PROYECTO FINAL DE CARRERA

La Neutralidad de Red: Gestión de tráfico mediante DPI/DFI

(Net Neutrality: Traffic management through DPI/DFI)

Estudios: Ingeniería de Telecomunicación

Autor: Juan Molina Rodríguez

Director/a: Daniel Ollé Oriol

Año: 2011

Proyecto realizado con el apoyo de la cátedra CMT-UPC.
Versión 1.0. Fecha: 31/12/2011.

Resumen del Proyecto

La Neutralidad de Red promueve una serie de principios orientados a mantener un Internet abierto, entre los que destaca el de otorgar un mismo trato a todos los paquetes que circulan por éste. Su planteamiento se ha desencadenado en relación a la controversia surgida en torno a los intereses privados que muestran operadores e ISPs frente a los de proveedores de servicio, aplicaciones y contenidos, y que se puede sintetizar en un problema de inversión y retorno de ésta en la infraestructura y gestión de Internet.

Esta problemática está derivando en el planteamiento de diferentes propuestas en el ámbito económico que van desde el cobro a proveedores de servicio para que contribuyan al coste de la infraestructura, hasta la aparición de modelos tarifarios que repartan mejor los costes sobre los usuarios, pudiendo dar lugar a planes de limitación de servicios o a la comercialización de diferentes niveles de QoS. La tendencia de aplicación de niveles de QoS se potencia además con las necesidades requeridas por los servicios multimedia e interactivos cada vez más comunes y asiduos en Internet. En ambos casos se requiere de una aplicación de gestión de tráfico, que por otra parte, es cada vez más empleada para dar solución a problemas de congestión. Para la correcta aplicación de ésta se hace necesaria la identificación y clasificación de paquetes, lo cual requiere de técnicas sofisticadas de análisis fundamentalmente debido a que ciertos protocolos son enmascarados u ofuscados para evitar su posterior gestión.

Debido a la importancia del desenlace de esta situación, este documento tiene como objetivo el de exponer la discusión de Neutralidad de Red para posteriormente realizar un estudio del estado del arte de las técnicas existentes para la gestión de tráfico mediante DPI/DFI, conocer sus posibilidades y juzgar su papel, y finalmente proponer una serie de recomendaciones para su empleo, que podrían sentar las bases de una futura regulación. Así, de modo introductorio se analizan varios aspectos relacionados con el foco de la discusión de Neutralidad de Red y de forma algo más profunda se analizan algunas técnicas de gestión de tráfico. En este ámbito, se estudian las arquitecturas NGN más relevantes con capacidades inherentes de otorgar diferentes niveles de QoS. También se analizan las técnicas de análisis profundo de paquetes DPI/DFI, haciendo especial hincapié en los aspectos prácticos de éstas mediante la realización de un ejercicio de análisis de tráfico real con una herramienta DPI.

La visión general que se suele tener sobre el empleo de técnicas de gestión de tráfico mediante DPI/DFI en Internet es la de una acción agresiva que va en contra de los derechos y la privacidad de los usuarios, además de representar una amenaza para que Internet sea una plataforma abierta y neutral. Veremos en este documento que esta visión no se corresponde con las posibilidades que su buen uso puede aportar en términos de eficiencia tanto a nivel técnico como económico, pudiendo dar paso a un modelo de Internet satisfactorio para todos los servicios y usuarios.

Resum del Projecte

La Neutralitat de Xarxa promou un conjunt de principis orientats a mantenir un Internet obert, entre els quals destaca el d'atorgar un mateix tracte a tots els paquets que circulen per la xarxa. El seu plantejament s'ha desencadenat en relació a la controvèrsia sorgida al voltant dels interessos privats que mostren operadors i ISPs enfront dels de proveïdors de servei, aplicacions i continguts, i que es pot sintetitzar en un problema d'inversió i retorn d'aquesta en la infraestructura i gestió d'Internet.

Aquesta problemàtica està derivant en el plantejament de diferents propostes en l'àmbit econòmic que van des del cobrament a proveïdors de servei perquè contribueixin al cost de la infraestructura, fins a l'aparició de models tarifaris que reparteixin millor els costos sobre els usuaris, podent donar lloc a plans de limitació de serveis o la comercialització de diferents nivells de QoS. La tendència d'aplicació de nivells de QoS es potencia a més amb les necessitats requerides pels serveis multimèdia i interactius cada vegada més comuns i assidus a Internet. En ambdós casos es requereix d'una aplicació de gestió de trànsit, que d'altra banda, és cada vegada més emprada per a donar solució a problemes de congestió. Per a la correcta aplicació d'aquesta es fa necessària la identificació i classificació de paquets, la qual cosa requereix de tècniques sofisticades d'anàlisi fonamentalment degut a que certs protocols són emmascarats o ofuscats per evitar la seva posterior gestió.

A causa de la importància del desenllaç d'aquesta situació, aquest document té com a objectiu el d'exposar la discussió de Neutralitat de Xarxa per a posteriorment realitzar un estudi de l'estat de l'art de les tècniques existents per a la gestió de trànsit mitjançant DPI/DFI, conèixer les seves possibilitats i jutjar el seu paper, i finalment proposar una sèrie de recomanacions per a la seva utilització, que podrien establir les bases d'una futura regulació. Així, de manera introductòria s'analitzen diversos aspectes relacionats amb el focus de la discussió de Neutralitat de Xarxa i de forma una mica més profunda s'analitzen algunes tècniques de gestió de trànsit. En aquest àmbit, s'estudien les arquitectures NGN mes rellevants amb capacitats inherents d'atorgar diferents nivells de QoS. També s'analitzen les tècniques d'anàlisi profund de paquets DPI/DFI, fent especial èmfasi en els aspectes pràctics d'aquestes amb la realització d'un exercici d'anàlisi de trànsit real amb una eina DPI.

La visió general que se sol tenir sobre l'ús de tècniques de gestió de trànsit mitjançant DPI/DFI a Internet és la d'una acció agressiva que va en contra dels drets i la privacitat dels usuaris, a més de representar una amenaça per tal que Internet sigui una plataforma oberta i neutral. Veurem en aquest document que aquesta visió no es correspon amb les possibilitats que el seu bon ús pot aportar en termes d'eficiència tant a nivell tècnic com econòmic, podent donar lloc a un model d'Internet satisfactori per a tots els serveis i usuaris.

Abstract

Net Neutrality promotes some principles aimed at maintaining an open Internet, including specially the idea of granting the same treatment to all packets flowing through the network. This approach has been triggered because of the controversy surrounding the private interests shown by operators and ISPs facing the ones of service, applications and content providers. This discussion can be synthesized in a return of investment problem in the Internet infrastructure and management.

This situation is leading to different approaches in the economic field, ranging from charging service providers so that they contribute to the cost of infrastructure, to the development of tariff models to distribute better the costs on users, which may result in plans to limit the access to some services or offering different QoS Levels. Trends on implementing QoS levels are also powered by the requirements of multimedia and interactive services. They are increasingly common and frequent on the Internet. In both cases is required the application of traffic management, which is also being used to solve congestion problems. For its correct application is necessary to identify and classify packets, which requires sophisticated analysis techniques because certain protocols are masked or obfuscated to prevent its subsequent handing.

Due to the importance of the outcome of this situation, this paper aims to present the discussion of Net Neutrality, study the state of the art of the existing techniques for traffic management through DPI/DFI, understand their potential and judge its role. Finally a set of recommendations are proposed, which could form a basis for a future regulation. Therefore, in an introductory way various aspects related to the focus of the discussion of Net Neutrality are exposed and some traffic management techniques are discussed in depth. In this context, the document reviews some of the most relevant NGN architectures with inherent abilities to grant different QoS levels through analysis of packets by DPI/DFI, with particular emphasis on the practical aspects of these by performing a real traffic analysis exercise by means of a DPI tool.

The general perception on the use of traffic management techniques through DPI/DFI on the Internet is that they implies an aggressive action against user's rights and privacy and also that suppose a threat to the Internet as an open and neutral platform. We will see in this document that this view does not correspond to the possibilities that a proper use of it can provide. It allows a better efficiency in terms of both technical and economic aspects and also may promote a successful Internet model covering all services and users.

Agradecimientos

Quiero mostrar mis agradecimientos a la Comisión del Mercado de las Telecomunicaciones por haber confiado en mí para la elaboración de este Proyecto. De forma más concreta a los que durante estos meses han sido mis compañeros en el Dirección Técnica y en especial a Rafael Bru Gibert, que me tuteló inicialmente, y a Daniel Ollé Oriol, que me ha guiado durante la mayor parte del transcurso del Proyecto y me ha ayudado en todo lo posible durante mi paso por esta casa.

Quiero mencionar también a Anna Calveras Auge del Departamento de Telemática de la ETSETB por su tiempo e implicación.

En el ámbito personal, como punto y final a mi titulación de Ingeniero de Telecomunicación, quiero acordarme también de los compañeros que me han acompañado durante la carrera. También de mis puntos de apoyo en el día a día: mi familia, mis amigos y mi pareja.

Gracias.

Índice

Lista de acrónimos 10
Definiciones 14
Capítulo I – Introducción 15
Capítulo II – Conceptos básicos sobre Internet 17
1 Estructura de Internet 18
1.1 Núcleo de Internet 18
1.1.1 Modelo inicial de Internet 19
1.1.2 Modelo actual de Internet 19
1.2 Red de acceso 21
2 El modelo OSI & TCP/IP 23
3 El principio 'end-to-end' 25
4 Factores económicos 26
4.1 Cadena de valor 26
4.2 El mercado bilateral 29
4.3 El mercado de acceso e interconexión IP 30
Capítulo III – Neutralidad de Red 34
1 Origen del debate 35
2 Casos destacados 36
3 Aspectos de la Neutralidad de Red 39
4 Contexto internacional 42
Capítulo IV - Gestión de tráfico 44
1 Antecedentes de la gestión de tráfico 46
2 Prácticas de gestión de tráfico 48
3 Tipos de tráfico y QoS 50
4 Gestión de tráfico basada en QoS y 'policing' 52
4.1 Gestión de tráfico en redes móviles 54
4.1.1 GSM/GPRS/EDGE, UMTS/HSPA - GPRS Core Network 56
4.1.1.1 Arquitectura de red 56
4.1.1.2 Niveles de QoS 57
4.1.1.3 Políticas de control 57
4.1.1.4 Análisis de tráfico en 2G/3G 57
4.1.2 LTE/SAE – Evolved Packet Core 58
4.1.2.1 Arquitectura de red 59
4.1.2.2 Niveles de QoS 61
4.1.2.3 Políticas de control 64
4.1.2.4 Análisis de tráfico en SAE/LTE 65
4.2 Gestión de tráfico en redes fijas 66
4.2.1 Cable - DOCSIS 66
4.2.1.1 Arquitectura de red 67
4.2.1.2 Niveles de QoS 68
4.2.1.3 Políticas de control 69
4.2.1.3.1 IPDR 69
4.2.1.3.2 PCMM 70
4.2.1.4 Análisis de tráfico en Cable 71
4.2.2 Acceso fijo - TISPAN 72
4.2.2.1 Arquitectura de red 72
4.2.2.2 Niveles de QoS 73
4.2.2.3 Políticas de control 74

4.2.2.4 Análisis de tráfico en accesos fijos 76
4.3 Comparativa de arquitecturas de gestión QoS y Policy 76
Capítulo V - Análisis del tráfico 79
1 Técnicas de análisis: SPI, DPI y DFI 80
1.1 Aplicaciones de DPI/DFI 83
2 Implantación de sistemas DPI/DFI para la gestión de tráfico 85
2.1 Ubicación de sistemas DPI/DFI 85
2.2 Integración de sistemas DPI/DFI 87
2.2.1 DPI/DFI dedicado 87
2.2.2 DPI/DFI integrado 87
2.2.3 Comparativa entre soluciones dedicadas e integradas 89
3 Mercado DPI/DFI 90
3.1 Fabricantes y soluciones relevantes 90
3.1.1 Fabricantes puros 91
3.1.1.1 Sandvine 91
3.1.1.2 Allot 91
3.1.1.3 Procera 92
3.1.1.4 Ipoque 93
3.1.2 Fabricantes clásicos 93
3.1.2.1 Cisco 93
3.1.2.2 Ericsson 94
3.2 Valor de mercado 95
4 Aspectos técnicos de DPI/DFI 97
4.1 Arquitectura de sistemas DPI/DFI 97
4.1.1 Interconexión: ATCA 97
4.1.2 Procesado de datos 98
4.1.2.1 Plano de datos y plano de control 99
4.1.2.2 Tipos de procesadores para comunicaciones 99
4.1.2.2.1 ASIC & NPU 100
4.1.2.2.2 Communication Processor 100
4.1.2.2.3 CPU multi-núcleo 101
4.1.2.2.4 Procesador de flujo 103
4.2 Clasificación de paquetes en flujos 107
4.3 Análisis DPI 111
4.3.1 Algoritmos de búsqueda DPI 113
4.3.1.1 'String Matching' 114
4.3.1.2 Regular Expression (RegEx) 115
4.3.1.2.1 Teoría de autómatas 116
4.3.1.2.1.1 NFA: Non-deterministic Finite Automata 117
4.3.1.2.1.2 DFA: Deterministic Finite Automata 118
4.4 Análisis DFI 119
5 Análisis de tráfico real: Ejercicio práctico 123
5.1 P2P (Peer-To-Peer) 123
5.1.1 BitTorrent 123
5.1.2 eDonkey 125
5.2 VoIP (SIP + RTP) 125
5.3 Email (SMTP + IMAP) 127
5.4 Conclusiones del ejercicio 130
Capítulo VI – Implicaciones, conclusiones y recomendaciones 131
1 Implicaciones 132
1.1 Modelo 'best effort' 132

1.2 Modelo de tráfico gestionado 133
1.3 Ventajas e inconvenientes 135
2 Conclusiones 137
3 Recomendaciones 144
Anexo A – Contexto regulatorio internacional 146
1 Unión Europea 146
1.1 Marco Legislativo 146
1.2 Declaración de la Comisión Europea sobre la Neutralidad de Red 148
1.3 Consulta pública 148
1.4 Comunicado de la Comisión sobre la Neutralidad de Red 151
1.5 Recomendaciones del Parlamento Europeo 151
2 EEUU 153
2.1 Internet Policy Statements 153
2.2 Report&Order : Preserving the Open Internet 154
3 Chile 156
3.1 Proyecto de Ley 156
3.2 Requisitos de transparencia 157
4 Holanda 160
4.1 Enmienda de Ley 160
5 Francia 162
5.1 Consulta pública sobre propuesta de directrices 162
5.2 Propuestas y recomendaciones 162
6 Reino Unido 165
7 Suecia 166
8 Canadá 167
8.1 Telecom Decision 2008-108 167
8.2 Telecom Regulatory Policy CRTC 2009-657 167
9 Noruega 169
10 Japón 170
Anexo B – Análisis de tráfico real 171
1 OpenDPI 171
2 Capturas de tráfico 172
2.1 P2P (Peer-To-Peer) 172
2.1.1 BitTorrent 172
2.1.2 eDonkey 174
2.2 VoIP (SIP + RTP) 176
2.3 Email (SMTP + IMAP) 177
Referéncias 179

Lista de acrónimos

µTP	Micro Transport Protocol
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AF	Application Function
AM	Application Manager
AM*	Acknowledge Mode
ANR	Agencia Nacional Reguladora
API	Application Programming Interface
A-RACF	Access-Resource and Admission Control Function
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes
AS	Autonomous System
ASIC	Application-Specific Integrated Circuit
ATCA	Advanced Telecom Computing Architecture
A-TDMA	Advanced-TDMA
BE	Best Effort
BEREC	Body of European Regulators for Electronic Communications
BGF	Border Gateway Function
BSS	Base Station Subsystem
CAIP	Canadian Association of Internet Providers
CALEA	Communications Assistance for Law Enforcement Act
CATV	Cable Television
CDN	Content Delivery Network
CM	Cable Modem
CMTS	Cable Modem Termination System
CoS	Classes of Service
CRTC	Canadian Radio-Television and Telecommunications Commission
DFA	Deterministic Finite Automata
DFI	Deep Flow Inspection
DiffServ	Differentiated Services
DL	DownLink
DNS	Domain Name Server
DOCSIS	Data Over Cable Service Interface Specification
DoS	Denial of Service
DPI	Deep Packet Inspection
DSCP	DiffServ Code Point
E/S	Entrada/Salida
EDGE	Enhanced Data Rates for GSM Evolution
EPC	Evolved Packet Core
EPS	Evolved Packet System

ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FTTH	Fiber To The Home
FTTx	Fiber To The x
GAS	Gateway Access Service
GBR	Guaranteed Bit Rate
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMX	Global Message eXchange
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HFC	Hybrid Fiber Coaxial
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IMS	IP Multimedia Subsystem
IntServ	Integrated Services
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IPER	IP Packet Error Rate
IPLR	IP Packet Loss Rate
IPS	Intrusion Prevention System
IPTV	IP Television
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU-T	International Telecommunication Union-Telecommunication
IXP	Internet Exchange Point
LLU	Local Loop Unbundling
LTE	Long Term Evolution
MAC	Medium Access Control
MCI	Microwave Communications, Inc.
MIT	Massachusetts Institute of Technology
MME	Mobility Management Entity
MMS	Microsoft Media Services
MPEG	Moving Picture Experts Group
MPLS	Multi-Protocol Label Switching
MSE	Message Stream Encryption
MSER	Multi-Service Edge Router
MSO	Multiple Service Operator
NASS	Network Attachment Subsystem

NAT	Network Address Translation
NFA	Non-deterministic Finite Automata NFA
NFP	Network Flow Processor
NGN	Next Generation Network
NP	Network Performance
NPT	Norway Post and Telecommunication-Authority
NPU	Network Processor Unit
NRTPS	Non Real Time Polling Service
NSN	Nokia Siemens Networks
OCS	On-line Charging System
OFCS	Off-line Charging System
OTN	Optical Terminal Node
OTT	Over The Top
P2P	Peer To Peer
PACE	Packet and Application Classification Engine
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCI	Peripheral Component Interconnect
PCMM	PacketCable MultiMedia
PCRF	Policy Charging and Rules Function
PDN	Packet Data Network
PDU	Packet Data Unit
PELR	Packet Error Loss Rate
PER	Packet Error Rate
PES	PSTN/ISDN Emulation Subsystem
PGW	PDN Gateway
PICMG	PCI Industrial Computer Manufacturers Group
PKI	Public Key Infrastructure
PON	Passive Optical Network
POP3	Post Office Protocol 3
PPE	Packet Processor Engine
PRE	PacketLogic Real-Time Enforcement
PS	Policy Server
PSM	PacketLogic Subscriber Manager
PSTN	Public Switched Telephone Network
PTS	Policy Traffic Switch
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RACS	Resource and Admission Control Sub-System
RC4	Rivest Cipher 4
RCEF	Resource Control Enforcement Function
RegEx	Regular Expressions
RKS	Record Keeping Server
RLC	Radio Link Control
RSVP	Resource Reservation Protocol

RTP	Real Time Protocol
RTPS	Real Time Polling Service
RTSP	Real Time Streaming Protocol
RTTE	Radio and Telecommunications Terminal Equipment
SAE	System Architecture Evolution
SAPC	Service-Aware Policy Controller
SASN	Service Aware Support Node
SBC	Southwéstern Bell Telecom, Inc.
S-CDMA	Synchronous Code Division Multiple Access
SDE	Service Delivery Engine
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPDF	Service Policy Decision Function
SPI	Stateful/Shallow Packet Inspection
SRTP	Secure Real Time Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SUBTEL	Subsecretaría de Telecomunicaciones
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TIC	Tecnologías de la Información y la Comunicación
TISPAN	Telecommunications Internet converged Services Protocols for Advanced Networking
TLS	Transport Layer Security
TM	Transparent Mode
UE	User Equipment
UGS	Unsolicited Grant Service
UGS-AD	Unsolicited Grant Service with Activity Detection
UL	UpLink
UM	Unacknowledged Mode
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
UTRAN	UMTS Terrestrial Radio Access Network
VoD	Video on Demand
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WSP	Wireless Session Protocol

Definiciones

- **IMS:** Marco de trabajo que define una arquitectura base para el soporte de telefonía y servicios multimedia sobre una estructura basada en IP.

- **Latencia:** Retardo que sufre un paquete desde su origen hasta que alcanza su destino.

- **Jitter:** Variación de la latencia medida en un flujo de paquetes.

- **PELR:** Tasa de paquetes que no alcanzan el destino. Dependiendo del tipo de servicio deben ser retransmitidos. Según la recomendación ITU-T Y.1540 se le denomina IPLR.

- **PER:** Tasa de paquetes recibidos con error. Dependiendo del tipo de servicio deben ser retransmitidos. Según la recomendación ITU-T Y.1540 se le denomina IPER.

- **QoS**[1]**:** Parámetros objetivos de la calidad del flujo de datos en una red o agregación de redes. Generalmente se tienen en cuenta los siguientes marcadores: {PELR, PER, jitter, latencia, ancho de banda}[2].

- **QoE:** Percepción subjetiva de la calidad recibida por los usuarios. Está fuertemente relacionado con la QoS.

- **Quíntupla:** Marcadores que definen un flujo unidireccional de datos: {dirección IP origen, dirección IP destino, puerto origen, puerto destino, protocolo de nivel 4}.

- **Servicios dedicados:** Servicios ofrecidos verticalmente por los ISPs sobre el mismo acceso que Internet. Un claro ejemplo es el servicio de TV sobre IP.

- **Streaming:** Transmisión de contenido multimedia para consumo inmediato sin almacenamiento completo.

[1] Esta definición está adaptada al documento. Según la definición de la recomendación ITU-T E.800 el término QoS es exclusivo para los parámetros extremo a extremo, definiéndose para cada red la Network Performance (NP). Según esta recomendación, la QoS es agregación de todas las NP.

[2] Parámetros según recomendación ITU-T Y.1540, aunque cambiando la nomenclatura de las tasas de error.

Capítulo I – Introducción

Internet se ha convertido en un eje fundamental de nuestra actividad social, cultural y económica. Su uso abarca casi todos los aspectos de nuestras vidas, habiendo penetrado de forma más directa y profunda que cualquier otra tecnología existente hasta la fecha. Tanto es así, que se habla de una transición hacia un modelo de sociedad de la información o del conocimiento en detrimento del modelo de sociedad productivo.

La Neutralidad de Red defiende una serie de principios de entre los que se destaca el que promueve que todos los paquetes de Internet deben ser tratados por igual. Este principio ha sido originado por un debate surgido en los últimos años en relación a cómo se debe financiar la inversión en la estructura de Internet, fundamentalmente en la lucha contra situaciones de congestión. Este problema, que a simple vista puede parecer algo sencillo, lleva tras de sí varios aspectos de difícil análisis que serán expuestos, y algunos de ellos analizados, a lo largo del documento.

Para centrar la cuestión se debe considerar que si bien el problema fundamental recae en un aspecto económico, lo cierto es que el fondo de la discusión está en el ámbito técnico. El crecimiento que se ha dado en los últimos años en el consumo de datos tanto en el escenario fijo como en el móvil está llevando a una situación de congestión en las redes, que a falta de inversión en más capacidad de red y bajo la influencia que ejerce la aparición de nuevos servicios sobre Internet que precisan de un mínimo de QoS para un funcionamiento aceptable (VoIP, VoD, IPTV, etc.), está siendo solventada con una gestión de tráfico más o menos acertada y no siempre a gusto de todos.

Así, mientras que la cuestión de inversión en mayor capacidad parece no avanzar hacia buen puerto, la industria de las telecomunicaciones ha venido desarrollando equipos y arquitecturas que son capaces de resolver algunos de los problemas de congestión y que permiten plantear nuevos modelos tarifarios. Para este fin, los métodos empleados se están basando en la identificación, clasificación y control del tráfico para su posterior tratamiento y filtrado, siendo la tecnología de análisis de tráfico DPI/DFI un elemento clave en este aspecto. Es por ello por lo que es relacionada de forma intrínseca con la Neutralidad de Red y su discusión.

Es en este ámbito donde se va a desarrollar la temática de este Proyecto, en el estudio, impacto e implicaciones de las tecnologías surgidas, y más concretamente en la tecnología DPI/DFI y su relación con la gestión de tráfico. Pese a ello, se pretende no dejar de lado las cuestiones relacionadas con la totalidad del debate de Neutralidad de Red ya que su causa y efecto están estrechamente vinculados.

Existen diferentes agentes implicados en este debate, cada cual con diferentes motivaciones e intereses, que se pueden englobar en cuatro grupos: usuarios, gobiernos o agencias reguladoras, operadores de red e ISPs y proveedores de servicio, contenidos y aplicaciones. El desarrollo de este debate es de gran importancia para cada uno de ellos y para la sociedad en general, ya que según cómo se resuelva la problemática surgida, el modelo de Internet que

conocemos hasta la fecha podría sufrir cambios considerables en varios aspectos como la accesibilidad, la QoS recibida o la tarificación.

La literatura publicada respecto a DPI/DFI y la Neutralidad de Red es extensa. Existen diversos documentos que tratan el tema sobre todo desde el punto de vista social y económico, sin atender en la mayoría de casos a razonamientos técnicos. El objetivo del presente Proyecto es, por tanto, el de realizar un estudio sobre el estado del arte de la tecnología DPI/DFI, su relación con la gestión de tráfico, las previsiones de crecimiento de este sector y su implicación e impacto dentro del debate de Neutralidad de Red. Para ello se estructura el documento en varios capítulos bien definidos.

En primer lugar se repasan brevemente en el capítulo II algunos aspectos básicos sobre Internet, su estructura y su modelo de negocio, que deben ser conocidos por el lector para situar debidamente el contexto del Proyecto. En el capítulo III se expone el debate de la Neutralidad de Red, su origen y algunos hechos relevantes acaecidos al respecto. También se resume la acción reguladora llevada a cabo a nivel internacional.

Posteriormente, en el capítulo IV se entra en el ámbito técnico de la cuestión y se describen la gestión de tráfico y algunas prácticas empleadas mediante su uso. De forma más profunda, se exponen las arquitecturas por las que el sector de las telecomunicaciones está apostando, basadas en la gestión de tráfico según QoS y servidores de políticas, ayudándose de técnicas DPI/DFI. En el capítulo V se describen y analizan las técnicas DPI/DFI, se justifica su necesidad y se relacionan con la gestión de tráfico. Se estudia su integración en las redes y algunas soluciones existentes. También se entra en los aspectos técnicos de su funcionamiento, tanto a nivel hardware como a nivel software para finalmente llevar a cabo una serie de pruebas sobre capturas de tráfico real, con el fin de visualizar algunas propiedades clave de esta tecnología y poner en práctica algunas de las consideraciones teóricas.

Por último, en el capítulo VI se estudian algunas de las implicaciones que puede tener la gestión de tráfico mediante DPI/DFI. También se valora qué puede suceder si no se aplica y se mantiene el modelo ‘best effort’. En este mismo capítulo se reflexiona sobre la polémica surgida en torno a DPI/DFI y su relación con algunos puntos críticos vinculados a la Neutralidad de Red para finalmente, en base a todo lo expuesto realizar unas recomendaciones que pueden sentar las bases para una futura aproximación reguladora.

Capítulo II – Conceptos básicos sobre Internet

Este capítulo pretende proporcionar algunos conocimientos básicos sobre Internet, tanto en el aspecto técnico y estructural como en el aspecto económico, ya que posteriormente serán necesarios para la comprensión de algunos apartados del documento.

Internet es una inmensa red de redes, un amplio conjunto de nodos que se conectan entre sí de modo que cualquier usuario que accede desde cualquier parte del mundo y con cualquier dispositivo, debería poder disponer de los contenidos, aplicaciones y servicios que éste ofrece.

Su evolución ha cambiado nuestras formas de vida de un modo asombroso, permitiendo unos niveles de comunicación e información inimaginables un par de décadas atrás. Hoy en día está presente en cualquier ámbito, y es una tecnología imprescindible para el desarrollo de nuestra actividad social, cultural y laboral.

1 Estructura de Internet

Internet se compone por miles de redes interconectadas entre sí. Resultaría muy difícil trazar una topología de Internet debido a que cada red se compone de infinidad de elementos (PCs, servidores, routers, switches, etc.) que contribuyen a formar parte de esta enorme red de redes.

Su crecimiento se ha dado sin previa planificación aunque su estructura, pese a que puede parecer caótica, mantiene un cierto orden. A nivel físico, podemos dividir Internet en dos grandes bloques, el núcleo de la red, y las redes de acceso.

1.1 Núcleo de Internet

El núcleo de Internet se compone de más de 50.000 sistemas autónomos (Autonomous System, AS) reconocidos por la Internet Assigned Numbers Authority (IANA)[3], que pueden ser organizaciones de diversa índole como universidades o empresas, ISPs, proveedores de servicios, contenidos y aplicaciones, etc.

La interconexión entre diferentes AS se realiza en función de los acuerdos que se hayan dado entre éstos. Aunque no todos los sistemas autónomos están conectados entre sí, poseen la información acerca de cómo acceder al resto, ya que en la mayoría de las ocasiones los datos tienen que viajar atravesando varios AS para llegar a su destino. Estos acuerdos se basan, a grandes rasgos, en dos modalidades que se diferencian básicamente por si el intercambio de tráfico se hace de forma gratuita o de pago.

- **Peering:** Se conoce por peering al acuerdo que suelen tomar dos o más redes independientes para intercambiar tráfico entre ellas de forma gratuita. En esta modalidad, no se intercambia tráfico para que transite desde o hacia otras redes ya que los dominios de encaminamiento permanecen inalterados.

- **Tránsito:** El tránsito se presta bajo remuneración, e implica un acceso de conectividad completa hacia y desde los destinos de Internet conocidos por las partes, lo cual requiere que se añadan las direcciones del dominio de enrutamiento del contratante de tránsito a las del ofertante de tránsito.

La conexión entre los diferentes AS puede ser remota, aunque cada vez más se tiende a la conexión en lugares físicos conocidos como los IXP (Internet Exchange Point) donde operadores e ISPs se asocian para conectar sus redes e intercambiar tráfico según los acuerdos dados.

[3] http://www.iana.org/. Entidad que supervisa la asignación de direcciones IP, entre otras labores.

1.1.1 Modelo inicial de Internet

Para comprender el origen de este tipo de acuerdos y métodos de conexión, hay que comprender la estructura de Internet, que se encuentra jerarquizada en varios niveles que van agregando a los anteriores. Se trata de una jerarquización de facto, que no está reconocida por ninguna autoridad y que ha prosperado según las leyes de mercado.

El nivel superior, o Tier-1, lo conforman el reducido conjunto de operadores que poseen visión completa de todo Internet en virtud de acuerdos de peering que han alcanzado con los demás operadores de su mismo nivel. La cobertura que ofrecen éstos es internacional, y proveen conexión a los ISPs que se encuentran por debajo de este nivel y posiblemente a otras redes de gran tamaño.

Por debajo de este nivel, se encuentran los operadores de cobertura nacional o regional, en la capa Tier-2. Los componentes de este nivel están conectados mediante acuerdos de tránsito a un operador del Tier-1, como mínimo, para poder alcanzar todo Internet. Generalmente también están conectados a otros operadores de su mismo nivel mediante acuerdos de peering o tránsito.

Éstos a su vez brindan conexión a los operadores de la capa más baja o Tier-3, conocidos como ISPs, que son los que generalmente ofrecen conexión a los usuarios finales. En esta capa, los ISPs suelen acceder a los contenidos de Internet mediante contratación de tránsito, ya que su alcance es limitado. La figura siguiente muestra un esquema de la estructura descrita.

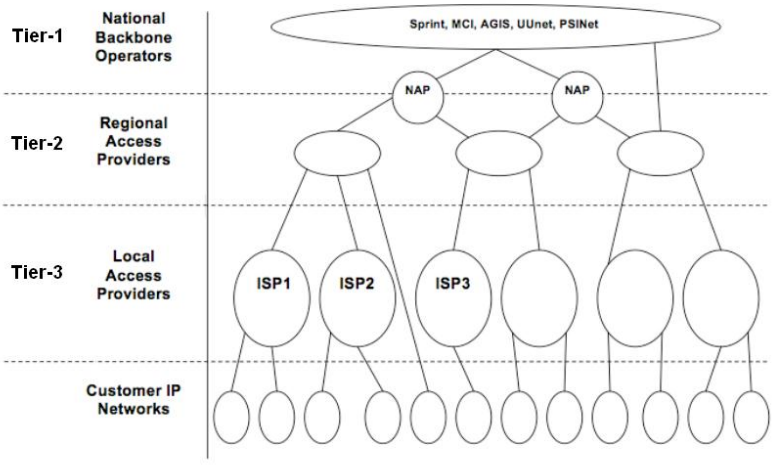

Ilustración 1: Esquema jerarquizado de Internet (1)

1.1.2 Modelo actual de Internet

La reciente evolución de las relaciones en la red ha llevado a que grandes proveedores de contenido, motores de búsqueda, operadores con grandes carteras de clientes minoristas o redes CDN (Content Delivery Network), entre otros agentes, estén pasando a formar una parte

muy importante de la estructura de Internet, de modo que se entremezclan con el modelo descrito anteriormente.

Tanto es así, que en un estudio realizado en 2009 por el ATLAS Internet Observatory (1) donde se muestra el flujo de transito recibido según el origen en un AS anónimo, se extrae que hay un fuerte ascenso de nuevos agentes como Google o Comcast, que aparecen entre los diez primeros suministradores de tráfico, junto con algunos de los ISPs del Tier-1.

Del mismo modo, también se analiza el tráfico generado por las CDN, que ofrecen un servicio de distribución de contenidos con objeto de mejorar las condiciones de acceso, reduciendo la latencia. Este estudio revela que entre las cinco principales CDN entregaban en 2009 aproximadamente el 10% del tráfico de Internet, tal y como se muestra en la gráfica siguiente.

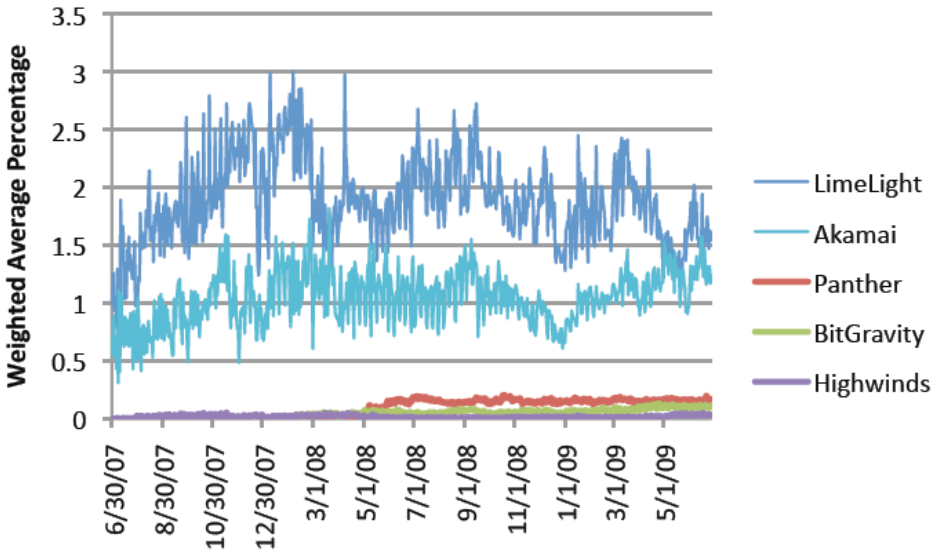

Ilustración 2: Porcentaje de tráfico generado por CDNs respecto al total de Internet (1)

Bajo esta situación, al modelo inicial de Internet se deben añadir los nuevos grandes agentes que por evolución del mercado han entrado a formar parte de esta estructura. Este hecho ha debilitado el modelo constituido por la prevalencia de los operadores Tier-1, disminuyendo los acuerdos de tránsito entre agentes y aumentando así los de peering además de otros tipos de acuerdos mixtos. Véase la figura siguiente en la que se muestra un esquema de este nuevo modelo. Se debe hacer hincapié en que este hecho no solo tiene impacto en el modelo estructural de Internet, sino que también en el económico, aspecto del que se habla en el apartado 4.3 de este capítulo.

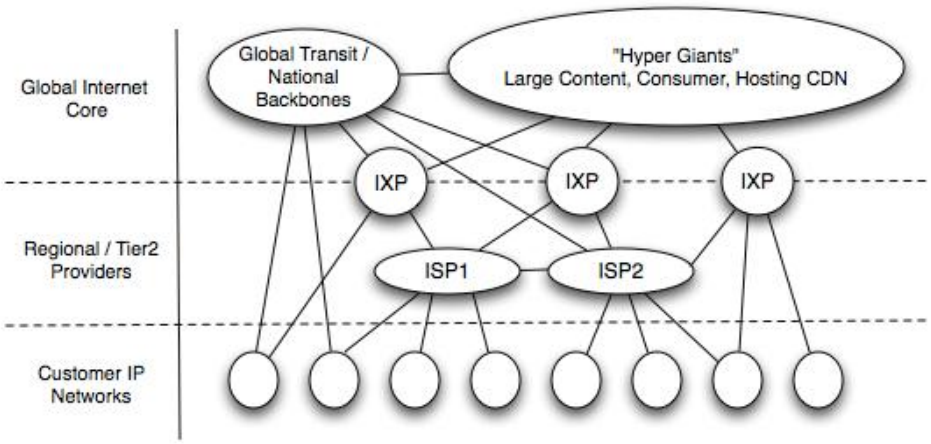

Ilustración 3: Esquema jerarquizado del Internet actual (1)

1.2 Red de acceso

Los ISPs de más bajo nivel son los encargados de prestar, bajo remuneración, el acceso a los usuarios finales. Para ello existen varias opciones, que dependen del medio y de la tecnología utilizada. En este apartado se listan y describen brevemente los medios de acceso y las tecnologías más extendidas.

- **Par de cobre:** Aprovechando el despliegue del par de cobre instalado para la telefonía fija se han desarrollado diferentes tecnologías, cada vez más eficientes, para llevar a cabo la conexión de datos sobre este medio. A nivel doméstico se suele acceder con la tecnología ADSL, el producto más extendido de la familia xDSL. Pese a algunas diferencias orientadas al tipo de servicio, flujos (necesidades de subida y de bajada) y requerimientos del usuario, las diferentes tecnologías xDSL tienen en común la adaptación al medio por el que se transmiten, es decir, el par de cobre. Es interesante remarcar la capacidad de optimización que se ha dado para este acceso, que en la versión más reciente de ADSL (ADSL2+) permite tasas de hasta 24 Mbps para el DownLink (DL) y 2,5 Mbps para el UpLink (UL).[4]

- **Cable:** Sobre la instalación de redes HFC (Hybrid Fiber Coaxial) empleadas por los proveedores de servicios de TV por cable (CATV) se comenzó también a ofrecer servicio de acceso a Internet. Pese a que se hablará más en detalle de esta tecnología en el apartado 4.2.1 del capítulo IV, cabe comentar que en este tipo de arquitectura es habitual que el ancho de banda sea compartido por varios usuarios. El estándar empleado para este tipo de comunicación es DOCSIS (Data Over Cable Service Interface Specification). Las velocidades máximas de acceso suelen superar de mucho a las de ADSL, pudiendo llegar e incluso rebasar los 100 Mbps (DOCSIS 3.0 especifica un DL 160 Mbps y UL de 120 Mbps). Además, a diferencia del xDSL, la calidad no

[4] ITU-T G.992.5 Annex M

depende de la distancia a la central, por lo que las velocidades suministradas suelen aproximarse más a los valores máximos.

- **Fibra óptica:** El auge de Internet y la demanda de velocidades cada vez superiores, que con toda probabilidad no podrán ser atendidas por par de cobre, hizo que se comenzara a comercializar los accesos de fibra, que permite tasas muy superiores. La mayoría redes empleadas se basan en el formato PON (Passive Optical Network) que se implementan sin elementos activos, es decir, que no se convierten la señal óptica a señal eléctrica hasta que no se alcanza el destino. Existen diferentes tipos dependiendo de hasta qué punto llega la fibra, de ahí el nombre FTTx (Fiber To The x), donde x hace referencia a dicho punto. Puede trabajar con velocidades muy elevadas, sobre todo en las modalidades FTTH (Fiber To The Home). La tendencia actual hace pensar que en un futuro este sea el método de acceso fijo a Internet por excelencia.

- **Radio:** El avance en el sector de las comunicaciones móviles también ha derivado en ofrecer acceso a Internet en movilidad, bien sea a través de terminales avanzados o 'smartphones', o bien con dispositivos para ordenadores. Así, se han venido desarrollando diferentes tecnologías para este fin (GSM/GPRS/EDGE, UMTS/HSPA, LTE) con tasas cada vez superiores que se pueden comparar e incluso superar a los métodos de acceso fijos. La nueva tecnología LTE de la 3rd Generation Partnership Project (3GPP), en proceso de implantación, promete ofrecer velocidades de descarga superiores a 100 Mbps por usuario.

2 El modelo OSI & TCP/IP

Debido a su relación con la definición de DPI/DFI, además de representar un pilar básico de las comunicaciones electrónicas, se expone brevemente en qué consiste el modelo OSI y también el modelo TCP/IP, que es el que realmente se emplea sobre Internet. OSI es modelo de red descriptivo creado por la ISO en el año 1984. Se trata de un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones en el que definen siete capas que hacen referencia a una división de los procesos que atraviesan los datos desde su origen hasta su destino.

- **Nivel 7:** La *capa de aplicación* interactúa y se comunica con el software, que es el encargado de realizar peticiones o envío de datos.

