do *gateway* multimídia utilizado para sua validação de desempenho, pode-se observar que as interfaces de rede a ele conectadas não representaram gargalos e limitações quanto às taxas, especialmente, máxima de transmissão associadas aos tráfegos por ele intermediados nos testes realizados anteriormente, de modo a demonstrar que os resultados obtidos, por exemplo, quanto ao perfil de tráfego (descritos na seção 5.2.1) não foram afetados por eventuais limitações quanto às suas interfaces de rede.

5.2.4 – Recursos de processamento, memória e processos

Quanto aos recursos, em especial, de processamento e memória disponíveis ao *gateway* multimídia quanto aos seus testes de validação funcional e de desempenho, estes estão limitados ao *hardware* utilizado para implementação de tal *gateway* multimídia, nesse caso com processador Intel Core I5 de 2,4 Ghz e com 4 Gb de memória RAM, dentre outros.

A partir de tais informações, bem como de informações de utilização de tais recursos obtidas nos testes referentes ao perfil de tráfego da Seção 5.2.1, pode-se identificar eventuais

limitações e gargalos que, de alguma maneira, possam contribuir negativamente quanto à utilização do *gateway* multimídia ao longo da rede, bem como quanto aos testes realizados anteriormente.

Nesse contexto, as Figuras 94 e 95 contemplam informações quanto à utilização de recursos de processamento e memória, respectivamente, pelo *gateway* multimídia quanto aos referentes ao perfil de tráfego da Seção 5.2.1:

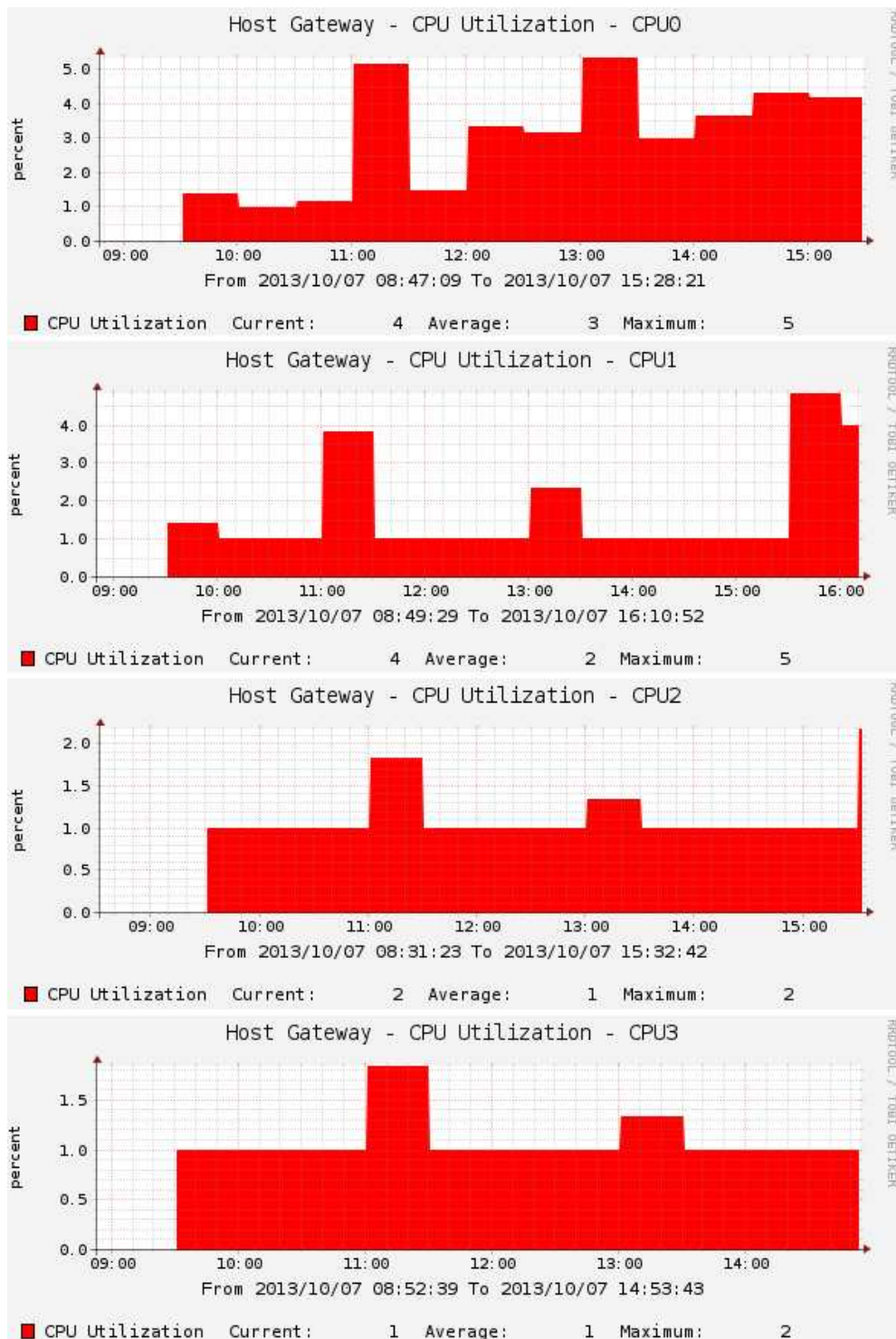


Figura 94 – Estatísticas de utilização de processamento pelo gateway multimídia.

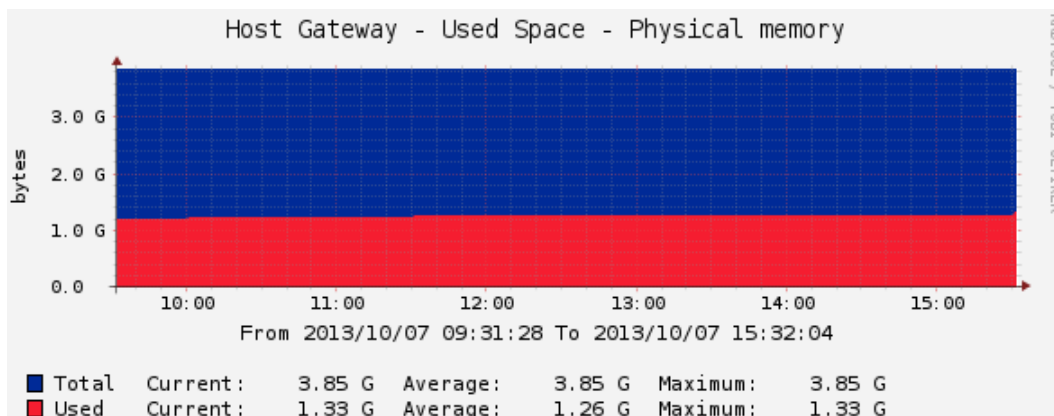


Figura 95 – Estatísticas de utilização de memória pelo gateway multimídia.

De modo similar aos recursos de rede descritos na seção anterior, observe que não houve gargalos quanto aos recursos de processamento e memória do *gateway* multimídia durante a realização de seus testes de desempenho, em que seu pico máximo de processamento foi de 5% de sua capacidade nominal máxima, enquanto a utilização de memória não ultrapassou 1,33 Gb, com percentual médio de processamento de entre 1% e 3% entre os 4 *cores* de seu processador e cerca de 30% (1,26 Gb) de utilização média de seus recursos de memória.

De modo complementar a tais informações, também é possível observar a quantidade de processos ativos no *gateway* multimídia durante seus testes de desempenho, conforme ilustra a Figura 96:

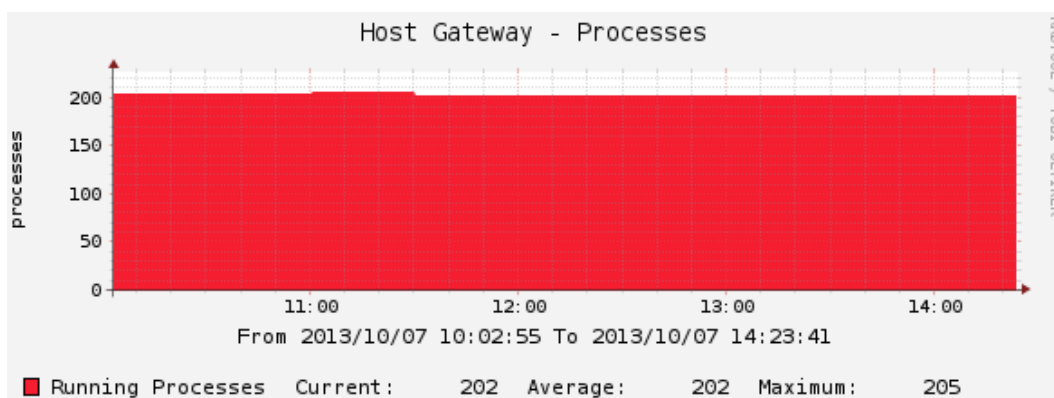


Figura 96 – Estatísticas de processos do gateway multimídia.