- **Nivel 6:** La *capa de presentación* tiene que ver con el formato en que los datos se presentan (JPEG, MPEG, etc.). Esta capa también actúa como la encargada del cifrado y compresión de datos.

- **Nivel 5:** La *capa de sesión*, crea, administra y termina sesiones de comunicaciones entre el remitente y el destinatario de tráfico de datos.

Estas tres capas componen junto con la información de usuario componen lo que se denomina la carga de un paquete, aunque en ocasiones y como veremos más adelante, también se considera como tal la capa de transporte, en la que se encuentran los puertos a los que se solicita conexión.

- **Nivel 4:** La *capa de transporte* se encarga de establecer la conexión extremo a extremo de forma independiente a las redes que atraviese. Para este fin se hace uso de los puertos, que representan un identificador de por qué vía se deben procesar los datos en cada máquina extremo.

- **Nivel 3:** La *capa de red* proporciona el direccionamiento y enrutamiento lógico, es decir, cómo un paquete se transporta entre varios nodos hasta alcanzar el destino. En el caso de Internet, el encargado de este nivel es el protocolo IP.

- **Nivel 2:** La *capa de enlace* de datos prepara el paquete para que pueda ser enviado a través de los medios físicos utilizados, lo que puede significar que lo prepara para un medio inalámbrico o bien para ser enviado a través de una conexión Ethernet. Hace uso de las direcciones MAC (Medium Access Control), que identifican unívocamente a cada dispositivo físico.

- **Nivel 1:** La *capa física* describe las características físicas de la comunicación y todo lo relativo a los detalles como los conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas.

En realidad, Internet se fundamenta sobre el modelo TCP/IP, que es previo a la definición del modelo OSI. No obstante, guarda una estrecha relación con éste y en la práctica se suele hablar de los niveles del modelo OSI aunque se esté trabajando sobre el modelo TCP/IP. La

diferencia más notable entre los modelos está en el nivel de aplicación ya que en TCP/IP se integran los niveles 5y 6 del modelo OSI en este nivel. La siguiente figura muestra las dos pilas de protocolos y las equivalencias entre ambas.

Ilustración 4: Modelos OSI y TCP/IP

Cabe señalar que en realidad estos modelos no dejan de ser algo teórico. Actualmente se pueden contar infinidad de protocolos, algunos de ellos de gran complejidad, que no se corresponden al detalle con las atribuciones definidas. Existen protocolos que llevan a cabo funciones que se atribuyen a varias capas de los citados modelos, y en ocasiones se emplean mecanismos de 'tunneling' que encapsulan protocolos dentro de otros. Pese a ello, para el propósito de este Proyecto serán útiles las funciones que se definen en cada capa, ya que tienen una estrecha relación con la definición de DPI/DFI.

3 El principio 'end-to-end'

El principio 'end-to-end' es una de las principales características del diseño de Internet. Consiste en que siempre que sea posible, las operaciones de los protocolos de comunicaciones deben llevarse a cabo en los puntos extremos de un sistema de comunicaciones, o lo más cerca posible de éstos (2).

Este principio fue expuesto en 1981 en el seno del MIT y su publicación pretendía contribuir a las consideraciones tomadas en la definición del modelo OSI de 1984. El texto original defiende que las funciones atribuidas a los niveles bajos de un sistema de comunicación pueden ser redundantes o de poco valor, y que tan solo son justificables si ofrecen una mejora al rendimiento global (3).

Esto significa que, según este paradigma, los nodos intermedios entre origen y destino sólo deben encargarse del envío de paquetes de datos, sin preocuparse por su contenido, su seguridad, o incluso del hecho de que lleguen a su destino. En efecto, los protocolos del modelo TCP/IP cumplen con este principio. El protocolo IP, que es el empleado para el enrutamiento y envío de los datos en el nivel 3, no se preocupa más que del origen y destino de los mismos, dejando al protocolo TCP las tareas de control de errores y congestión, retransmisiones, etc. con un enfoque extremo a extremo. En otras palabras, la red no posee apenas inteligencia y tan solo se encarga de transmitir lo que desde los extremos se le indica.

El hecho de que este principio se haya posicionado como un punto central sobre el diseño de Internet responde a diversos argumentos. Gracias a que la inteligencia está en los extremos, Internet se caracteriza por ser un medio apolítico y libre, en el que cualquier aplicación tiene cabida. Sobre una red que no se preocupa sobre el contenido de su tráfico es difícil mantener un control o vigilancia. En esta misma línea también se debe resaltar el hecho de que Internet sea un medio abierto a nivel económico, debido a que no existen discriminaciones debidas al origen de los datos, lo cual da las mismas oportunidades a cualquier aplicación para establecerse en el mercado de servicios.

Otro factor clave es la simplicidad tecnológica que este modelo conlleva. El hecho de no dotar de inteligencia a la red implica una flexibilidad técnica y una sencillez de procesado que de otro modo, y como veremos a lo largo de este documento, necesita de una serie de herramientas complejas. Esta simplicidad también hace que nuevas tecnologías de acceso sean fácilmente integrables en el conjunto de Internet (4).

4 Factores económicos

La economía que se ha generado en torno al sector de las Tecnologías de la Información y la Comunicación (TIC) ha venido propiciada por el éxito de Internet. Las TIC generan unos ingresos de 2.700 billones (miles de millones) de euros, cerca de un 7% del PIB mundial, y podría alcanzar el 20% de éste en los próximos 10 años (5). Hay motivos y previsiones para creer que Internet podría convertirse en la espina dorsal de nuestra economía, pasando de un modelo de economía productiva a un modelo de economía del conocimiento.

La generalización de los accesos a Internet de banda ancha ha multiplicado la demanda de contenidos e información así como de otras actividades económicas que utilizan esta plataforma para llegar a los consumidores finales. Existen novedosos modelos de negocio, cuyos ejemplos paradigmáticos son empresas como Youtube, Google, Skype o Facebook, a la vez que han surgido en la red numerosas iniciativas sin ánimo de lucro, como por ejemplo, Wikipedia.

El modelo comercial de Internet presenta ciertas complejidades que se quieren introducir, sin pretensión de exhaustividad, en este apartado. En primer lugar, se expone la cadena de valor de Internet para acto seguido analizar algunos puntos críticos que se derivan del modelo del mercado bilateral.

4.1 Cadena de valor

La cadena de valor de Internet se puede desglosar en cinco grandes bloques. Debido al carácter cambiante e innovador de Internet este modelo debe adaptarse constantemente a los nuevos cambios comerciales (6)

- **Derechos de contenidos:** En este bloque se engloban los propietarios de los derechos de contenido. El modelo comercial que adoptan intenta preservar, expandir y proteger el valor de sus servicios.

- **Servicios online:** Se entienden como tal servicios de comunicación online, motores de búsqueda, plataformas de entretenimiento, transacciones online, etc. Su modelo de negocio actual se basa generalmente en ofrecer servicios gratuitos para el usuario, y sus ingresos provienen generalmente de la publicidad.

- **Habilitación de servicio:** Aquí se funden todos los agentes que de un modo u otro, hacen posible el mantenimiento en todos los aspectos de Internet. Estamos hablando de hospedaje y desarrollo de webs y redes de distribución (CDN), pero también de proveedores de pago seguro por Internet o agencias de publicidad online. En este bloque son la innovación y el vanguardismo lo que marcan el valor del servicio. Ejemplo de ellos son el avance en los servicios de distribución, el 'cloud computing', publicidad inteligente, etc.

- **Conectividad:** Se engloban todos los operadores e ISPs. Desde los operadores de núcleo o Tier-1 hasta los operadores e ISPs minoristas, pasando por los puntos de interconexión o IXP. En este campo el mercado es competitivo y dinámico, debido al constante aumento de la demanda en las capacidades y al ajuste del precio.

- **Usuario:** Este último bloque contempla la capa de usuario tanto en la parte hardware como en la parte software. En ambos aspectos nos encontramos en un momento de expansión en cuanto a que dispositivos podemos emplear para conectarnos a Internet, así como de aplicaciones que disponemos para hacerlo de forma óptima y segura.

Ilustración 5: Elementos en la cadena de valor de Internet

Las empresas de Internet, entendiendo como tales a toda entidad que vende, comercializa, u ofrece servicios, requieren de las redes para su actividad. No sólo las utilizan sino que se benefician de las acciones y mejoras que realizan los operadores y las agencias públicas, tales como la extensión de la cobertura, las acciones para el incremento de la penetración de los servicios de banda ancha o las mejoras en la capacidad de las redes.

A su vez, los operadores se benefician del incremento y variedad de las aplicaciones en la red en la medida en que hacen más atractiva la contratación de los servicios para los usuarios. No obstante, si se analiza eslabón por eslabón, se detecta uno de los factores que más dan que hablar sobre este modelo de negocio y que desatan una buena parte del debate de Neutralidad de Red. En el gráfico siguiente, extraído de un estudio realizado por A.T.Kearney (6), se muestra la evolución de la capitalización de los diferentes grupos de la cadena de valor (base 100 en 2004).

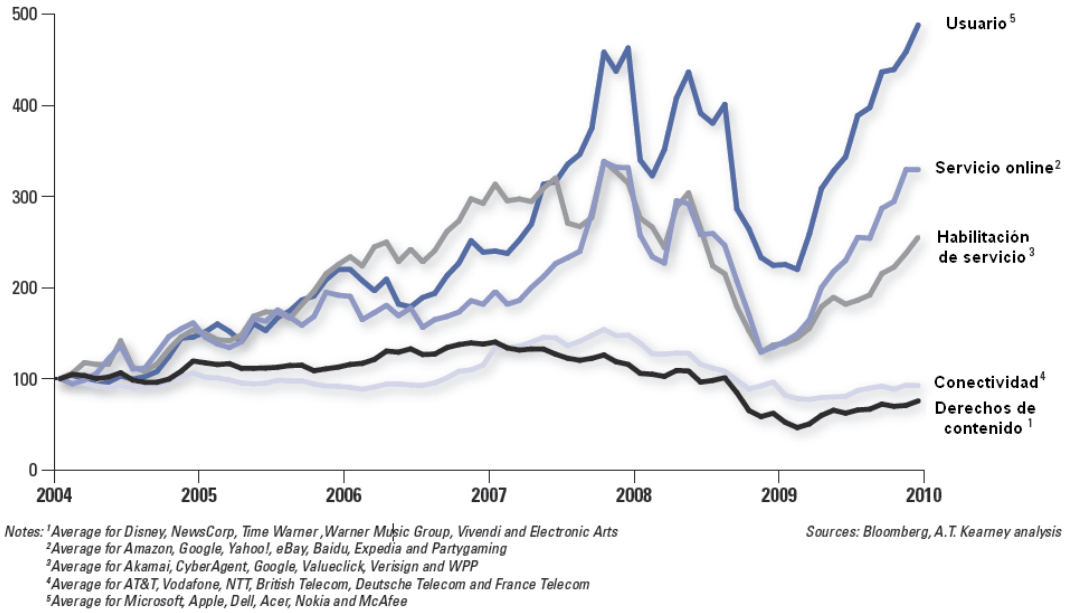

Ilustración 6: Evolución por sectores del mercado de Internet (6)

Como se puede observar, el crecimiento en los sectores de servicios online y de habilitación de servicios supera notablemente al de conectividad. Cabe comentar en este punto que existen ciertas críticas al estudio sobre el que se realiza la gráfica. En relación a los datos en los que se basa, se ataca la elección de empresas exitosas para el sector de servicios online, con lo que se dice se falsea el resultado marcando un mayor distanciamiento con el sector de conectividad, donde se ubican los operadores (7). Si bien este es un hecho que admite consideración, también es cierto que los operadores seleccionados para el estudio son algunos de las más notables que lideran el sector, con lo que la equiparación parece ser equilibrada. En cualquier caso, esta crítica pone de relevancia las dos partes del problema, lo cual justifica una de las motivaciones del Proyecto.

Desde el punto de vista de los operadores, el comportamiento de la gráfica se achaca a la fuerte inversión que éstos deben llevar a cabo para garantizar el funcionamiento de las redes, ya que son los únicos encargados de gestionarlas y de mantenerlas. También suele estar generalizada la visión en el sector de los operadores de que hay quien se está enriqueciendo, básicamente los proveedores de servicios, aplicaciones y contenidos, a costa de esta situación. Ejemplo de ello son las declaraciones del CEO (8) de SBC y posteriormente de AT&T (operadores estadounidenses), Edward Whitacre, en una entrevista el año 2005 dónde declaraba que Internet no puede ser gratuito para Google, MSN y demás. Afirmaba que los operadores poseen las redes, que han invertido un capital y que esperan un retorno sobre esta inversión. Declaraciones muy similares hizo en España el presidente de Telefónica, César Alierta, en el año 2010 (8).

Por otro lado, los proveedores de servicios, aplicaciones y contenidos, se muestran en general partidarios a mantener una red abierta. En 2009, varios de los proveedores de servicio más

influyentes de los EEUU y del mundo (Google, Facebook, Skype, Youtube, Amazon, eBay, etc.) enviaron una carta al presidente de la Federal Communications Commission (FCC), dándole su apoyo en la lucha por preservar la Neutralidad de Red y alegando que "*los empresarios, tecnólogos y capitalistas de riesgo han sido capaces de desarrollar nuevos productos y servicios en línea acorde con la garantía de acceso neutral y no discriminatorio para los usuarios, que ha impulsado una era sin precedentes de crecimiento económico y creatividad*". En el mismo texto también defienden que "*las empresas ya existentes han sido capaces de aprovechar el poder de Internet para desarrollar líneas de productos innovadores, llegar a nuevos consumidores y crear nuevas formas de hacer negocios. Internet abre un mercado competitivo y eficiente. Esto permite competir a las empresas de todos los tamaño*" (9).

Al margen de ésta controversia, lo que es un hecho es que la capacidad de la red aumenta a un ritmo elevado. El tráfico de datos se ha venido multiplicando aproximadamente por cuatro cada dos años y la popularización de los 'smartphone' está desembocando en problemas de congestión de las redes móviles. Según datos de Cisco, el tráfico en los últimos cinco años se ha multiplicado por ocho y crecerá hasta cuatro veces más en los próximos cinco (10). Ante esta situación, los operadores parecen no querer mover ficha en la inversión de mayor capacidad de red, pretendiendo que este coste se reparta también con los proveedores de servicio.

Como se puede apreciar, se trata de un asunto no trivial, en el que existe una cierta tensión entre operadores e ISPs frente a proveedores de servicios, aplicaciones y contenidos. El motivo de esta controversia tiene una gran base en el modelo económico sobre el que se sustenta Internet, aunque existe otra vertiente ligada intrínsecamente a la manera en que Internet ha llegado a ser lo que es, es decir, a su carácter abierto y libre. En el ámbito económico, cabe analizar Internet con el modelo denominado mercado bilateral.

4.2 El mercado bilateral

Para exponer este concepto se hace uso de un sencillo símil: un recinto de exposición. En un evento de este tipo, una empresa organizadora se encarga de la infraestructura, es decir: montar las carpas, pedir los permisos, habilitar las condiciones necesarias, etc. En una situación normal, las diferentes entidades que quieran tener su espacio en la exposición deberán pagar al organizador una cuota por anunciarse o vender sus productos. Por otro lado, el usuario que quiera asistir al recinto también deberá pagar una cierta cantidad para acceder a los servicios que se ofertan. Si la situación está en equilibrio todo el mundo sale beneficiado.

Partiendo de esta situación, imaginemos que la exposición ha tenido mucho éxito. Todos los anunciantes y vendedores quieren tener su espacio, y más y más gente desea asistir a dicho evento. El organizador se verá presionado para que amplíe la infraestructura y dar cabida a todos los usuarios y anunciantes, pero si nadie está dispuesto a invertir en dicha infraestructura y el organizador tiene ya un buen modelo de negocio, no querrá ampliar si no prevé obtener más beneficios.

Si bien es un símil muy simplificado, es una buena aproximación de lo que está sucediendo con Internet. En un lado del mercado, estan los usuarios que utilizan los servicios de acceso que les proporciona el ISP, mientras que en el otro estarían ubicados los proveedores que utilizan la infraestructura para proporcionar sus productos a los usuarios finales. De acuerdo con la teoría del mercado bilateral, podría pues plantearse la posibilidad de que los proveedores de servicios y aplicaciones pagaran a los ISPs lo cual redundaría en teoría en una disminución de los precios de los abonados y por consiguiente en un incremento de la demanda de servicios de acceso.

Sin embargo, esta aproximación también ha sido criticada atendiendo a diversos argumentos. Por ejemplo, en base a la existencia de efectos de red (el valor de la red es mayor como mayores son los elementos conectados), a la existencia de beneficios que no son meramente económicos (por ejemplo, el beneficio que supone la puesta a disposición de información sin un ánimo directo de lucro) o el efecto positivo sobre la innovación que supone el modelo actual al poder cualquier agente ofrecer sus productos a la totalidad de usuarios de Internet sin tener que efectuar ningún pago más que el de acceso por ello.

Aunque el análisis de este modelo económico se sitúa fuera del ámbito de este Proyecto, es necesario mencionar que las teorías económicas formulan que en este tipo de mercados se maximiza el bienestar social fijando precios a ambos lado del mercado en función de las elasticidades de las respectivas funciones de demanda. No obstante lo anterior, existen otros factores, como la presencia de externalidades, que también tienen un impacto en dichos sistemas de fijación de precios (11).

4.3 El mercado de acceso e interconexión IP

Para comprender el origen de la discusión de Neutralidad de Red se debe conocer también el mercado de operadores e ISPs, que se puede desglosar a varios niveles. En el núcleo de Internet, tradicionalmente los ingresos obtenidos por los operadores Tier-1 han sido debidos al tránsito de Internet en la interconexión IP, ya que un ISP de nivel bajo nivel debe contratar-lo para tener visibilidad completa de Internet. No obstante, la evolución de grandes agentes tales como Google (un 6,4% del tráfico total de Internet) (12), Microsoft o Yahoo!, (13) que han implementado sus propias redes y transmiten su tráfico mayoritariamente mediante acuerdos de peering, está transformando este modelo. La demanda de estos servicios condiciona a los ISPs a ceder a acuerdos, Google por ejemplo, se conecta por peering a cerca del 70% de ISPs (12). A raíz de esta situación han ido perdiendo fuerza los grandes operadores Tier-1 debido al tránsito, y por contra han aumentado los ingresos de los mayores proveedores de servicios debidos a la publicidad. Estas cifras están en consonancia los datos comentados anteriormente acerca de los ingresos en los diferentes sectores. Este planteamiento conforma uno de los aspectos de la Neutralidad de Red, que se analizaran en el apartado 3 del siguiente capítulo.

A un nivel más bajo, en los accesos, es donde se encontrarían operadores e ISPs de Tier-2 y Tier-3. Se debe tener en cuenta además en entornos regulados la figura del operador mayorista (generalmente posicionados como Tier-2). Éste es aquel que posee una red de

acceso propia y que mediante acuerdos mayoristas (comerciales o regulados) permite la conexión entre el cliente final (conectado a la red del operador mayorista de acceso) y el ISP al que el cliente final contrata su servicio de acceso a Internet. Generalmente el operador mayorista es un agente verticalmente integrado, es decir, un operador que también proporciona el servicio de acceso a Internet (además de posiblemente otros servicios dedicados) a clientes finales haciendo uso de su red. Por lo tanto, el operador mayorista compite con el ISP minorista a la par que posibilita su conexión con el usuario final (esta situación es la que se da en la mayoría de países europeos, y también en Canadá). Para que en este contexto no se produzcan situaciones de abuso o anticompetitivas, se hace necesaria una regulación del mercado que salvaguarde la competencia entre ISPs.

Se debe tomar en consideración que es básicamente por los accesos por lo que el conjunto de operadores e ISPs obtienen sus ingresos. En los entornos regulados se estimula la competencia para acabar ofreciendo mejoras al usuario final por lo que los operadores mayoristas deben ceder los accesos a terceros. El hecho de que la regulación fije el precio que deben pagar los ISPs a los operadores mayoristas por el acceso, puede hacer frenar la iniciativa de inversión en éstas. En los EEUU, como veremos más adelante, este modelo de regulación no se da por lo que las consideraciones aquí tomadas no aplican, no obstante sigue planteándose la discusión de que se enriquecen los proveedores servicio, aplicaciones y contenidos a costa de la inversión de los operadores e ISPs, alegando estos últimos que existe poco margen de maniobra para explotar su modelo de negocio.

En relación a como se financian los operadores e ISPs es también de destacar también la forma en que se paga generalmente por el acceso: la tarifa plana. Este modelo de contrato puede verse como algo beneficioso para el usuario final, ya que con él tiene un control sobre el gasto económico sin tener que preocuparse por limitaciones, pudiendo fácilmente interactuar a través de Internet. Desde el punto de vista de los ISPs este formato cada vez es menos deseado, ya que las demandas mayores saturan las redes y no reparten bien los costes. El hecho de que se siga ofertando se debe básicamente a una cuestión de competencia y simplicidad de gestión, y podría acabar desapareciendo. La siguiente ilustración muestra un plan tarifario aplicado en Colombia para telefonía móvil que pretende corroborar este hecho.

Ilustración 7: Planes de Internet móvil ofrecidos por Telefónica Colombia (14)

Por otra parte, en el ámbito móvil las condiciones de acceso han hecho que se dé un caso especial. El formato de tarifa plana (en muchos casos limitada a una cantidad de descarga) que se oferta para los accesos de banda ancha junto con la creciente demanda de servicios de correo electrónico, chat y VoIP está afectando al modelo de negocio de los operadores, ya que compiten con sus servicios tradicionales (voz, SMS, MMS) de forma directa y más agresiva que en el escenario fijo. El argumento de que existe una limitación en el acceso radioeléctrico ha dado alas a los operadores móviles para gestionar su tráfico, y en general esto ha derivado en una cierta permisividad en este escenario en cuanto a su relación con la Neutralidad de Red.

Para dar una idea más detallada sobre los flujos monetarios relacionados con el tráfico de Internet en el siguiente esquema se muestran diferentes situaciones simplificadas cómo se accede y quiénes pagan para consumir o para proveer contenido. En el lado del usuario final el procedimiento es claro, éste paga por un acceso a Internet a su ISP. La parte más interesante se encuentra en la interconexión y pago entre proveedores de servicio y operadores, ISPs o CDNs.

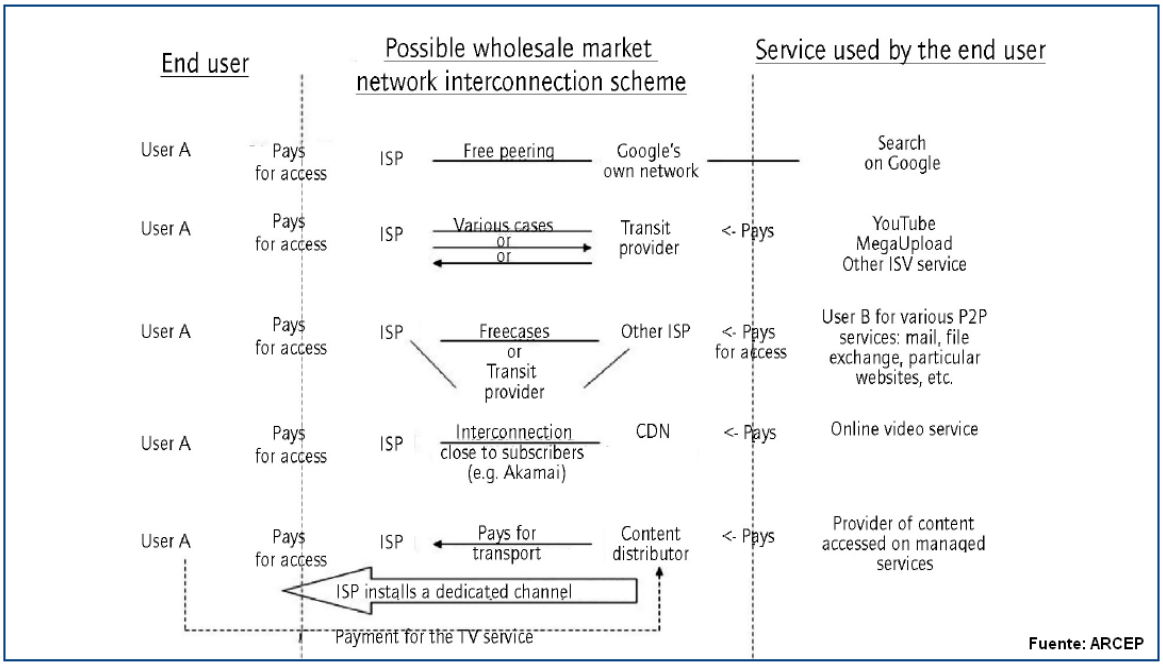

Ilustración 8: Modelo de ingresos en la interconexión IP (5)

En el primero de los casos, se estaría dando una situación como la comentada anteriormente en la que un proveedor de servicio se conecta a un ISP mediante acuerdos de peering. El segundo caso muestra la situación que se daba en el modelo inicial de Internet (véase apartado 1.1.1) en la que un ISP de bajo nivel acuerda con un operador situado en una capa superior (Tier-2 o Tier-1) el acceso al tráfico ofrecido por un tercero. El tercer caso muestra un intercambio de tráfico P2P (Peer To Peer), que suele darse entre ISPs de bajo nivel por las características de estos protocolos. El cuarto caso incluye el servicio ofrecido por las CDNs, que en la práctica pueden ser vistas como una red paralela a Internet, cobrando por acercar los contenidos a los usuarios y poder ofrecer así una mejor calidad. El último caso es similar al

cuarto, pero se resalta la reserva de canales dedicados para servicios Over The Top (OTT), que es como se suele denominar a los servicios habituales como VoD, VoIP sobre Internet, videoconferencia, etc.

Para acabar de tener una visión sobre el modelo comercial de los ISPs resulta también interesante ver los servicios que éstos ofrecen, y que se relacionan con el último caso expuesto en referencia a los servicios dedicados. En la actualidad un ISP generalmente proporciona conectividad telefónica, acceso a Internet y en muchos casos también IPTV. Así, se entremezclan servicios verticales que son ofrecidos por el operador cómo la telefonía y la IPTV, con servicios que provienen de terceros a través de Internet. Este hecho, como se verá a lo largo del documento, está muy relacionado con el foco del debate de Neutralidad de Red.

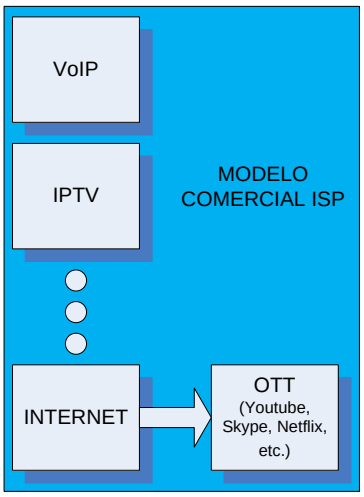

Ilustración 9: Modelo comercial ISP

Dada esta estructura de flujos monetarios, la evolución hacia los nuevos servicios que provee Internet como TVIP, streaming o descarga directa avanzan a un ritmo constante. Este tipo de servicios exigen una gran tasa de transferencia de datos o en algunos casos una mínima garantía de QoS para su usabilidad. Por ello y por las crecientes situaciones de congestión en las redes, se está derivando en un modelo basado en la discriminación de servicios, que en su versión más extrema podría llegar a acabar con el modelo actual 'best effort' y tender a la aplicación de planes específicos según la demanda de consumo de los clientes. Este hecho representa una de las bases del debate sobre la Neutralidad de Red, que se abarca en el siguiente capítulo.

Capítulo III – Neutralidad de Red

En este capítulo se define el concepto de Neutralidad de Red, sus orígenes y las líneas de actuación que se están dando a nivel global. Se pretende con ello dar una visión sobre qué aspectos abarcan la discusión y qué agentes hay implicados.

La Neutralidad de Red es la postura de quienes defienden la igualdad del tráfico sobre Internet. Sus principios surgen en relación a la creciente problemática de los flujos monetarios en torno a Internet, analizada en el capítulo II. Las posibles soluciones que se plantean para abordar este problema, llevan a una corriente de propuestas que hacen peligrar el carácter abierto y libre que ha definido Internet hasta ahora.

Sus principios tienen por fin estimular que Internet sea una herramienta abierta y libre, que aporte el máximo a la sociedad sirviendo como plataforma a la innovación y facilitando la máxima interacción entre personas. Esta visión se basa en afirmar que una red pública que maximice la usabilidad de ésta debe tratar cualquier contenido, sitio o plataforma por igual. En términos técnicos esto se asocia al principio 'end-to-end' descrito en el apartado 3 del capítulo II.

1 Origen del debate

El foco de la discusión de la Neutralidad de Red se ha dado en los EEUU, debido a algunos factores de su modelo de mercado que se diferencian al modelo europeo, sobre todo en las redes fijas. En Europa se ha trabajado para estimular el mercado con medidas como en el LLU (Local Loop Unbundling) o el acceso mayorista 'bitstream', entre otras, que han ayudado a que exista competencia entre ISPs.

Por el contrario, en los EEUU no se ha conseguido estimular una competencia real, por lo que la situación ha derivado en un mercado con operadores minoristas a nivel local, que constituyen en muchas ocasiones un monopolio de facto (o un duopolio entre proveedores DSL y cable). Esto implica un riesgo elevado, pues dificulta la vigilancia y da pie a la aplicación de políticas propias y en ocasiones poco éticas (5). Debido a esta situación y como se verá a continuación, es en los EEUU donde más intensamente se ha vivido el debate y donde más casos de violación de los principios de la Neutralidad de Red se han dado. De hecho, es probable que si en los EEUU se diera un escenario competitivo, toda esta discusión no hubiese adquirido la dimensión que actualmente tiene (15).

La definición de Neutralidad de Red se atribuye a Tim Wu, profesor de la Columbia Law School, que aplicó este nombre retomando un concepto de las antiguas redes telegráficas, en las que no se podía discriminar según el contenido o procedencia de los mensajes. En 2003 presentó un documento bajo el título de "Network Neutrality, Broadband Discrimination" (16), en el que preveía, antes de que se hubiesen dado hechos que lo justificasen, una cierta problemática futura y cada vez más creciente entre los intereses privados de los ISPs y operadores y el interés público por un Internet competitivo e innovador.

Los aspectos iniciales que originaron el debate de la Neutralidad de Red, según el propio Wu, se centraron en cuatro puntos clave, que mantienen cierta relación con lo que a día de hoy se sigue discutiendo. Así, preveía problemas en cuanto: a bloqueo de aplicaciones, servicios o contenidos; una posible tendencia de monopolización de ISPs sobre sus clientes, pudiendo cobrar un precio de terminación a terceros; una priorización de ciertos proveedores de servicio, aplicaciones o contenidos según acuerdos comerciales con ISPs; y una falta de transparencia (17).

Las ideas de Wu hacen una clara diferenciación entre las redes públicas y las redes privadas. Se entiende que una red es privada cuando no está interconectada con otras redes, y dentro de este ámbito se justifica el empleo de cualquier técnica de gestión y diferenciación (por ejemplo, en las redes de TV por cable) ya que en estas redes la discriminación de contenidos es una parte intrínseca de los servicios que ofrece. Sin embargo, en una red pública e interconectada, la discriminación en un punto de la red puede afectar a otro.

2 Casos destacados

Veremos en este subcapítulo algunas de las acciones que han desatado la denuncia social. Si bien no han sido especialmente numerosas, sí que se les ha dado notable importancia (sobre todo en los EEUU) y de hecho, si se ha magnificado el debate de la Neutralidad de Red es en gran parte debido a algunas de estas acciones, que han hecho encender la alarma y han llevado a discutir qué técnicas de gestión de tráfico son o no permisibles.

La mayoría de casos han surgido en torno a dos tipos de tráfico que son críticos para los ISPs y operadores. Se trata del tráfico P2P y de la VoIP. El primero es crítico y molesto para ISPs en general, debido a que consume un ancho de banda elevado y ocupa grandes proporciones de la capacidad de la red, se estima que aproximadamente el 23% del tráfico total de Internet, aunque ha llegado a suponer un porcentaje más elevado (actualmente está en decrecimiento, en gran parte debido al auge de servicios de streaming) (10) (18). El segundo es crítico sobre todo en operadores tradicionales de telefonía que a la par son ISPs, ya que entra claramente en conflicto con su modelo de negocio de voz tradicional.

En la Unión Europea se han reportado algunos casos de acciones contrarias a la Neutralidad de Red, aunque en general no han tenido tanto impacto mediático como en Norteamérica. Así, según el grupo de reguladores europeos BEREC (Body of European Regulators for Electronic), han habido casos de (19):

- Limitación de P2P & streaming en Francia, Grecia, Hungría, Lituania, Polonia y Reino Unido.

- Bloqueo o cargos extra en telefonía móvil por el uso de VoIP en Austria, Croacia, Alemania, Italia, Holanda, Portugal, Rumania y Suiza.

Como casos recientes más destacables se pueden citar los siguientes. En Alemania, en abril de 2009, el principal operador móvil T-Mobile anunció que estaba bloqueando la aplicación Skype, alegando que se aplicaba esta política para evitar problemas de congestión (20)

En el Reino Unido, entre 2009 y 2010, se produjo una reducción de la tasa para el acceso al servicio conocido como iPlayer, de la BBC. British Telecom introdujo una política de restricción de la tasa de streaming permitida en el periodo de tiempo que estaba dando problemas de congestión (17:00h – 00:00h) (21). Otros casos que han tenido un cierto eco han sido los de las compañías servidoras de publicidad NebuAd y Phorm. Se dieron prácticas de inyección de publicidad objetiva previo análisis DPI de las preferencias de los usuarios (2). En concreto, NebuAd lo llevó a cabo mediante DPI, utilizando esta tecnología para escanear los paquetes y luego insertar código JavaScript haciéndose pasar por el servidor origen (22) (23) (24).

En Holanda, en junio de 2011 se aprobó una reforma de Ley a favor de la Neutralidad de Red, la cual está expuesta en el apartado 4.1 del anexo A. Esta decisión fue una reacción al plan de uno de los proveedores más influyentes del país, KPN, de adoptar un plan tarifario que pretendía incluir un coste extra por el uso de los servicios de mensajería como WhatsApp[5] o de

[5] http://www.whatsapp.com/. Servicio de mensajería instantánea sobre Internet para terminales móviles.

VoIP como Skype. Se ha sabido además que también en Holanda, T-Mobile llevaba a cabo bloqueos de VoIP y que KPN y Vodafone utilizaban DPI/DFI para identificar los paquetes de datos enviados a través de las aplicaciones citadas (25).

Más importantes fueron los casos que se dieron en Norteamérica, desde el año 2005 y en pleno inicio de este debate. Por aquel entonces ya se observaba la intención de preservar la Neutralidad de Red por parte de la FCC, como quedó constancia en el caso Madison River, en las condiciones que el regulador impuso para las fusiones de SBC con AT&T y la de Verizon con MCI y más adelante en 2007, con el caso Comcast.

Caso Madison River Communications

En marzo de 2005, meses antes de la primera declaración de principios para preservar la Neutralidad de Red por parte de la FCC (ver anexo A), se mostró por primera vez la disposición del regulador a preservar el carácter libre de la red. La FCC procedió a la apertura de una investigación sobre Madison River Communications, debido a que este operador local de telefonía empleaba técnicas de gestión de tráfico para bloquear tráfico según los puertos utilizados por servicios de VoIP. El caso se resolvió sin llegar a finalizarse la investigación, habiendo aceptado la empresa dejar de discriminar en contra del tráfico VoIP y haciendo un pago voluntario de 15.000 $ al Tesoro de EEUU (26). Si bien no se trata de un precedente formal, ya que no se establece oficialmente que se hubieran violado las leyes, sí que se hizo visible la intención por parte de la FCC de hacer cumplir unos principios asociados a la Neutralidad de Red.

Caso Comcast

Este caso tuvo mucha repercusión debido a su relación con las normas propuestas por la FCC. En 2007 grupos de consumidores denunciaron ante la FCC que la compañía proveedora de servicios por cable Comcast estaba haciendo uso de técnicas de gestión de tráfico para interrumpir y degradar el tráfico P2P (en especial el tráfico de la aplicación BitTorrent) por su red.

Aunque en principio Comcast negó rotundamente alguna relación con estos sucesos, más adelante se evidenció que se estaban reiniciando conexiones P2P entre usuarios de Comcast, mediante el envío de paquetes TCP RST y empleando tecnología de Sandvine, concretamente el equipo *PTS8210,* el cual se cita en el apartado 3.1.1.1 del capítulo V (27) (28). De este modo se conseguía que las aplicaciones buscasen nuevos 'peers' fuera de la red de Comcast (aproximadamente la mitad de las peticiones de conexión P2P que recibía el competidor Time Warner provenía de la red de Comcast) (29). Finalmente la compañía de cable, afirmó que se estaba haciendo uso de técnicas de gestión de tráfico, aunque alegando que se trataba de una medida para garantizar la eficiencia en su red.

Ante la presión de la situación, en marzo de 2008 Comcast y BitTorrent acordaron trabajar juntos para gestionar de forma efectiva el tráfico en momentos de pico. No obstante, en agosto de 2008, la FCC consideró que Comcast había cometido una infracción por prácticas consideradas discriminatorias y contrarias a los principios de la 'Internet Policy Statement' (véase apartado 2.1 del anexo A) y tomó medidas contra Comcast por aplicar técnicas de gestión no razonables y por impedir a sus consumidores acceder al contenido deseado. Concretamente, la FCC ordenó a Comcast revelar los detalles de sus prácticas de gestión en un plazo de 30 días, presentar un plan de cumplimiento para poner fin a las prácticas infractoras a finales del año, y dar a conocer al público los detalles de su compromiso de prácticas en el futuro (30).

Comcast, por su parte, apeló la decisión cuestionando abiertamente la autoridad de la FCC para dictaminar acerca de las prácticas de gestión usadas, aunque previamente había acordado compensar a los posibles afectados por sus prácticas de gestión con hasta 16 millones de dólares (27) (29). El caso finalmente acabó con la resolución por los tribunales sentenciando que la FCC no dispone de suficiente autoridad para regular este campo.

Caso Bell Canada

El caso más destacado en Canadá fue el del operador Bell Canada en 2008, debido a que recibió una denuncia por parte de la CAIP (Canadian Association of Internet Providers), una asociación de ISPs, por la ralentización de paquetes P2P (31). La ralentización se producía tanto a nivel minorista como mayorista en su servicio Gateway Access Service (GAS), que es la denominación que recibe el mecanismo por el cual los ISPs se conectan a la red de Bell Canada (32).

Bell Canada admitió hacer uso de técnicas de gestión de tráfico para degradar el tráfico P2P en periodos de pico, aunque alegó que dichas prácticas eran necesarias para garantizar un buen funcionamiento de sus redes. En un principio tan solo aplicaron las medidas a sus clientes minoristas aunque meses más tarde determinaron que esta medida no resolvía los problemas de congestión, y decidieron aplicarla a también a sus clientes mayoristas en el servicio GAS. Al estarse aplicando tanto a sus clientes mayoristas como a sus clientes minoristas, alegaron que con esta medida no se afectaba a la competencia (27). Por este motivo, la Canadian Radio-Television and Telecommunications Commission (CRTC) finalmente dictaminó que no se trataba de una medida discriminatoria aunque a raíz de este hecho se lanzó una consulta pública que posteriormente derivó en unas reglas de la CRTC (ver apartado 8 del anexo A).

3 Aspectos de la Neutralidad de Red

A raíz de acciones como las comentadas en el apartado anterior, empezó a tomar forma la defensa de Neutralidad de Red por parte, sobre todo, de grupos de usuarios y proveedores de servicios, contenidos y aplicaciones. Según éstos, los intereses de los operadores e ISPs frente a la situación a la que se ha llegado en cuanto al uso y explotación de Internet, hace peligrar varios aspectos del modelo actual.

Así, según sus defensores, existen varios elementos que debido a la dinámica que está siguiendo el mercado, hacen temer por la Neutralidad de Red. Aunque es difícil definirlos de forma unívoca ya que mantienen entre sí una fuerte relación, a continuación se clasifican según varios de los aspectos más relevantes.

- **Competencia:** Influencia de los operadores de red con mayor poder de mercado para imponer sus políticas de gestión de tráfico y tarificación. Un buen modo de solventar este problema es que se estimule la existencia de varios ISPs.

- **Accesibilidad:** Derecho de los usuarios para poder acceder a cualquier contenido o servicio sin importar el medio de acceso o dispositivo sobre el que realice la conexión. Este punto afecta sobre todo al acceso móvil debido a que el medio físico para el acceso radio es más limitado que el fijo.

- **Transparencia:** Derecho de los usuarios a conocer, entender y comprobar los parámetros contratados, así como las posibles medidas de gestión de tráfico empleadas. Dado que la mayoría de clientes no son capaces de comprender los servicios que están contratando y mucho menos de analizar si se cumplen los parámetros establecidos, se pide en este sentido que se expongan los parámetros contratados y las medidas que se puedan llevar a cabo de forma clara y comprensible.

- **Bloqueo:** Prohibición del acceso a un cierto contenido, servicio o aplicación. Este procedimiento es considerado el más radical contra la Neutralidad de Red. Se puede dar por varios motivos, aunque normalmente se relaciona con tipos de tráfico molestos o poco deseados por los ISPs, como en el caso de tráfico P2P o VoIP. También podría darse debido a acuerdos comerciales o estratégicos entre ISPs y proveedores de servicio, por ejemplo.