Nesse caso, quanto aos processos ativos no *gateway* multimídia, observe que praticamente não há alterações entre os períodos das 10hs (início dos testes) até as 14hs (testes ainda em execução), em que o pico máximo de processos ativos chegou a 205 com média de 202 durante a realização dos testes quanto a sua validação de desempenho.

Sendo assim, pode-se perceber que não houve limitações quanto aos recursos de processamento e memória, bem como mudanças bruscas quanto à quantidade de processos ativos junto ao *gateway* multimídia, de modo a demonstrar que, por exemplo, os resultados obtidos quanto ao perfil de tráfego (descritos na seção 5.2.1) não foram afetados por eventuais limitações quanto a tais recursos de processamento e memória.

6 – Conclusões

Num cenário em que diversas propostas acadêmicas e soluções tecnológicas vêm sendo estudadas, desenvolvidas e implementadas de modo a contribuir para a evolução e escalabilidade da rede (Internet), especialmente, quanto à sua arquitetura funcional, bem como à sua infraestrutura física e lógica, de modo a suportar, com qualidade, todos os requisitos impostos a ela, especialmente quanto aos tráfegos *stream* e elástico pertinente às aplicações multimídia que a utilizam enquanto infraestrutura básica e global de comunicação, o *gateway* multimídia proposto e implementado no presente projeto de pesquisa objetiva contribuir como solução complementar a tais propostas acadêmicas e tecnológicas, em que demonstra-se, na Seção 4.2, que é possível distinguir e encaminhar os diferentes fluxos de tráfegos *stream* e elástico gerados por aplicações multimídia de áudio, voz, vídeo ou dados, por exemplo, a partir de informações presentes no cabeçalho do protocolo IP, nesse caso referindo-se aos campos ToS (*Type of Service*) do protocolo IPv4 e TC (*Traffic Class*) do protocolo IPv6, ambos com 8 bits de comprimento, hoje tidos (reformulados) como DSCP (*Differentiated Services Codepoint*) [RFC 2474], com 6 bits de comprimento, e ECN (*Explicit Congestion Notification*) [RFC 3168] com 2 bits de comprimento.

Para tal, quanto à identificação do tráfego multimídia, na Seção 4.3, demonstra-se que é possível identificar até 64 (2^6) tipos de tráfegos distintos a partir do campo DSCP, em que, de modo especial ao IPv4, pode-se estruturar tais identificadores de tráfego de modo a possibilitar, também, a identificação dos canais de comunicação eventualmente associados a tais fluxos de tráfego, assim como se dá pelo campo “*Flow Label*” do IPv6, de modo que tal campo seja “pseudo implementado” também no IPv4. De modo a exemplificar e, posteriormente, comprovar tal possibilidade, no presente projeto de pesquisa, o DSCP é estruturado para suportar a identificação de 4 serviços multimídia distintos (serviços de dados, áudio, voz e vídeo), utilizando 2 bits para identificar tais serviços, com os 4 bits restantes sendo utilizados para identificar até 4 canais de transmissão associados a cada um desses serviços multimídia.

Nesse contexto, pelo fato do *gateway* multimídia necessitar que os diferentes tipos de tráfegos estejam devidamente identificados quanto ao campo DSCP, a Seção 4.5 propõe, se aplicável, a utilização de um adaptador de tráfego multimídia de modo a realizar a classificação e rotulação de tais tráfegos, ambos de modo transparente aos seus sistemas finais e respectivas aplicações transmissora e receptora do conteúdo multimídia, de modo que nenhuma alteração seja necessária em tais sistemas finais e aplicações, possibilitando que o *gateway* multimídia seja implementado de modo transparente na rede e se porte, de modo macro, como um roteador qualquer ao longo de uma comunicação fim-a-fim na Internet, por exemplo.

De modo a contribuir quanto às questões voltadas à temporização e largura de banda exigidas, especialmente, por aplicações multimídia de tráfego *stream*, a Seção 4.4 descreve alguns mecanismos de escalonamento e regulação que, posteriormente implementados no *gateway* multimídia, demonstram que é possível, a partir dos identificadores de tipos de tráfegos quanto ao campo DSCP do cabeçalho do protocolo IP, dar certas prioridades quanto a tais fatores aos tipos de tráfego que necessitem dos mesmos, de modo a minimizar os efeitos quanto à percepção de velocidade e de atrasos e variações de atrasos às aplicações receptoras de tais tráfegos.

Quanto à implementação do *gateway* multimídia, de modo a simplificar e facilitar eventuais manutenções em sua estrutura funcional, os recursos de identificação/distinção de tipos de

tráfegos distintos, bem como os mecanismos para qualidade de serviço foram implementados de forma modular (assim como as camadas do Modelo de Referência ISO/OSI ou da Arquitetura TCP/IP, como exemplo), ambos tendo como base os identificadores de tipos de tráfego quanto ao campo DSCP do cabeçalho do protocolo IP, e utilizando de soluções de *software* livre especialmente fornecidas pelo sistema operacional Linux e pela solução Netfilter/Iptables, possibilitando que trabalhos futuros possam ser realizados e beneficiados quanto a tal ambiente/estrutura de desenvolvimento.

Por sua vez, de modo a comprovar os fundamentos e propostas funcionais e organizacionais quanto ao campo DSCP pelo *gateway* multimídia, bem como da utilização de um adaptador de tráfego multimídia para que a implementação de tal *gateway* seja efetivamente transparente aos sistemas finais e aplicações transmissora e receptora do conteúdo multimídia, as seções do Capítulo 5 demonstram que os mecanismos funcionais quanto ao *gateway* multimídia e ao adaptador de tráfego multimídia são válidos e funcionais (Seções 5.1.1, 5.1.2 e 5.1.3) e que, por meio de comparações de resultados obtidos a partir da utilização do *gateway* multimídia com resultados obtidos sem sua utilização, não influenciam em questões voltadas ao perfil (características) dos tráfegos trocados entre as aplicações transmissora e receptora do conteúdo multimídia (Seção 5.2.1), bem como quanto à questões voltadas a erros, atrasos e variações de atrasos (Seção 5.2.2), sejam estas embasadas em transmissões cabeadas ou sem fio (*wireless*). Nesse mesmo capítulo, também demonstra-se, em especial, que os recursos de rede (Seção 5.2.3) e de processamento e memória (Seção 5.2.4) disponíveis ao *gateway* multimídia não sofreram alterações bruscas de comportamento durante seus testes de desempenho, de modo que não houve sobrecarga quanto a tais recursos, bem como eventuais influências dos mesmos quanto às suas validações de desempenho.

Sendo assim, de modo resumido, pode-se concluir que é possível utilizar de identificadores quanto ao campo DSCP do cabeçalho do protocolo IP (de versões 4 e 6) para realizar a identificação de diferentes tipos de tráfego multimídia ao longo da rede, sendo possível, inclusive, a identificação de eventuais canais de comunicação associados a tais tipos de tráfego, e que a utilização de um *gateway* multimídia é viável e funcional para identificar, distinguir e direcionar tais distintos tipos de tráfego de modo intermediário e transparente às aplicações e sistemas finais transmissores e receptores dos mesmos, agregando recursos adicionais a tais aplicações e sistemas finais, tais como mecanismos de qualidade de serviço e de eventuais filtragem de tráfegos antes que os mesmos cheguem aos seus sistemas finais/aplicações receptoras de modo a contribuir com as propostas acadêmicas e tecnológicas que objetivam a evolução e escalabilidade da rede (Internet), além de fornecer um novo ambiente para o estudo de soluções voltadas às redes multimídia, de modo geral.

Por fim, quanto aos trabalhos futuros, o desenvolvimento de uma interface gráfica que possibilite a administração e utilização simplificada do *gateway* multimídia, bem como da customização de uma distribuição Linux (nesse caso, referindo-se especialmente ao *Kernel* do sistema) para, especialmente, esse propósito (viabilização de um *gateway* multimídia) são extremamente favoráveis à sua estrutura funcional e operacional. De modo complementar, outras abordagens podem enfatizar a forma com a qual as aplicações multimídia podem ser identificadas, distinguidas, tratadas e encaminhadas pelo *gateway* multimídia, de modo a adicionar novos recursos ao mesmo e possibilitar maior flexibilidade quanto à sua estrutura funcional. Quando aplicáveis, essas mesmas abordagens também podem ser utilizadas para o adaptador de tráfego multimídia, de modo a também contribuir para sua estrutura funcional e operacional.