- **Discriminación:** Dar un trato diferente a los paquetes según sea su procedencia o tipo de protocolo o aplicación, por ejemplo. Este procedimiento es contrario al principio 'end-to-end' visto en el apartado 3 del capítulo II y al modelo 'best effort'. Pese a ello, es una práctica bastante asentada en momentos de congestión. Para llevarla a cabo se emplea gestión de tráfico mediante DPI/DFI, como se analizará en los siguientes capítulos.

- **Diferenciación:** Ofrecer sobre el mismo acceso a Internet otros servicios dedicados como IPTV o VoD, por ejemplo, otorgándole unos parámetros QoS mejores que al

acceso a Internet. Nótese que no se incluye en este apartado la VoIP, debido a que se suele enfocar como un servicio a parte tal y como ha venido haciéndose con la telefonía tradicional.

- **Tarificación:** Modificar el formato de pago por los accesos a Internet. Podrían darse varios escenarios, por ejemplo el pago según los servicios disponibles (ver Ilustración 7) o según planes de QoS contratada. Este punto está en estrecha relación con los anteriores, en el primer caso porqué se estaría dando un caso de bloqueo, mientras que en el segundo se podría considerar un caso de discriminación.

- **Interconexión IP:** Prácticas de priorización o limitación del ancho de banda en la interconexión de nodos del núcleo de Internet. La situación que se ha dado en el modelo de Internet (ver apartado del 1.1.2 capítulo II) puede dar a lugar a acuerdos para el intercambio de tráfico que perjudiquen al usuario final.

- **Innovación:** Impacto que podría causar a la innovación la tarificación y la discriminación según contenidos o QoS. Estas prácticas implicarían que los contenidos no serían accesibles para todos los usuarios de Internet, o al menos no con las mismas condiciones que al resto de contenidos, afectando a la posibilidad de que una nueva aplicación, servicio o contenido se popularizarse, por el simple hecho de no ser accesible a todos los usuarios de Internet.

- **Privacidad:** Posibilidad de interceptar y comprender las comunicaciones de los usuarios sobre Internet. Debido a que las tecnologías empleadas para la gestión de tráfico suelen emplear la tecnología DPI, que es capaz de analizar al detalle el contenido de un paquete no cifrado, se teme por la pérdida de privacidad en las comunicaciones sobre Internet.

- **Libertad de expresión:** Limitación del acceso o uso de aplicaciones servicios o contenidos para la información y opinión. Debido a que Internet se ha convertido en un elemento clave en las comunicaciones modernas, se teme por la capacidad de censura que pueda adquirir un ISP o entidad gubernamental debido a la aplicación de medidas de gestión de tráfico, filtrado e inspección poco éticas. También podría verse afectada por los mismos motivos comentados en el caso de la innovación.

Para combatir algunas de estas tendencias se han venido asentando una serie de principios que componen la base de la Neutralidad de Red y que pretenden prevenir situaciones como las aludidas. Como se analiza en el siguiente apartado y se detalla en el anexo A, varios de los países más influyentes del mundo se han pronunciado al respeto, contribuyendo también a sentar estas bases. Así, según sus defensores, existe una visión más o menos generalizada de que para garantizar un Internet que maximice el beneficio social se deben cumplir los siguientes requisitos.

- **No se debe limitar el acceso a ningún contenido, servicio o aplicación legal de Internet.**
- **Los usuarios deben ser capaces de conectar cualquier dispositivo a Internet.**
- **Los usuarios deben poder escoger entre diferentes ISPs y proveedores de servicios, contenidos y aplicaciones.**
- **Cualquier gestión llevada a cabo por un ISP debe ser transparente e inteligible para el usuario final.**
- **No debe aplicarse gestión de tráfico sobre Internet, excepción hecha de su empleo en momentos de congestión tratando todos los paquetes por igual o por motivos de seguridad.**

4 Contexto internacional

El debate originado en relación a la Neutralidad de Red ha acabado involucrando a gobiernos y/o agencias reguladoras de gran parte de los países desarrollados. De forma genérica, las líneas de actuación han seguido una actitud pasiva, probablemente a la espera de que se dé una necesidad demostrable para tomar una posición firme. No obstante ha habido algunas excepciones, y algunos Estados han llevado más allá la cuestión y han incluido la Neutralidad de Red en su legislación (Chile y Holanda).

En este apartado se desarrolla una extracción de los datos más relevantes de los pasos dados a nivel internacional. Para ello, se muestra en la siguiente tabla un resumen en base a algunos de los parámetros más destacados en las diferentes aproximaciones reguladoras en cuanto a la Neutralidad de Red, para los Estados que más influyentemente se han pronunciado al respecto. Se han empleado algunos de los ítems que hacen referencia a la Neutralidad de Red especificados en el apartado anterior, listados de modo que una mayor concentración de '+' se denote una posición estricta favorable a la Neutralidad de Red, y por tanto a mayor número de '-'más distante a ésta.

ITEM	EEUU	Chile	Holanda	Francia	Reino Unido	Canadá
Accesbilidad	*	+	+	+	+	+
Transparencia	+	+	+	+	+	+
No-Bloqueo	*	+	+	+	+	+
No-Discriminación	*	+	+	+	*	-
No-Tarificación	+	*	+	*	-	-
No-Diferenciación	-	*	-	-	-	*

Ilustración 10: Comparativa aproximaciones regulatorias (+: a favor; *: neutro / ambiguo; -: en contra)

La posición de la Comisión Europea no se ha incluido en la tabla ya que aunque forma una parte muy activa en la creación de un marco común y armonizado, todavía no se ha pronunciado de forma explícita sobre las medidas a tomar, habiendo declarado tan solo la necesidad de que exista transparencia y un control por parte de las Agencias Nacionales Reguladoras (ANR) sobre posibles casos conflictivos. El organismo formado por el conjunto de las ANR europeas, el BEREC, ha trabajado los aspectos de QoS y transparencia lanzando dos documentos con directrices en sendos aspectos en diciembre de 2011, que se pueden consultar en (33) y (34).

Las diferentes aproximaciones de las líneas de acción responden básicamente al contexto de la situación en cada estado. Tal y como se ha comentado, la situación en los EEUU y la situación en Europa responden a planteamientos diferentes, por nombrar los escenarios de mayor peso. Además son de destacar las actuaciones dadas en Chile debido a su condición de pionero.

Nótese como medida fundamental en todos los Estados que se han pronunciado la importancia de la transparencia como medida necesaria (aunque no suficiente) para conseguir la Neutralidad de Red. Chile, que es el primer país que está aplicando estos principios, va más allá y exige unos niveles de transparencia muy detallados (véase apartado 3.2 del Anexo A). También el no bloqueo y la accesibilidad a cualquier servicio, contenido o aplicación es un punto presente en casi todas las propuestas.

Resulta curioso que la mayor polémica ha sido dada en los EEUU, y que sin embargo sus medidas a favor de la Neutralidad de Red no son demasiado estrictas. En general, se muestran partidarios a sus principios, aunque hacen una diferenciación entre redes fijas y móviles dando una cierta permisividad a estas últimas ya que sólo se prohíbe el bloqueo y discriminación de servicios y aplicaciones en el entorno fijo, de ahí la valoración representada en la tabla resumen.

Las medidas adoptadas en Holanda, junto con las ya impuestas en Chile, se posicionan como las más extremas a favor de la Neutralidad de Red. En Holanda no se justifica una gestión de tráfico más que en casos de congestión y tratando todo el tráfico por igual y no se permite la diferenciación de tarificación de forma explícita. En el otro extremo estarían las medidas adoptadas por Canadá o Reino Unido, que son las más permisivas para los ISPs y operadores.

El resto de parámetros varía según cuan extremas son las ideas de neutralidad. En general la gestión de tráfico se permite tan sólo en momentos de congestión o por motivos de seguridad, salvo en el caso de Canadá donde se dice explícitamente que el retardo de tráfico P2P es aceptable, sin llegar al bloqueo y en situaciones que lo justifiquen. La aplicación de servicios dedicados es generalmente permisible, aunque siempre aludiendo a que éstos no deben perjudicar el acceso a Internet.

Para mayor detalle de las medidas propuestas o aprobadas en los países miembro más influyentes se recomienda la lectura del Anexo A, donde se extraen los apartados más relevantes y se referencian las fuentes originales.

Capítulo IV - Gestión de tráfico

Como se ha visto en los capítulos anteriores la situación existente en torno a la congestión en Internet ha derivado en el debate de Neutralidad de Red, que engloba varios aspectos que se relacionan en gran medida con la gestión de tráfico. Por ello en este capítulo se repasa qué es la gestión de tráfico y su relación con esta problemática, para luego abordar de forma detallada las arquitecturas modernas NGN (Next Generation Network) de gestión mediante QoS más relevantes. Es en este ámbito donde se encuentra la realidad tecnológica del debate de Neutralidad de Red además de representar el objetivo fundamental de estudio de este documento, junto con su relación con la tecnología DPI/DFI, que será estudiada en el capítulo V.

En un sentido amplio se cataloga la gestión de tráfico como el conjunto de técnicas que se emplean para distribuir contenidos a través de una red. En Internet, la aplicación de gestión de tráfico de modo no neutral es contraria al principio 'end-to-end', que ha sido analizado en el capítulo II y que define como uno de los pilares básicos de Internet que el procesado de la información transmitida debe llevarse a cabo en los nodos extremo de la red.

Se ha visto en el apartado 3 del capítulo III que existen varios aspectos que conforman esta problemática, y varios de ellos relacionados directamente con la gestión de tráfico. Más concretamente, todo punto que implica el tratamiento de datos o información está vinculado a la gestión de tráfico, como por ejemplo el bloqueo, la discriminación o la diferenciación. La siguiente ilustración, elaborada por el regulador francés ARCEP, da una buena muestra de que niveles de gestión de tráfico se consideran aceptables o no en base a los principios de Neutralidad de Red.

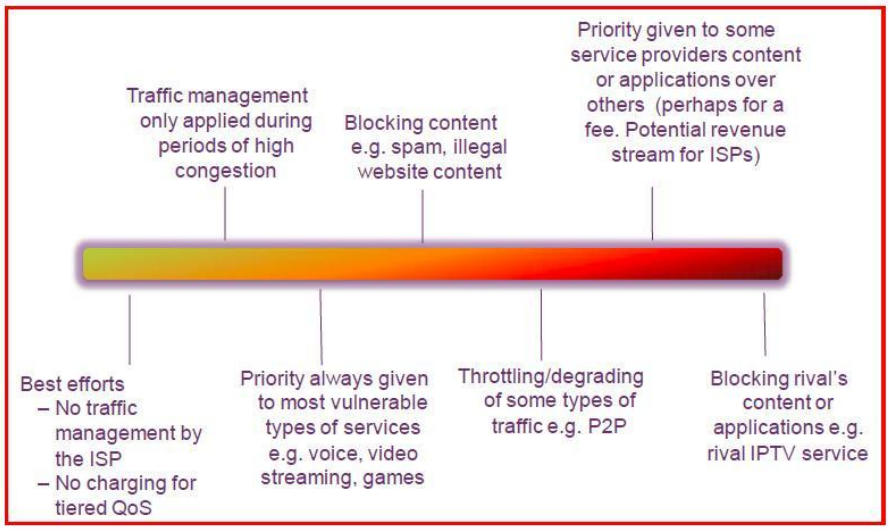

Ilustración 11: Niveles de gestión de tráfico en relación a la Neutralidad de Red (5)

Así, en el extremo más favorable a la Neutralidad de Red no se admite que se practique gestión de tráfico ni tarificación por diferenciación de QoS. En una posición menos estricta se

encontraría la aceptación de la gestión de tráfico sólo en momentos de congestión, y todavía un poco más lejos iría la aplicación de ésta atendiendo a diferentes prioridades según los requerimientos de los servicios. En un punto medio se encontraría una postura que permitiese el bloqueo de contenidos, pero tan sólo atendiendo a motivos legales o de seguridad. Entrando en la zona contraria a la Neutralidad de Red, se aceptarían medidas como la limitación de tráficos como el P2P, y en una posición aún más extrema aún se cita el bloqueo de aplicaciones o servicios según acuerdos comerciales. En la situación más opuesta a la Neutralidad de Red se encontraría el empleo de la gestión de tráfico para bloquear sitios rivales, o entorpecer los servicios de la competencia, por ejemplo.

1 Antecedentes de la gestión de tráfico

En los albores de Internet los consumidores de datos eran pocos y livianos. La optimización del tráfico tuvo poca prioridad ya que la congestión se producía por motivos ajenos al consumo o perfil de utilización de los usuarios y las limitaciones venían dadas por la propia naturaleza de la tecnología de acceso. Además, los primeros proveedores de Internet mediante conexión dial-up, modelaron sus servicios con pocas expectativas de uso. Así, hasta el inicio de la problemática tratada en este Proyecto, la gestión de tráfico en Internet se ha venido llevando a cabo de forma más o menos neutral y respondiendo al principio 'best effort'.

Por neutral se debe entender que la transmisión de paquetes IP se realiza sin distinciones según contenido, aplicación, procedencia u origen. En términos técnicos esto se traduce en la aplicación de las mismas reglas para todo tipo de paquetes, con lo que en casos de congestión se descartarían paquetes de modo aleatorio. El término 'best effort' indica que la transmisión de datos se hace lo mejor que se puede, lo cual implica que no existe ninguna garantía de QoS. Esto supone uno de los principales problemas a los que se enfrentan a día de hoy los operadores para la aplicación de unas ciertas garantías de QoS en un entorno que no ha sido diseñado para ello.

Poco a poco Internet se fue popularizando y así se fueron desarrollando los conocidos como accesos de banda ancha, nuevas tecnología de acceso para aumentar la capacidad y la calidad de las conexiones. Internet era en ese momento un paradigma de cliente-servidor, donde los usuarios consumían información generada por terceros y la publicación de contenido generado por los usuarios se limitaba en gran medida al correo electrónico. Por ello el desarrollo de las tecnologías de ancho de banda de acceso asimétrico como ADSL.

A la par se comenzaron a desarrollar sistemas de compartición de ficheros P2P, como Napster, que fue desmantelado por motivos legales. No obstante, aparecieron en sustitución otros programas P2P similares y sus respectivos protocolos, tales como Gnutella o Kazaa. Éstos se popularizaron rápidamente haciendo crecer notablemente el consumo de datos y variando el modelo cliente-servidor debido a las características de este tipo de tráfico, el cual se transmite generalmente sin alcanzar los niveles altos del núcleo de red debido a que los clientes son al tiempo servidores. Este hecho comenzó a dar problemas de congestión ya que las redes de acceso estaban diseñadas para un volumen de descarga limitado y para volúmenes de subida pequeños.

Tradicionalmente, estos problemas de congestión se han venido solucionando con el sobredimensionado de la red. Este método se lleva a cabo de modo que los enlaces se diseñan para que el ancho de banda disponible exceda el máximo esperado en un determinado margen de tiempo (hora cargada). El modo de calcular este ratio depende de una amplia variedad de factores incluyendo la topología o arquitectura de red, el volumen de tráfico, el número y tipo de usuarios, la combinación de aplicaciones que se ejecutan, variación histórica de las cargas de tráfico, la tecnología del enlace o los valores de comercialización, entre otras cosas. No obstante, el crecimiento de datos ha sido muy elevado en los últimos años, y la inversión en mayor capacidad de red no ha avanzado en la misma medida.

En esa situación, los ISPs comenzaron a introducir sistemas sencillos de detección y alteración de tráfico en los accesos e implementaron sistemas para bloquear el tráfico dirigido a los puertos empleados por este tipo de aplicaciones. Así apareció la primera forma de gestión de tráfico sobre Internet, que se corresponde con lo que se suele denominar análisis de tráfico SPI (Stateful/Shallow Packet Inspection).

Para burlar las restricciones de puertos, los desarrolladores de este tipo de protocolos llevaron a cabo modificaciones en los sistemas de compartición tales como el uso de puertos dinámicos o la ofuscación de protocolos. Como reacción a este hecho, en lo que constituye el punto de inflexión en el desarrollo de la tecnología de análisis, aparecieron una nueva clase de soluciones destinadas a ofrecer un control algo más inteligente, capaz de gestionar sesiones, modelar tráfico y añadir prioridades. Esto se consiguió en gran medida gracias a la tecnología DPI/DFI.

El crecimiento en el consumo hizo que los ISPs empezaran a impulsar políticas de gestión de tráfico cada vez más definidas, argumentando mejoras de eficiencia y seguridad. Esta gestión se ha mantenido más o menos estable hasta la fecha, y sin más problemas salvo cuando se ha dado algún caso destacado (como los analizados en el apartado 2 del capítulo II).

En los últimos años, el comportamiento del tráfico vuelve a inclinarse por el modelo cliente-servidor debido a la popularización de servicios de transmisión multimedia (el vídeo - 40% del tráfico de Internet - ha superado al tráfico P2P - 23% del tráfico de Internet - por primera vez en 10 años) (10). Este contenido multimedia demanda un gran ancho de banda en sentido descendente y unas necesidades mínimas de QoS.

Si bien el sobredimensionado sigue siendo una técnica ampliamente utilizada para lograr una calidad aceptable en redes IP, está siendo gradualmente reemplazada por otras técnicas de gestión del tráfico ya a que a medio y largo plazo esta solución no resulta efectiva. Esto es en gran parte debido a la problemática expuesta en los capítulos anteriores en relación a la inversión en mayor capacidad de red, junto con la aparición de aplicaciones en Internet que requieren características de QoS especialmente exigentes (VoIP, VoD, IPTV, etc.). Además, la constante aparición de nuevas aplicaciones en Internet hace que sea difícil planificar con sentido una red, ya que para ello se necesita una cierta capacidad de control del comportamiento de las aplicaciones y suscriptores. También es un factor a comentar que un sobredimensionado resulta poco útil cuando se trata con tráfico P2P ya que generalmente las aplicaciones para gestionar este tipo de tráfico son diseñadas para consumir ancho de banda de forma adaptativa (a mayor ancho de banda disponible, mayor es el volumen de tráfico cursado).

2 Prácticas de gestión de tráfico

Las prácticas de gestión de tráfico pueden responder a diferentes planteamientos que van desde lo más simple, como limitar el volumen de tráfico de un abonado, hasta algo más sofisticado como gestionar las diferentes aplicaciones dinámicamente según sus necesidades de latencia y ancho de banda. En este caso y en términos simples, los ISPs pueden controlar el tráfico en tres dimensiones: la red, el servicio o aplicación y el contrato del suscriptor.

Las acciones llevadas a cabo a nivel técnico son varias y dependen de la aplicación y contexto de la gestión de tráfico dada. Entre otras, algunas de las que se emplean para gestionar tráfico se basan en bloqueo o inserción de paquetes, limitación de velocidad de flujos, priorización de protocolos, priorización de usuarios, desconexión de sesiones o generación de notificaciones de eventos (35). De forma más genérica, se suele diferenciar entre dos técnicas de gestión según la exhaustividad de los parámetros controlados (36).

- **'Throttling':** Lleva a cabo un control del volumen de tráfico que atraviesa una red en un periodo especifico y encola o incluso elimina paquetes en caso de congestión.

- **'Shaping':** Controla de modo exhaustivo el volumen de tráfico, la tasa de transferencia y demás parámetros del tráfico que fluye por la red, resultando más sofisticado que el 'throttling'.

Mediante este conjunto de acciones es posible determinar prácticas de gestión tan complejas como se quiera, en función de las necesidades técnicas o a los planes de contratación de los ISPs, por ejemplo. A continuación se listan una serie de prácticas que dan una visión de hasta qué punto se puede llegar a controlar los parámetros de las conexiones.

- **Práctica basada en consumo umbral:** Práctica basada en controlar el consumo de un usuario en un período de tiempo específico (generalmente en un mes) hasta llegar a un cierto umbral, a partir del cual o bien se reduce la velocidad de conexión o bien se tarifica por los datos extra. Es aplicada sobre todo por operadores móviles y se suele ofertar como una "tarifa plana". Con este sencillo método el operador tiene garantizado un consumo medio por usuario, de modo que la planificación de su red se pueda basar en este dato. Esta técnica no precisa de equipos sofisticados de análisis.

- **Práctica basada en bloqueo:** Este método ejecuta un bloqueo del tráfico generalmente considerado como indeseable para ISPs como puede ser el P2P u otras aplicaciones que consuman un ancho de banda excesivo. Para ello es imprescindible el uso de equipos da análisis profundo ya que el tipo de aplicaciones perseguidas por esta forma de gestión generalmente no respetan los 'well-known ports' o bien son ofuscadas (véase más adelante el apartado 1 del capítulo V). Esta práctica atenta claramente contra los principios de Neutralidad de Red y de forma genérica es catalogada como una técnica no aceptada (excepción hecha del bloqueo de malware y/o spam).

- **Práctica basada en aplicación:** Este modelo se basa en las propiedades de cada aplicación o servicio para proporcionar unos parámetros que garanticen una QoS aceptable. Esto permitiría, por ejemplo, dar prioridad a servicios como VoIP ante otros servicios de menor prioridad o no interactivos. Los paquetes de VoIP serían eliminados sólo en caso de que el enlace estuviese saturado de VoIP (hecho muy poco probable). Los demás paquetes serían eliminados los primeros en caso de congestión. En un caso intermedio el funcionamiento sería aceptable para todos los tráficos. Este modelo tiene la dificultad de determinar quién establece la prioridad de los paquetes. O bien lo hace la propia aplicación de usuario o bien el ISP, pudiendo dar lugar a situaciones injustas o viéndose la necesidad de emplear un análisis detallado para así clasificar y proporcionar correctamente los parámetros necesarios (37).

- **Práctica basada en usuario:** El actual modelo de uso del ancho de banda basado en TCP[6] no es eficiente para otorgar una proporción justa o equitativa de éste si se valora desde el punto de vista del usuario. Algunas aplicaciones abren múltiples conexiones TCP o emplean UDP (que no realiza un control de flujo) para obtener un mayor ancho de banda. Por ello, este formato se basa en repartir la capacidad del ancho de banda para que en media todos los usuarios obtengan el mismo valor (38). Para que sea efectiva, la gestión basada en el consumo de usuario debe ser medida en períodos de tiempo relativamente cortos ya que de lo contrario no combatiría la congestión (37). A diferencia de la técnica basada en la aplicación, esta técnica proporciona al operador una herramienta importante para dar una calidad media constante sin atentar de modo agresivo a los principios de Neutralidad de Red, y sin unas implicaciones técnicas muy exigentes.

- **Práctica basada en usuario/aplicación:** La combinación de estos dos métodos es probablemente una de las soluciones más equitativas. Durante los períodos de congestión de la red, el modelo basado en el usuario garantiza el reparto del ancho de banda, mientras que cuando no se produce este problema, los recursos son repartidos según las necesidades de cada aplicación o protocolo (37). Como veremos a continuación, las arquitecturas para las Next Generation Network (NGN) se aproximan en gran medida a este formato.

[6] TCP emplea un mecanismo de control de flujo, de modo que hasta que no se ha confirmado la recepción en el destino de un paquete no se envía el siguiente.

3 Tipos de tráfico y QoS

Debido en buena parte al freno del sobredimensionado de redes y atendiendo también a otros aspectos, la solución al problema de congestión tiende a pasar por la gestión de tráfico y la diferenciación y/o discriminación de servicios y contenidos. Es innegable que los diferentes servicios sobre Internet necesitan requerimientos de QoS diferentes para ofrecer una buena QoE al usuario final. Para los juegos en línea o telefonía por Internet se agradecerán condiciones de baja latencia y jitter, pero el consumo de ancho de banda será pequeño. Sin embargo, las grandes descargas no se verán casi afectadas por la latencia y jitter pero necesitarán de un gran ancho de banda.

Veamos una valoración algo más detallada en la siguiente tabla, cuyos valores se extraen de las recomendaciones de la ITU-T Y.1541 (39) y hacen referencia a flujos unidireccionales extremo a extremo. Aunque los valores especificados por la ITU-T pueden ser los mismos en diferentes tipos de servicio, hay algunos servicios que son más sensibles a ciertos parámetros que a otros, motivo por el que pueden tener otra valoración aún y compartiendo el mismo valor de parámetro (5) (40).

Servicio	QoS requerida	Atributos
Navegación Web	Baja: 'Best effort'	• Consumo variable • Tolerante a latencia, jitter y PELR
VoIP	Alta: Baja latencia y jitter	• Consumo bajo (< 320 kbps llamada) • Muy sensible a latencia (< 100 ms) y jitter (< 50 ms) • Sensible a PELR (< 10^{-3})
Videoconferéncia	Muy alta: Baja latencia, jitter y PELR	• Consumo elevado • Muy sensible a latencia (< 100 ms) y jitter (< 50 ms) • Muy sensible a PELR (< 10^{-3})
Streaming	Media: Bajo PELR	• Consumo elevado • Tolerante a latencia (1 s) y jitter (no especificado) • Sensible a PELR (< 10^{-3})
Transferencia archivos P2P	Baja: 'Best effort'	• Consumo elevado (múltiples conexiones) • Tolerante a latencia, jitter y PELR
Juego Online	Alta: Baja latencia, jitter y PELR	• Consumo bajo • Muy sensible a latencia (< 100 ms) y jitter (< 50 ms) • Sensible a PELR (< 10^{-3})
Direct Download	Baja: 'Best effort'	• Consumo muy elevado • Tolerante a latencia, jitter y PELR
Señalización	Media : Baja latencia y PELR	• Consumo bajo • Sensible a latencia (< 100 ms) y PELR (< 10^{-3}) • Tolerante a jitter (no especificado)
TVIP	Muy alta: Baja latencia, jitter y PELR	• Consumo muy elevado • Muy sensible a latencia (< 100 ms) y jitter (< 50 ms) • Muy sensible a PELR (< 10^{-6})

Ilustración 12: Requerimientos de QoS según tipo de servicio

Es importante considerar que la provisión de ciertos requerimientos de QoS mediante su priorización a las aplicaciones o servicios comentados no causa necesariamente una degradación global del servicio. Por ejemplo, dar una mayor prioridad al tráfico VoIP (alrededor del 2% del tráfico global de Internet) (10) que a P2P no afecta en absoluto el ancho de banda disponible para éste, debido a que la proporción de tráfico de uno frente a otro es considerablemente menor. Es más, un aumento del tráfico VoIP sería casi imperceptible en relación al volumen de tráfico P2P. Sin embargo, si hay dos tipos de aplicaciones de gran consumo, por ejemplo VoD y P2P, las prioridades pueden tener un efecto adverso sobre la aplicación de menor prioridad. En el caso específico de IPTV, muchos de los ISPs que ofrecen este servicio han optado por construir una red separada dedicada sólo a ese servicio para evitar conflictos y degradación de servicios.

Teniendo en cuenta estas consideraciones parece claro que el trato que se tendría que dar a cada tipo de tráfico debería ser el que maximice la QoE del usuario, para lo que es necesaria la aplicación de gestión de tráfico. Ahora bien, si se acepta que el empleo de prioridades es una buena solución, surge el problema de determinar quién decide la priorización del tráfico.

Algunas propuestas abogan por permitir a los usuarios escoger sus prioridades, lo cual requiere un conocimiento acerca de la QoS de las aplicaciones y protocolos que un usuario final no posee, además de la sobrevaloración a que daría lugar este formato. La solución más extendida pasa por que sea el ISP quien asigne las prioridades en función del servicio en uso, del contrato del suscriptor o de ambos factores.

4 Gestión de tráfico basada en QoS y 'policing'

A lo largo del documento se ha expuesto y justificado la tendencia que existe hacia una gestión de tráfico basada en las propiedades de cada tipo de tráfico y en base a diferentes planes de suscriptor. Esto es debido a que existe un enfoque común hacia el cual se están orientando casi todas las especificaciones relevantes y que se basa en la gestión mediante control dinámico y diferenciado de QoS junto con el uso de servidores de políticas, concepto al que nos referiremos mediante su término inglés 'policing'. Esta forma de gestión, si bien puede ser considerada contraria a lo que defienden las bases de Neutralidad de Red, está siendo ampliamente desarrollada e implementada.

Las nuevas necesidades de gestión por parte de los operadores e ISPs han propiciado el desarrollo de lo que se conoce como NGNs, que están siendo definidas por varios organismos de la industria de las telecomunicaciones respondiendo a sus orígenes y diseños específicos (generalmente, el medio de acceso). Existe un objetivo convergente de estas propuestas de arquitectura de red por parte de dichos organismos a la hora de ofrecer una cierta QoE. Para ello las diferentes aproximaciones se están basando en una gestión del control de la QoS de modo que ésta pueda ser subministrada para conectar, controlar y garantizar diferentes niveles de ésta.

Por otro lado, según una visión estricta de la Neutralidad de Red, existirían dos opciones para la oferta de servicios diferenciados a través de una red: o bien se aceptan las reglas de la Neutralidad de Red en Internet; o bien se construyen redes privadas para ofrecer los servicios diferenciados, aplicando éste concepto también a los denominados servicios dedicados comentados en el apartado 4.3 capítulo II. Esto se fundamenta en la afirmación de que una diferenciación de servicios o de QoS es útil en redes pequeñas, pero su escalabilidad a la totalidad de Internet es ineficiente. Esta ineficiencia se atribuye a la dificultad de llevar a cabo un control extremo a extremo, provisionando de forma independiente a las redes que se atraviese, de unos parámetros de QoS. La siguiente ilustración muestra la división de ámbitos de QoS, dónde la dificultad radica en la obtención de una QoS_{TOTAL} y por tanto de una buena QoE.

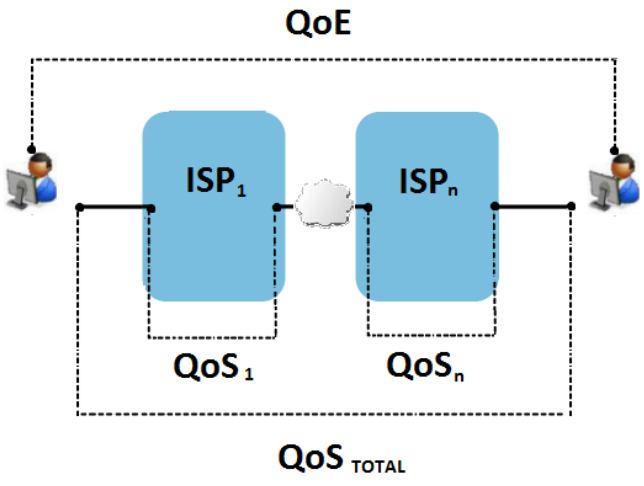

Ilustración 13: QoS y QoE en la interconexión de redes

En efecto, hasta la fecha, sobre las redes IP tradicionales 'best effort' el control de QoS se ha venido logrando generalmente mediante dos mecanismos que no han funcionado a nivel global. El primero, la combinación de la reserva de recursos IntServ (Integrated Services) (41) y RSVP (Resource Reservation Protocol) (42) que falló por su escasa escalabilidad (43). El segundo, el marcado de paquetes según prioridades DiffServ (Differenciated Services) (44), resultó el método más efectivo y extendido en Internet sin llegar a ser un éxito debido a la dificultad de tener que implementarse en todos los saltos de la red para su correcto funcionamiento. (38)

DiffServ representa una solución relativamente simple para clasificar el tráfico en un pequeño número de CoS (Classes of Service) con el fin de dar prioridad a algunos tipos de tráfico. Una clasificación típica DiffServ distingue entre VoIP, tráfico sensible al tiempo de latencia y tráfico 'best-effort'. DiffServ se utiliza a menudo en asociación con MPLS (Multi-Protocol Label Switching) (45), habiendo sido ambos definidos por la Internet Engineering Task Force (IETF). MPLS añade una etiqueta a los paquetes que atraviesan una red IP permitiendo entre otras funcionalidades la creación de caminos virtuales. Tanto DiffServ como MPLS se crearon hace algo más de una década y son utilizados por empresas en redes privadas que utilizan IP, y por algunos proveedores de Internet para controlar la calidad de ciertos servicios, pero no resulta actualmente escalable para un control extremo a extremo (36).

Debido al fracaso de estos métodos para la implementación de QoS extremo a extremo, el diseño de las NGN abandona estos modelos y apuesta por un modelo de gestión de QoS en el que la señalización necesaria para negociar una transferencia de datos no viaja en la misma ruta lógica que los datos en sí. Por lo tanto aparece la figura de una entidad que se debe encargarse de la autorización, el mapeo y la provisión de medios para aplicar las políticas de QoS, que se define bajo un marco de referencia de arquitecturas basadas en 'policing', buena parte de cuya nomenclatura y estructura se basa en el RFC 2753 (46).

Para el establecimiento de este control aparece la entidad de 'policing' que tiene la función de determinar extremo a extremo la provisión de reglas. Este elemento generalmente se basa en el uso de un sistema automatizado de reglas lógicas simples que al concatenarse pueden permitir políticas complejas (36). Su decisión se determina en respuesta a la información recibida de la red, el cliente y la aplicación en uso, entre otros posibles datos. Una característica importante de las herramientas de 'policing' es que generalmente tienen enlaces a bases de datos de suscriptores y facturación, por lo que éstas pueden ser valiosas para la prestación de servicios personalizados, y de hecho tienen un enfoque de control orientado al contrato del suscriptor más que sobre la aplicación en uso.

Las arquitecturas de gestión de políticas se han venido normalizado en los últimos años por varios e importantes organismos internacionales estandarizadores de telecomunicaciones. Éstos incluyen 3GPP y 3GPP2, que trabajan en la creación de estándares para operadores de redes móviles, la ETSI (European Telecommunications Standards Institute) que creó una arquitectura enfocada las telecomunicaciones fijas como parte de su arquitectura TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) para las NGN y CableLabs, que creó una arquitectura para los Multiple Service Operator (MSO) de cable. Los problemas y soluciones a la hora de tratar la gestión del tráfico

están determinados en parte por la red subyacente y sus características. Las redes de los operadores fijos, los operadores móviles y los operadores de cable plantean diferentes desafíos. No obstante, como se verá a continuación, hay una buena cantidad de elementos comunes en las soluciones y en el grado de implementación.

Así, de entre varios organismos que han elaborado sus propuestas de NGN son de destacar los tres siguientes, ya que son los dominantes y los que marcan tendencia en sus respectivos medios de acceso.

- 3GPP PCC (Policy and Charging Control)
- CableLabs PCMM (PacketCable MultiMedia)
- TISPAN RACS (Resource and Admission Control Sub-System)

En los siguientes apartados del capítulo se analizan las arquitecturas citadas y algunos aspectos relevantes de sus respectivos contextos, distinguiendo redes fijas y redes móviles, para luego extraer los puntos comunes y discrepancias de forma más detallada e identificar el papel de las tecnologías de análisis DPI/DFI en dichas estructuras.

4.1 Gestión de tráfico en redes móviles

Los dispositivos móviles han experimentado un creciente éxito en penetración y uso. Esto ha desembocado en una demanda de datos sin precedentes y en un crecimiento de conexiones móviles cada vez mayor. De los aproximadamente 3.400 millones de personas que tendrán banda ancha en 2014 a nivel mundial, se espera que alrededor del 80% serán abonados a servicios móviles, y la mayoría serán atendidos por HSPA y LTE (47).

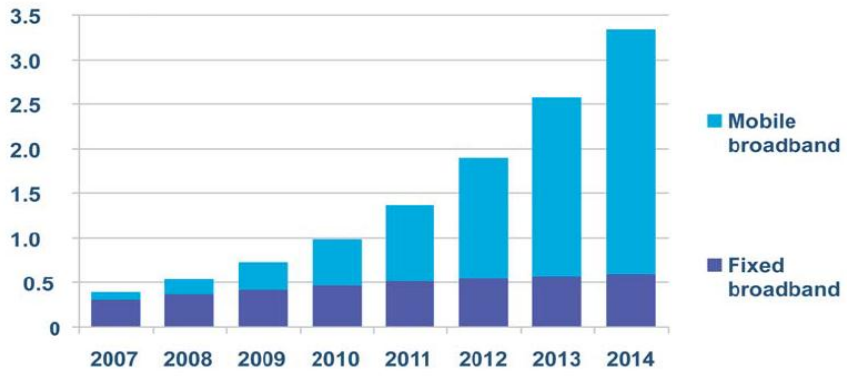

Ilustración 14: Comparación y previsión de suscripciones fijas y móviles (2007 - 2014), en miles de millones (47)

La gestión de tráfico en el entorno móvil se presenta casi como una necesidad por parte de los operadores ya que el acceso tiene unas limitaciones más restrictivas que cualquier otro tipo de

medio. Esto es debido a que se trata de un medio variante (que depende de circunstancias ambientales), limitado (el rango espectral útil en comunicaciones está acotado) y compartido (varias señales electromagnéticas son transmitidas por el mismo medio, lo que produce interferencias). Según el teorema de Shannon-Hartely esta limitación viene determinada por la siguiente ecuación:

$$C = B \cdot log_2(1 + \frac{S}{N})$$

Donde C = Capacidad de canal [bit/s], B = Ancho de banda [Hz], S/N = Relación señal a ruido. Analizando este teorema se deduce que fijando el ancho de banda B, que es un recurso limitado, lo que nos determina la capacidad del canal es la relación S/N. Si esta relación crece, la capacidad C también lo hará, pero siguiendo un ritmo logarítmico. Esto implica que los esfuerzos para aumentar la relación de potencia señal a ruido cada vez tienen menos repercusión en la capacidad de canal. Por ejemplo, si se consigue una eficiencia 3x en la S/N, esto tiene un efecto de 2x en la capacidad C, mientras que si se consigue una mejora 10x en la S/N, esto repercutirá en la capacidad C en un factor 3,4x.

Por su parte, el crecimiento del consumo de datos debido a la comercialización del accesos a Internet en movilidad ha llevado a una situación inesperada, tanto que el servicio tradicional que se prestaba por parte de éstos se ha visto desbordado dando mucho más servicio a datos que a voz.

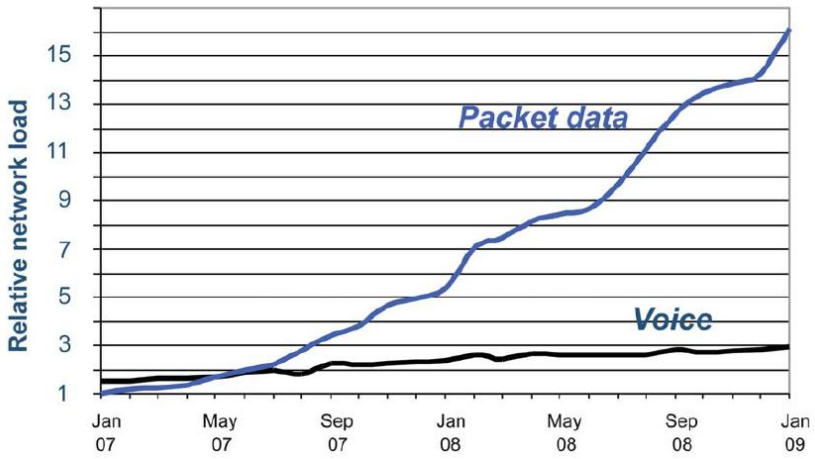

Ilustración 15: Comparación de incrementos de carga entre voz y paquetes en 3G/WCDMA (2007 – 2009) (47)

Este proceso evolutivo se ha basado en la implementación de GPRS sobre GSM, que se definió por la ETSI y que actualmente se mantiene por la 3GGP. GPRS definía la primera implementación de conmutación de paquetes en la red GSM y aportó nuevos tipos de servicio y conexión a Internet, entre otros. Posteriormente apareció EDGE como evolución de GSM/GPRS y haciendo de puente hacia la 3G, que se estableció con la definición de UMTS/HSPA y de CDMA2000, por parte de la 3GGP y la 3GPP2 respectivamente.

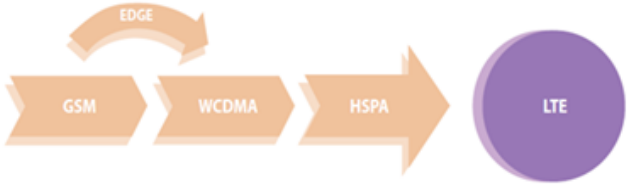

Ilustración 16: Evolución de estándares 2G/3G/4G de la 3GPP (48)

Es importante notar que toda esta evolución se ha sustentado sobre la misma estructura de núcleo de red, la GPRS Core Network y la única condición de adaptación se ha venido dando básicamente en las estaciones base.

4.1.1 GSM/GPRS/EDGE, UMTS/HSPA - GPRS Core Network

No es el objetivo de este Proyecto entrar a analizar las características de las redes móviles, pero para su enlace con la gestión de tráfico se deben tener en cuenta los elementos y funciones que configuran la red.

4.1.1.1 Arquitectura de red

En el ámbito de interés para a la gestión de tráfico de datos debemos considerar los siguientes elementos (49):

- **Serving GPRS Support Node (SGSN):** Se trata del nodo que está al servicio de la red de acceso (GERAN/UTRAN) y que por lo tanto maneja el acceso radio. Por ello se encarga de la autenticación de usuarios, del control de admisión, de la movilidad y gestión de sesiones y de la recopilación de datos para facturación. Cada SGSN tiene a su cargo cierto número de BSS (Base Station Subsystem), y gestiona el cambio de zona de un terminal de usuario. Es responsable también de la transmisión, enrutamiento y creación de túneles de paquetes de datos hacia su correspondiente GGSN.

- **Gateway GPRS Support Node (GGSN):** El GGSN es la interfaz con las redes PDN (Packet Data Network), como por ejemplo Internet. Su función principal es el enrutamiento de paquetes de datos desde la red PDN al SGSN, la retransmisión de datos, la creación de túneles, la gestión de sesiones y la recopilación de datos de facturación. También se encarga de la AAA (Authentication, Authorization and Accounting) para la salida a Internet.