Referências

- [1] Youtube. Estatísticas diversas. Disponível em http://www.youtube.com/t/press_statistics. Último acesso em 19/10/2013.
- [2] Skype: The Big Blog. 35 Million People Concurrently Online on Skype, 2012. Disponível em: http://blogs.skype.com/en/2012/03/35_million_people_concurrently.html. Último acesso em 19/10/2013.
- [3] Wang, W. Zhang, X.; Shi, W.; Lian, S.; Feng, D. Understanding and Analyzing Network Traffic. Network, IEEE. IEEE Journals & Magazines, 2012.
- [4] Lakhina, A.; Papagiannaki, K.; Crovella, M.; Diot, C.; Kolaczyk, E. D.; Taft, N. Structural analysis of network traffic flows. ACM SIGMETRICS Performance Evaluation Review, 2004.
- [5] Khalifa, O. O.; Issa, S.; Olanrewaju, R. F.; Al Khazmi, El M. A. Development of a scalable video compression algorithm. Computer and Communication Engineering (ICCCE), 2012 International Conference on. IEEE Conference Publications, 2012.
- [6] Lazaris, A.; Koutsakis, P.; Paterakis M. A new model for video traffic originating from multiplexed MPEG-4 videoconference streams. McMaster University, Canada, 2007.
- [7] Li, I. Effects of ON-OFF Variability in Two-State Pareto Traffic Models on Multimedia Application Transmission Performance. Networked Computing and Advanced Information Management, 2008. IEEE Conference Publications, 2008.
- [8] La Corte, A. Modeling superposition of ON-OFF correlated traffic sources in multimedia applications. INFOCOM 95. Fourteenth Annual joint conference of the IEEE Computer and Communications Societies. Bringing Information to People. Proceedings. IEEE, 1995.
- [9] Hirachi, S.; Ogose, S. Traffic model for multimedia mobile radio communications. Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual. IEEE Conference Publications, 2003.
- [10] Choy, M.Y.; Mir, N.F. Performance modeling of multimedia traffic in mobile wireless networks. MILCOM 2000. 21st Century Military Communications Conference Proceedings. IEEE Conference Publications, 2000.
- [11] Golaup, A.; Holland O.; Aghvami , H. Concept and Optimization of an Effective Packet Scheduling Algorithm for Multimedia Traffic over HSDPA. University of London – UK, 2005.
- [12] Dandan, Z.; Xuming F.; Longjie, Z. Novel Multimedia Traffic Modeling Based CAC Scheme for CDMA Communication Systems. Southwest Jiaotong University, China, 2007.
- [13] Adzic, V.; Kalva, H.; Furht, B. Optimizing video encoding for adaptive streaming over HTTP. Consumer Electronics, IEEE Transactions on. IEEE Journals & Magazines, 2012.
- [14] Haimi-Cohen, R.; Hearn, J.; Scheutzow, M.; Levy, E.P.; Wu, L.J.; Livescu, D.; Wilford, P.A. Flexible and robust video delivery based on self-contained multimedia segments. Sarnoff Symposium (SARNOFF), 2012 35th IEEE. IEEE Conference Publications, 2012.

- [15] De Schepper, K.; De Vleeschauwer, B.; Hawinkel, C.; Van Leekwijck, W.; Famaey, J.; Van de Meersee, W.; De Turck, F. Shared Content Addressing Protocol (SCAP): Optimizing multimedia content distribution at the transport layer. Network Operations and Management Symposium (NOMS), 2012. IEEE Conference Publications, 2012.
- [16] Manohar, N. R.; Mehra, A.; Willebeek-LeMair, M. H. e Naghshineh, M. A framework for programmable overlay multimedia networks. IBM Research Division, New York, USA, 1999.
- [17] Dahmouni, H.; Girard, A.; Ouzineb, M.; Sanso, B. The Impact of Jitter on Traffic Flow Optimization in Communication Networks. Network and Service Management, IEEE Transactions on. IEEE Journals & Magazines, 2012.
- [18] Tian, H.; Yang, W. Study on QoS of Multimedia Traffics in MAC Layer Based on 802.11. Information Science and Applications (ICISA), 2012 International Conference on Information Science and Applications. IEEE Conference Publications, 2012.
- [19] Kamadyta, A.; Bandung, Y.; Langi, A. Z. R. Performance analysis of supporting QoS for multimedia in IEEE 802.11e. Cloud Computing and Social Networking (ICCCSN), 2012. IEEE Conference Publications, 2012.
- [20] Salman A. A Simulation-Based Comparison of Multimedia Traffic Prioritization Schemes for High-Performance Input-Queued Packet Switches. King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia, 2006.
- [21] Pinotti, F. L. Simulação e Emulação de Tráfego Multimídia em Redes IP. Dissertação de Mestrado. Faculdade de Tecnologia. Universidade Estadual de Campinas, 2011.
- [22] F. L. Pinotti, T. R. B. Oliveira, E. L. Ursini and V. S. Timóteo, An IP-based multimedia traffic generator, Proceedings of the International Workshop on Telecommunications - IWT, 2011.
- [23] Kurose, J. F.; Ross, K. W. Redes de Computadores e a Internet: Uma Abordagem Topdown. 5ª Edição. São Paulo: Pearson Addison Wesley, 2010.
- [24] Tanenbaum, A. S. Redes de Computadores. 4ª Edição. Rio de Janeiro: Campus, 2003.
- [25] Gallo, M. A.; Hancock, W. M. Comunicações entre computadores e tecnologias de rede. São Paulo: Thomson Learning, 2002.
- [26] Peng, G. CDN: Content Distribution Network. Department of Computer Science, State University of New York at Stony Brook, Stony Brook, 2008.
- [27] Oottamakorn, C.; Mao, S.; Panwar, S.S. On Generalized Processor Sharing With Regulated Multimedia Traffic Flows. IEEE Transactions on Multimedia. IEEE Journals & Magazines, 2006.
- [28] Golaup, A.; Aghvami, H. A multimedia traffic modeling framework for simulation-based performance evaluation studies. Centre for Telecommunications Research, Kings College London, University of London, 26-29 Drury Lane, London WC2B 5RL, UK, 2005.

- [29] Lima, A. B. Contribuições à Modelagem de Teletráfego Fractal. Tese de doutorado. Universidade de São Paulo, 2008.
- [30] Fonseca, J. S.; Martins, G. A. Curso de Estatística. 6ª Edição. São Paulo: Atlas, 2010.
- [31] Spiegel, M. R. Estatística. 3ª Edição. São Paulo: Pearson Makron Books, 2009.
- [32] Cisco Systems. DiffServ - The Scalable End-to-End Quality of Service Model. White Paper, 2005.
- [33] Netfilter/Iptables Project. Disponível em: <http://www.netfilter.org>. Último acesso em 19/10/2013.
- [34] Iproute2 Project. Disponível em: <http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2>. Último acesso em 19/10/2013.
- [35] Rockwell Automation. Software Arena. Disponível em <http://www.arenasimulation.com>. Último acesso em 19/10/2013.
- [36] Iperf Project. Disponível em: <http://iperf.sourceforge.net/>. Último acesso em 19/10/2013.
- [37] Postel, J. Internet Protocol. RFC 791, 1981.
- [38] Almquist, P. Type of Service in the Internet Protocol Suite, RFC 1349, 1992.
- [39] Deering, S.; Hinden, R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, 1998.
- [40] Nichols, K.; Blake, S.; Baker, F.; D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474, 1998.
- [41] Ramakrishnan, K.; Floyd, S.; D. Black. The Addition of Explicit Congestion Notification (ECN) to IP. RFC 3168, 2001.
- [42] Blake, S.; Black, D.; Carlson, M.; Davies E.; Wang Z. e Weiss W. An Architecture for Differentiated Services. RFC 2475, 1998.
- [43] Heinanen, J.; Baker, F.; Weiss, W.; Wroclawski, J. Assured Forwarding PHB Group. RFC 2597, 1999.
- [44] Davie, B.; Charny, A.; Bennett, J.C.R.; Benson, K.; Le Boudec, J.Y.; Courtney, W.; Davari, S.; Firoiu, V.; Stiliadis, D. An Expedited Forwarding PHB (Per-Hop Behavior). RFC 3246, 2002.
- [45] Shenker, S.; Wroclawski J. General Characterization Parameters for Integrated Service Network Element. RFC 2215, 1997.