4.1.1.2 Niveles de QoS

En los estándares 3G (UMTS) ya se incluyen cuatro tipos de CoS definidos en (50) con unos parámetros específicos para los siguientes tipos de datos:

- **Conversación:** Definido para tráfico en tiempo real con un retardo y jitter bajo. Pensado para servicios como VoIP o videoconferencia.

- **Streaming:** Orientado para tráfico de video que aunque no requiera de una baja latencia sí que se vería afectado por un jitter muy elevado. Enfocado, como su nombre indica, al servicio de streaming.

- **Interactivo:** Diseñado para navegación web, responde a un modelo 'best effort' aunque teniendo en consideración que el tráfico debe ser entregado en un cierto intervalo de tiempo.

- **Background:** Pensado para tráfico sin fuertes exigencias temporales, como por ejemplo el tráfico que genera la comunicación vía email.

4.1.1.3 Políticas de control

Para la gestión de políticas de control de cobro y facturación ya se incluyen ciertos elementos relativos a políticas de control en las redes 2G/3G (51).

- Servicio de gestión de clientes prepago, implementado originalmente para proporcionar servicios de voz simples. No ha dejado de ampliarse para incluir los nuevos servicios cómo itinerância, mensajería y datos.

- Políticas de control implementadas para apoyar los servicios de datos existentes. Esto incluye algunas funciones de tipo PCRF (detallada en el apartado siguiente), pero no el control dinámico que ofrece el Evolved Packet Core (EPC) de la 4G.

- Plataformas de análisis DPI/DFI y posterior decisión que permiten un control detallado de los flujos IP. Su inclusión para servicios como políticas de facturación provocan una disminución del rendimiento de hasta el 50% (52).

- Integración de sistemas de cobro y facturación en redes.

4.1.1.4 Análisis de tráfico en 2G/3G

El análisis de tráfico en redes 2G/3G (en realidad podríamos particularizar a redes 3G) ha sido aplicado de forma gradual atendiendo a necesidades de tratamiento de congestión y para

hacer cumplir políticas de operador, basándose en la implantación de equipos con funcionalidades DPI/DFI. La ubicación para la instalación de estos equipos depende de factores como el volumen de tráfico y las tecnologías de acceso empleadas, aunque generalmente se lleva a cabo junto al GGSN ya que éste es el punto común de accesos 2G/3G e incluso de otras tecnologías como WLAN (Wireless Local Area Network), además de tratarse del elemento que se encuentra conectado a la red externa de paquetes, como se muestra en la siguiente ilustración.

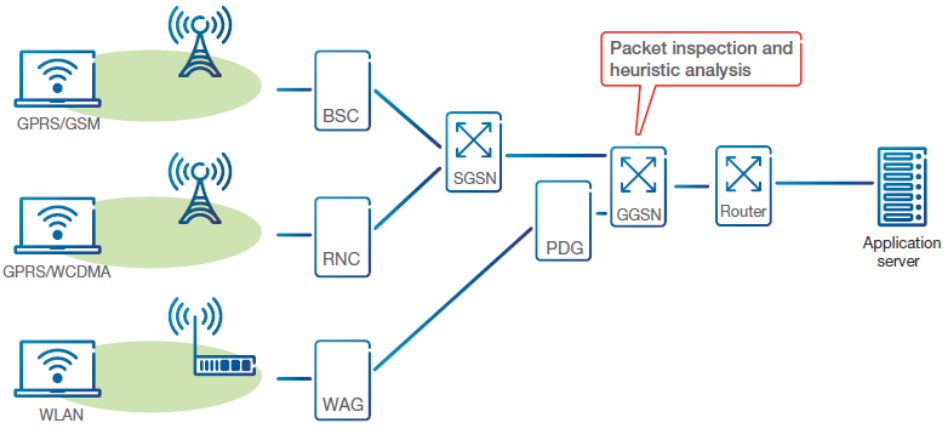

Ilustración 17: Estructura 2G/3G para inclusión de DPI/DFI (53)

4.1.2 LTE/SAE – Evolved Packet Core

Las necesidades que exigen las nuevas y crecientes aplicaciones y servicios han llevado a la definición por parte de la 3GPP de LTE/SAE (Long Term Evolution/System Architecture Evolution). Por abuso de lenguaje se suele atribuir al término LTE toda la tecnología que se incorpora en 4G, aunque LTE estrictamente se refiere sólo a las normas de acceso de radio introducido por el 3GPP en la versión 8. La evolución de toda la arquitectura se engloba por lo tanto bajo LTE/SAE, formando parte de ella el llamado Evolved Packet System (EPS), que incluye el EPC, el nuevo núcleo para la red 4G.

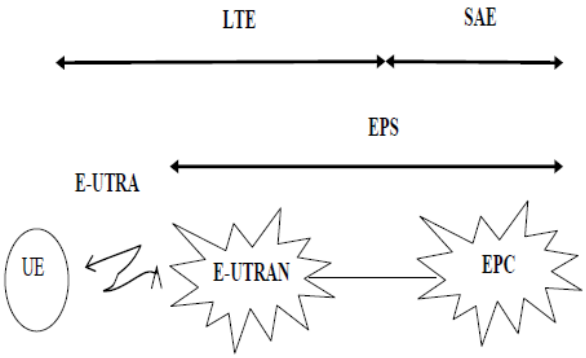

Ilustración 18: Nomenclatura de los elementos de la red LTE (54)

LTE/SAE surge ante la situación actual en la que las tecnologías GSM/EDGE y UMTS/HSxPA (definidas todas por la 3GPP) representan más del 85% de los abonados móviles (55). Con LTE/SAE se prevé garantizar una mejora sobre las anteriores tecnologías móviles y se espera un avance sustancial de rendimiento, capacidad de datos y reducción de latencia. Este nuevo paradigma de red permite una buena complementación con los sistemas anteriores para hacer más simple el proceso evolutivo. En la siguiente ilustración se muestra el esquema de red para LTE/SAE junto con el esquema también del GPRS Core Network de 2G/3G.

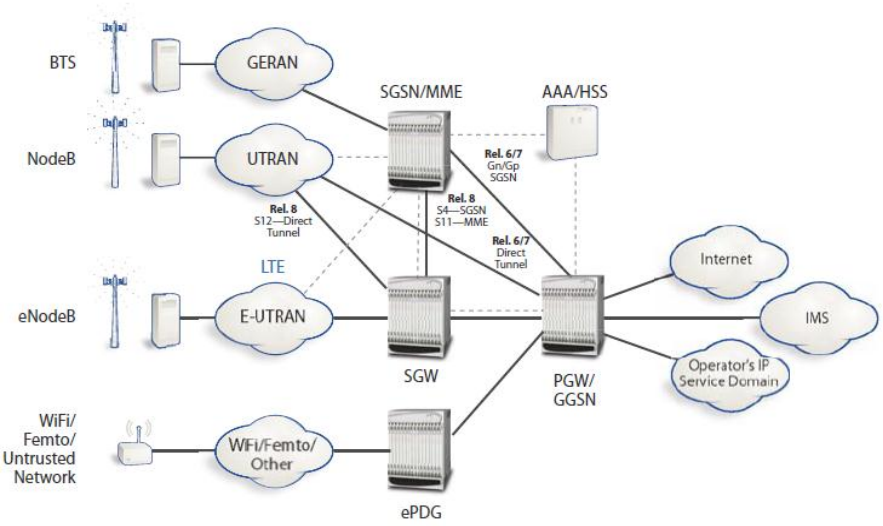

Ilustración 19: Integración GPRS/UMTS/LTE (48)

La diferencia más significativa es el uso de un nuevo paradigma para el servicio de voz, llevándose a cabo sobre VoIP y convirtiendo la nueva red EPC en una red 'all-IP'. Esto pone fin a un período de más de 20 años durante el cual se ha implementado la arquitectura de conmutación de circuitos en toda la red. Por este motivo, la introducción del EPC es más significativa para LTE que la del GPRS Packet Core lo fue para las redes 2G/3G.

LTE/SAE trata la voz como una de las muchas aplicaciones de red basadas en IP, aunque con algunos matices que la hacen más importante, ya que requiere un rendimiento excelente en una red de paquetes en la que convergen diferentes tipos de tráfico. Al convertirse a una red IP se elimina la conmutación de circuitos que garantizaba una cierta QoS extremo a extremo, por lo que esta función se debe implementar con nueva tecnología, de ahí la importancia de esta arquitectura de red para la temática del Proyecto.

4.1.2.1 Arquitectura de red

EPC representa un cambio en las arquitecturas de redes móviles, introduciendo nuevos requerimientos y funcionalidades en el núcleo de la red. Debe ser capaz de diferenciar entre

varios servicios y niveles de QoS, además de poder de trabajar con un caudal de datos considerablemente superior que en 3G.

Debido a la importancia que toma esta arquitectura por ser el referente en la provisión de parámetros de QoS se exponen, sin entrar en detalles, los elementos y las funciones principales. La siguiente ilustración representa los diferentes bloques funcionales de la arquitectura, que son comentados a continuación (48) (52) (55) (56).

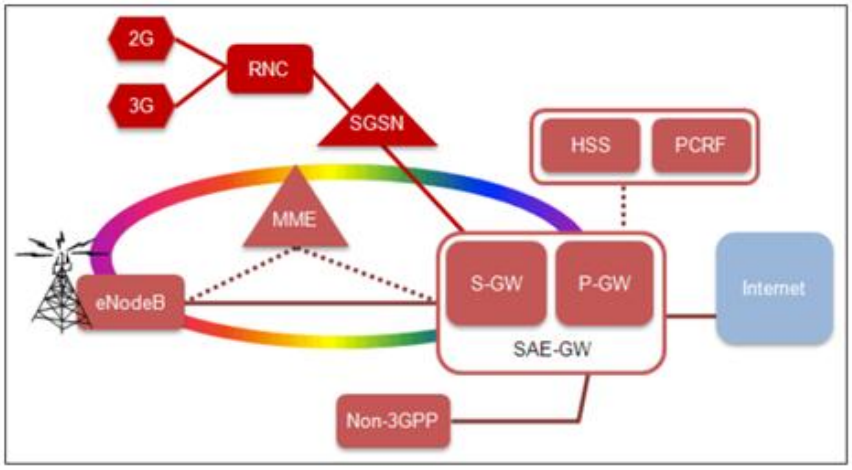

Ilustración 20: Arquitectura LTE/SAE (56)

- **eNodeB:** Se encarga de varias tareas, incluyendo la gestión de los recursos de radio, control de admisión, aplicación de la QoS negociada hacia el UE (User Equipment), difusión de información de celda, cifrado y compresión de cabeceras de los paquetes de datos de usuario.

- **Serving Gateway (SGW)**: El SGW se encarga del enrutado y envío de paquetes de datos de usuario al tiempo que actúa como punto de anclaje en 'handover' en LTE y entre LTE y otras tecnologías del 3GPP. Administra y almacena datos del contexto del UE, tales como parámetros del servicio o información de la red.

- **Mobility Management Entity (MME):** El MME es punto de control de nodos para el acceso a la red LTE. Toda la gestión de la movilidad se trata en el núcleo y se convierte en responsabilidad de esta entidad. Para ello, requiere de una gran capacidad de procesado en el plano de control, garantizando la interoperabilidad con los sistemas móviles 2G/3G. Incluye funciones de seguimiento del UE, selección inicial y reubicación de SGW, autenticación de usuario (mediante interacción con el HSS), etc.

- **PDN Gateway (PGW):** El PGW proporciona conectividad a las redes externas de paquetes de datos como Internet. El PGW lleva a cabo la aplicación de políticas (función PCEF, véase en el siguiente apartado), el filtrado de paquetes por usuario,

soporte de facturación, interceptación legal y detección de paquetes mediante técnicas avanzadas de análisis (DPI/DFI).

- **Policy Charging and Rules Function (PCRF):** Esta entidad realiza funciones del plano de control necesarias para dar una gestión dinámica y soporte a las funciones de facturación y QoS, que se detallan en el siguiente apartado.

- **Home Suscriber Server (HSS):** Es la base de datos de usuario con soporte hacia IMS (IP Multimedia Subsystem). Contiene información de los suscriptores (perfiles de abonado). Se encarga de la autenticación y autorización del usuario y también puede aportar información sobre su ubicación.

4.1.2.2 Niveles de QoS

La gestión de QoS extremo a extremo es esencial en LTE para ser capaz de ofrecer los nuevos servicios disponibles con baja latencia y en tiempo real, y sobre todo por el hecho de tratar la voz como VoIP. Esto debe ser logrado garantizando al mismo tiempo la escalabilidad de los usuarios, servicios y sesiones de datos.

Para este fin, se ha llevado a cabo un movimiento de cuatro CoS disponibles en 3G a nueve perfiles de QoS con unas especificaciones determinadas, definidos como QoS Class Identifier (QCI). De este modo, cada operador puede determinar dinámicamente para cada servicio un nivel de QoS en función de sus políticas de gestión. Cada servicio o flujo del plano de datos se gestiona en conexiones virtuales conocidas como SDF, que no son más que la separación en flujos a nivel 4 según el análisis de quíntupla: {dirección IP origen, dirección IP destino, puerto origen, puerto destino, protocolo de nivel 4}.

Los SDF, a su vez, son transportados a nivel conceptual a través de las portadoras QCI. En la figura siguiente se muestra el escenario en el que uno o más SDF se agregan y se transportan por las diferentes portadoras. Como portadora se debe entender el elemento que es capaz de separar el tráfico según los citados parámetros, con una visión extremo a extremo entre el UE y el PGW.

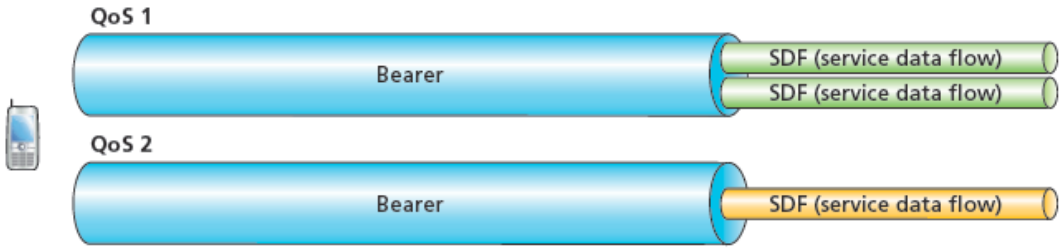

Ilustración 21: Modelo de QCI transportando diferentes SDF (52)

Los diferentes QCI especifican el tratamiento que debe dar cada portadora a los paquetes que ésta maneje. La 3GPP ha definido unos valores estandarizados de QCI, entre cuyos parámetros se encuentran, según si existe una cierta garantía mínima de velocidad de transferencia o no, estos formatos (57):

- **Guaranteed Bit Rate (GBR):** Estas portadoras tienen una tasa mínima que se adquiere gracias a que existen unos recursos permanentemente establecidos (mediante una función de control admisión en el eNodeB, por ejemplo). Las tasas pueden ser superiores si hay recursos disponibles.

- **Non- Guaranteed Bit Rate (Non-GBR):** No garantizan ninguna tasa en particular y no reservan recursos de forma permanente.

En la siguiente figura se muestran los diferentes tipos de portadoras o QCI según diferentes configuraciones de los parámetros citados. Los valores de latencia y PELR, aunque se encuentran definidos en las especificaciones de la arquitectura (57), no son más que valores de referencia, y dan una idea de los parámetros que se deberían asignar para cada uno de los servicios que mapean, desde el PGW hasta el UE. Como se puede apreciar, se definen portadoras con parámetros específicos para buena parte de los servicios que se han diferenciado ya en el apartado 3 del capítulo anterior, además de otras con un enfoque a la oferta de servicios con un trato diferenciado (QCI 7 y 8). Para más detalle se recomienda la consulta de las especificaciones de la 3GPP (57).

QCI	Tipo	Prioridad	Latencia	PERL	Ejemplos
1	GBR	2	100 ms	10^{-2}	VoIP
2		4	150 ms	10^{-3}	Videoconferéncia
3		3	50 ms	10^{-3}	Juego Online (en tiempo real)
4		5	300 ms	10^{-6}	Streaming
5	Non-GBR	1	100 ms	10^{-6}	Señalización
6		6	300 ms	10^{-6}	Servicios priorizados (Streaming, Navegación Web, P2P, etc.)
7		7	100 ms	10^{-3}	Servicios dedicados
8		8	300 ms	10^{-6}	Servicio "premium"
9		9	300 ms	10^{-6}	Servicio "base"

Ilustración 22: Configuración de parámetros de los QCI

Si bien la definición de estas portadoras puede agilizar la distribución de los tipos de tráfico, a mayor número de QCIs más compleja será la tarea de decisión en el eNodeB. Dicho nodo tiene que tratar con la organización del punto más congestionado de la red, el acceso radio. Para solventarlo el transporte entre el UE y el eNodeB incluye algunas técnicas de optimización en el nivel 2. Se llevan a cabo sobre la capa RLC (Radio Link Control) y proporcionan tres modos diferentes de fiabilidad para los datos (55):

- **Acknowledge Mode (AM*):** Apropiado para transmisiones en tiempo no real, tales como descargas de archivos.

- **Unacknowledged Mode (UM):** Apto para el transporte de servicios tiempo real sensibles a los retardos y que no pueden esperar retransmisiones.

- **Transparent Mode (TM):** El modo de TM se usa cuando el tamaño de PDU (Packet Data Unit) es conocido a priori, básicamente en señalización.

La capa RLC también ofrece mecanismos de eliminación de duplicados y segmentación de cabeceras para mayor eficiencia. Además existen dos tipos de retransmisiones con el fin de proporcionar más fiabilidad (55).

La gestión en el acceso supone un desafío porque independientemente de las políticas de QoS, este medio será un factor limitador por sus características físicas, por lo que sistemas sofisticados de QoS difícilmente serán aplicables. Inicialmente se prevé un uso de estos tres servicios que se muestran en la figura (señalización, VoIP y datos).

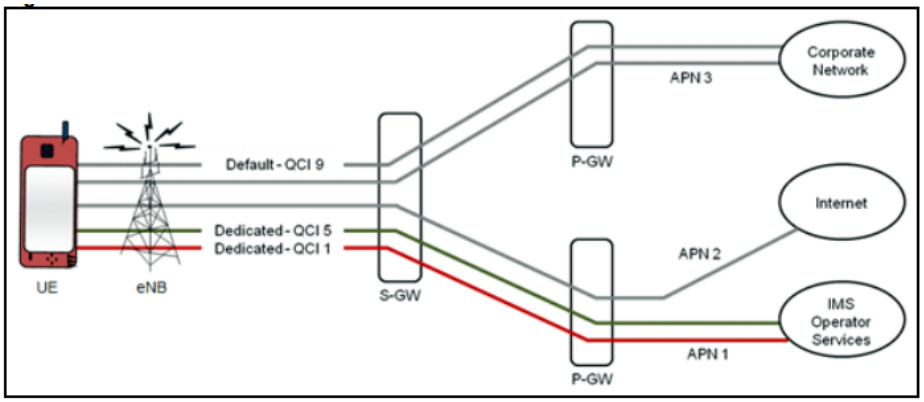

Ilustración 23: Aproximación de usos de QCI (58)

En el proceso de asignación de QoS, inicialmente se pasa por un estado por defecto en el que se establece la conexión entre el UE y el PGW, asignándose una portadora básica que se mantiene durante toda la vida útil de la conexión. Esta portadora por defecto es del tipo sin un GBR aunque según los modelos que adopten los operadores se le podrá asignar una QoS según el tipo de suscripción. A parte de ésta, se puede añadir dinámicamente una portadora dedicada según las asignaciones en base a los tipos de datos y las políticas del operador (54).

Un paquete IP que entra al sistema es marcado con una cabecera que contiene la identificación del portador con los parámetros apropiados de QCI, para lo cual, operadores y/o ISPs disponen de dos herramientas. Por un lado el tipo de servicio (HTTP, P2P, streaming, VoIP, etc.) y por otro el tipo de suscripción (prepago, postpago, tipo de tarifa, etc.). En cualquier caso es el núcleo de red quien toma la decisión de modificar una portadora, aunque en función de los parámetros citados y/o a través del empleo de análisis de tráfico.

El PGW se encarga del mapeo de las portadoras al nivel de enlace subyacente que típicamente será basado en Ethernet. Este nivel no es consciente del concepto de portadora y podrá utilizar

técnicas de QoS IP estándar, como MPLS o DiffServ, cuyo valor de cabecera es el DSCP (DiffServ Code Point). La siguiente ilustración muestra este comportamiento.

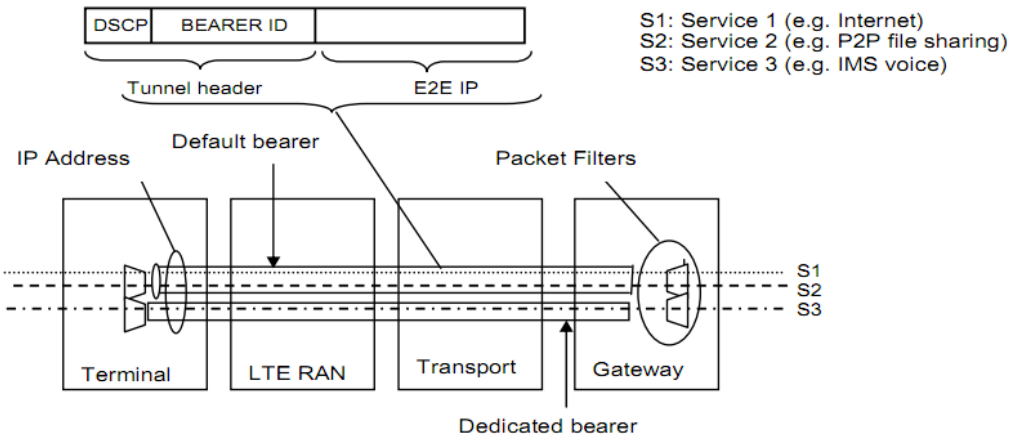

Ilustración 24: Visión extremo a extremo de QCI (54)

4.1.2.3 Políticas de control

En el núcleo LTE/SAE la selección y aplicación de los diferentes tipos de servicio se determinan mediante unas políticas y reglas definidas por el operador de la red y conocidas como PCC. Se trata de una arquitectura sofisticada que permite el control dinámico de los servicios IP de un suscriptor en base a sus flujos de datos.

Esto se consigue por medio de un análisis detallado y aplicando una gestión de QoS que permite controlar dinámicamente los requisitos de los servicios que se prestan. Esto representa un gran cambio respecto a los anteriores sistemas móviles, donde el servicio de control se realizaba principalmente a través de la autenticación del UE por la red. El sistema PCC controla y gestiona dinámicamente todas las sesiones de datos y proporciona interfaces apropiadas para los sistemas de cobro y facturación, permitiendo así también nuevos modelos de tarificación a los operadores.

El control dinámico sobre QoS y facturación hace posible, por ejemplo, la definición de unos servicios de ancho de banda por niveles o la compra por tiempo limitado del acceso a un contenido específico o con QoS mejorada.

Los bloques funcionales del PCC son los que se muestran en la siguiente ilustración y se describen a continuación (58).

- **Policy Charging and Rules Function (PCRF):** Entidad que proporciona las políticas de control y las decisiones a tomar en base a los flujos de datos.

- **Policy and Charging Enforcement Function (PCEF):** Implementado con el PGW, se encarga de la aplicación de las políticas del PCRF, también proporciona la medición para apoyar la facturación.

- **On-line Charging System (OCS):** Proporciona la gestión de crédito o saldo y reporta a la PCEF información basada en el tiempo, el volumen de tráfico, etc.

- **Off-line Charging System (OFCS):** Recibe información de la PCEF y genera registros de datos para el sistema de facturación.

- **Application Function (AF):** Elemento del plano de control que representa a las aplicaciones que requieren una política dinámica de QoS.

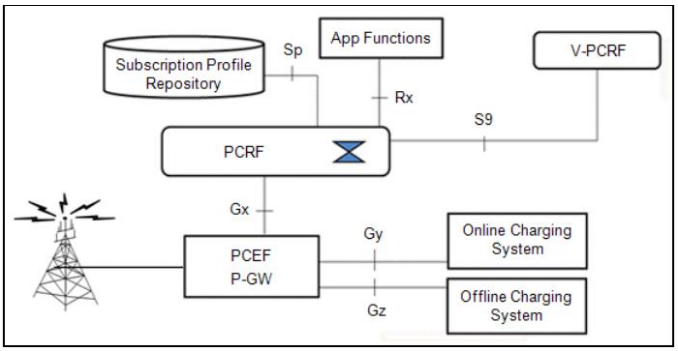

Ilustración 25: Arquitectura PCC de 3GPP (58)

El control de QoS se aplica por cada flujo de datos en el PCEF, que utiliza las reglas del PCRF para clasificar el tráfico. Las reglas pueden ser predefinidas o dinámicamente provisionadas por el PCEF derivándose desde el PCRF con la información subministrada por la AF (por ejemplo, el ancho de banda requerido) y por el propio PCEF (por ejemplo, nivel de QoS necesario) en función de la aplicación/protocolo, además de por otros datos del suscriptor.

La provisión de normas a través del PCRF a la PCEF puede llevarse a cabo de dos modos (59)

- **'Push':** Cuando la provisión no es solicitada, por lo tanto el PCRF puede decidir la prestación de reglas sin necesidad de obtener una solicitud de la PCEF.

- **'Pull':** Cuando la provisión ha sido solicitada por una petición de la PCEF. Una serie de reglas de filtrado en el PCEF detectan los paquetes relevantes. Las reglas PCC resultantes en base a esta detección contienen los indicadores QCI y las tasas permitidas para el flujo en cuestión.

4.1.2.4 Análisis de tráfico en SAE/LTE

Si bien no se define explícitamente en las especificaciones de LTE/SAE, el despliegue de equipos del tipo DPI/DFI, bien como plataformas independientes o bien como parte del PGW, está estrechamente relacionado con la filosofía de esta arquitectura.

Como muestra más clara es de notar la función 'pull' de petición de QoS, donde es el PCEF quien solicita unos parámetros basándose en el tipo de tráfico. Sin su uso esta función deja de cobrar sentido en muchos casos, ya que como veremos en el capítulo V, el análisis profundo de tráfico se hace necesario para la correcta clasificación de protocolos o servicios.

El control extremo a extremo de QoS es capaz de combinar la capacidad de la entidad DPI/DFI para identificar los servicios OTT con la información de la PCRF, con el fin de que esta proporcione las políticas basadas en el perfil de QoS basándose en la aplicación o servicio y en el suscriptor (60)

De forma similar a lo expuesto en el apartado 4.1.1.4 la función de análisis se lleva a cabo en el PGW ya que es el punto de salida hacia las redes PDN e Internet, y en efecto es donde los fabricantes incluyen dichas funciones, como se verá en el siguiente capítulo.

4.2 Gestión de tráfico en redes fijas

Las redes fijas de acceso se suelen englobar básicamente en tres tipos, según el medio de transmisión: cable, par de cobre o fibra. Los dos primeros tipos son los que históricamente han tenido más penetración debido a que en la era de la popularización de Internet se aprovechó el medio físico existente, el cable coaxial en redes HFC y el par de cobre telefónico. En ambos casos se fueron adaptando de la mejor forma posible a las necesidades de una comunicación de banda ancha creciente, dando lugar a los estándares DOCSIS y xDSL, que hasta la fecha han conseguido ir optimizando los respectivos medios para la transmisión de datos.

No obstante, estas dos infraestructuras no son las más adecuadas para este cometido. Se debe tener en cuenta que el cable inicialmente se diseñó para llevar señal TV unidireccional, y el par de cobre para señal telefónica, por lo que presentan limitaciones notables. Así poco a poco han ido desarrollándose las tecnologías de FTTx, que sí presentan unas buenas características para los servicios de hoy en día, pero su despliegue es lento y costoso.

Igual que se ha hecho en el subcapítulo 4.1, en este apartado se revisan las características de las arquitecturas existentes que tienen relación con la gestión de tráfico basada en QoS y 'policing'.

4.2.1 Cable - DOCSIS

El cable, debido a sus características intrínsecas, es el medio fijo que presenta una mayor necesidad para la gestión de tráfico por tratarse de un enlace físico compartido generalmente por varios usuarios, creando un mayor incentivo para los operadores de este tipo de redes para mantener un control.

Además hay que tener en cuenta que la mayoría de las compañías de cable se han convertido a los llamados MSO, que ofrecen acceso a Internet y telefonía, así como televisión. Dado que

las redes de cable fueron diseñados originalmente sólo para las señales de televisión unidireccionales, esto ha requerido una constante evolución en la ingeniería de las redes, siendo la arquitectura básica de una red de televisión por cable considerablemente diferente de las arquitecturas utilizadas en redes de telecomunicaciones con origen en la telefonía.

El estándar DOCSIS es el encargado de proporcionar los mecanismos para el control en tiempo real de flujos de QoS y de ofrecer servicios integrados. Esta norma está estandarizada por el consorcio CableLabs y es aceptado a nivel mundial por fabricantes y otros estandarizadores, entre ellos la ETSI, que se encargó de adaptar las versiones de DOCSIS a las necesidades europeas con la definición de euroDOCSIS (en la versión DOCSIS 3.0 ya se incluye un anexo para la especificación europea).

Hasta la fecha existen cuatro definiciones de DOCSIS (61):

- **DOCSIS 1.0:** Primera especificación DOCSIS publicada en marzo de 1997. Se trata de la especificación base que incluye un acceso a Internet 'best effort' con una tasa de 5 Mbps de bajada.

- **DOCSIS 1.1:** Especificación DOCSIS publicada en abril de 1999 y que ofrece una gestión de QoS para servicios sensibles al retardo además de añadir mejoras de seguridad y una tasa de bajada de hasta 10 Mbps.

- **DOCSIS 2.0:** Especificación salida a la luz en diciembre de 2001 y que aumenta hasta 30 Mbps las tasa de bajada, gracias en parte a la inclusión de dos nuevos tipos de modulación: S-CDMA y A-TDMA (Synchronous Code Division Multiple Access/Advanced Time Division Multiple Access). Añade soporte a servicios simétricos y permite el desarrollo de módems de bajo coste.

- **DOCSIS 3.0:** Especificación publicada en agosto de 2006 que puede permitir velocidades de hasta 160 Mbps de bajada (130 Mbps de subida). Además añade mejoras de seguridad y gestión de canales QoS con soporte para IPv6.

4.2.1.1 Arquitectura de red

El cable coaxial se empleó inicialmente para distribuir señales de TV en zonas donde la difusión radioeléctrica era complicada tratándose tan sólo de un medio de distribución unidireccional. El ancho de banda que puede proporcionar es grande aunque limitado, y al aumentar la oferta de canales por allá en los años 90 se fue incorporando fibra óptica en las partes centrales de la red dando lugar a la topología HFC. De este modo se pasó de sistemas de distribución a sistemas bidireccionales completos de telecomunicaciones con capacidad de transmitir servicios de voz y datos.

En una red de arquitectura HFC la fibra llega hasta un OTN (Optical Terminal Node), punto donde se convierte la señal del dominio óptico al eléctrico. A partir de aquí la distribución se

hace mediante cable coaxial, que es compartido por una cantidad de usuarios finales que suele oscilar entre 8 y 500, dependiendo fundamentalmente de hasta dónde llegue la fibra óptica. En las instalaciones modernas, este coaxial es bidireccional y transporta los servicios de TV, datos y posiblemente telefonía VoIP (aunque existen soluciones que ofrecen el servicio de telefonía sobre par de cobre paralelo al coaxial), por lo que se deben garantizar unos ciertos parámetros de QoS diferenciados para el correcto funcionamiento de los servicios comentados.

Los componentes principales de la arquitectura DOCSIS son el Cable Modem (CM), ubicado en las instalaciones del cliente, y el CMTS (Cable Modem Termination System), ubicado en la cabecera de la red. El CM tiene como función principal la de 'gateway' pasando del protocolo de la red de coaxial a, generalmente, un protocolo Ethernet. El CMTS tiene la función de agregación y control. El siguiente esquema muestra la distribución de los elementos comentados.

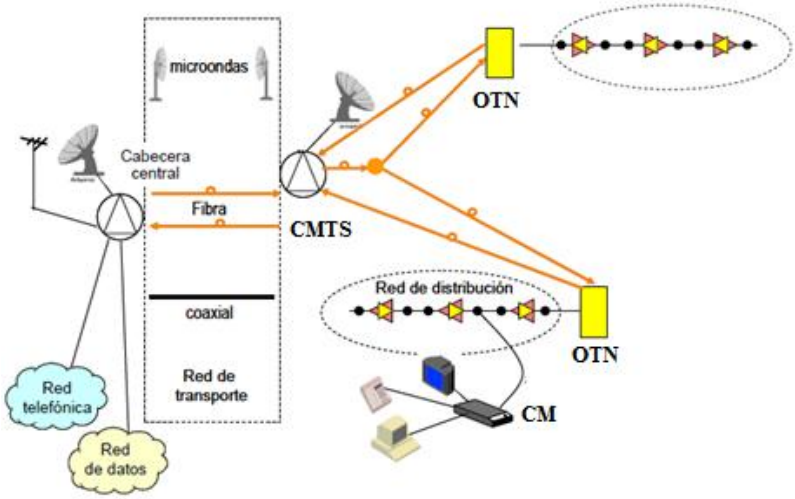

Ilustración 26: Arquitectura de red HFC (61)

4.2.1.2 Niveles de QoS

Con la evolución hacia DOCSIS 3.0, una serie de complementos se han ido introduciendo en previsión a los problemas asociados a la adopción generalizada de servicios de alta velocidad. La industria del cable ha manifestado desde un principio la necesidad de una mejor medición de uso y gestión de QoS como herramientas para asegurar una QoE y gestión del tráfico óptimas. Para este fin se han introducido sobre las normas CableLabs el IPDR (Internet Protocol Detail Record) y el PCMM para llevar a cabo la medición de uso y un control dinámico de QoS, respectivamente.

Así, DOCSIS incluye desde su versión 1.1 la posibilidad de ofrecer gestión de tráfico según la QoS demandada mediante el PCMM. Para ello se define el 'service flow' (equivalente al SDF definido por la 3GPP) que no es más que un flujo unidireccional de paquetes. La comunicación entre el CMTS y el CM establece un nivel de QoS controlando el tráfico de acuerdo a los

parámetros que se definan para el flujo de servicio en concreto y respondiendo a necesidades de latencia, fluctuación del retardo (jitter) o capacidad (62).

Los servicios básicos definidos son (61) (63) (64):

- **Unsolicited Grant Service (UGS):** Ofrece soporte para flujos de servicio en tiempo real con tamaños de paquete fijos (por ejemplo la VoIP) con la reserva de recursos fijos del enlace.

- **Real Time Polling Service (RTPS):** Ofrece soporte para flujos de servicio en tiempo real con tamaños de paquete variable, como por ejemplo el envío de video por streaming codificado con el formato MPEG (Moving Picture Experts Group).

- **Unsolicited Grant Service with Activity Detection (UGS-AD):** Se diseña para soportar flujos del tipo UGS que pueden permanecer inactivos durante un periodo de tiempo (por ejemplo, VoIP con supresión de silencios) para así liberar recursos del medio mientras no son empleados.

- **Non Real Time Polling Service (NRTPS):** Diseñado para dar servicio a flujos que generalmente requieren un gran ancho de banda pero que no requieren transferencia en tiempo real (transferencias del tipo P2P o 'Direct Download').

- **Best Effort (BE):** Servicio para el tráfico sin garantías (navegación web, email, etc.).

4.2.1.3 Políticas de control

Para la gestión de las políticas de control en las redes de tecnología DOCSIS se han venido empleando dos mecanismos que de forma complementaria se han encargado de las funciones de medición y de gestión.

4.2.1.3.1 IPDR

El IPDR se introdujo con la versión de DOCSIS 2.0 como alternativa al Simple Network Management Protocol (SNMP) para el control de uso y facturación y para mejorar algunos defectos conocidos de la utilización de éste en redes de alta velocidad. IPDR se basa en un modelo en el que el CMTS envía de forma periódica las exportaciones de un lote de registros a un colector, que procesa y gestiona los datos.

Este modelo simple ofrece un medio eficiente y escalable para recoger un análisis grueso de la red que antes sólo estaban disponibles a través de SNMP o mediante sistemas propietarios. El esquema IPDR tal y como se definió en DOCSIS 2.0 se basa en que cada registro lleva una cuenta de bytes transportados por flujo de servicio. Además de la métrica de uso, IPDR incluye reportes de SLA (Service Level Agreement) para paquetes perdidos y retardados. La

especificación IPDR para transmitir un lote de registros de forma periódica establece un periodo de más de 15 minutos (62). Esto supone una limitación para el control de servicios que requieren actualizaciones en tiempo real, como servicios prepago, gestión de cuotas o gestión del tráfico, por lo que se deben contemplar alternativas a IPDR para la gestión de éstos.

Además, IPDR no proporciona una sustitución completa de SNMP, lo cual, unido al hecho de que los campos en los registros IPDR con la información de SLA son algo difíciles de interpretar, limita seriamente la utilidad general de IPDR y la posiciona como una tecnología para servicios de tiempo no real (62).

4.2.1.3.2 PCMM

PCCM constituye una técnica para ofrecer servicios diferenciados de QoS a través de una infraestructura de cable basada en IP, pero no está diseñado para gestionar el tráfico de forma dinámica. No obstante, ofrece oportunidades significativas para mejorar los servicios ya que los operadores pueden ofrecer garantías de QoS para servicios multimedia mediante la infraestructura de acceso DOCSIS.

Para llevar el control de QoS, se define un marco para proporcionar diferentes niveles de servicios multimedia a través de un acceso DOCSIS (versión 1.1 o superior) asignando los flujos de servicio descritos en el apartado anterior según una clasificación basada en un análisis de quíntupla.

La arquitectura PCMM se compone de los siguientes bloques funcionales, que son representados más adelante en la ilustración (65) (66):

- **Aplication Mananger (AM):** Se le atribuye el control de sesiones. El cliente se comunica con la AM de forma directa mediante la red IP solicitando un servicio con QoS y esta se encarga hacer la petición al PS y de reservar los recursos del flujo de servicio si éstos están disponibles.

- **Policy Server (PS):** Es el responsable de la coordinación de las peticiones de QoS por parte de los AM, además de determinar los parámetros necesarios para las diferentes aplicaciones multimedia.

- **Cable Modem Termination System (CMTS):** El CMTS es el encargado de la ejecución y cumplimiento de la QoS asignada. Realiza el control de admisión y gestiona los recursos de los diferentes flujos de servicio. Se comunica para ello con el PS y el RKS.

- **Record Keeping Server (RKS):** Realiza una función de mediación entre los elementos PCMM y las aplicaciones internas para la facturación. Recibe mensajes de eventos relacionados con las decisiones de política del PS y notificaciones de los parámetros de QoS desde la CMTS.

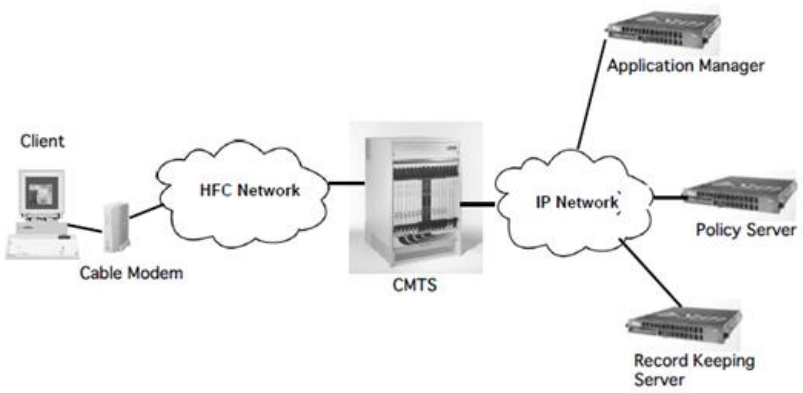

Ilustración 27: Arquitectura de PCMM (66)

En este modelo, el PS es el responsable de tomar las decisiones de 'policing' basadas en las reglas definidas por los operadores, mientras que el punto de aplicación es el CMTS. El PS está conectado con la AM y con el CMTS, el cual realiza el control de admisión en la petición de establecimiento de QoS y es donde se adopta la decisión y establece el flujo correspondiente.

En una secuencia típica de establecimiento de conexión la aplicación del cliente solicita un determinado ancho de banda a la AM, la cual comprueba en el PS si las políticas de negocio permiten esta aplicación y con qué parámetros. El PS confirma entonces la disponibilidad de recursos y autoriza la concesión de QoS al CMTS. El CMTS es el encargado de determinar si el ancho de banda está disponible y en caso afirmativo establece el 'service flow' con la QoS pactada. El CMTS enviaría entonces un mensaje de notificación de QoS a la RKS, y el PS por su parte le enviaría un mensaje del evento, según las políticas definidas (66).

La arquitectura PCMM identifica tres clases de clientes según su capacidad de hacer peticiones de QoS (66):

1. **Clientes que no especifican una QoS determinada:** En este tipo de cliente es la AM quien hace la petición de QoS en nombre del cliente.

2. **Clientes que soportan señalización QoS pero no la autorización:** Este cliente es consciente de la existencia de PCMM y por lo tanto se comunica con un AM para solicitar una QoS.

3. **Clientes que soportan señalización QoS y autorización:** Este último grupo realiza la petición de QoS mediante el protocolo RSVP y no interactúan con la AM.

4.2.1.4 Análisis de tráfico en Cable

La inclusión de equipos con capacidad de análisis DPI/DFI puede resolver algunos de los problemas a la hora de llevar una gestión eficiente en redes HFC, ya que los dispositivos de análisis permiten clasificar los paquetes con un control más preciso que la clasificación basada

en la quíntuplas. El mayor control ofrece la posibilidad de clasificar los paquetes según cada aplicación y asociar estos paquetes a los flujos de servicio respectivos.

Una vez que un dispositivo de DPI ha clasificado correctamente un paquete o flujo, puede entonces dirigir, marcar, etiquetar, bloquear, limitar la velocidad, etc. de los paquetes o flujos. Este control es considerablemente más amplio que el que puede ofrecer PCMM y en efecto el uso de DPI junto con servidores de políticas ha sido extendido en la industria del cable (62).

4.2.2 Acceso fijo - TISPAN

La gestión de tráfico en las redes fijas de NGN como pueden ser el xDSL o la fibra no presentan un problema notable de congestión en el acceso en comparación con las redes móviles y cable. No obstante, la tendencia convergente en materia de provisión de QoS entre tecnologías lleva a la generalización de una visión extremo a extremo en las políticas de gestión, por lo que una arquitectura global está siendo desarrollada.

El organismo TISPAN, es una entidad de normalización fundada en 2003 dentro de la ETSI, y se centra en definición de una NGN basada en las especificaciones IMS de 3GPP como núcleo de red. Establece por lo tanto un marco funcional para las NGN que soporta una combinación de comunicaciones fijas y móviles sobre la base de IMS (67).

Hasta la fecha existen tres versiones (68) (69):

- **TISPAN Release 1**: Salida a la luz en 2005. Se focaliza en el acceso xDSL, dando cabida no obstante a conexiones WLAN. Integra el manejo de contenidos multimedia con especial hincapié en servicios conversacionales en tiempo real como VoIP o videoconferencia. Añade un subsistema de emulación de la red PSTN/ISDN (Public Switched Telephone Network/Integrated Services Digital Network).

- **TISPAN Release 2:** Segunda especificación TISPAN de 2007. Mejora el acceso a los recursos de acuerdo al perfil de usuario según suscripción y uso de servicios. Se centra también en IPTV.

- **TISPAN Release 3:** Especificación en desarrollo que trabaja en mejoras de IPTV, interconexión de redes y mejoras de seguridad y QoS, entre otras funcionalidades (70).

4.2.2.1 Arquitectura de red

Las tecnologías de acceso fijo suelen presentar un problema potencial de congestión en el nivel de agregación y no presentan un problema en el acceso, en gran medida debido a que el medio de acceso no es compartido. Así, a diferencia de los modelos 3GPP y CableLabs, el modelo de red de TISPAN considera la aplicación de QoS con una visión global de la red, es decir, contemplando acceso, agregación y núcleo.

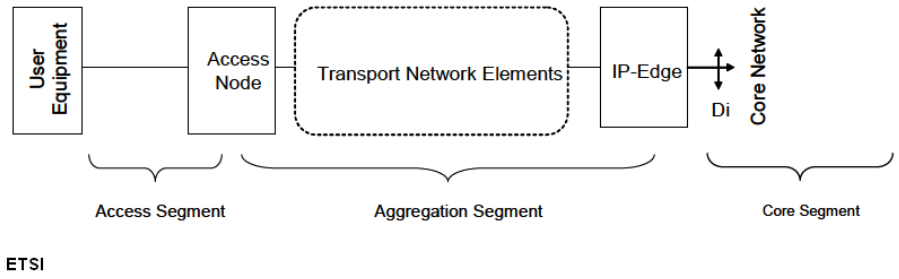

Ilustración 28: Arquitectura genérica de red fija (70)

En este escenario no se analiza el diseño de la red de acceso ya que que las soluciones de estandarización contemplan una visión extremo a extremo para un núcleo de red integrado. No obstante, sí que se citan los elementos que componen esta arquitectura, que incluyen: un subsistema de base de datos y AAA llamado NASS (Network Attachment Subsystem); un subsistema de control de recursos y admisión conocido como RACS; un subsistema multimedia IMS; un subsistema PES (PSTN/ISDN Emulation Subsystem) de emulación de los servicios tradicionales de telefonía; y otros subsistemas, aplicaciones multimedia y componentes de servicios comunes de estos subsistemas (servidor HSS, función de facturación, seguridad, función de señalización, función de intercomunicación, etc.). Véase la Ilustración 29 más adelante para ver su esquema funcional.

4.2.2.2 Niveles de QoS

Para la gestión de la QoS TISPAN define el RACS, un componente fundamental para soportar el control de QoS extremo a extremo en un entorno NGN. Uno de los propósitos iniciales de la norma fue permitir que las compañías telefónicas que migren hacia VoIP pudiesen ofrecer un servicio telefónico que emule el servicio tradicional en el establecimiento de la llamada, es decir, dar la posibilidad de denegar una solicitud de conexión si se considera que la red está demasiado congestionada para realizar la llamada.

Para ello ofrece servicios basados en la política de control de transporte en base a las aplicaciones. Esto permite la petición y reserva de recursos de transporte en el acceso y en las redes centrales dentro de su cobertura. También incluye puntos de interconexión entre éstas a fin de soportar el establecimiento de QoS extremo a extremo y funciones de control de admisión. El control de admisión contempla la autorización, las reglas específicas de la política del operador, y la comprobación de disponibilidad de recursos de transporte sobre la base del perfil de usuario almacenado en las bases de datos de acceso a la red.

La arquitectura RACS proporciona una asignación de QoS mediante la adopción de al menos uno de los dos modelos dinámicos de control de QoS (70):

- **QoS garantizado:** Servicio de entrega de tráfico con valores definidos de todos o algunos de los parámetros de QoS tales como rendimiento, latencia, jitter y PELR. Se implementa mediante control de tráfico y aplicación de políticas.

- **QoS relativo:** Servicios de tráfico de entrega sin valores definidos en el ancho de banda logrado, tasas de PELR o retardo de paquetes. Se implementa mediante marcado de paquetes.

4.2.2.3 Políticas de control

Bajo el control del NASS y del RACS, la capa de transporte proporciona conectividad entre los terminales de forma transparente a las tecnologías de transporte utilizadas en las capas inferiores a IP, tanto en la red de acceso como en el núcleo de red. De este modo se pone en práctica la separación y la interacción entre la capa de servicios y la capa de transporte o datos. Para la gestión y aplicación de políticas de QoS se emplean las entidades que describen a continuación (67) (71) (72):

- **Service Policy Decision Function (SPDF):** Toma las decisiones de 'policing' mediante el uso de las reglas del servicio o definidas por el operador de red, y determina si se atiende la petición mediante el A-RACF o directamente por el BFG.

- **Acces-Resource and Admision Control Function (A-RACF):** Asistido por el NASS, el A-RACF se encargada de la decisión de la admisión y reserva solicitada por el SPDF en base a la disponibilidad de recursos en las redes IP bajo su control (acceso y agregación).

- **Resource Control Enforcement Function (RCEF):** Ubicado en el nodo externo de la red de acceso, se encarga de la aplicación de políticas de forma independiente o en conjunto con el BGF, en función del tipo de petición de servicio.

- **Border Gateway Function (BGF):** Ubicado en el borde del núcleo de la red, se trata de un 'gateway' o pasarela del plano de datos. El BGF lleva a cabo funciones de aplicación de las políticas (además de otras, como la gestión de NAT) bajo el control de la SPDF y proporciona el encaminamiento entre dos redes IP.

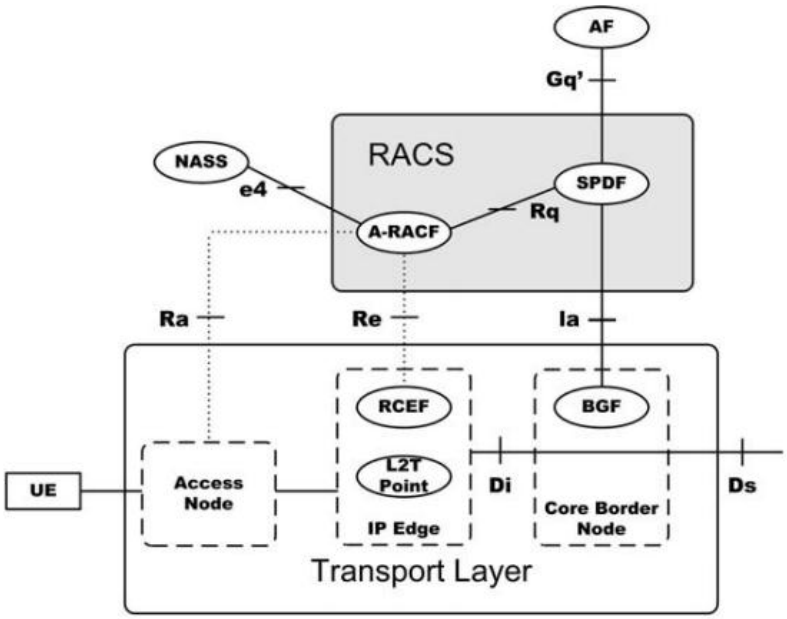

Ilustración 29: Arquitectura TISPAN (72)

Nótese que tanto el RCEF y el BGF pueden aplicar políticas de tráfico, llevar control de flujos y marcar los paquetes, mientras que el BGF, además, puede realizar servicios adicionales como la asignación de recursos por uso, métrica de flujos y poner en práctica el manejo de NAT. Dependiendo de la decisión del SPDF, las solicitudes de recursos pueden ser enviadas a través de un A-RACF a la RCEF y/o directamente al BGF.

Antes de admitir el tráfico de usuarios, la funcionalidad de control de admisión proporcionada por el RACS realiza las siguientes comprobaciones (en una operación sencilla en red interna). En primer lugar, se verifica la autenticación de los usuarios con ayuda de los perfiles almacenados en el NASS. En segundo lugar, el RACS aplica las políticas almacenadas en el SPDF específicas del operador para luego comprobar la disponibilidad de recursos mediante la A-RACF. Por último, las decisiones de política de control de admisión y se aplican en el RCEF, ubicado en el acceso a la red (72). El establecimiento de la conexión extremo a extremo plantearía un proceso similar, aunque de mayor complejidad.

El aprovisionamiento de reglas de control en el marco TISPAN puede darse tanto en modo 'push' como en modo 'pull' (70).

- **'Push':** Modelo en el que el RACS autoriza una petición de reserva en base a las políticas definidas, reserva los recursos necesarios y da la orden al RCEF para que aplique la QoS pactada.

- **'Pull':** Tras una petición de reserva originada en el cliente y solicitada por el RCEF, el RACS reserva los recursos necesarios y da confirmación al RCEF.

4.2.2.4 Análisis de tráfico en accesos fijos

Debido a la naturaleza de los accesos fijos sobre los que trabaja TISPAN, no ha sido en este ámbito donde más se han desarrollado las tecnologías de análisis profundo en comparación con las redes móviles o cable. No obstante, la integración de sistemas y equipos dispuestos para este fin suelen ser polivalentes e instalables en redes IP con cualquier tipo de acceso. La tendencia es tal que para poder tener un control sobre el tráfico extremo a extremo será imprescindible tener equipos DPI/DFI.

4.3 Comparativa de arquitecturas de gestión QoS y Policy

En contraposición con las soluciones de otros organismos de normalización, el estándar PCMM es maduro y usado a escala mundial. No obstante, la interoperabilidad con otras redes no se aborda directamente dentro de las especificaciones de PCMM, ya que la atención se centra en calidad de servicio en la red de acceso o en la red del operador. No obstante, la compatibilidad con otras redes en cuanto a funciones como NAT e IMS forman parte de la especificación PacketCable versión 2.0.

PCMM se puede ver como una base de la PCC, que representa en la actualidad el modelo de referencia. La diferencia fundamental radica en que la norma PCMM asume un control dinámico de QoS, mientras que la arquitectura PCC abarca tanto la dinámica de control de QoS como el control de facturación. El PCC de 3GPP especifica el uso del protocolo DIAMETER como el método para exportar la información de carga a los sistemas internos, que en contraste con IPDR es más flexible en cuanto a los parámetros disponibles y las tasas que puede soportar. Esto lo hace muy adecuado para aplicaciones en tiempo real de carga como el prepago de datos. Pese a las diferencias, CableLabs ha llegado a un acuerdo con 3GPP, lo cual significa que su entidad de gestión PCMM se alinea con la política de control PCC de la 3GPP.

Por el contrario, la cooperación entre TISPAN con su modelo RACS y 3GPP no ha dado lugar a una visión compartida. Los diferentes enfoques para las redes fija y móvil es uno de los factores de esta diferenciación de arquitecturas. El estándar RACS especifica la funcionalidad implementándola en la red de acceso, debido a que en las redes fijas la falta de capacidad es un problema potencial en el nivel agregado.

Por su parte, los recursos críticos en el acceso de redes inalámbricas se producen en el enlace radio, por lo que no es prioritario el control de la asignación de recursos con una perspectiva extremo a extremo. Las especificaciones del modelo de la 3GPP se apoyan en versiones anteriores que ya añadían funcionalidades en el núcleo, por lo que apostaron por una versión centralizada. La siguiente ilustración muestra esta diferencia de planteamientos.

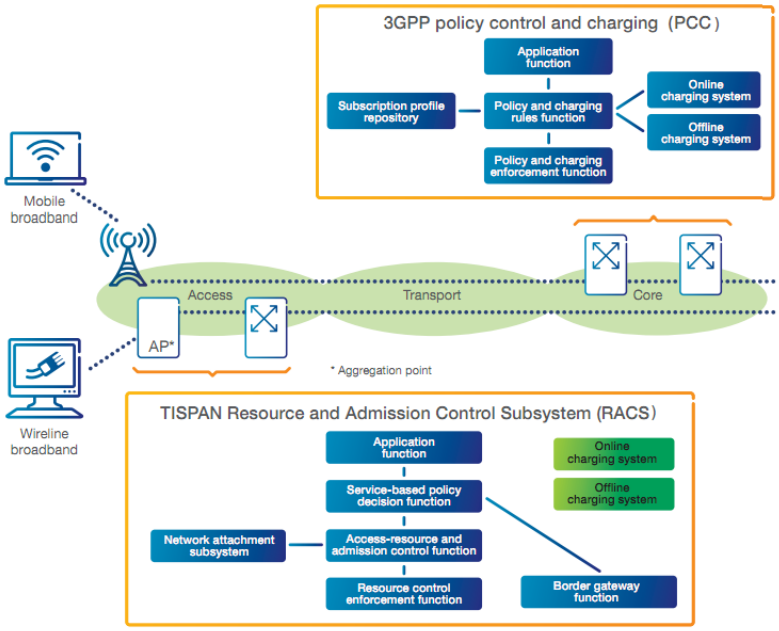

Ilustración 30: Enfoque PCC/3GPP y RACS/TISPAN (53)

A continuación se incluye una figura que extrae los puntos comunes de las entidades y funcionalidades que se llevan a cabo en cada una de las arquitecturas, separadas en plano de transporte, plano de control y plano de servicio.

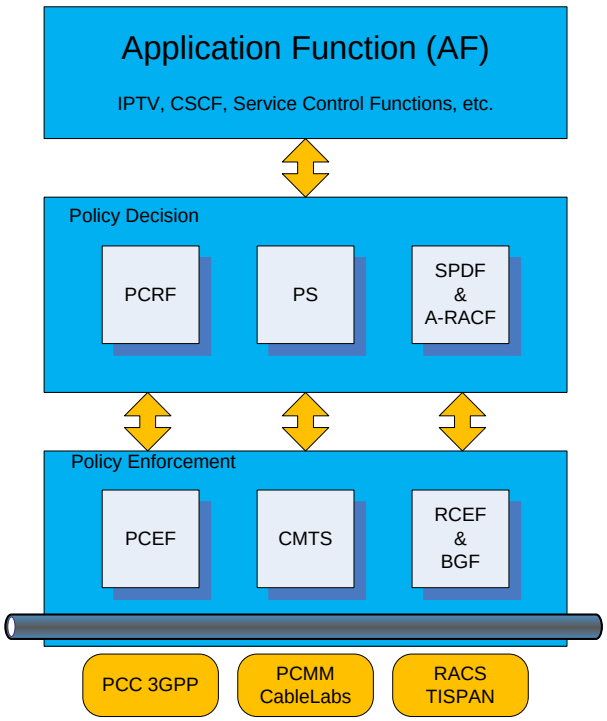

Ilustración 31: Comparativa entidades según plano de transporte y plano de control

Las propuestas consideradas en el dominio cable y móvil se centran en el control de los recursos específicos para cada tecnología de acceso a la red para la provisión de QoS mientras que TISPAN, al tener una visión más global e integradora tiene en cuenta también la red de agregación y de interconexión. Por lo tanto, el uso de dos entidades de decisión de 'policing' (SPDF & A-RACF) en la arquitectura NGN se justifica por la necesidad de aportar una solución escalable en escenarios de múltiples redes y dominios. Esta separación responde a un planteamiento de gestión de red interna o externa. En la decisión interna un proveedor está trabajando en una arquitectura de red propia y por lo tanto con sus políticas de entrega. Sin embargo, en el modo externo un proveedor debe evaluar la información entregada por terceros en el plano de control antes de gestionar los datos (53) (70) (71).

La alineación entre las diferentes entidades, si bien no es completa, es cada vez más apreciable. La convergencia de redes fijas y móviles es un hecho que se acabará produciendo a la larga y esto se ve reflejado en estas aproximaciones. Como factor común es de destacar la necesidad de tener un control sobre el tráfico a fin de poner en práctica la aplicación de diferentes niveles de QoS, por lo que como se muestra en el siguiente capítulo, se hace necesaria la utilización de técnicas de análisis DPI/DFI.

Capítulo V - Análisis del tráfico

En este capítulo se describen las tecnologías que se emplean para la clasificación y análisis de tráfico, que se conocen como DPI y DFI. Éstas se encuentran en un momento de máximo desarrollo debido a su estrecha relación con la gestión de tráfico y la asignación de QoS, y por su relación con la Neutralidad de Red.

El empleo de DPI/DFI es común desde hace varios años en aplicaciones de detección de spam, malware y ataques tipo DoS (Denial of Service), además de en sistemas tipo firewall. Actualmente su uso está creando cierta polémica en relación con el debate de la Neutralidad de Red, ya que su evolución ha hecho posible que se pueda emplear de modo que apenas afecte a la calidad de las comunicaciones, permitiendo nuevas funcionalidades a los ISPs.

Es importante resaltar que el conjunto de técnicas DPI/DFI se encarga tan solo del análisis de tráfico, aunque de ellas pueden derivan varias aplicaciones. Cualquier crítica o valoración se debería hacer en función de la aplicación en cuestión, y no de forma genérica a la tecnología. Por ello, la referencia a DPI/DFI en este documento se hace en el aspecto de análisis y reconocimiento de tráfico, y no a su aplicación posterior.

Los detractores de DPI, que básicamente son asociaciones de usuarios y proveedores de servicios como ya se ha visto en el capítulo II, alegan que esta tecnología viola los derechos de privacidad de las comunicaciones ya que permite analizar de forma exhaustiva el contenido de los paquetes. También aducen que implica una nueva forma de gestión de tráfico que permite formas de control por parte de los ISPs que amenazan seriamente el modelo abierto de Internet. Por su parte, los operadores de red e ISPs, se posicionan a favor de un uso de DPI/DFI que les permite solucionar problemas de congestión, prevenir ataques y malware, y obtener un retorno en sus inversiones mediante la aplicación de nuevos modelos tarifarios. Este debate, tal y como se ha visto a lo largo del capítulo III, constituye una de las bases de la Neutralidad de Red.

A continuación se hace una explicación sobre qué es DPI y DFI para luego dar un repaso a la evolución que ha seguido esta tecnología y las aplicaciones que se le da, a fin de enfatizar la función que tiene en cuanto a la gestión de tráfico. Posteriormente se analizarán las claves técnicas que hacen posible que esta tecnología sea capaz de trabajar con flujos de datos de cerca de 100 Gbps y analizar el tráfico de millones de suscriptores.

1 Técnicas de análisis: SPI, DPI y DFI

En la literatura se suele hablar de DPI para referirse tanto al análisis en cuestión como a las aplicaciones posteriores a este análisis. Incluso a veces se mezcla el concepto DFI, que se basa en otro principio. Para más confusión, previamente a la aparición de la tecnología DPI se empleaba otro tipo de análisis más simple conocido como SPI. Para clarificar estos términos, en este apartado se define cada uno de ellos.

Formalmente no existe una definición oficial sobre que es DPI ya que a diferencia de la gran mayoría de las tecnologías empleadas en las telecomunicaciones, no se trata de una técnica estandarizada. La definición según Wikipedia dice (73):

> *"…es el acto de inspección realizado por cualquier equipo de red de paquetes que no sea punto final de comunicación, utilizando con algún propósito el contenido que no es el encabezado (típicamente la carga útil) del paquete. Esto contrasta con la inspección superficial de paquetes (usualmente llamada Stateful Packet Inspection) que sólo inspecciona el encabezado de un paquete."*

Esta definición de DPI es algo ambigua en el sentido de que no queda claro que se interpreta como el encabezado de un paquete. Si consideramos que un punto intermedio de la red tan sólo se necesita la información del paquete hasta el nivel 3, entonces se podría considerar que la carga es desde este nivel en adelante.

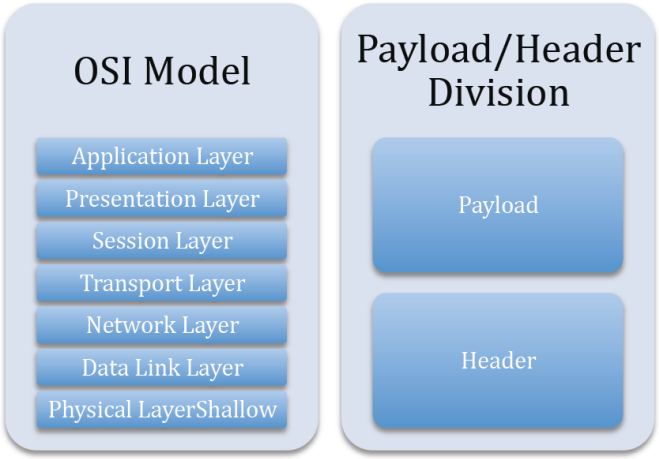

Ilustración 32: Separación entra cabecera y carga de un paquete (74)

El análisis de cabeceras de nivel 4 ha sido empleado con anterioridad a DPI y en la actualidad es implementado de forma genérica en firewalls y algunos routers, llevando a cabo habitualmente una inspección de lo que se conoce como quíntupla o flujo, lo cual precisamente es lo que se define como análisis SPI. Si consideramos que la información del

nivel 4 referente a los puertos ya forma parte de la carga del paquete IP, un análisis de esta capa ya se consideraría DPI.

Por tanto, según esta definición se podría catalogar SPI como un conjunto reducido de DPI. Para evitar malentendidos, se limita el uso de SPI para el análisis hasta la cabecera de la capa de transporte, y el uso de DPI cómo el análisis más allá de la cabecera de ésta, es decir, el análisis de la capa de aplicación e incluso los datos de usuario.

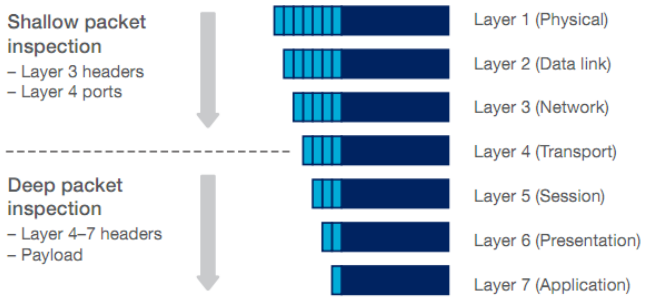

Ilustración 33: Límite entre SPI/DPI (53)

Así, a partir de este punto se define DPI como:

> ***"DPI es el análisis e inspección, en un punto de la red diferente de las terminaciones, de un paquete más allá de la cabecera del nivel 4 del modelo OSI, llegando incluso a analizar el contenido del mismo"***

Siendo la definición de SPI:

> ***"SPI es el análisis e inspección, en un punto de la red diferente de las terminaciones de la comunicación, de las cabeceras de un paquete hasta la cabecera del nivel 4 del modelo OSI,"***

La motivación para el desarrollo de DPI se fundamenta en que la clasificación tradicional basada en el análisis de las cabeceras de los niveles 2 a 4 del modelo OSI (SPI) no es un mecanismo fiable a día de hoy para determinar información sobre el protocolo y la aplicación que transporta un paquete. Existen estudios que determinan que en el peor de los casos un análisis basado en las cabeceras en estos niveles tan sólo es capaz de clasificar el 30% del tráfico (en el mejor de los casos un 70%) (75). Esto se debe fundamentalmente a que se lleva a cabo un proceso de enmascaramiento.

- **Enmascaramiento:** Se trata de una técnica utilizada por ciertos protocolos que hacen un uso no en acorde a los 'well-known ports' para evitar su reconocimiento. En su versión más simple, las conexiones se suelen realizar a través del puerto 80, que es el definido para las conexiones HTTP. Posteriormente las aplicaciones han evolucionado de modo que se emplean diferentes combinaciones de puertos para que sea más difícil su detección.

Debido a este uso irregular de las asignaciones de números de puertos, que son definidos por la IANA, se requiere el empleo de técnicas más sofisticadas que SPI para reconocer el tipo de datos que atraviesan una red. DPI permite clasificar protocolos en tiempo real, pudiendo llegar a analizar si fuese necesario hasta la información de usuario. Esto se consigue mediante la búsqueda de firmas, entendiéndose como tal un identificador que los desarrolladores de DPI/DFI asignan a la búsqueda de un protocolo o aplicación. En el apartado 4.3 se analiza este procedimiento.

Pese a la mejora que supone para la clasificación de paquetes respecto a SPI, los equipos convencionales DPI tienen algunas deficiencias a la hora de reconocer algunas aplicaciones y/o protocolos, sobre todo al tratar con tráfico cifrado u ofuscado. Cabe no confundir estos dos términos, que a menudo se suelen emplear como sinónimos (76) (77):

- **Cifrado:** Es la técnica mediante la cual se codifica la información de un paquete haciendo uso de algoritmos matemáticos complejos con el fin de establecer una comunicación de forma segura consiguiendo privacidad, confidencialidad, autenticidad, etc. Los métodos de cifrado más extendidos se basan en la dificultad de aplicar una ingeniería inversa para descifrar el mensaje (se podría conseguir por fuerza bruta, pero el tiempo necesario con la capacidad de procesado actual seria de órdenes de tiempo muy elevados). Uno de los métodos más empleados es RC4 (Rivest Cipher 4), que es la base de SSL/TLS (Secure Socket Layer/Transport Layer Security).

- **Ofuscación:** Esta técnica, a diferencia del cifrado, está enfocada eludir el análisis DPI, en muchos casos sin preocuparse de asuntos típicos de éste como la privacidad o la confidencialidad. Para ello, el envío de datos se hace de forma que se ocultan las operaciones deterministas tales como las secuencias o paquetes de tamaños fijos, habituales en procesos de establecimiento de la conexión o 'handshake', por ejemplo. Esto se consigue mediante la mezcla y alteración de los datos, haciendo que el proceso de análisis sea más complejo de lo necesario e incluso cifrando los datos o parte de ellos. Un buen ejemplo del empleo de esta técnica se da en el popular cliente eMule. (78) También se considera ofuscación el empleo de mecanismos de 'tunneling' del tipo SSH (Secure Shell) o HTTPS (HyperText Transfer Protocol Secure) (77). En el caso del protocolo BitTorrent incluso se define este tipo de cifrado como Message Stream Encription (MSE) o también, de modo más explícito como Packet Header Encryption (PHE). (79) Skype, por su parte, emplea el método de cifrado Advanced Encryption Standard (AES) además de trabajar sobre un protocolo propietario, lo cual dificulta aún más su identificación (80).

Por la evolución de estas técnicas se ha dado el desarrollo del análisis DFI, que lleva a cabo un análisis heurístico o de comportamiento para determinar qué tipo de tráfico está fluyendo por la red. DFI es capaz de detectar una aplicación (o amenaza) a partir del comportamiento del flujo de paquetes, en lugar de buscar el protocolo o el uso de puertos dentro del mismo paquete. Este hecho es importante, porque cada vez más tráfico está cifrado o es transmitido mediante 'tunneling' a través de la red, y más aplicaciones son enmascaradas u ofuscadas.

Así, con DFI se consigue que el cifrado u ofuscación tenga poco efecto sobre la precisión y capacidad de clasificación. Aunque el cifrado impide acceder al contenido de los paquetes, por lo que protege la privacidad la comunicación, esto no imposibilita que se pueda determinar el protocolo que se está empleando. Esta idea será desarrollada en el ejercicio expuesto en el apartado 5 de este capítulo.

No obstante, cabe señalar que el análisis SPI no es siempre exacto, ya que se basa en un reconocimiento de patrones. La aparición de nuevos protocolos y aplicaciones hace que SPI se tenga que ir actualizando en consecuencia. La mayoría de los suministradores suelen ofrecer suscripciones a versiones de software con los últimos algoritmos para la detección de tráfico enmascarado. Este tipo de análisis se detalla en el apartado 4.4.

1.1 Aplicaciones de DPI/DFI

En este subcapítulo se hace una breve descripción de las aplicaciones que tiene esta tecnología con el objetivo de dar una visión general de las posibilidades que ofrece. Originalmente este tipo de análisis fue utilizado como una herramienta de control de tráfico off-line para llevar a cabo una planificación de las redes previo conocimiento del tráfico que estaba consumiendo su capacidad. Posteriormente se empleó para ayudar a identificar y bloquear el tráfico P2P (siendo éste aún a día de hoy de los mayores desafíos de DPI/DFI), prevenir ataques del tipo DoS, ofrecer servicios jerarquizados mediante clasificación del tráfico, gestión de control parental e incluso la inyección de publicidad orientada al usuario en base a la información extraída de su tráfico, entre otros.

De forma más global, las técnicas de DPI/DFI se pueden emplear en una amplia variedad de funciones:

- **Seguridad de red:** Equipos IDS/IPS (Intrusion Detection System/Intrusion Prevention System) que incorporan funciones DPI/DFI con el fin de filtrar malware, spam, intrusiones, pérdida de datos, etc. tanto a nivel de usuario o empresarial como a nivel de operador.

- **Cumplimiento de políticas:** Control de acceso y provisión de uso justo de los servicios permitidos, en redes fijas e inalámbricas. Está vinculado con reglas del tipo PCC de la 3GPP estudiada en el anterior capítulo, por lo que se relaciona también con la gestión de tráfico.

- **Vigilancia:** Colaboración con agencias de seguridad nacionales o internacionales. Por ejemplo, en los EEUU algunos de los grandes agentes de Internet han revelado que han instalado equipos de DPI/DFI para fines de monitoreo e intercepción en tiempo real. Esto se ha hecho en colaboración con el gobierno y la Agencia de Seguridad Nacional, en aplicación de la ley CALEA (Communications Assistance for Law Enforcement Act). Más concretamente, el 50% del tráfico de AT&T pasa por los filtros del gobierno norteamericano (81).

- **Censura:** En algunos países se emplea para hacer que los ISP puedan bloquear cualquier contenido que se considere ilegal o perjudicial. Estos enfoques van desde filtrado de sitios con pornografía infantil, hasta la censura de lo que se considerar una amenaza para gobiernos o la estabilidad pública. En China, por ejemplo, se ha utilizado junto con otras técnicas para bloquear y filtrar contenidos no aprobados por el régimen (82)

- **Inyección o modificación de datos:** Empresas como NebuAd y Phorm han hecho uso de DPI para ofrecer publicidad inyectando anuncios en función de los intereses de los usuarios, deduciendo las preferencias de los consumidores mediante un análisis detallado de su tráfico de Internet.

- **Facturación y medición:** A través de un reconocimiento preciso de los servicios empleados, se pueden contar los volúmenes o las tasas de tráfico permitiendo definir a los ISPs tarifas ajustadas y diferenciadas según tipos de tráfico.

- **Gestión de tráfico:** Se puede utilizar para identificar y posteriormente gestionar anchos de banda y contenidos gracias a su capacidad de clasificación en tiempo real. Esto da opción a los ISPs de ralentizar o incluso bloquear totalmente tráfico no deseado. Por otra parte, también puede ser utilizado para optimizar el encaminamiento del tráfico basándose en el tipo de datos transferidos. Se diferencia del punto anterior “Cumplimiento de políticas” por no estar relacionado con elementos de ‘policing’.

2 Implantación de sistemas DPI/DFI para la gestión de tráfico

La gestión de tráfico mediante DPI/DFI es una técnica relativamente nueva. Se suele atribuir este hecho a que el hardware ahora es lo suficientemente poderoso para llevar a cabo esta inspección, aunque esto no es del todo cierto. Las tasas de datos en Internet también han crecido considerablemente, al igual o incluso más que el rendimiento de cualquier elemento hardware (CPU, memoria, bus, etc.). La razón para el crecimiento de esta tecnología es el continuo aumento de datos y la complejidad de las aplicaciones, que desafían los métodos anteriores para llevar a cabo una planificación y optimización de la red.

En el capítulo IV se ha analizado el estado del arte de las técnicas de gestión de tráfico y su tendencia a ofrecer servicios por niveles de QoS. Existe un creciente interés y demanda de las arquitecturas de 'policing', que pueden manejar una amplia gama de tareas de gestión. En su mayoría se definen bajo estándares internacionales reconocidos, a diferencia de DPI/DFI, y tienden a centrarse en la información del suscriptor para aplicar los parámetros de QoS necesarios. Es en este punto donde resulta necesario tener en cuenta la aplicación en uso, y por tanto donde DPI/DFI juega un papel crucial.

Se puede catalogar el empleo de DPI/DFI en la gestión de tráfico en dos grandes grupos de prácticas. Hay aplicaciones de DPI/DFI que aumentan las capacidades de cumplimiento de políticas que puedan existir en las redes NGN tales como PacketCable, o la red 3G o LTE, todas ellas con capacidad dinámica de políticas. Tanto el tráfico del suscriptor como el tráfico del plano de control son analizados, con el propósito de relacionar a los suscriptores con las políticas que se dirigen hacia ellos, y también para la detección de eventos de interés (aplicación prohibida, aplicación que podría beneficiarse de la gestión del tráfico, etc.).

El segundo grupo es aquel en el que las capacidades de la red no requieren una aplicación dinámica de políticas, generalmente debido a la adaptación de una arquitectura que no contempla dichos mecanismos. Al igual que en el primer caso, tanto el tráfico de usuario como el de la red se controlan y se notifican a los eventos apropiados para permitir las decisiones sobre las acciones a tomar.

2.1 Ubicación de sistemas DPI/DFI

Los equipos DPI/DFI actúan directamente sobre el flujo de bits, por lo que deben ser robustos frente a los puntos de fallo para evitar contribuir a la pérdida de comunicaciones. Inicialmente, los equipos DPI se desplegaron fundamentalmente en los puntos de agregación principales y en puntos de interconexión. Actualmente se distribuyen más ampliamente y más cerca del cliente, lo que mejora la capacidad de aplicar controles por suscriptor o por servicio.

Es importante determinar en qué medida estos equipos son integrables en los diferentes entornos existentes tales como redes móviles, redes HFC o redes fijas. Dada la naturaleza de las redes IP, los elementos DPI/DFI pueden ser instalados en cualquier lugar de red, contiguo a routers o ‘gateways’, o pueden ubicarse como elementos separados.

La solución a emplear dependerá de varios factores entre los cuales destacan el volumen de tráfico y el número de tecnologías de acceso empleadas. Por lo tanto, la ubicación de los equipos de análisis ya sean DPI/DFI, SPI o una combinación de ellos dependerá de los diferentes estándares de redes fijas y móviles y del diseño de la red en cuestión. En la práctica se suele llevar a cabo en tres puntos de convergencia de las redes, según la distancia al suscriptor (53)

- En routers multi-servicio (MSER), siendo el punto más cercano al suscriptor.
- En nodo de conexión de salida a las redes PDN (GGSN, PGW).
- En routers de interconexión con otras redes.

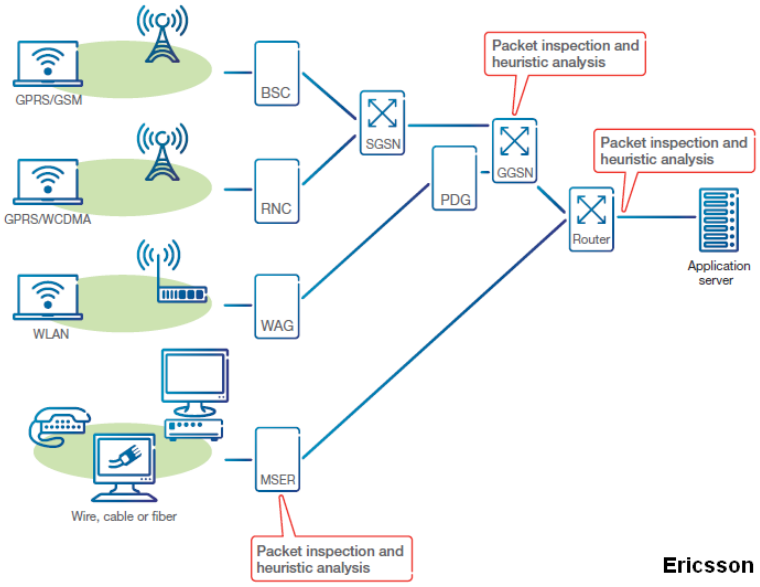

Ilustración 34: Posibles configuraciones para la ubicación de equipos DPI/DFI (53)

Los equipos pueden ser distribuidos y cooperar con las capacidades inherentes a la red. Por ejemplo, con un volumen de tráfico elevado, una solución posible pasaría por emplear varios puntos de análisis DPI/DFI y pre-análisis SPI. Así se limitaría el número de nodos con funcionalidades complejas haciendo una selección del tráfico que debería ser analizado en profundidad. Otra solución sería el empleo de equipos que trabajen en post-proceso para llevar a cabo así una detección de paquetes sin afectar en absoluto al procesado de tráfico, tomando medidas a posteriori. Esta forma de proceder se adaptaría a puntos que no necesitasen un control dinámico.

2.2 Integración de sistemas DPI/DFI

Los equipos de análisis DPI/DFI requieren ser ubicados en la ruta de los datos, con lo que las soluciones existentes pasan por integrar estas funcionalidades en los elementos de red existentes o bien en añadir equipos compatibles con las nuevas funcionalidades de forma independiente o dedicada.

2.2.1 DPI/DFI dedicado

En esta solución se ejecuta DPI/DFI en equipos separados independientes que se pueden instalar de forma flexible en diferentes puntos de la red. Los fabricantes de soluciones independientes son los que tienen una mayor cuota de mercado en el sector de DPI/DFI.

Algunas ventajas e inconvenientes de la utilización soluciones dedicadas se listan a continuación (83).

Ventajas:

- Buena escalabilidad, flexibilidad y modularidad.
- En general buen rendimiento, debido a que sus funciones son dedicadas.

Inconvenientes:

- Complejidad derivada de la interconexión con los demás elementos de red.
- Fiabilidad limitada debido a que presenta varios puntos de fallo.
- Añade latencia debido a que se añaden más saltos en la red y se llevan a cabo tareas redundantes (empaquetado y desempaquetado, por ejemplo).

2.2.2 DPI/DFI integrado

Este formato se basa en integrar DPI/DFI y las aplicaciones asociadas en el equipo adecuado para cada tipo de red. A medida que la tecnología avanza, cada vez más elementos de red (routers, 'gateways', GGSN, CMTS, PGW, etc.) incluyen funcionalidades inherentes para bloquear y/o gestionar el tráfico.

Para dar una muestra de hasta qué nivel de integración puede llevar a cabo un equipo de estas características se lista a continuación los diferentes entornos en los que se puede instalar el equipo *Cisco ASR 5000*, que incorpora de forma integrada la capacidad de análisis DPI/DFI (84).

UMTS/HSPA
Gateway GPRS Support Node (GGSN)
Serving GPRS Support Node (SGSN)
CDMA/HRPD/eHRPD
Packet Data Serving Node (PDSN)
Foreign Agent (FA)
Home Agent (HA)
HRPD Serving Data Gateway (HSGW)
LTE Evolved Packet Core (EPC)
Mobility Management Entity (MME)
Serving Gateway (SGW)
PDN Gateway (PGW)
Evolved Packet Data Gateway (ePDG)
WiMAX
Access Service Network (ASN) Gateway
Home Agent (HA)
Wi-Fi
Security Gateway
Call Session Control Function (CSCF)
Femtocelulas
Security Gateway
Home Node B Gateway (HNBGW)
Call Session Control Function (CSCF)

Ilustración 35: Funciones del *Cisco ASR 5000*

Las ventajas e inconvenientes de la utilización de este formato se listan a continuación (83).

Ventajas:

- Eficiencia al aprovechar el empaquetado y desempaquetado para varias funciones de red y análisis.
- Mayor fiabilidad debida a una menor concentración de posibles de puntos de fallo.

Inconvenientes:

- El rendimiento puede verse afectado al estar activas todas las funcionalidades posibles.
- No es práctico el despliegue de equipos integrados en redes ya implementadas.
- Escalabilidad limitada.

2.2.3 Comparativa entre soluciones dedicadas e integradas

Las soluciones integradas no son escalables en la medida en que lo son las dedicadas o independientes. Para soportar varias tecnologías de acceso además de para dar soporte a aspectos de facturación son necesarios varios puntos de análisis en el núcleo de red, lo cual da más maniobrabilidad en el caso de equipos independientes. Además, el uso de soluciones independientes hace posible el empleo de diferentes fabricantes lo cual añade riqueza en las funcionalidades.

Cada vez más, las soluciones integradas combinan tecnología de 'policing' con la tecnología DPI/DFI aunque hay que considerar que los fabricantes de equipos independientes generalmente llevan más tiempo en el mercado, por lo que el desarrollo de su tecnología es más maduro y más fácilmente instalable en redes ya implementadas. En la práctica, en muchos casos se hace uso de equipos independientes, incluso junto a equipos que poseen capacidad de análisis DPI/DFI integrada.

En el aspecto económico existen ciertas discrepancias según quien realiza las valoraciones, con lo que es difícil hacer una comparación objetiva en este ámbito. En principio, las soluciones dedicadas tienen algunas desventajas intrínsecas comparadas con las soluciones integradas ya que añadir más elementos en la red tiene un coste operacional más elevado. De acuerdo con un estudio encargado por Cisco (83) en el que se compara el TCO (Total Cost of Ownership) de una red con una solución independiente y otra con una solución integrada sirviendo a un millón de suscriptores, el modelo integrado tiene unos costes totales del 17% inferiores (siendo el coste operativo inferior en un 38%).

No obstante, de acuerdo a otro estudio realizado por el fabricante de equipos con solución dedicada, Allot Communications (85), se afirma que el coste de su producto es del 55% menos que en las soluciones integradas (un 80% menos en gastos directos de software y hardware y un 37% menos debido a costes operativos).

3 Mercado DPI/DFI

El campo de la tecnología DPI/DFI es muy dinámico y la gama de equipos y capacidades disponibles muy amplia. Se pueden contar por decenas los proveedores que comercializan equipos DPI/DFI de desarrollo propio.

Los méritos del equipamiento DPI se centran en una serie de criterios técnicos como (36):

- El número protocolos (o firmas) que son capaces de analizar.
- La capacidad que tienen para reconocer protocolos que han sido deliberadamente enmascarados u ofuscados.
- Velocidad a la que se actualizan las bases de datos para la detección de protocolos. Muchos proveedores ofrecen un servicio de actualización permanente sobre la base de versiones de software, de forma análoga a la que ofrece a los usuarios de software de seguridad o de detección de virus.
- El tiempo de latencia que añaden a la red.
- La capacidad de los enlaces y/o el número de suscriptores gestionables, con algunos suministradores capaces de manejar tráfico a 100 Gbps y administrar redes con millones de clientes.
- Las características de la CPU empleada, que afectará a la velocidad a la que el equipo de DPI/DFI identifica y actúa sobre la información. Generalmente son tecnologías de vanguardia que emplean procesado 'multi-threading' y paralelismo.
- Capacidad para manejar amenazas de seguridad tales como la denegación de servicio (DoS).

3.1 Fabricantes y soluciones relevantes

Como se ha visto en el apartado 2.2 se puede dividir el mercado de productos DPI/DFI en dos grandes bloques. El primero es el de los fabricantes puros de DPI mientras que el segundo es el de fabricantes de equipos de telecomunicaciones que han añadido estas funcionalidades de análisis para entrar a competir en este mercado. Entre todos, se pueden contar por decenas. En este apartado se hace una revisión de los fabricantes y productos más importantes de acuerdo a su cuota de mercado (86).

3.1.1 Fabricantes puros

Se engloban en este grupo los fabricantes que ofrecen soluciones independientes tanto de análisis y detección DPI/DFI como de la gestión posterior. En el apartado 2.2.1 ya se han visto algunas de sus características, pasamos ahora a ver algunas de las empresas que se encargan de su desarrollo y comercialización, y cómo llevan a cabo la soluciones.

3.1.1.1 Sandvine

Esta compañía canadiense fundada en 2001 comenzó trabajando para los MSOs norteamericanos. En su transcurso ha ido ampliando su oferta hasta el día de hoy, en que ofrece servicios para cualquier tipo de ISP (cable, DSL, FTTx, móvil, etc.) siendo el fabricante que lidera el sector. Entre sus clientes más importantes destacan Telefónica (con alrededor de 250 millones de suscriptores) y Comcast (con más de 17 millones de suscriptores) (87).

Su línea de productos emplea un enfoque de dos niveles distribuidos tanto para la recogida de análisis de red como cumplimiento de políticas. Los dos elementos fundamentales que forman la base de la plataforma son el *Policy Traffic Switch (PTS)* y *Service Delivery Engine (SDE)*. Ambos elementos operan en tiempo real uno en el plano de datos y el otro en el control, respectivamente.

El equipo *PTS* analiza el tráfico mediante DPI y DFI. Se divide en cuatro líneas: *PTS8210, PTS14000, PTS22000* y *PTS24000*. Se diferencian básicamente por los caudales aceptados, siendo la primera enfocada a conexiones con caudales de 1-4 Gbps, las dos siguientes enfocadas a los bordes y puntos de agregación de la red con caudales de 10-20 Gbps (el *PTS22000* específicamente diseñado para redes LTE), y la última enfocada a enlaces de núcleo con un caudal de hasta 80 Gbps (88).

El *SDE* actúa como interfaz de la decisión de políticas de los elementos de red y sistemas externos, maneja los cambios de suscriptor y proporciona control de políticas. Entre otros estándares, es compatible con PCCM de CableLabs y Euro-CableLabs y con el PCRF del 3GPP (89).

3.1.1.2 Allot

Allot Communications se fundó en 1996 y en la actualidad ofrece una amplia gama de equipos de DPI/DFI inteligentes para la optimización de servicios IP en una amplia variedad de entornos. Su clientela se compone de muchos ISPs pequeños aunque también se pueden contar algunos operadores grandes, sobre todo móviles (90).

Los equipos de Allot se pueden desplegar en cualquier entorno independientemente del acceso, aportando soluciones para el control de la congestión, la aplicación de políticas

integradas (PCRF), medición, protección ante ataques, etc. Para ello disponen de una línea de productos con diferentes funcionalidades (91).

La familia de productos *NetEnforcer* están orientados a la gestión del ancho de banda en redes IP para proporcionar visibilidad, actuando como punto de aplicación de las políticas implementadas por los operadores de la red (equivalente al PCEF de la PCC). Es capaz de supervisar, identificar, clasificar, priorizar y gestionar el tráfico de la red. Trabaja a tiempo real, con capacidades des de los 2 Mbps en el modelo *AC-400* hasta los 15 Gbps en la gama más alta *AC-10000*.

También ofrecen una serie de 'gateways' con funcionalidades DPI/DFI, los *Service Gateway*. Son plataformas escalables que se emplean para optimizar el ancho de banda y llevar un control de consumo para redes fijas y móviles (es compatible con los entornos de red 3G, 4G/LTE). Incluye funciones similares al *NetEnforcer*, y se compone de plataformas modulares y flexibles que admiten hasta 8 millones de suscriptores y tráfico a velocidades de hasta 160Gbps. Configuraciones en clúster pueden llegar a soportar hasta 1 Tbps de capacidad total.

3.1.1.3 Procera

Procera es fabricante de equipos de DPI/DFI desde 2001. Su línea de productos se puede integrar en cualquier entorno, y es desplegada en redes de más de 600 clientes (92). Inicialmente enfocado a ISPs locales, en lo últimos años se ha introducido en el sector de los Tier-1.

La línea de productos *PacketLogic* de Procera ofrece un conjunto de soluciones basadas en DPI/DFI, haciendo gala de mejorar la calidad y la longevidad de sus redes y permitir un control de seguridad. Para ello ofrecen soluciones que aportan las funcionalidades requeridas, dividiéndose en diferentes grados de análisis y aplicación.

El *PacketLogic Real-Time Enforcement (PRE)* utiliza múltiples plataformas de hardware que operan bajo un mismo sistema operativo, ofreciendo una amplia gama de configuraciones. La gama más baja (*PL5600*) ofrece un caudal 4 Mbps, 2.000 abonados y 80.000 sesiones por equipo. El modelo más complejo (*PL10000*) es capaz de tratar con 120 Gbps, 10 millones de abonados y 60 millones de sesiones. Todas las soluciones tienen cabida en la estructura modular ATCA (Advanced Telecom Computing Architecture), que será comentada en el siguiente apartado (93).

El *PacketLogic Subscriber Manager (PSM)* se encarga de las tareas de control de suscripción, facturación y políticas, permitiendo la aplicación de planes tarifarios inteligentes basándose en los suscriptores, lo que permite la creación de servicios novedosos. Es compatible con la arquitecturas PCC y PCMM (94).

3.1.1.4 Ipoque

Ipoque es un proveedor de soluciones para la gestión de tráfico con sede en Alemania, y es la empresa líder en Europa. Fundada en 2005 cuenta a día de hoy con clientes alrededor del mundo. Las soluciones que proporciona Ipoque según las diferentes funciones que llevan a cabo: gestión de tráfico, análisis de tráfico, estadísticas de red o 'policing' (95).

Para la gestión de tráfico mediante análisis DPI/DFI se encuentra el *PRX Traffic Manager* que ofrece una visión completa y detallada de aplicaciones y de usuarios. Esta información se emplea para poner en práctica las reglas definidas por el administrador de priorización, restricción, bloqueo, etc. Es un equipo versátil instalable en escenarios fijos y móviles, además de adaptarse a varias necesidades trabajando con flujos desde 400 Mbps y 32.000 usuarios en el *PRX-1100* hasta los 75 Gbps y 6 millones de usuarios en el *PRX-10G.* Entre sus productos también se encuentra el *DPX Network Probe,* diseñado para realizar tareas de vigilancia e inteligencia a nivel estatal (agencias de seguridad, etc.).

El *PRX-PE Traffic Manager* constituye una solución para una aplicación junto con servidores 'policing' de terceros, proporcionando datos en tiempo real para la contabilidad relacionada con los sistemas de cobro y facturación. En las redes 4G desempeña el papel de PCEF recibiendo las reglas de políticas desde el PCRF.

3.1.2 Fabricantes clásicos

A este grupo pertenecen grandes fabricantes de equipos de telecomunicaciones que han ido añadiendo funcionalidades del tipo DPI/DFI en equipos clásicos como routers o 'gateways', además de haber desarrollado algunos de ellos equipos independientes. Se trata de, entre otros, Ericsson (con la adquisición de Redback en 2006) (96), Alcatel-Lucent, Juniper, Huawei, Nokia Siemens Networks (NSN) y Cisco (con la adquisición de P-Cube en 2004 y Starent en 2009) (97). En este documento tan sólo se hace un análisis de los más relevantes en la temática del Proyecto: Cisco y Ericsson. El primero por ser el mayor proveedor de equipos de telecomunicaciones y el segundo por su estrecha relación con la definición del marco PCC de la 3GPP y por su posición como proveedor líder de equipos para redes móviles.

3.1.2.1 Cisco

Cisco Systems, fundado en 1984, es de los fabricantes de dispositivos de telecomunicaciones más importantes, así como el líder mundial en soluciones de red e infraestructuras de Internet. Como tal, se ha visto en la necesidad de incorporar elementos de análisis en varios de sus productos, además de desarrollar también soluciones dedicadas.

Como solución dedicada estrella se encuentra el *Cisco 8000 Service Control Engine (SCE)*, diseñado para implementaciones a nivel de operador que requieren alta capacidad de análisis y gestión de tráfico IP. Incorpora una arquitectura patentada de aceleración de hardware que

emplea múltiples procesadores RISC de alta velocidad. Su núcleo altamente programable puede controlar y administrar hasta 32 millones de sesiones simultáneas unidireccionales a través de una red IP y un máximo de 1 millón de usuarios simultáneos, con un caudal máximo de 30 Gbps. Es extensible y escalable, pudiéndose conectar en clúster en función de las necesidades. Se puede integrar en el núcleo de la red, en los puntos de interconexión, y en los extremos de la red. Es capaz de detectar alrededor de 600 protocolos, incluyendo P2P mediante reconocimiento adaptativo o DFI (98).

Para la versión integrada destaca el *Cisco ASR 5000*, que es mencionado en este Proyecto en varias ocasiones a modo de ejemplo. El detalle de las funciones que puede desempeñar se ha descrito en la Ilustración 35. Este sistema puede reconocer diferentes flujos, lo que le permite configurar y gestionar el tráfico mientras interactúa con diferentes aplicaciones. La plataforma consigue esta inteligencia debido al uso de DPI/DFI.

3.1.2.2 Ericsson

Esta compañía de origen Sueco y con presencia en alrededor de 180 países se encarga del desarrollo de equipos de telecomunicaciones en los campos de la telefonía, tanto fija como móvil, y de las comunicaciones sobre Internet. Ericsson está muy presente en el campo de la telefonía móvil, tanto es así que el 40% del tráfico de telefonía móvil atraviesa redes con su tecnología (99). Además, ha desempeñado un papel muy activo en la definición de las especificaciones de LTE/SAE, sobre todo en la definición del EPC.

En su gama de productos se incorporan soluciones de análisis independiente, aunque enfocadas a redes móviles. Este es el caso del *Service Aware Support Node (SASN*), una herramienta de inspección de tráfico en redes multi-proveedor y multi-acceso, siendo la inspección DPI/DFI la base de su funcionamiento. Sus principales aplicaciones están enfocadas al control de políticas y de facturación, junto con el *Service Aware Policy Controller* (*SAPC*) efectuando las funciones de PCRF. Sus funciones incluyen la inspección de una amplia gama de protocolos, la aplicación de políticas, la gestión avanzada de tráfico, el filtrado e inserción de contenidos, apoyo a facturación y recopilación de estadísticas (100).

Como solución integrada, su equipo *Gateway GPRS Support Node - Mobile Packet Gateway* (*GGSN-MPG*) proporciona una interfaz inteligente entre las redes móviles (GSM, WCDMA y LTE) hacia Internet. Está diseñado de modo que con una simple actualización de software, el GGSN puede evolucionar a un 'gateway' de paquetes para el EPC. En tal escenario, el *GGSN-MPG* admite al mismo tiempo tráfico de GSM, WCDMA y LTE, permitiendo una transición gradual. Incorpora funciones clave derivadas de la gestión de tráfico, tales como la facturación según aplicación y el control de políticas y de uso justo, haciendo uso para ello de DPI/DFI (101).

3.2 Valor de mercado

El mercado del sector tanto DPI/DFI como de los servicios de 'policing' está en pleno auge, y las previsiones para su futuro inmediato prevén una continuidad. Existen varios estudios sobre el volumen de mercado del sector, de los que a continuación se extraen los datos más destacables.

En 2008 Light Reading publicó un informe en el que decía que el valor del mercado de la gestión inteligente de tráfico (englobando vendedores de equipos tanto independientes como integrados y servidores 'policing') en todo el mundo era alrededor de 450 millones de dólares, y proyectaba que crecería a más del billón de dólares en 2012. Se estimó que la mayor parte del crecimiento procedería de la utilización de DPI/DFI y del empleo de gestión de políticas en las redes móviles (36).

En la actualidad tan solo el mercado compuesto por los vendedores de equipos independientes de DPI se estima en 500 millones de dólares según otro estudio realizado por Infonetics Research de octubre de 2011 (102). Este mismo estudio augura un crecimiento de algo más del triple (1,6 billones de dólares) para el 2015, debido a que se espera un fuerte crecimiento en el segmento de DPI/DFI en los mercados emergentes (este de Asia, Oriente Medio y África) donde los problemas de congestión de red causados por un rápido crecimiento de suscriptores se harán patentes. En el campo de los servidores de gestión 'policing' Infonetics Research espera un valor de mercado en el 2015 de alrededor de 1,6 billones de dólares.

Por su parte, la consultora ABI Research espera que para el 2016 los operadores se gasten 1,5 billones de dólares en tecnología DPI, además de 1,8 billones de dólares en servicios de optimización de tráfico y de 1,2 billones de dólares en equipos de gestión de políticas, según un estudio de octubre de 2011 (103). En este mismo informe también se prevé que pese a que la mayor parte de los ingresos correrán a cuenta de los grandes vendedores de equipos, con tanto capital en el sector habrá un crecimiento de compañías más pequeñas.

Otro estudio realizado por Light Reading en agosto de 2011 es menos optimista y sitúa el valor del mercado de gestión de tráfico mediante QoS (DPI/DFI, servidores 'policing', etc.) en los 2 billones de dólares aproximadamente. Resaltan el crecimiento en el sector de servidores de políticas basados en el PCRF y PCEF de la 3GPP, que valoran a fecha del estudio en cerca de 800 millones de dólares (104).

De los diferentes estudios se extrae que las compañías con las compañías con más ingresos son Sandvine, con cerca de una cuarta parte de los ingresos en el sector DPI/DFI, seguida de Cisco, Allot y Procera, que entre las tres conformarían cerca del 35% del sector (86).

La siguiente figura muestra de modo aproximado y promediando los valores aquí expuestos la evolución del volumen de mercado del sector. Nótese que al hablar de PCRF se quiere referenciar al conjunto de servidores 'policing', aunque debido a su peso en el sector se ha decidido emplear esta nomenclatura.

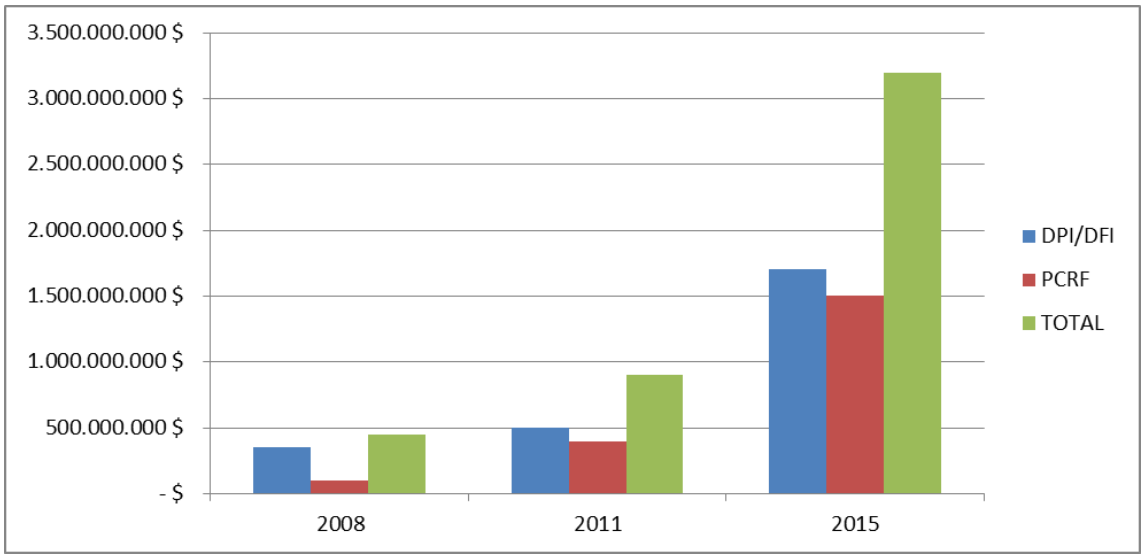

Ilustración 36: Estimación y evolución del valor de mercado de gestión de tráfico

4 Aspectos técnicos de DPI/DFI

Los requerimientos necesarios para llevar a cabo tareas de telecomunicaciones siempre han sido de los más exigentes. Las altas velocidades de transmisión y gran capacidad de procesado de datos son también un desafío en el sector DPI/DFI.

Con el fin de mantener un alto nivel de rendimiento y baja latencia, la solución convencional para hacer frente a este desafío pasa por el uso de múltiples procesadores para el tratamiento de paquetes de forma simultánea, haciendo uso de técnicas de paralelismo y 'multi-thread'.

Estas técnicas conllevan problemas de escalabilidad. Según un estudio de Intel, un procesador de 8 núcleos en un servidor Web da un rendimiento de 4,8x en lugar de 8x (105). Por tanto, para conseguir un buen rendimiento se debe asegurar que los sistemas estén diseñados en conjunto para explotar el paralelismo tanto a nivel hardware cómo a nivel software.

Con un buen uso, el impacto que causa un equipo capaz de llevar a cabo gestión de tráfico mediante DPI/DFI es poco apreciable en términos de latencia. Concretamente, del orden de 30 - 100 µs con tamaños de paquete convencionales de 1518 bytes, habiéndose tomado como referencia tres equipos de distintos fabricantes (106) (107) (108). Si retomamos la tabla del apartado 3 del capítulo III, considerando que el tiempo de latencia más exigente es del orden de 50 ms, vemos que de hecho el impacto es prácticamente nulo.

4.1 Arquitectura de sistemas DPI/DFI

Las soluciones DPI/DFI encuentran su mayor desafío en la velocidad y capacidad de procesado a la que deben trabajar para que sean lo más transparentes posible al paso de los datos. Para ello es imprescindible un rendimiento óptimo a nivel de hardware, que debe ser específicamente diseñado para llevar a cabo estas funciones. En este aspecto resulta importante tanto la interconexión de elementos como la arquitectura de los componentes de procesado.

4.1.1 Interconexión: ATCA

ATCA son una serie de especificaciones del grupo PCI Industrial Computer Manufacturers Group (PICMG)[7], dirigidas a cumplir las necesidades de interconexión para la próxima generación de equipos para telecomunicaciones. Las empresas que participan en el trabajo ATCA han aportado conocimientos del mundo de la industria debido a que se compone de fabricantes de equipos de telecomunicaciones e informáticos, empresas de software y proveedores de chasis, conectores y fuentes de alimentación.

Esta serie de especificaciones contempla las últimas tendencias en tecnologías de alta velocidad de interconexión y los procesadores de última generación para conseguir una buena

[7] http://www.picmg.org/

integración y flexibilidad, por lo que quedan especificados los requisitos mecánicos, físicos y estructurales de los chasis para la interconexión de equipos.

Para muchos ISPs y sus respectivos proveedores, ATCA se ha convertido en un estándar fiable y abierto. El hecho de contemplar gran cantidad de opciones y características para la interconexión de equipos han convertido a ATCA en una plataforma idónea para los requisitos de aplicación DPI/DFI (109).

Aunque ATCA tiene beneficios para varias de las aplicaciones centradas en las telecomunicaciones, también existen algunos inconvenientes que pueden hacer que sea menos competitiva en escenarios que no requieran de ciertas características de alto nivel. Sobre todo en escenarios con dispositivos de red de tamaño y prestaciones menores, pudiendo provocar limitaciones de ancho de banda y adición de latencia peores que los proporcionaría una estructura propietaria (110).

En cualquier caso, ya sea bien a través la interconexión de varios elementos mediante el estándar ATCA, o bien mediante la integración de funciones en estructuras independientes, es de vital importancia la compenetración de los diferentes elementos entre sí y con los elementos de procesado.

4.1.2 Procesado de datos

La implementación de sistemas capaces de realizar DPI/DFI requiere procesadores con atributos específicos para que puedan cumplir con las exigencias de una tarea de procesado que supone una gran capacidad de análisis a velocidades muy elevadas. Los desafíos más destacados para ese fin recaen en cumplir con las siguientes prestaciones (111).

- Alto rendimiento y baja latencia.
- Inteligencia dinámica y programable para mantener el ritmo de la evolución de los protocolos y amenazas.
- Fiabilidad y velocidad en la criptografía.

Una de las opciones que más se ha venido empleando para llevar a cabo DPI/DFI se basa en el uso de procesadores de propósito general (básicamente, Intel x86) con ayuda de periféricos y aceleración de hardware. Las crecientes necesidades de procesado demandadas por grandes caudales de datos (10-40-100 Gbps) y número de sesiones y/o usuarios, dan lugar a que constantemente se diseñen y optimicen nuevas arquitecturas.

No todos los procesadores son creados del mismo modo ni para el mismo fin. Para llevar a cabo operaciones tan exigentes como las que se dan en un sistema de comunicación de alto rendimiento es necesario emplear más de un tipo de procesador para cumplir con los estrictos requisitos de gestión de paquetes, seguridad y virtualización (111) (112).

4.1.2.1 Plano de datos y plano de control

Dependiendo del nivel de comunicación que se desee analizar, es mejor emplear una arquitectura u otra en función de las características y requerimientos de los tipos de datos a procesar. Lo primero que se debe considerar es la diferenciación entre lo que se considera el plano de control y el plano de datos.

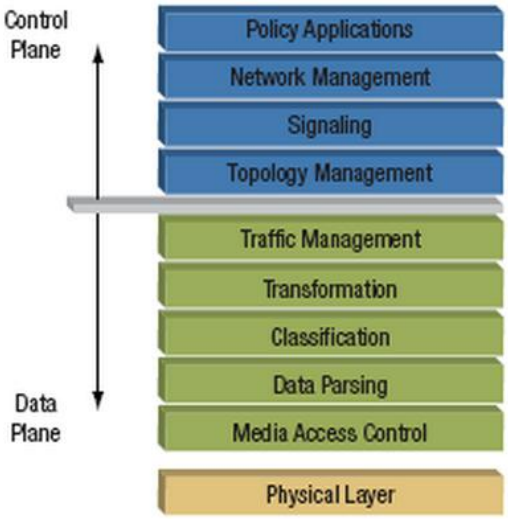

Ilustración 37: Funciones atribuibles al plano de control y al plano de datos (112)

El plano de datos (también plano de usuario) se encarga de las funciones relacionadas directamente con los flujos de información. Su correcta implementación es esencial para la velocidad de flujo de tráfico. Se incluyen en esta fase tareas de control de acceso, clasificación y transformación, procesado de los datos y manejo de paquetes, conversión serie-paralelo, sincronización y transferencias de datos a memoria. Estas funciones son atribuibles a los niveles 2 y 3 del modelo OSI.

El plano de control se encarga de llevar a cabo funciones de mantenimiento que no son estrictamente indispensables para el envío de tráfico a través del sistema como la aplicación de políticas o la gestión de congestión, por ejemplo. Estas funciones se pueden realizar generalmente con una prioridad más baja que las funciones de plano de datos ya que no son imprescindibles para su correcta transmisión a nivel físico (112).

4.1.2.2 Tipos de procesadores para comunicaciones

El hecho de que existan dos grandes bloques de tareas para el procesado de las comunicaciones da lugar a que existan diferentes soluciones físicas para su desempeño. Así, el tipo de tareas a realizar se relaciona íntimamente con el hardware que se emplea para tal efecto, atendiendo unas características y necesidades concretas. A continuación se clasifican

los tipos de chip que se han venido empleando en sistemas de comunicaciones y se expone su relación con la tecnología DPI/DFI.

4.1.2.2.1 ASIC & NPU

La solución óptima para el tratamiento en el plano de datos es el uso de o ASICs (Application Specific Integrated Circuit) o NPUs (Network Processor Unit). Los ASIC aportan un buen rendimiento y un bajo coste, aunque carecen de niveles de programación, necesarios para ofrecer algo de adaptabilidad. Los NPUs se diseñaron para solventar la poca flexibilidad de los ASIC y a diferencia de éstos acceden a las instrucciones desde un firmware que se incorpora en el mismo chip, lo cual aporta flexibilidad a costa de perder algo de velocidad. Una forma de compensar este hecho se soluciona en algunas implementaciones de NPU con ayuda exterior como motores de clasificación, gestores de tráfico y controladores MAC. Este tipo de hardware se encuentra en equipos como routers o switches donde las funciones a realizar son predefinidas y optimizadas para el tratado de paquetes, filtrado en los niveles 2 y 3 del modelo OSI, enrutamiento, etc.

Para elaborar las tareas del plano de control mediante estos elementos existen varias posibilidades. Una de ellas pasa por combinar NPUs con procesadores de propósito general, ya que éstos se adaptan bien a las tareas requeridas en este ámbito. El problema es que esta solución se necesita complementar habitualmente con el uso de memorias externas además de la memoria que probablemente será necesaria para que el procesador ejecute las tareas de control, añadiendo latencia al procesado. Otra solución pasa por integrar todas las funciones, control y datos, en un mismo chip, que toma el nombre de 'Communication Processor', y que se analiza seguidamente.

4.1.2.2.2 Communication Processor

Los 'Communication Processor' surgen como elementos de red para llevar a cabo tareas tanto del plano de control como del plano de usuario. La principal diferencia con los NPU radica en que se componen por un procesador multi-núcleo de propósito general, que lleva a cabo la totalidad de las funciones. Se consigue así que se requiera un único bloque de memoria con las ventajas de velocidad y simplicidad que esto implica frente a la solución de NPUs con procesadores de propósito general, donde las funciones de cada elemento quedan delimitadas. Esto repercute en una reducción del consumo de energía, del espacio y del coste frente a una solución basada en NPUs.

En la siguiente ilustración se muestran ambas estructuras, observándose la separación entre el procesador de propósito general y los procesadores de paquetes (NPUs) en la primera solución. Para la solución mediante el 'Communication Processor' tan solo se requiere de un único núcleo de proceso, aunque ayudado por elementos hardware que tratan con los datos correspondientes a la capa de usuario.

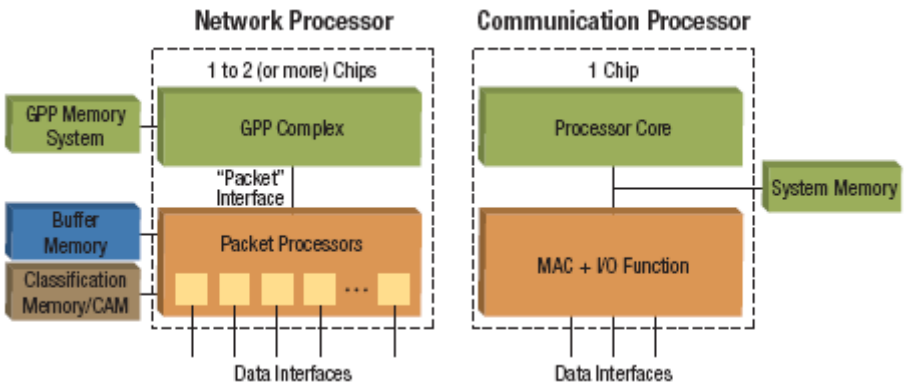

Ilustración 38: Diferencia estructural de NPU y 'Communication Processor' (112)

Un 'Communcation Processor' se puede ver como un chip programable genérico, como los microprocesadores de propósito general, pero optimizado para el procesado de paquetes. Este diseño posibilita una solución ágil en los procesos que requieran estrecha conexión entre el control y las funciones de plano de datos. Para no perder las ventajas de velocidad debidas a emplear elementos hardware, se suele complementar con módulos de aceleración, que manejan la funcionalidad de la capa MAC (nivel 2 del modelo OSI) de forma más eficiente de lo que lo hace un procesador de propósito general.

Con este tipo de procesadores se pueden llevar a cabo funciones de todo tipo ya que agrupa funciones del plano de datos y control. Entre ellas se encuentran el cifrado, manipulación de cabeceras IP, tratamiento de flujos e incluso análisis DPI/DFI, aunque no del modo más eficiente. Para llevar a cabo esta tarea es idóneo el uso de CPUs multi-núcleo.

4.1.2.2.3 CPU multi-núcleo

El hardware empleado en la capa de control está formado comúnmente por arquitecturas multi-núcleo de propósito general (x86, PPC, MIPS) ya sea junto a NPUs, módulos de aceleración de hardware o como parte de los 'Communication Processor'. Esto es debido a que constituyen una solución eficiente para realizar las tareas requeridas a este nivel, ya que aprovechan que el trabajo a realizar es altamente paralelizable.

Cuando un fabricante de procesadores lanza un nuevo producto con una frecuencia de funcionamiento más alta, el rendimiento de las aplicaciones en general aumenta sin ningún cambio de código. Esto ha funcionado bien durante muchos años, porque los fabricantes de procesadores han podido disimular la latencia y cuellos de botella a través del empleo de almacenamiento en caché y de paralelismo de instrucciones. En la actualidad, debido a limitaciones térmicas y eléctricas, esto ya no es posible, y los fabricantes de procesadores están recurriendo a la explotación de paralelismo a nivel de 'thread' a través de procesos de virtualización con el fin de seguir ofreciendo mejoras (113). Esta tecnología consigue que una CPU física se divida a varias CPU lógicos, atendiendo cada una de éstas a un hilo o 'thread' y

empleando esta clasificación para la separación de diferentes flujos de datos para su tratamiento independiente.

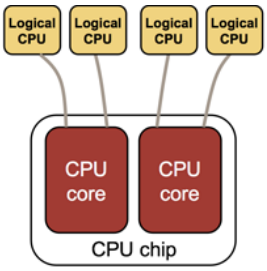

Ilustración 39: Ejemplo de virtualización de un CPU

Con esta tecnología se hace posible consolidar múltiples dispositivos de red o aplicaciones en un único sistema físico de modo que cada flujo puede ser tratado por separado por una máquina virtual, mejorando así la distribución de los elementos y permitiendo minimizar el impacto de acceso a memoria. La virtualización se está haciendo cada vez más importante en los equipos de infraestructura de red y aplicaciones.

Los procesadores de propósito general son los más adecuados para análisis de flujos complejos, correlación, manipulación de bases de datos, recopilación de informes, entre otros. También para llevar a cabo DPI/DFI, que es una aplicación más compleja que la mayoría de las que actúan sobre la red. No obstante, aún y que son los más adecuados para el plano de control en el nivel 7, tienen algunas características que no se adaptan bien a para su uso en análisis DPI/DFI, tales como:

- Capacidad de procesado hardware de paquetes reducida (tratamiento de cabeceras, compresión, etc.)
- Limitación para procesar millones de flujos simultáneos
- Latencia elevada
- Limitación en procesado de seguridad
- Limitación en el procesado de E/S (Entrada/Salida)

La siguiente ilustración muestra precisamente este comportamiento, los ASIC y NPU son los óptimos para el procesado hardware del plano de datos, los 'Communication Processor' añaden funcionalidad software a éstos últimos pero no llegando al punto que requiere el análisis complejo de paquetes, con lo que para esta función lo más idóneo son los CPU tradicionales.

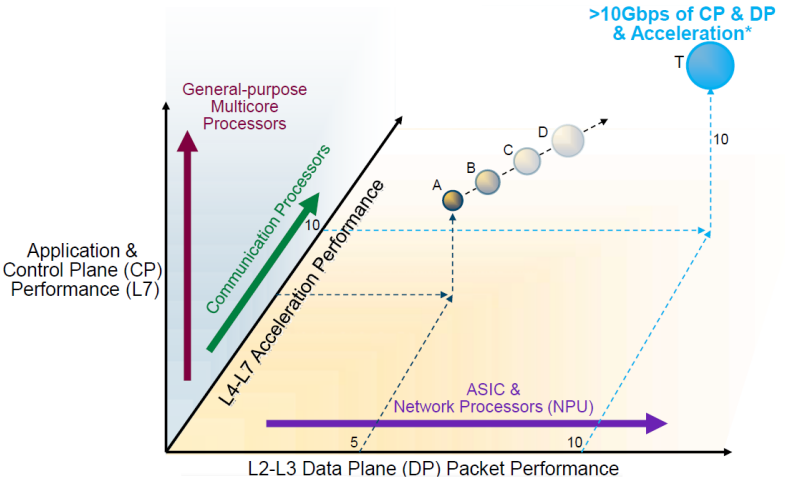

Ilustración 40: Comparación de tipos de procesadores para redes (114)

4.1.2.2.4 Procesador de flujo

Para subsanar las deficiencias para aplicaciones de comunicación a alta velocidad de los procesadores de propósito general, se ha desarrollado un tipo de procesador llamado Network Flow Processor (NFP) pensado para trabajar con CPUs multi-núcleo y optimizar el procesado de los flujos de datos.

En un procesador de flujo se espera que se incluyan funcionalidades como:

- **Clasificación de flujos:** Capacidad de separar flujos de datos según lo que se ha definido como quíntupla.
- **Manejo de múltiples flujos:** Habilidad para tratar en tiempo real múltiples flujos con el fin de disminuir las necesidades de almacenamiento en memoria y aportar agilidad.
- **Virtualización:** Capacidad de llevar a cabo una virtualización eficiente de los CPUs para que se traten los flujos de forma independiente en CPUs virtuales.
- **Balanceo de carga:** Mecanismo para repartir los flujos de paquetes en los diferentes CPUs virtuales con el fin de conseguir que el trabajo se realice sin esperas.

Para separar y clasificar flujos es necesario mantener un seguimiento sobre los datos de modo que se pueda analizar una comunicación completa. Esto es posible mediante procesos basados en uso de almacenamiento (generalmente externo, ya que las memorias caché son insuficientes) o bien mediante pre-procesado, paralelismo y uso de memorias caché.

Para proceder del primer modo se debe capturar y almacenar el tráfico para poder mantener un seguimiento de su estado y relacionarlo con otros paquetes de su mismo flujo. Esta forma de actuar se basa en el uso de memorias externas, por lo que se presenta como una solución tediosa ya que la cantidad de datos a analizar puede ser muy elevada, sobre todo en equipos

que se sitúen en redes de agregación o de núcleo, añadiendo latencia al proceso (del orden de 200 ciclos para una operación a DRAM) (114) y creando cuellos de botella.

En el segundo caso la forma de actuar se basa en realizar una buena clasificación de los paquetes. Para ello el primer paso es un pre-procesado de cabeceras para determinar así el flujo de comunicación al que pertenece. Mediante esta técnica el tráfico de red se puede organizar en varios caminos que pueden equilibrar la carga entre los núcleos físicos o virtualizados de la CPU.

Gracias a esta separación se puede fijar cada flujo en un núcleo o 'thread' específico de modo que las tareas a realizar por cada uno de ellos se puedan centrar íntegramente a las funciones del plano de control tales como el análisis de paquetes. Así se consigue que cada flujo sea almacenado en la memoria caché del núcleo que corresponda aportando velocidad al proceso. La siguiente ilustración hace referencia a este concepto, el primer bloque realiza la clasificación de flujos, que son enviados a las CPUs según pertenezcan o no a la misma comunicación.

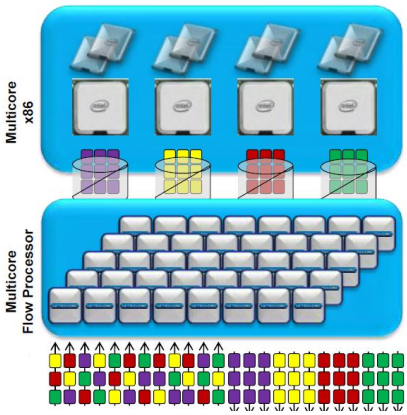

Ilustración 41: Efecto del empleo de NFP (115)

Existen dos versiones de este tipo de procesador que se pueden ver como una evolución o mejora sobre los NPU trabajando junto a CPUs y sobre los 'Communication Processor'. La diferencia fundamental entre éstos con los procesadores de flujo radica en que los primeros son capaces de tratar los paquetes (realizar búsquedas, procesado de paquetes y manipulación del contenido de datos) basándose en la tablas de información asociadas (red, dirección o usuario), mientras que el procesador de flujo de red maneja los paquetes basándose no sólo en el mismo paquete y las tablas asociadas, sino también en un análisis de quíntupla del flujo TCP o UDP al que el paquete pertenece. Esto permite una clasificación de los flujos de datos que aporta gran agilidad al proceso de análisis DPI/DFI.

Aunque las diferentes arquitecturas existentes son difícilmente generalizables, en un primer grupo se encontrarían soluciones como el QuantumFlow Processor de Cisco (116) o el NFP-3200 de Netronome (117), donde el procesado del plano de control se lleva a cabo de forma externa. La siguiente ilustración muestra este hecho, viéndose la interfaz de conexión hacia el

CPU para el procesado del plano de control (a la derecha del esquema). El resto de elementos se encargaría de las diferentes tareas del plano de datos, separación de flujos y demás, llevándose a cabo el procesado en este ámbito por los PPE (Packet Processor Engine).

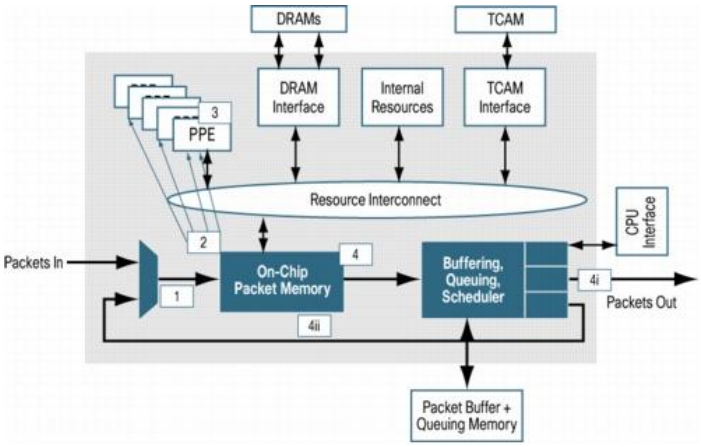

Ilustración 42: Esquema del QuantumFlow Processor de Cisco (116)

En el segundo grupo, del que destacan los modelos XLP832 de NetLogic RMI (118), el OCTEON II CN68XX de Cavium (119) o el QorIQ de Freescale (120), se integran todas o gran parte de las funcionalidades en un solo chip. En la siguiente ilustración se muestra este formato, en el que se puede apreciar la estructura multi-núcleo y 'multi-thread', que se ve reforzada por múltiples bloques funcionales encargados de tares como la seguridad, el empleo de RegEx (Regular Expressions) o la clasificación de paquetes, entre otros.

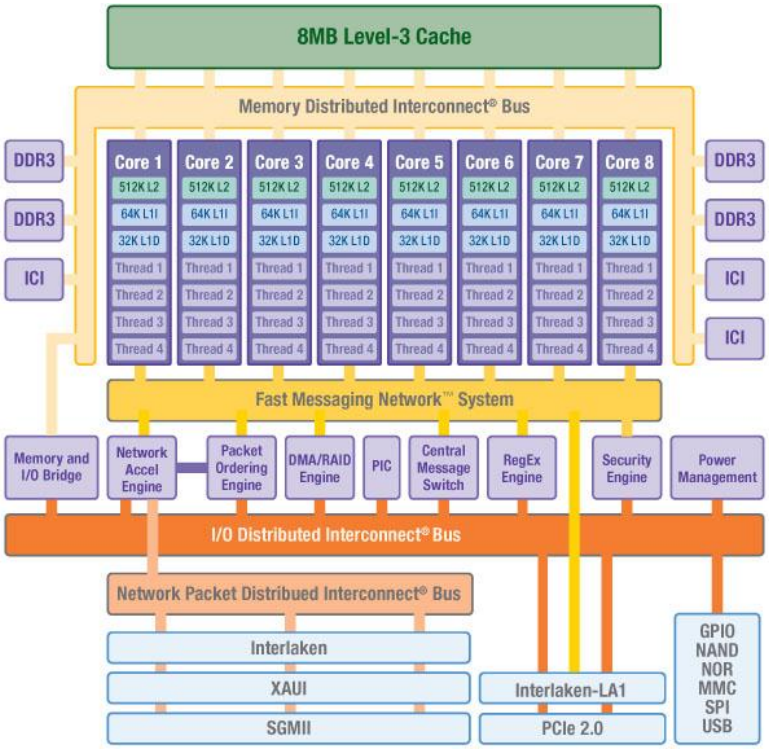

Ilustración 43: Esquema funcional del XLP832 de NetLogic (118)

Sea cual sea el tipo de solución, todos convergen hacia una estructura similar, en la cual se pueden encontrar los siguientes puntos comunes:

- Múltiples núcleos
- Hardware dedicado para las operaciones de red comunes
- Interfaz de memoria de alta velocidad
- Interfaces E/S de alta velocidad
- Interfaz con CPU de propósito general (en soluciones que no integran plano de control)

La siguiente figura se pretende mostrar cómo se integra todo el sistema. En concreto, se trata de la solución propuesta por Netronome, que está pensada para trabajar con procesadores Intel x86. Se puede apreciar la función del NFP como punto intermedio entre el plano de datos (niveles 2 a 4 del modelo OSI) y el plano de control.

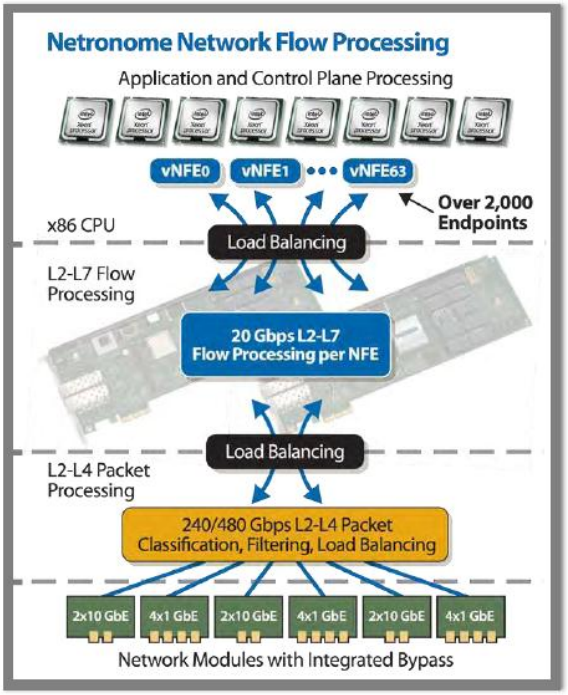

Ilustración 44: Sistema completo con NFP (114)

Igual que en los NPU y los 'Communication Processor' la necesidad de realizar las tareas del plano de control a velocidad de línea requiere que la CPU se complemente con dispositivos externos de aceleración, por ejemplo para procesado de protocolos seguros como MACSec, IPSec o SSL. Así, aunque las funcionalidades que implementa un procesador de flujo dependen del fabricante, es habitual que éste incorpore motores de criptografía integrada, hardware PKI (Public Key Infrastructure) para acelerar la exponenciación modular necesaria para el cifrado,

apoyo para codificación Hash, hardware dedicado a la generación de números aleatorios, y en algunas implementaciones motores de búsqueda de expresiones regulares (más adelante veremos su relación con DPI/DFI).

Los módulos de aceleración de hardware se basan en aprovechar las características del formato de los paquetes. Por ejemplo, la mayor parte del procesado del plano de datos requiere sólo una pequeña parte de la PDU o cabecera. Así, si una unidad de E/S se configura para enviar una porción predefinida de la PDU a la memoria caché en su recepción, esto permite que cuando se inicia la acción pertinente en base a esta cabecera, la información requerida ya se encuentre en la caché, lo que reduce la latencia.

4.2 Clasificación de paquetes en flujos

Para un correcto procesado basado en paralelismo se debe llevar a cabo una clasificación de paquetes en flujos. Para ello, todos los paquetes que pertenecen al mismo flujo son clasificados de forma conjunta.

El balanceo de carga, la distribución de paquetes y su planificación son esenciales para conseguir las prestaciones necesarias de cara a llevar a cabo un análisis e inspección profunda de paquetes con buenas prestaciones. Cuando se implementa en línea, los objetivos de un planificador de paquetes de DPI/DFI son de maximizar el rendimiento y minimizar la latencia media.

El principio de funcionamiento se muestra en el siguiente esquema, donde el tráfico se pre-analiza y clasifica para ser enviado a los diferentes bloques de procesado según sean las reglas de clasificación definidas.

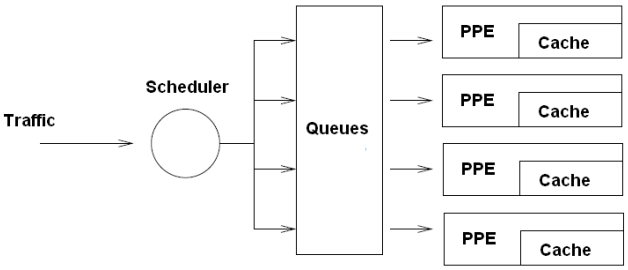

Ilustración 45: Esquema global de clasificación de paquetes

El objetivo de la clasificación de paquetes es el de maximizar la cantidad de tráfico de red que puede ser inspeccionado afectando lo menos posible al sistema. Un buen planificador de paquetes debería cumplir con las siguientes propiedades (113).

- **Balanceo de carga:** El trabajo se debe distribuir uniformemente en todos los 'threads' de modo que no haya un núcleo con alta carga mientras otros esperan. Los sistemas operativos son los encargados de compensar el desequilibrio de la carga.

- **Coste computacional bajo:** El coste de la gestión y organización de paquetes (en términos de memoria y ciclos de CPU) debe ser pequeña en comparación con el trabajo realizado en el paquete.

- **Ordenación por flujos:** Es conveniente que el orden de salida de los paquetes de un flujo se mantenga según el orden de llegada. Así el procesado de los paquetes que pertenecen a la misma conexión se podrán ejecutar en el mismo núcleo y por lo tanto se garantizará un buen uso de la caché.

- **Optimización de caché:** Conviene que los paquetes se organicen de modo que los paquetes anteriores del mismo flujo estén en caché. Se relaciona con la ordenación por flujos.

- **Mínimo jitter:** Es necesaria una mínima variación de la latencia en los paquetes del mismo flujo, para poder así llevar un ritmo uniforme y ajustado de procesado.

En la actualidad existen varias técnicas empleadas para la organización de los paquetes, de las cuales se hace un breve repaso a continuación.

Clasificación basada en el paquete

La asignación de los recursos se hace paquete a paquete atendiendo a factores diversos. Desde algo simple como una asignación por turnos hasta algo más complejo cómo la asignación de los recursos según la carga que procesa cada uno. Esta forma de proceder efectúa un buen balanceo de carga entre los diferentes motores de procesado pero no es buena en cuanto al orden de los paquetes ni en consecuencia en cuanto al uso de las memorias cache, lo cual puede afectar al rendimiento. Este modelo es empleado en dispositivos de redes pero no es válido para el empleo de DPI/DFI ya que no solo no hace una separación de flujos de datos sino que tampoco mantiene el orden de los paquetes. El modelo NAPI del kernel de Linux responde a este planteamiento (121).

Clasificación basada en flujos de paquetes

Los paquetes se asignan a sus flujos mediante el análisis de quíntupla y éstos a su vez a un recurso determinado. Para ello se mantiene una tabla de los flujos activos y su relación al núcleo de procesado.

Ilustración 46: Ejemplo de clasificación por flujos

Al generarse un flujo, éste se asigna al recurso con menos carga. En este modelo todos los paquetes de un flujo se procesan por el mismo recurso por lo que el orden en los paquetes se mantiene y es eficaz en el uso de la memoria caché. Como punto negativo hay que destacar que la tabla de flujos activos debe ser mantenida, y en el caso de que existan muchos flujos activos puede necesitar de una capacidad de memoria notable, ocupando varios ciclos de reloj para las búsquedas. En cuanto al balanceo de carga es posible que no exista equilibrio debido a que los flujos presentan diferentes números de paquetes y/o de bytes. La primera versión de este modelo de organización de flujos se especificó por Microsoft (122).

Clasificación basada en hash fijo

Existen dos modalidades de aplicación de hash fijo, el método directo y método indirecto. En el primer caso se aplica la función hash al subconjunto de la quíntupla y se emplea el resultado en la asignación del recurso haciendo el modulo con el número de recursos disponibles. Este método no necesita el empleo de tablas y por lo tanto no es necesaria memoria adicional.

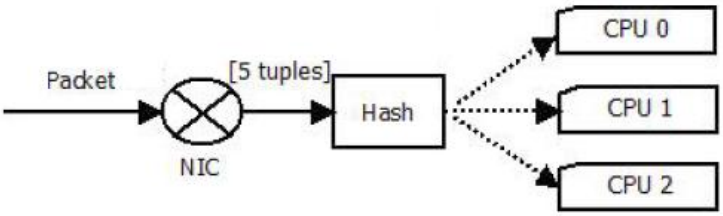

Ilustración 47: Modelo de clasificación basado en hash fijo (123)

En el método indirecto, se usa el resultado de la función hash haciendo el modulo con el tamaño de la tabla que indexa las asignaciones a cada recurso de procesado. Este resultado es el índice a la tabla.

En ambos casos los paquetes con la misma quíntupla tienen el mismo valor de hash, de modo que son asignados a un mismo recurso. Esto implica que el orden de los paquetes se mantiene y por lo tanto es eficiente en cuanto al uso de las caché. Por el contrario, se tiene una falta de

control sobre la asignación de recursos lo que puede dar lugar a un balanceo de carga desequilibrado.

Clasificación basada en hash adaptativo

Esta opción combina la funcionalidad de la organización basada en hash fijo añadiendo la funcionalidad de cambiar la asignación de recursos cuando la carga está desequilibrada. Cuando un desequilibrio es detectado se intenta corregir calculando una nueva tabla de direccionamiento. Este método mejora el citado anteriormente en cuanto a balanceo de carga, aunque por otro lado añade más necesidad de procesado.

Clasificación basada en ráfagas de flujos

Este método trata de combinar el balanceo de carga con el buen uso de la memoria caché y la entrega de paquetes de forma ordenada. Igual que en el método de organización basado en el flujo de paquetes se debe mantener una tabla de direcciones, aunque en este caso sólo es necesario indexar los flujos que tienen paquetes en el sistema. Un flujo que entra al sistema contiene el número de paquetes que hay ya dentro del sistema o una marca de tiempo del último paquete que asignó a ese flujo.

Cuando llega un paquete se asigna a un flujo en base a la quíntupla. Si el flujo existe en el sistema de paquetes, el paquete se asigna a los recursos de procesado del dicho flujo. Si por el contrario no existe el flujo o ya no hay paquetes de ese flujo en el sistema, el paquete es asignado al recurso menos cargado. En esto modelo se da eficiencia en el uso de la caché y se mantiene un orden en los paquetes. Además se equilibra el balanceo de carga ya que los flujos no son unívocamente relacionados con un recurso.

Aplicación a DPI/DFI

Determinar que opción es la óptima para el empleo de DPI/DFI no es trivial. Las técnicas citadas anteriormente se diseñaron para aplicaciones menos exigentes que DPI/DFI y la información empleada para tomar las decisiones de la organización en los paquetes no se corresponde íntegramente con lo que esta técnica necesita. Como muestra de este hecho debe resaltarse que los métodos citados básicamente tienen un tiempo de procesado fijo mientras que el número de instrucciones que DPI necesita para procesar un paquete varía en gran medida en función del protocolo en uso. Queda en manos de cada fabricante la elección o creación de un método para la clasificación más adecuada para su sistema.

4.3 Análisis DPI

Los sistemas DPI consiguen descifrar el contenido de las comunicaciones mediante la búsqueda de texto o cadenas de bytes para su comparación con una serie de reglas. Muchos protocolos se basan en texto y pueden ser fácilmente identificados determinando si se hallan ciertas palabras clave. De forma similar, algunos virus o ataques malware se pueden identificar también mediante la búsqueda de ciertas cadenas de bytes, o 'string matching'. La siguiente ilustración muestra un ejemplo claro sobre cómo se puede burlar un análisis basado en el número de puertos escondiendo una aplicación P2P sobre un paquete aparentemente de tráfico HTTP.

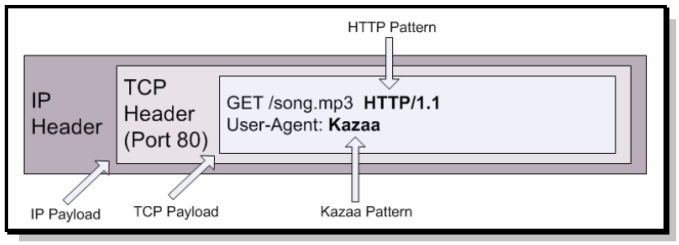

Ilustración 48: Ejemplo de detección DPI (76)

El procedimiento empleado por cada solución responde a diseños propietarios, con lo que es difícil generalizar un método de trabajo. No obstante, para comprender el proceso de análisis seguido se describe el modelo que emplea Cisco en su arquitectura *Cisco ASR 5000* (124). En ésta se llevan a cabo los dos tipos de análisis discutidos en el apartado 1 de este capítulo:

SPI: inspección de la capa 3 (cabecera IP) y la capa 4 (por ejemplo, UDP o TCP).

DPI: inspección de las capas 7 y 7+ (datos de usuario). En este nivel el fabricante remarca las siguientes funcionalidades:

- Detección del Uniform Resource Identifier (URI) en el nivel 7 del modelo OSI (por ejemplo, http:, mailto:, ftp: etc.).
- Identificación de destino real en el caso de solicitud a través de un proxy, donde una inspección SPI sólo revelaría la dirección IP y el número de puerto del proxy de destino.
- Des-encapsulación de cabeceras de los protocolos complejos de capa superior como el GPRS Tunneling Protocol (GTP).
- Verificación de que el tipo tráfico cumple con el número de puerto indicado en el protocolo de la capa 4 en acorde con los 'well-known port'.

La secuencia de análisis empleada en este equipo se describe a continuación, haciendo referencia a la siguiente ilustración:

1. Los paquetes a analizar son dirigidos al analizador de protocolos en función a una Access Control List (ACL) definida según las políticas de gestión.

2. Los paquetes pasan por una inspección SPI a través de los siguientes analizadores:

    a) analizador de portadora (nivel 2)

    b) analizador de paquetes IP (nivel 3)

    c) analizador de segmentos ICMP, TCP, UDP, etc. (nivel 4)

3. Los datos que se obtienen en la inspección SPI se comparan con las reglas definidas en el sistema.

4. Cuando coinciden los parámetros encontrados en el analizador SPI con los definidos en las reglas de enrutamiento, el paquete se envía a la capa de DPI correspondiente 7 ó 7+.

5. Después de que el paquete haya sido inspeccionado y analizado por el analizador de protocolos:

    a) el paquete reanuda el flujo normal,

    b) la salida de este análisis desemboca en la aplicación de acciones que se deban llevar a cabo (cambio de dirección, emisión extra de facturación, etc.).

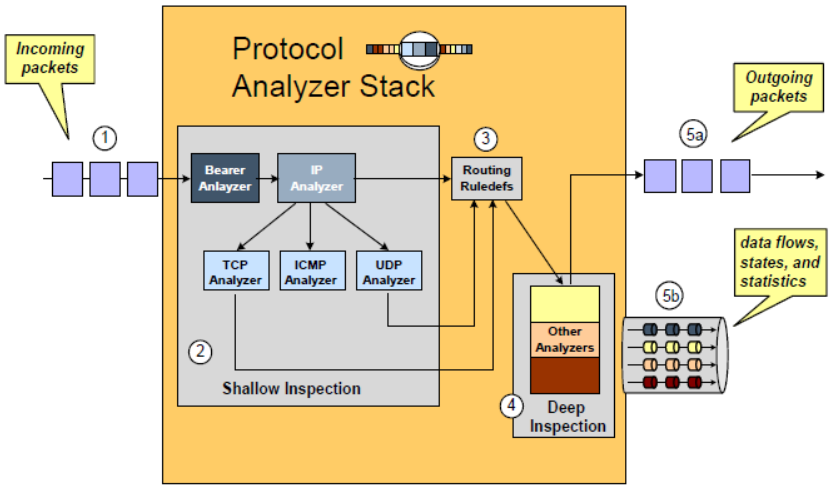

Ilustración 49: Proceso de reconocimiento del *Cisco ASR 5000* (124)

En el transcurso del análisis los paquetes pasan por un bloque analizador de protocolos, que se compone de módulos individuales para cada uno de los tipos soportados. Este elemento lleva a cabo una inspección de protocolos complejos, tales como RTSP (Real Time Streaming Protocol) o SIP (Session Initiation Protocol). La siguiente ilustración muestra la pila de protocolos que emplea este equipo dando algunos ejemplos. Cada uno de los nombres de protocolo que aparecen es utilizado para representar a los analizadores individuales, que se centran en los campos y estados indicados y que son los que se deben comparar con los paquetes de entrada.

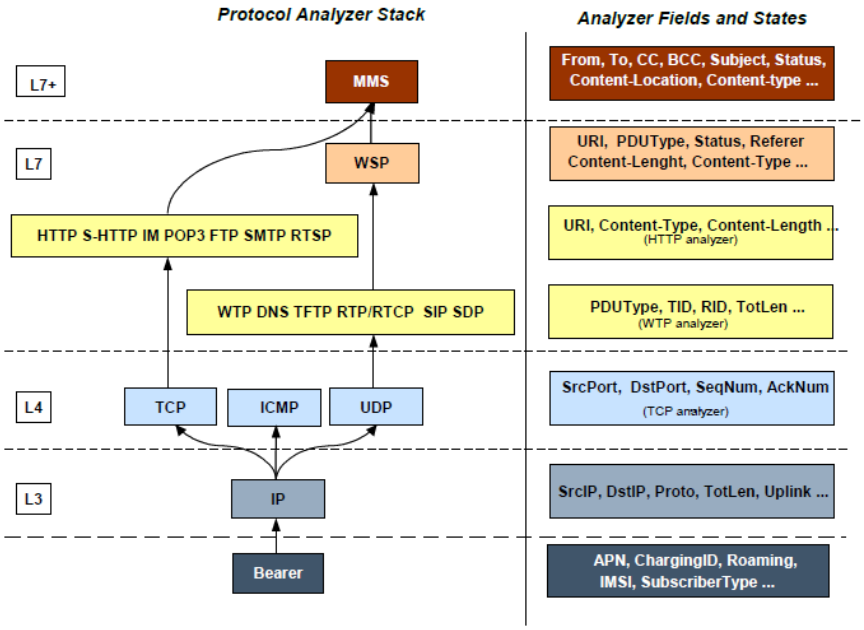

Ilustración 50: Pila de análisis de protocolos del *Cisco ASR 5000* (124)

4.3.1 Algoritmos de búsqueda DPI

Se ha visto el procedimiento que se emplea para la búsqueda y tratamiento de paquetes de forma global, pero no como actúa DPI. En este apartado se hace una revisión de las técnicas que se suelen emplear para el análisis que va más allá de las cabeceras.

De entre las técnicas para la búsqueda y comparación de patrones según los diferentes algoritmos disponibles para aplicaciones de red y DPI se destacan las siguientes características de mérito:

- **Número de búsquedas:** Las aplicaciones habituales, como los motores de búsqueda, analizan un texto varias veces para diferentes cadenas de búsqueda, haciendo uso de una estructura de indexación y consiguiendo que la complejidad sea baja. En las aplicaciones de red la búsqueda se realiza una sola vez sobre la información online, haciendo que la complejidad sea mayor.

- **Compresión:** Algunos algoritmos son capaces de realizar la búsqueda sobre texto comprimido, añadiendo velocidad al proceso.

- **Exactitud en la búsqueda:** Pueden darse situaciones en que el resultado de la búsqueda sea aproximado. También existe la opción de la búsqueda exacta.

- **Complejidad en tiempo:** Mientras que algunos algoritmos presentan una complejidad temporal lineal, otros presentan una de tipo sublineal, siendo este último caso más rápido en media.

- **Número de patrones:** Existen algoritmos con capacidad de búsqueda múltiple mientras que otros tan sólo permiten una búsqueda individual.

- **Expresividad:** Los patrones a buscar van desde expresiones fijas a expresiones regulares, siendo estas las que aportan mayor expresividad (flexibilidad a la hora de buscar patrones).

Antes de entrar a analizar las opciones existentes, se debe comentar que existe una notación específica para la clasificación de la complejidad en algoritmos computacionales, que en su terminología en ingles se conoce como 'big O notation'. Esta notación indica la tendencia asintótica del comportamiento del parámetro al que se refiere (normalmente, dificultad o tiempo de procesado). Así, una algoritmo que para una entrada de longitud n presenta un tiempo de procesado que responda a $T(n) = n^2+n+1$, según esta notación se representará como $O(n^2)$. Este parámetro será citado en los siguientes apartados para dar una idea de las prestaciones de los algoritmos que se exponen a continuación.

4.3.1.1 'String Matching'

Las primeras aplicaciones DPI emplearon estas técnicas de búsqueda de cadenas. El funcionamiento básico es simple, se trata de comparar los datos que circulan en la red con un conjunto de cadenas específicas definidas en las reglas de búsqueda. Este modelo es el que empleó Snort[8], un conocido software 'open source' para IDS/IPS.

'String matching' hace un filtrado de texto para la búsqueda de un patrón concreto, por lo que esta forma de búsqueda de patrones excluye el texto que no cumple con las características exactas. Por ello resulta ineficiente en los desafíos de hoy en día, ya que las aplicaciones pueden burlar fácilmente este método con una simple alteración como la desordenación o la inclusión de caracteres intermedios.

Así, aunque el 'string matching' es un algoritmo simple y por tanto rápido para la búsqueda de patrones, carece de niveles de expresividad o flexibilidad por lo que su aplicación para la

[8] http://www.snort.org/

obtención de firmas no es suficiente para hacer frente a técnicas de ataque ni el dinamismo con el que se modifican a día de hoy algunos protocolos.

4.3.1.2 Regular Expression (RegEx)

En la actualidad, la búsqueda de expresiones regulares ha reemplazado a los patrones explícitos de 'string-matching' como el lenguaje por excelencia para la búsqueda de información en el escaneo de paquetes. Su uso generalizado se debe a su poder expresivo y la flexibilidad para describir los patrones útiles.

Ejemplos de aplicaciones de código abierto que emplean su uso son el Linux Application Protocol Classifier (L7-filter)[9], Bro[10] (otro software IDS/IPS) o el mismo Snort, que ha ido incorporando reglas de este tipo. Por otro lado, aunque son flexibles y permiten mayor maniobrabilidad, las expresiones regulares tradicionalmente han requerido grandes cantidades de memoria y capacidad de procesado, lo que ha venido limitando su aplicabilidad en el contexto de redes.

La metodología de búsqueda de expresiones regulares se encuentra definida por una serie de caracteres que indican los criterios para la localización de patrones. En la siguiente figura se muestran algunos de los caracteres más empleados y una posible aplicación como ejemplo.

Carácter	Significado	Ejemplo	Solución
^	Indica la posición inicial de la cadena a identificar	^abc	Busca una cadena que comienza con "abc"
|	Relación OR clásica	ab|cd	Busca "ab" o "cd"
.	Comodín para un solo carácter	a.c	Busca cualquier cadena "aac", "abc", "acc", "adc", etc.
?	Cuantificador que denota uno o menos	ab?	Busca "ab" o "a"
*	Cuantificador que denota cero o más	ab*c	Busca "ac", "abc", "abbbbbc", etc.
+	Cuantificador que denota uno o más	ab+c	Busca "abc", "abbbbbc", etc.
{}	Repetición	ab{2}	Busca "abab"
[]	Grupo de caracteres	[abc]	Busca "a", "b" o "c"
[^]	Exclusión de carácter	[^ab]	Busca cualquier cadena menos "ab"

Ilustración 51: Significado caracteres de búsqueda de expresiones regulares

Las técnicas empleadas para la búsqueda y análisis de expresiones regulares se basan en la teoría de autómatas. En el campo que nos ocupa están basadas en las modalidades Non-deterministic Finite Automata (NFA) y en Deterministic Finite Automata (DFA), siendo ésta última la más empleada. No obstante, estos modelos de búsqueda de expresiones regulares a menudo no se adaptan estrictamente a los requerimientos necesarios a día de hoy. DFA muestra un crecimiento exponencial del espacio de estados (que implica un aumento de necesidades de memoria) por cada carácter que se añada a su entrada, y NFA, que no da problemas notables en cuanto a necesidades de memoria, resulta inaceptablemente lento para la aplicación DPI (125).

[9] http://l7-filter.sourceforge.net
[10] bro-ids.org/

La aproximación basada en autómatas es popular básicamente por dos razones: en primer lugar por el hecho de que el tiempo de ejecución queda acotado en el peor de los casos como veremos se verá a continuación, incluso cuando se dan ataques con el objetivo de hacer saturar el algoritmo; en segundo lugar, debido a que la construcción de un algoritmo basado en autómatas es sistemática y ha sido ampliamente estudiada para otras aplicaciones (126). A continuación se hace una breve introducción a la notación de teoría de autómatas para el posterior análisis de las técnicas DPI citadas.

4.3.1.2.1 Teoría de autómatas

La teoría de autómatas es el campo de la ciencia informática que estudia el empleo de máquinas abstractas y los métodos de resolución de problemas que éstos pueden llevar a cabo.

Los parámetros para la representación de un autómata se definen en una quíntupla:

$$\{Q, \Sigma, \delta, A, q_0\}$$

- Q: Conjunto finito de estados posibles.
- Σ: Conjunto finito de símbolos legibles.
- δ: Función de transición.
- q_0: Estado inicial del sistema, $q_0 \in Q$.
- A: Conjunto de estados aceptación, $A \in Q$.

Este paradigma de la teoría computacional es empleado en variedad de aplicaciones tales como el procesado de textos o compiladores de programación. Recientemente su uso ha sido adaptado al análisis DPI. En este tipo de aplicaciones de red, Σ suele contener los 256 símbolos pertenecientes al código ASCII extendido. Entre el conjunto de estados, hay un solo estado q_0 inicial y un conjunto de estados de aceptación, que se compone por los estados que darían un resultado positivo a la búsqueda.

Veamos de forma simplificada y aplicado al campo de RegEx como trabaja un autómata. Inicialmente recibe una palabra o secuencia de entrada, que está formada por el conjunto de símbolos Σ. Considerándose tanto el estado presente (inicialmente q_0) como el símbolo de entrada, se aplica la función de transición correspondiente (δ) y se salta hacia el siguiente estado o estados del conjunto Q. Este procedimiento finaliza cuando se completa la lectura de la palabra o secuencia de entrada. Dependiendo de en qué estado final acabe el autómata, la entrada es reconocida por el sistema (si se finaliza en alguno de los estados $A \in Q$), o por el contrario es descartada. El conjunto de palabras reconocidas por un autómata se conoce como

el lenguaje de éste. Según si el autómata responde al paradigma NFA o DFA llevará a cabo la transición de diferente modo, siendo éste un parámetro diferenciador entre ambos métodos.

4.3.1.2.1.1 NFA: Non-deterministic Finite Automata

NFA representa un formato algo complejo de comprender, aunque a nivel computacional se traduce al mecanismo más simple. Los estados de un autómata de este tipo pueden, o no, tener una o más transiciones por cada símbolo del alfabeto. Es decir, por definición debe poseer al menos un estado $q \in Q$, tal que para un símbolo $a \in \Sigma$ del alfabeto, exista más de una transición $\delta(q,a)$ posible. Esto se traduce en que en este tipo de autómata la función de transición da como resultado un conjunto estados, permitiendo que existan varios estados activos simultáneamente (127).

El autómata da como aceptada una palabra si existe al menos un camino desde el estado q_0 a un estado final F asignado a la palabra de entrada. Si una transición no está definida, de manera que el autómata no puede saber cómo continuar leyendo la entrada, la palabra es rechazada.

En la siguiente ilustración se muestra un ejemplo de cómo llevaría a cabo el mapeo de estados un algoritmo NFA para una búsqueda sencilla (abcd | abdc). Cabe mencionar que este ejemplo pretende tan sólo mostrar el principio de funcionamiento NFA. Es interesante comprender que los estados q_1 y q_2 y los estados q_3 y q_4 estarían activos a la vez ya que ésta es la característica básica de NFA, lo cual implicaría un doble procesado para un mismo carácter.

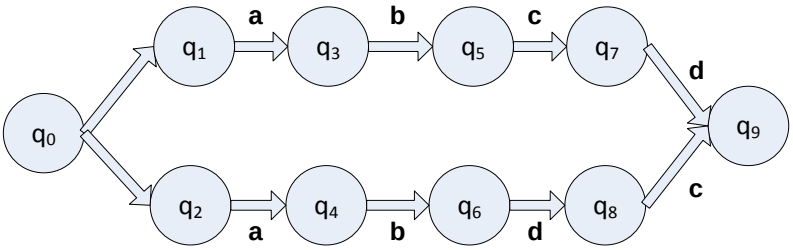

Ilustración 52: Evolución de estados en NFA para la búsqueda abcd | abdc

Este modelo se encuentra prácticamente en desuso debido a su lentitud. Según un estudio (128) teórico basado en el peor caso, para la detección de una palabra de longitud n, ésta puede necesitar solo O(n) estados mientras que la complejidad de procesado para un carácter a la entrada es del orden $O(n^2)$. Esto se traduce en un espacio de estados pequeño (baja necesidad de memoria) y una necesidad de procesado cuadrática (tiempo de computación elevado).

4.3.1.2.1.2 DFA: Deterministic Finite Automata

A diferencia de NFA, DFA es rápido y fácilmente combinable, aunque su empleo puede llevar a situaciones de desbordamiento de memoria. Cada estado de un autómata de este tipo tiene una transición por cada símbolo del alfabeto. En esta versión la función de transición da lugar a un nuevo estado definido, a diferencia de lo que ocurre en NFA. Esto hace que sólo pueda haber un estado activo ya que para cada estado q ∈ Q en que se encuentre el autómata, y con cualquier símbolo a ∈ Σ del alfabeto leído, existe siempre a lo sumo una transición posible δ(q,a) (127). El motivo por el que el consumo de memoria es elevado radica en el mapeo de todos los estados posibles al autómata para una RegEx dada, consiguiendo así que posteriormente el tiempo de procesado necesario para procesar una cadena sea menor.

En el ejemplo del siguiente esquema se muestra ahora la misma búsqueda que en el apartado anterior (abcd | abdc) pero habiendo convertido el autómata a un DFA. En este caso la transición de un estado al siguiente es unívoca y queda determinada por el estado anterior y el carácter leído. Con este formato el procesado necesario es menor ya que para un carácter dado solo existe un estado en el cual se procesa su búsqueda (recordemos que en NFA esto no sucede). En este ejemplo concreto no se aprecia la mayor necesidad de memoria, e incluso el espacio de estados es menor en DFA que en NFA. Se pretende tan solo dar una visión de la base del funcionamiento, y no entrar a valorar los cálculos de coste computacional o necesidades de memoria (espacio de estados), cuya complejidad se escapa al objetivo de este Proyecto.

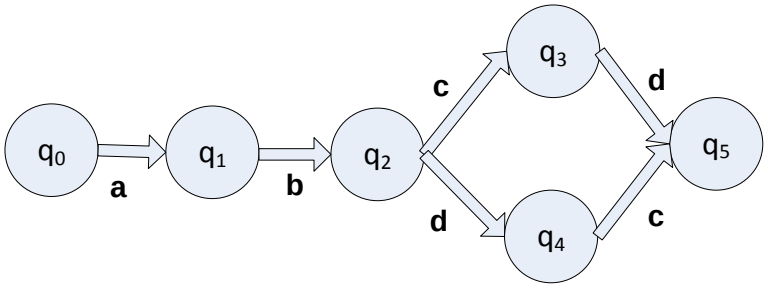

Ilustración 53: Evolución de estados en DFA para la búsqueda abcd | abdc

Para detectar una palabra de longitud n, DFA puede llegar a generar $O(\Sigma^n)$ estados con las necesidades de memoria que esto implica. Por ejemplo, Cisco se ve en la necesidad de emplear comúnmente alrededor de un gigabyte de memoria para poner en práctica el análisis basado en autómatas para RegEx, con lo que el coste de la memoria a menudo representa una parte considerable del coste del sistema (129). Por contra la complejidad de procesado para un carácter a la entrada se simplifica hasta el orden de O(1), de ahí el hecho de que se trate de un algoritmo rápido.

Debido a los inconvenientes en cuanto a necesidades de memoria que presenta DFA se han desarrollado algunas versiones con capacidad de mejorar algunas de sus carencias. El algoritmo D^2FA (Delayed Input DFA) es capaz de reducir las necesidades de memoria a base de

perder algo de velocidad. En un algoritmo convencional de DFA los estados están marcados por identificadores que se emplean para indexar las entradas en una tabla. D^{2}FA reemplaza los identificadores del estado con etiquetas de contenido que incluyen parte de la información que normalmente se almacena en la entrada de la tabla. Esto permite omitir algunas transiciones que de lo contrario deberían ser procesadas, requiriendo por ello menos capacidad de almacenamiento (129).

La adaptación hardware hacia esta aproximación queda latente en las propiedades de muchos procesadores para DPI. Así, éstos suelen incorporar módulos aceleradores. Ejemplo de ello se muestra en el procesador Canvium Octeon MIPS64 (130), que como se aprecia en la siguiente ilustración incluye una unidad TCP, un motor de compresión/descompresión de datos, y hasta dieciséis motores de búsqueda de expresiones regulares en un solo chip que según el fabricante es capaz de analizar mediante RegEx un caudal de hasta 15 Gbps (basándose en lo que ellos denominan Hyper Finite Automata).

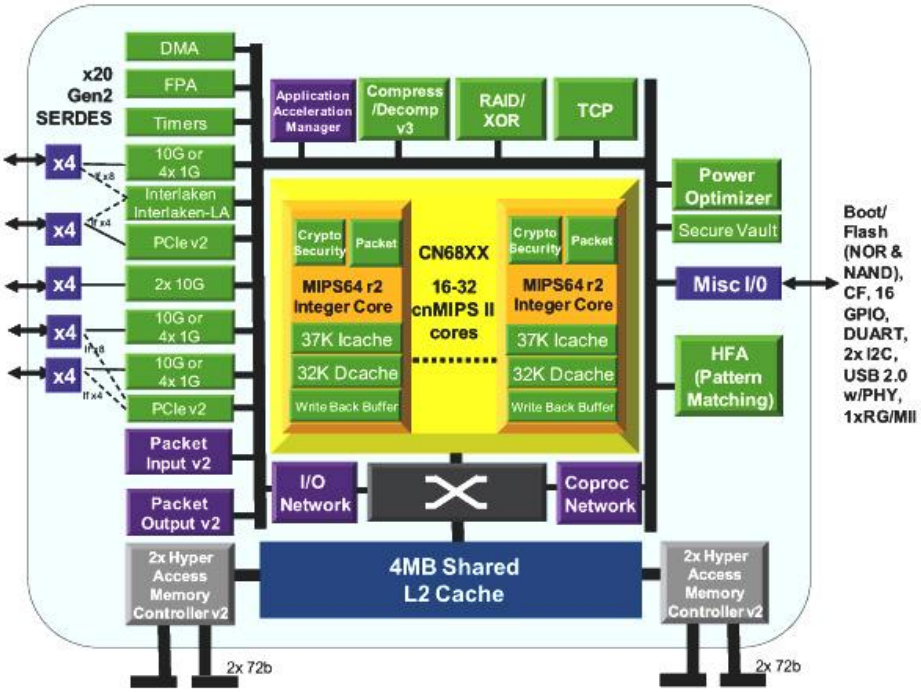

Ilustración 54: Bloque modular del Cavium Octeon II (130)

4.4 Análisis DFI

Al inicio de este capítulo se ha definido DFI y se ha justificado su necesidad a la hora de reconocer tipos de tráfico cuando este se encuentra ofuscado o cifrado. En este apartado se va un poco más allá y se explican algunos de los mecanismos que permiten una clasificación de paquetes sin realizar un análisis DPI.

El proceso de reconocimiento del tipo de tráfico analiza características del flujo tales como el ritmo de envío o la duración y tamaño de los paquetes. Posteriormente se utilizan junto con los números de puerto y las direcciones origen y destino para mejorar la identificación. En el

caso de detección P2P, estas estadísticas se combinan además con información acerca del diámetro de red (distancia más corta media entre pares de nodos, medida en número de saltos) y los equipos que actúan como servidores y clientes (77).

Un método para llevar a cabo DFI se basa en el reconocimiento de patrones en el establecimiento de una conexión, o lo que es lo mismo, el proceso de 'handshake'. Si siempre se cumple éste, al reconocerse se puede intuir que esa conexión pertenece al protocolo o aplicación correspondiente. No obstante, este mecanismo tiene algunas debilidades. Si bien el hecho de que se cumpla con el patrón hace que la comunicación pueda ser la que se corresponde con lo almacenado en la librería de protocolos, no tiene por qué serlo necesariamente. Esto es lo que se suele denominar un "falso positivo", y puede llevar al error en la aplicación de políticas. También existe el concepto inverso, "falso negativo", que se da en aquellos casos en que no se puede determinar con exactitud la aplicación o protocolo en uso.

La siguiente ilustración muestra un ejemplo de establecimiento determinista en base a la longitud y número de paquetes que puede dar lugar al reconocimiento de un protocolo. Una herramienta DFI que detectase este patrón de 'handshake' llevaría a cabo un seguimiento de quíntupla para tener identificado el flujo durante su tiempo de duración. En el caso de cambiar puertos de forma dinámica se debería tener en cuenta tan solo las direcciones IP, haciendo la identificación cada vez menos robusta. Nótese que éste método sólo es capaz de identificar el protocolo si detecta el establecimiento de la conexión, en caso contrario se le tornaría imposible.

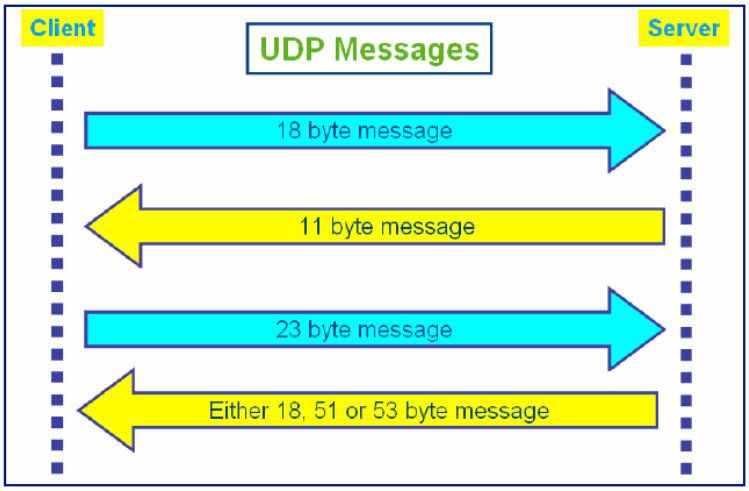

Ilustración 55: Establecimiento de conexión en Skype (versiones previas a 2.0) (76)

Otra técnica habitual es la obtención de un histograma de la longitud de los paquetes para la comparación con una base de datos de histogramas. Por ejemplo, los paquetes P2P de la capa de control son mucho más cortos que los paquetes HTTP puros (P2P se suele enmascarar en el protocolo HTTP), como se muestra en la ilustración a continuación.

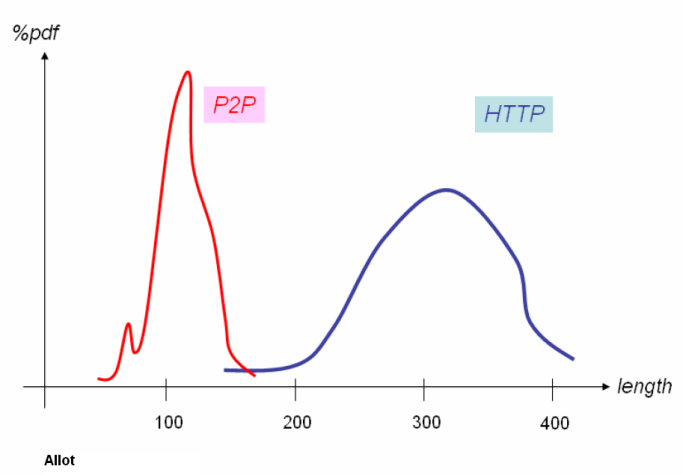

Ilustración 56: Histograma de longitud de paquetes P2P y HTTP (76)

Esta forma de detectar el tráfico es poco robusta y afinada. Si bien puede determinar a grandes rasgos el tipo de tráfico analizado, sería muy difícil que mediante este mecanismo se pudiese afinar a un protocolo concreto. Además, para poder dar por bueno un análisis basado en estadística se necesitan una cantidad mínima de paquetes, con lo que sería necesario un tiempo de espera notable.

El empleo de los métodos citados acarrea ciertas dificultades, pero precisamente en el desarrollo de este tipo de técnicas consiste la labor de los proveedores de DFI. El uso de técnicas DFI conlleva una fuerte necesidad de actualización y seguimiento de protocolos ya que los parámetros que analizan son fácilmente eludibles o aleatorizables, con lo que su detección supone un gran desafío, y un constante pulso frente a los diseñadores de aplicaciones o protocolos.

Siguiendo con el equipo *Cisco ASR 5000* (124) analizado en el apartado 4.3 de este capítulo, se describe ahora cómo se lleva a cabo la detección de P2P mediante análisis DFI en este sistema. La detección de tráfico P2P se hace antes del DPI debido a que así presenta algunas ventajas que se citan textualmente:

- algunos protocolos como BitTorrent y Orb utilizan tráfico HTTP para la configuración inicial. Así, si el análisis de P2P se realiza después del análisis DPI, es posible que estos protocolos puedan pasar desapercibidos.

- algunos protocolos, como Skype, utilizan los 'well-known ports' (como 80 y 443). En este caso, el motor de análisis HTTP trataría estos paquetes como no válidos.

- la detección de protocolos basados en firmas y no en análisis heurístico será más sencilla cuando el análisis P2P se realice antes de DPI, por haberse descartado ciertos paquetes.

Resulta también interesante ver algunas dificultades que quedan especificadas en cuanto a la detección de P2P se refiere y que dan una buena muestra de la complejidad que implica la detección mediante DFI de numerosos protocolos. Algunos ejemplos:

- **Skype:** La detección de tráfico Skype no puede captar el tráfico de la mayoría de los plug-ins de terceros con lo que su detección puede no ser exacta si el tráfico se mezcla con otros tipos de tráfico en el mismo flujo.

- **eDonkey:** El cliente eMule, trabaja también con el protocolo llamado Kademlia. Este protocolo es una implementación de un DHT (Distributed Hash Table) y es utilizado para la búsqueda de nuevos 'peers' y no es detectado.

- **Jabber:** La mayoría de los clientes que utilizan Jabber para mensajería instantánea ofrecen otros servicios como llamada de voz o de transferencia de archivos. Estos servicios no son detectados como Jabber, además, cuando utiliza cifrado SSL (Secure Socket Layer) no se puede detectar.

- **Gnutella/Morpheus:** Algunos de los clientes que utilizan el protocolo Gnutella para compartir archivos también pueden utilizar otros protocolos de intercambio de archivos, que no serán detectados. El cliente Morpheus crea una gran cantidad de flujos TCP, sin ningún tipo de patrón en el inicio de la aplicación, haciendo que estos flujos no sean detectados.

- **Otras limitaciones:** La mayoría de los comportamientos heurísticos en base a ciertos patrones son vistos por el analizador. Los protocolos P2P emiten estos patrones de forma regular, pero si el sistema pierde los flujos, pueden no ser detectados.

5 Análisis de tráfico real: Ejercicio práctico

En este apartado se expone la realización de algunos ejercicios de análisis de tráfico mediante un motor de búsqueda DPI. Para ello se ha hecho uso de OpenDPI (con la ayuda del analizador de tráfico Wireshark[11], para más detalle véase Anexo B). Se trata de un componente de software libre desarrollado por el proveedor de soluciones de gestión de tráfico Ipoque.

Se ha expuesto en el apartado 1 de este capítulo que el tráfico ofuscado es, en general, inmune al análisis DPI, ya que la información que transporta es deliberadamente tratada (cifrada o no) para que tan sólo pueda recuperarla el receptor en el destino. Cabe recordar que el propósito de cifrar una comunicación, a priori, responde a motivos de privacidad, autentificación, integridad, etc. Para dar una muestra de esta idea, además de extraer otras conclusiones, se analizan los dos tipos de tráfico que más controversia crean, el tráfico P2P y la VoIP. También se estudia la transmisión y recepción de correo electrónico, para comprender ciertos relacionados con la privacidad. Para más detalle sobre el ejercicio consúltese el Anexo B, donde también se encuentran las capturas de pantalla de las que se extraen los datos aquí comentados.

5.1 P2P (Peer-To-Peer)

Debido al creciente interés de los ISPs en controlar que tráfico fluye por sus redes, los desarrolladores de ciertos protocolos perseguidos, siendo el más destacado el tráfico P2P, han ido añadiendo la opción de cifrar el tráfico para ocultar la información referente al protocolo o aplicación asociados.

5.1.1 BitTorrent

Se han analizado bloques de tráfico generados por dos clientes BitTorrent, que es el protocolo P2P más extendido (18), cifrando y sin cifrar la comunicación. La opción de cifrar suele estar desactivada por defecto y en la configuración de los clientes se puede modificar.

Se han empleado dos clientes para dar mayor fiabilidad al ejercicio: *qBittorrent*[12] y el popular *µTorrent*[13]. La elección de éstos se ha basado en que para su configuración de cifrado permiten las opciones de forzado y de deshabilitación, que son las que interesan para mostrar el efecto del cifrado. El empleo de *µTorrent* se ha llevado a cabo sin habilitar su utilidad de emplear lo que sus desarrolladores denominan Micro Transport Protocol (µTP), que representa una versión de BitTorrent pensada para trabajar sobre UDP y que no es detectada por OpenDPI.

No es objeto de este ejercicio analizar este protocolo, pero comentar que a diferencia de TCP, UDP no incluye mecanismos de control del flujo ni se preocupa de que los paquetes lleguen al

[11] http://www.wireshark.org/
[12] http://www.qbittorrent.org/
[13] http://www.utorrent.com/

destino. Así se consigue un mayor aprovechamiento del ancho de banda que en TCP (porque éste incluye control de flujo, aunque se suele burlar abriendo múltiples conexiones) y se resta latencia al proceso de envío. Según sus desarrolladores el ancho de banda se adapta al estado de la red, con lo que se beneficia tanto al usuario como al conjunto de red.

Otros clientes que se han empleado para realizar este ejercicio incluyen opciones de cifrado menos estrictas. En concreto, el cliente *BitTorrent Transmission*[14] (cliente por defecto en algunas distribuciones basadas en Linux) da la opción de permitir cifrado en lugar de deshabilitarlo, con lo que los resultados de la prueba no aportan ningún valor ya que al no poder anularlo por completo, las conexiones entrantes que solicitan una comunicación cifrada son permitidas y por lo tanto no se puede forzar a que todo el tráfico cursado sea no cifrado.

Para valorar los resultados del ejercicio se han extraído los parámetros más relevantes de las capturas de tráfico realizadas. En primer lugar hay que aclarar que la capacidad de clasificación es mayor, en todos los casos, con la herramienta OpenDPI que en el análisis realizado por Wireshark. Esto es debido a que Wireshark tan solo realiza un análisis del tipo SPI (análisis y seguimiento de puertos conocidos).

		Wireshark		OpenDPI	
qBitorrent	Paquetes IP	BT (#)	BT (%)	BT (#)	BT (%)
Sin cifrar	15249	2672	17,52%	**11478**	**75,27%**
Cifrado	15122	0	0,00%	**0**	**0,00%**

		Wireshark		OpenDPI	
µTorrent	Paquetes IP	BT (#)	BT (%)	BT (#)	BT (%)
Sin cifrar	15310	3407	22,25%	**12422**	**81,14%**
Cifrado	15118	0	0,00%	**105**	**0,69%**

Ilustración 57: Comparativa resultados

Nótese que pese a que todo el tráfico generado durante las capturas de la muestras es debido al cliente P2P, el máximo detectado de tráfico BitTorrent es de 81,14%. Después de analizar varias muestras de tráfico se llega a la conclusión de que esto es debido a que el motor OpenDPI sólo es capaz de clasificar un flujo como BitTorrent si detecta el proceso de 'handshake' entre los extremos de la comunicación. Es decir, si el cliente se encuentra intercambiando tráfico antes de comenzar el análisis o si no se detecta la comunicación inicial, se pierde el flujo y no es posible determinar el protocolo del nivel 7 (este concepto está en línea con las especificaciones del *Cisco ASR 5000*, descritas en el apartado 4.4 del capítulo V).

En cualquier caso, el objetivo de este ejercicio es mostrar cómo la ofuscación anula el análisis DPI, y en efecto se puede apreciar este hecho. Para un mismo análisis en idénticas condiciones pero activando la opción de cifrado u ofuscación, el motor OpenDPI es incapaz de clasificar ningún paquete como BitTorrent, ya que esta tarea se debería realizar mediante análisis DFI.

[14] http://www.transmissionbt.com/

5.1.2 eDonkey

De forma idéntica a los análisis anteriores, se ha capturado también el tráfico generado por el conocido cliente *eMule*[15], que opera sobre el protocolo P2P eDonkey. Pese a que no es tan empleado como BitTorrent (18), este formato es también ampliamente empleado para la descarga de ficheros P2P. El cliente *eMule* incorpora un mecanismo para habilitar y deshabilitar la ofuscación, que realmente está basado en el cifrado de algunos patrones del protocolo que en caso contrario son fácilmente detectables. Según los propios desarrolladores, esta técnica está diseñada para eludir la detección en caso de que se sospeche que el ISP realice gestión de tráfico. Se resalta que no se consigue con ello el anonimato ni la privacidad del usuario (78).

Igual que para el caso de BitTorrent, se resumen los datos más relevantes en una tabla para mayor facilidad de análisis.

		Wireshark		OpenDPI	
eMule	Paquetes IP	e2k (#)	e2k (%)	e2k (#)	e2k (%)
Sin ofuscar	14988	18	0,12%	**14606**	**97,45%**
Ofuscado	14980	153	1,02%	**0**	**0,00%**

Ilustración 58: Análisis OpenDPI sobre captura *eMule* ofuscado

Para este caso, en el análisis SPI realizado por Wireshark se obtienen unos datos peculiares, ya que como se puede observar se detectan más paquetes cuando se ofusca el protocolo que en el caso no ofuscado. Este hecho pone de relevancia que un análisis SPI basado en el número de puertos es en muchos casos totalmente ineficiente. Por el contrario, analizando las mismas capturas mediante OpenDPI se puede ver como la detección en el caso no ofuscado es muy buena, del 97,45%, mientras que la ofuscación hace al tráfico eDonkey invisible para esta herramienta.

5.2 VoIP (SIP + RTP)

Se analizan en este caso dos capturas de tráfico de VoIP sobre los protocolos SIP (131) y RTP (Real Time Protocol) (132). La elección de este formato de VoIP se debe a que estos protocolos son estándares de la IETF, mientras que los protocolos de otras formas de VoIP más populares, como Skype, emplean códigos propietarios que son cifrados u ofuscados por defecto para evitar su detección. Además, en el caso concreto de Skype, no es posible su detección mediante el motor OpenDPI.

[15] http://www.emule-project.net/

Se han analizado dos capturas de tráfico generadas con un cliente de VoIP libre llamado *Blink*[16] en el transcurso de una llamada estándar, habiéndose capturado alrededor de 1000 paquetes de datos entre el establecimiento y finalización de la misma. Este cliente emplea el protocolo RTP para la transmisión del contenido, y SIP para la señalización (establecimiento, modificación y terminación de sesiones). Las opciones de cifrado que permite son mediante TLS (133) para la señalización mediante SIP, y SRTP (Secure Real Time Protocol) (134) para el contenido de la llamada mediante RTP. En este ejercicio se ha llevado a cabo el cifrado de la llamada y no de la señalización.

En las siguientes ilustraciones se muestran los datos de interés:

		Wireshark		OpenDPI	
Blink	**Paquetes IP**	**RTP (#)**	**RTP (%)**	**RTP (#)**	**RTP (%)**
No cifrado	1091	1037	95,05%	**1034**	**94,78%**
Cifrado	1063	1021	96,05%	**1018**	**95,77%**

Ilustración 59: Comparativa resultados

***Blink* sin cifrar**

Source	Destination	Protocol
192.168.0.196	81.23.228.129	RTP

Ilustración 60: Detalle análisis Wireshark sobre captura *Blink* sin cifrar

***Blink* cifrado**

Source	Destination	Protocol
192.168.0.196	81.23.228.129	SRTP

Ilustración 61: Detalle análisis Wireshark sobre captura *Blink* cifrado

Los resultados son suficientemente claros, ya que como se puede apreciar en la tabla, la identificación del protocolo es prácticamente del 100% en todas las situaciones. En ambos casos, tanto Wireshark como OpenDPI son capaces de clasificar los paquetes RTP tanto si están cifrados como si no lo están. De hecho, ni tan siquiera distinguen entre RTP y SRTP (véase apartado 2.2 del Anexo B) salvo en las capturas hechas más en detalle para cada paquete en Wireshark (Ilustración 60 e Ilustración 61). En este caso, el hecho de cifrar (que no ofuscar) la comunicación no impide que se pueda reconocer el protocolo sobre el que se está trabajando,

[16] http://icanblink.com/

tanto empleando análisis SPI como DPI. Así, con este ejercicio se muestra un comportamiento contrario al caso de BitTorrent, ya que en este último el cifrado se hace no por motivos de privacidad sino por una cuestión de ofuscación, es decir, para evitar su detección por DPI.

También se pretende hacer resaltar con este resultado que la tecnología DPI empleada para la gestión de tráfico no tiene como objetivo, o al menos la necesidad, de comprender el contenido de las comunicaciones para clasificar los paquetes según los protocolos empleados. De hecho, como se puede observar en las capturas de OpenDPI, se cataloga igual el tráfico RTP y SRTP, cuando el primero podría ser comprensible para cualquier punto intermedio, mientras que el segundo sólo sería recuperable por el destinatario.

5.3 Email (SMTP + IMAP)

En este ejercicio se han analizado el envío y recepción de correo electrónico estándar mediante SMTP (Simple Mail Transfer Protocol) (135) e IMAP (Internet Message Acces Protocol) (136), respectivamente. Para ello se ha empleado el popular cliente de correo *Thunderbird*[17], que permite configurar múltiples opciones y trabajar con varias cuentas de correo. Para realizar este ejercicio se ha empleado una cuenta de GMX[18], debido a que este servicio de correo permite trabajar sobre conexiones no seguras de SMPT e IMAP, mientras que otros servicios más populares como *Gmail* o *Hotmail* no lo permiten.

La elección de IMAP como el protocolo de recepción de correo ha sido por simple configuración inicial del cliente *Thunderbird*. La diferencia con POP3 (Post Office Protocol 3) (137) radica en que IMAP mantiene una sincronización con el servidor mientras que POP3 tan sólo descarga en cada máquina donde esté corriendo una copia del correo desde el servidor. Para el propósito de este ejercicio, también se podría haber trabajado con POP3.

Se ha realizado el envío y recepción de un mensaje con un contenido concreto (passwd: 12345) que quiere hacer hincapié en cómo se podrían fácilmente detectar datos en comunicaciones no cifradas. Para ello se ha realizado tanto el envío como la recepción en modo seguro (sobre TLS) o en modo no seguro.

El envío de email estándar se hace mediante el protocolo SMTP, que trabaja sobre el puerto 25 TCP, mientras que la recepción se hace sobre el protocolo IMAP sobre el puerto 143. En el caso de trabajar sobre TLS, el protocolo SMTPS trabaja sobre el puerto 465 mientras que IMAPS lo hace sobre el puerto 993. Se añade la captura de la configuración para cada uno de los casos.

En este caso no se han extraído los datos de Wireshark debido a que no aportan ninguna información relevante debido a que en todo momento se hace uso de los 'well-known ports' y por consiguiente la identificación mediante SPI es inmediata. En cambio, se incluyen, en el

[17] http://www.mozilla.org/es-ES/thunderbird/
[18] http://www.gmx.es/

caso de email sin cifrado, las capturas resultantes de realizar una búsqueda de la palabra *passwd* sobre el fichero *.pcap*[19] con el editor de texto *Notepad++*[20].

Email sin cifrado

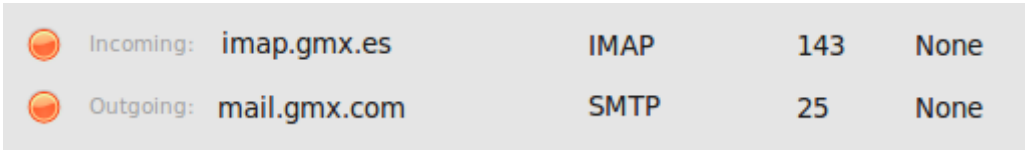

Ilustración 62: Detalle configuración *Thunderbird* sin cifrado

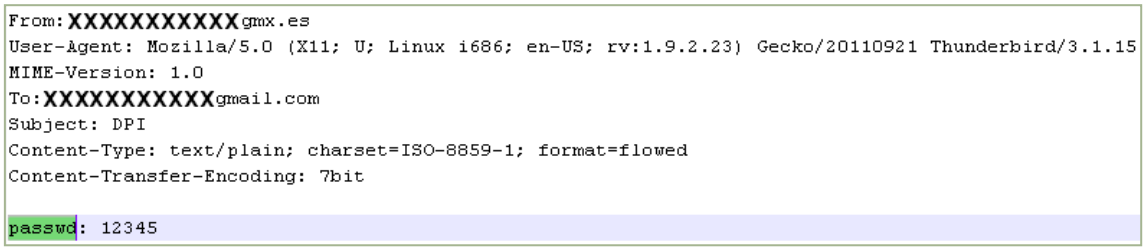

Ilustración 63: Búsqueda de *passwd* sobre fichero *.pcap* de envío (SMTP) sin cifrado

Ilustración 64: Búsqueda de *passwd* sobre fichero *.pcap* de recepción (IMAP) sin cifrado

[19] Packet Capture es una API para la captura de tráfico de red.
[20] http://notepad-plus-plus.org/

Email cifrado

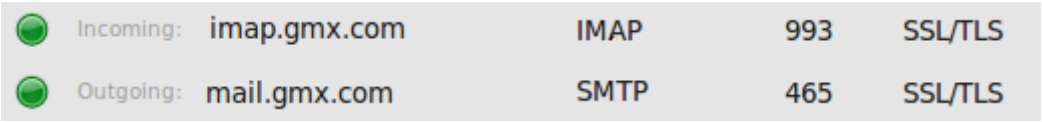

Ilustración 65: Detalle configuración *Thunderbird* cifrado

En primer lugar, hay que señalar que la detección por parte de OpenDPI se ajusta a lo esperado. Es también de destacar que en el caso sin cifrado, para el envío SMTP se detectan varios paquetes IMAP, algunos DNS (Domain Name Server) además de otros desconocido (ver apartado 2.3 del Anexo B). Este hecho se atribuye a cuestiones de conexión y sincronización con el servidor (por ejemplo, los paquetes IMAP se deben a que al enviar un mensaje por SMTP, el cliente *Thunderbird* lo vuelve a descargar mediante IMAP para mantener sincronizada la carpeta Enviados o similar).

En el caso cifrado, la información referente a la capa de aplicación de los paquetes (nivel 7) sólo muestra el protocolo empleado (SSL). Nótese que aunque el contenido es inaccesible salvo por el receptor, el protocolo TLS no se esconde. En este caso, el empleo de SPI analizando los puertos empleados sería una buena forma de clasificar el tráfico TLS, aunque no es generalizable tal y como se ha visto con el protocolo eDonkey en el apartado 5.1.2.

Nótese también que en la captura de configuración del cliente en el caso no cifrado, aparece un indicador a la izquierda de cada uno de los parámetros de configuración que alerta sobre el hecho de que se está conectando de forma no segura con los servidores (en el caso cifrado también aparece, pero en verde, lo cual indica que la conexión es segura). Esta configuración "no segura" es la que servicios como *Gmail* o *Hotmail* ni tan si quiera permiten, como se ha dicho anteriormente para justificar el empleo de GMX.

Como se puede observar en las respectivas capturas de pantalla para la búsqueda de la palabra *passwd* en el caso no cifrado (Ilustración 63 e Ilustración 64) el mensaje viaja en texto plano, por lo que desde cualquier punto intermedio entre origen y destino y sin demasiada complejidad se podría acceder al contenido de la comunicación. Para el caso cifrado estas capturas no se han añadido ya que el contenido del fichero *.pcap* es totalmente incomprensible, incluso las direcciones origen y destino aparecen cifradas, quedando visible tan solo el dominio del servicio de correo *(@gmail.com* y *@gmx.com*).

Con este ejercicio se quiere resaltar que si bien DPI tiene la capacidad de buscar información en el contenido de los paquetes, es responsabilidad de los usuarios no compartir información privada sin cifrar. El empleo de mecanismos seguros está muy desarrollado a día de hoy, con lo que el envío de información sin cifrar es una irresponsabilidad por parte del usuario. De hecho, tal y como se pone de manifiesto en este apartado, algunos servidores de correo tan sólo permiten trabajar sobre conexiones seguras. Incluso el cliente de correo empleado avisa al usuario si la conexión sobre la que va a trabajar es no segura.

5.4 Conclusiones del ejercicio

Después de ver los diferentes resultados y de comprender las diferentes motivaciones se resaltan en este apartado algunas conclusiones interesantes.

- **DPI es efectivo siempre que no haya ofuscación, en caso de que ésta exista es imposible determinar protocolos de niveles superiores ya que la información no es comprensible.**
- **DFI es necesario para clasificar protocolos ofuscados, por los motivos comentados en el punto anterior.**
- **DPI puede analizar fácilmente el contenido de un paquete no cifrado.**
- **DPI, en su aplicación para la gestión de tráfico, no tiene necesidad comprender el contenido de las comunicaciones para la clasificación de los protocolos.**
- **La ofuscación está claramente orientada a la no detección, mientras que el cifrado responde a necesidades de seguridad.**
- **SPI es útil si se analizan servicios que siguen las definiciones de los 'well-known port'.**
- **SPI cómo única forma de análisis no es fiable, ya que el análisis basado en los números de puerto es fácilmente vulnerable a técnicas de enmascaramiento.**

Capítulo VI – Implicaciones, conclusiones y recomendaciones

Este capítulo se centra en hacer una valoración global y extraer las conclusiones más importantes sobre todo lo expuesto anteriormente. Para ello se proponen dos escenarios posibles según se apliquen o no las técnicas de gestión en desarrollo, para luego dar paso a las conclusiones y recomendaciones relacionadas con la gestión de tráfico mediante DPI/DFI.

A lo largo del capítulo III se ha dado una visión global sobre los diferentes factores que forman parte del debate de la Neutralidad de Red, y se ha focalizado en los capítulo IV y V en la gestión de tráfico según QoS con mecanismos de análisis DPI/DFI, haciendo especial hincapié en este último aspecto.

Se ha visto que hay diversos campos que conforman el debate acerca de la Neutralidad de Red, y que responden a varios planteamientos (ver sección 3 del capítulo III) que aunque relacionados entre sí, se pueden dividir en tres grandes ámbitos: económico, social y técnico. De estos tres grandes ámbitos, en este documento se ha profundizado sobre los equipos y las tecnologías relacionadas con la problemática del debate de Neutralidad de Red, por lo que las conclusiones e implicaciones del presente Proyecto versarán sobre esta línea, sin dejar de lado no obstante las demás consideraciones ya que es en los ámbitos económico y social donde recae el grueso de la discusión y su impacto.

1 Implicaciones

En este apartado se pasa a valorar qué impacto e implicaciones puede tener la gestión de tráfico (o su ausencia) mediante el uso de DPI/DFI en Internet y se extraen las ventajas e inconvenientes que pueden representar la utilización de esta forma de gestión.

Como se ha visto en el capítulo III, salvo casos concretos, no se han dado situaciones de fuerte tensión ni se ha vislumbrado una intención firme de cambio en el modelo Internet. No obstante, si el crecimiento del consumo de datos se mantiene al ritmo actual se alcanzará un punto en que la situación se verá desbordada. Como se ha expuesto en el capítulo IV la industria está apostando por un modelo de Internet claramente gestionado, por lo que existen desde el punto de vista técnico, dos posibles escenarios que pueden surgir al respecto.

1.1 Modelo 'best effort'

El primer escenario sería el de mantener Internet tal y como ha venido gestionándose hasta ahora, es decir siguiendo el modelo 'best effort' y cumpliendo, con una definición laxa de los principios de Neutralidad de Red. En este sentido, cabe recordar que el modelo actual de Internet no responde completamente a un modelo 'best effort', siendo uno de los factores que repercuten en este hecho es la oferta de servicios dedicados o verticales, que se ha visto reservan un cierto ancho de banda para ser transmitidos por el mismo acceso que los servicios de Internet.

Omitiendo este hecho, en este escenario sería previsible que se diesen serios problemas de congestión, debido a que el consumo de datos crece a mayor velocidad de lo que lo hace la capacidad de red. Ante esta situación, la solución a nivel técnico sería simple, se procedería eliminando los paquetes que desbordasen las colas de modo aleatorio, sin preocuparse del contenido de los mismos. Como se ha justificado en el apartado 3 del capítulo IV, este hecho tiene en su contra que tratar por igual todos los tipos de tráfico cuando no lo son es poco eficiente y contribuye a una pérdida de QoE para el usuario final.

Una posible escapatoria al problema de la congestión implicaría la inversión en más capacidad de red, aplicando lo que se ha definido anteriormente como exceso de aprovisionamiento. Esta forma de combatir la congestión se torna poco eficiente, por varios motivos expuestos en el apartado 1 del capítulo IV. Además, dada la coyuntura actual, en la cual la posición de los operadores hace pensar que no se muestran favorables a afrontar una inversión en este ámbito, este hecho podría acabar derivando en un aumento de los precios en alguno o ambos lados del acceso.

Si suponemos que los proveedores de servicios siguiesen pagando una cuota de acceso, o conectándose a los ISPs en algún IXP cercano mediante acuerdos bilaterales, todo el coste recaería en los usuarios finales por lo que sería previsible un aumento de precios. Si esto sucediese, con bastante probabilidad se frenaría la difusión de la banda ancha por simple ley de demanda. Esto a su vez podría acabar repercutiendo en la pérdida de valor de los servicios

ofertados en Internet debido al decremento de su público, con lo que se frenaría la innovación e inversión en Internet en varios niveles.

Siguiendo con este supuesto, se podría fijar el precio en función de las leyes de mercado, pagando por servicios usados. En algunos países, y sobre todo en el ámbito móvil, ya se han desarrollado planes de servicio específicos según el uso de Internet, lo cual tendería a ajustarse a este principio. El problema de este formato de tarificación, sobre todo en el escenario fijo, sería que pasar de un modelo de tarifa plana a un modelo de pago por uso sería complejo, debido sobre todo a la presión de los usuarios y a la competencia existente (en el mercado europeo). En este sentido, y pese a las citadas dificultades, el formato de tarifa plana impone cada vez más limitaciones y parece tender a la desaparición en beneficio de la diferenciación de precios.

Por otra parte, otra opción que podría darse sería la de responsabilizar a los proveedores de servicios, contenidos y aplicaciones por el tráfico que éstos generan, formato que se relaciona con lo expuesto en el apartado 4.2 del capítulo II acerca del mercado bilateral. De este modo los operadores podrían reinvertir en las redes de tal modo que se balancease el pago por acceso a ambos lados de Internet. Entre otras complejidades, este modelo implicaría un estudio a fondo de cómo se debería tarificar a los proveedores de forma justa, proporcional y competitiva. Una crítica a este modelo se basa en que esta situación podría darse el caso de pérdida de contenidos no rentables en Internet, con lo que podrían desaparecer muchas iniciativas sin ánimo de lucro de gran valor para la sociedad.

En cualquiera de los casos, al aplicar alguno de estos modelos se respetarían los principios de Neutralidad de Red que promueven el pluralismo de Internet, y se trataría a todo usuario y proveedor del mismo modo, sin discernir más que en lo económico entre quien consume contenido y quien lo crea y mantiene. El cambio a nivel técnico con el modelo actual sería mínimo, por lo que no implicaría un coste adicional a la estructura de red.

1.2 Modelo de tráfico gestionado

El segundo escenario que se puede dar a nivel tecnológico, es el de implantar un sistema de gestión de tráfico que permitiese optimizar los recursos disponibles. Esta solución es la que la industria está desarrollando y es la que ha sido expuesta a lo largo del apartado 4 capítulo IV de este documento. El enfoque que tiene es claro, diferenciar el tráfico según sean sus propiedades y requisitos.

La estructura de referencia en este ámbito, el modelo PCC de la 3GPP, está diseñado claramente para obtener un control de tarifación y consumo muy detallado, lo cual abre muchas posibilidades a los ISPs a la hora de ofrecer las tarifas que consideren apropiadas. La cantidad de opciones que se pueden plantear es muy amplia ya que la tecnología de gestión existente permite unos niveles de diferenciación y priorización tan detallados como se quiera, con lo que las variantes en el sentido económico son difícilmente predecibles.

La aplicación de este modelo puede frenar la inversión de los operadores en ampliar la capacidad de sus redes, ya que se centra en la inversión de los ISPs en gestionar eficientemente y de forma rentable la capacidad disponible. Este factor debe ser equilibrado ya que por muy buena que sea la gestión del tráfico, si se desborda la capacidad de transmisión, la situación se volvería insostenible.

Se van a suponer algunas de las posibles salidas, a nivel económico, que se derivarían de la aplicación de este sistema. Es evidente que la aplicación de estos modelos requiere una inversión por parte de los operadores de red e ISPs, debido a que es en la capa más baja del modelo de Internet donde la congestión representa un problema mayor. La interconexión a niveles altos, por el momento, no representa un punto conflictivo, aunque en un futuro podría llegar a serlo, debido al cambio del modelo de Internet expuesto en el apartado 1.1.2 del capítulo II.

El caso es que esta inversión debe ser recuperada, y aquí es donde aparecen las diferentes hipótesis sobre cuál sería el impacto en términos de tarificación. En resumidas cuentas, las opciones son las mismas que las que se han planteado en el escenario 'best effort', es decir, la subida de precios a alguno o ambos de los lados del mercado de Internet, pero ahora con unos niveles de flexibilidad y oferta de servicios más amplia.

Dada la implementación de redes capaces de diferenciar entre diferentes niveles de QoS, lo más probable es que la tarificación fuera en base a estos niveles de calidad. Una buena aproximación sería la de ofrecer un servicio 'best effort' básico sobre el que se trabajaría por defecto. A partir de aquí, se podrían ofrecer ciertas garantías de QoS para los servicios que el suscriptor seleccionase. Este modelo sería similar al que se ofrece a día de hoy por los operadores con servicios verticales como VoIP o TVIP, pero con la diferencia de que en este caso se plantea también para los servicios OTT. Esta propuesta representa una solución que respetaría las preferencias de los usuarios, y que podría resolver el problema del retorno de la inversión. La aplicación de este modelo pasaría por una supervisión de las técnicas empleadas, ya que la posibilidad de dar diferentes tratos a diferentes servicios podría dar lugar a técnicas poco éticas o discriminatorias.

En la misma línea, se podrían dar otras soluciones no tan flexibles y abiertas, basadas en el mismo principio. Una de ellas podría ser la de ofrecer planes de servicio esta vez limitando el acceso a los servicios no contratados. Así, podrían darse diferentes servicios a diferentes precios. Por ejemplo, navegación web, navegación web + VoIP, navegación web + VoIP + streaming, etc. Esta propuesta sería más agresiva de cara a los usuarios, ya que a diferencia de la anterior, en este caso se cierran servicios según las tarifas, mientras que en anterior no se prohibiría el acceso a ningún servicio.

Asimismo, estas dos formas de gestión podrían combinarse además con posibles acuerdos comerciales entre proveedores de servicio e ISPs. Es decir, podría ofrecerse un cierto nivel de QoS si la búsqueda realizada se hace con Google en vez de con Bing[21], o si la llamada sobre VoIP es sobre Skype en vez de con Viber[22], por poner dos ejemplos conocidos. El desarrollo de

[21] http://www.bing.com/. Motor de búsqueda de Microsoft.
[22] http://www.viber.com/. Aplicación de VoIP para móviles.

un formato como este sería previsiblemente nocivo para la innovación en Internet, ya que la entrada de nuevos servicios sería más dificultosa de la que se da en la actualidad.

Como escenario poco probable a largo plazo se situaría el caso en que se aplicase gestión de tráfico sin que esto cambiase el modo de tarificar a los consumidores. Resultaría poco probable porque aunque la gestión de tráfico puede resolver los problemas de congestión en momentos puntuales no sería más que un parche al problema existente. Además, el enfoque que tienen las arquitecturas capaces de proporcionar inteligencia a la red, está claramente marcado por dar flexibilidad de tarificación.

En conjunto, el hecho de diferenciar servicios tendría unas implicaciones beneficiosas en el sentido de que se haría un uso justo por parte de los usuarios, ya que cada cual pagaría por lo que consumiese o por la calidad que obtuviese, y los usuarios más pesados no perjudicarían al resto. Por el contrario, tal y como ya se ha resaltado, según qué formulas pueden perjudicar a la innovación y restar valor a Internet, o a ciertos servicios que se desarrollan sobre éste.

A parte de las complejidades económicas en que derivaría este modelo a nivel de tarificación, a nivel técnico implicaría una fuerte inversión con el empleo de DPI/DFI como algo casi ineludible y cooperación entre entidades y organizaciones. La provisión de QoS extremo a extremo es un importante desafío en la interconexión de redes, y aunque se están desarrollando arquitecturas para este fin, todavía no existe una solución homogénea.

1.3 Ventajas e inconvenientes

Para intentar sintetizar lo expuesto en este apartado y para dar una visión de que implicaciones tiene la gestión de tráfico mediante el conjunto de técnicas de inspección profunda de paquetes, se listan algunas de las ventajas e inconvenientes.

Ventajas:

- Uso más eficiente de la red que en el caso ‘best effort’.
- Mejoras en las condiciones de los accesos, el mayor punto de congestión.
- Mejoras en el rendimiento promedio de los usuarios de Internet a costa de limitar los recursos para los consumidores pesados.
- Oferta de servicios a medida, incluyendo ciertas garantías de QoS, a un precio ajustado al nivel de servicio requerido.
- Mejoras en la seguridad de la red.

Inconvenientes:

- Limitación en el acceso a ciertos servicios o contenidos de Internet, por lo que se podría producir un freno a la innovación.
- Mal uso de la censura de protocolos o aplicaciones, pudiendo afectar a la libertad de los usuarios para acceder a cualquier servicio o aplicación.
- Riesgo de violación de la privacidad, debido a las capacidades técnicas que ofrece la tecnología DPI/DFI.
- Freno a la inversión para el aumento de capacidad de Internet.
- Aparición de modelos tarifarios complejos.

2 Conclusiones

Neutralidad de Red

El fenómeno social que ha supuesto la popularización de Internet y su crecimiento carente de planificación han llevado a la situación en la que nos encontramos en la actualidad, en la que existe un pulso entre los intereses privados de los que lo gestionan con los intereses de los proveedores de servicios, contenidos y aplicaciones. Esta problemática contempla otras vertientes además de la estudiada en este Proyecto, como la de acuerdos de interconexión y contribuciones económicas de los agentes de Internet, terminales que limitan el uso del acceso a Internet u otras más éticas como las que responden a derechos sociales como la libertad de expresión.

- **La Neutralidad de Red representa un pulso entre intereses de operadores e ISPs frente proveedores de servicios, contenidos y aplicaciones.**
- **La Neutralidad de Red contempla diferentes aspectos dentro de la misma problemática.**

La acción reguladora y política, aunque sigue este tema con atención y en general se posiciona cerca de los principios de la Neutralidad de Red, no ha tomado grandes determinaciones, excepción hecha del caso de Chile, Holanda y tras mucha polémica y algunos años de lucha parece ser que los EEUU. La aplicación de técnicas de gestión de tráfico mediante DPI/DFI dependerá en gran medida de las determinaciones por parte de los Estados o ANRs. Se ha visto en el capítulo II que existen diferentes aproximaciones, algunas de ellas que apuestan por una regulación estricta (caso de Chile u Holanda), pero otras que dan pie a su aplicación (Reino Unido o Canadá).

- **La acción reguladora sigue con atención el desarrollo, generalmente en una posición cercana a la Neutralidad de Red.**
- **Por sus posibilidades y ventajas, la aplicación de la gestión de tráfico mediante DPI/DFI previsiblemente será desplegada, a menos que lo prohíba una regulación muy estricta de Neutralidad de Red.**

El problema básico de dónde surge todo este debate es un problema de beneficios y/o retorno de la inversión en el conjunto de Internet, más concretamente en su infraestructura y en la gestión de congestión. Cuando ésta se da se puede optar por llevar a cabo gestión del tráfico para solventar el problema y ofrecer una buena QoE al usuario final, o bien se puede tratar todo el tráfico por igual, con lo que desde el punto de vista técnico se perjudica a la mayoría sin beneficiar a nadie. Es una evidencia que no todo el tráfico es igual ni requiere de las

mismas prestaciones, por lo que un Internet que siga el modelo 'best effort', desde el punto de vista técnico, carece de sentido a día de hoy. El hecho de diferenciar el tráfico según la QoS requerida se perfila como una solución lógica y eficiente, y puede contribuir a una mejora de la QoE.

Dando éste principio por bueno, el problema que se plantea es el de abordar este modelo en el ámbito económico. El empleo de la gestión de tráfico llevando a cabo nuevos esquemas tarifarios implica varios puntos de laborioso planteamiento. Por ejemplo la aparición de tarificación por uso, por niveles de QoS, o por acceso a ciertos servicios, además de otros posibles modelos que puedan surgir. También se debe abordar el tema de la oferta de servicios dedicados, punto sobre el que ARCEP determina que no deben ser comercializados bajo la denominación de acceso a Internet.

- **El problema fundamental se centra en una cuestión de inversión y retorno de ésta para ofrecer una buena QoE y solventar problemas de congestión.**
- **La gestión de tráfico responde a principios de eficiencia técnica, por lo que en este sentido, el modelo 'best effort' carece de justificación con la coyuntura existente.**
- **La aplicación de nuevos modelos tarifarios para el tráfico gestionado representa una tarea de laboriosa.**

Analizado a grandes rasgos, el modelo de Internet representa un nuevo paradigma en lo económico y en lo social debido a varios motivos de difícil análisis. Entre éstos se encuentra su dinamismo y el de todo lo que esto conlleva, y el hecho de que hasta la fecha ha representado una plataforma de lanzamiento para la innovación. Otro motivo fundamental es que Internet se ha posicionado como algo más que un mero servicio de telecomunicaciones, gracias a la capacidad de ofrecer libremente acceso a información y comunicación de forma global.

No obstante, si se analizase únicamente el aspecto económico este punto sería bien simple, el ancho de banda, a falta de mayor inversión en capacidad, se puede ver como un bien escaso, y como tal su precio se debe ajustar al mercado (en un entorno competitivo). Además, la teoría económica afirma que cuanto más diversificados están los precios más cerca del óptimo económico se encuentra un producto. Es de notar que ninguna de estas afirmaciones no acaban de encajar con el modelo actual de Internet. El precio no se acaba de ajustar a lo que la teoría económica propone en consonancia con el mercado bilateral, y los precios hasta la fecha, no se encuentran diversificados, sino que operan bajo un formato de tarifa plana.

- **Con la diversificación de tarifas, desde el punto de vista económico, se puede conseguir una mayor eficiencia, salvo en lo que a innovación se refiere.**

- **El modelo tarifario de Internet no es necesariamente el mejor adaptado a las indicaciones de la teoría económica, debido a sus orígenes, su aportación a la sociedad y su naturaleza abierta.**

Si se acaba siguiendo la tendencia del mercado, el hecho de ofrecer tarifas diferenciadas puede repercutir en que la entrada de servicios novedosos se vea afectada. Un buen modo de ejemplificar este hecho lo encontramos en servicios como YouTube o Google, que comenzaron a funcionar con una conexión estándar a Internet. Imponer este tipo de tarifas hace que la accesibilidad a servicios de este tipo se vea limitada, y con ello sus probabilidades de éxito. Además, este modelo suele estar mal visto por los consumidores. Un motivo básico, y de mucho peso, reside en que durante varios años se haya ofrecido como un 'buffet libre' donde pagando una tarifa plana mensual un usuario puede hacer un uso ilimitado de éste, facilitando del mismo modo su capacidad de experimentar y contribuir a la publicación de contenidos de forma simple y asequible.

- **La tendencia del mercado es la de diversificar tarifas de acceso, lo cual podría dar lugar a un freno a la innovación.**

Gestión de tráfico mediante DPI/DFI

Las tarifas diferenciadas tienden a basarse en ofrecer acceso a ciertos servicios según las garantías de QoS entregadas, para lo cual se ha visto en el capítulo IV que existen mecanismos cada vez más sofisticados y completos. Pese a que su implantación y desarrollo no es todavía estable, los esfuerzos en éste campo hacen pensar que su futura aplicación es más que probable. En concreto, se han revisado algunas técnicas de gestión de tráfico y se han analizado las nuevas tendencias en las arquitecturas para las redes de comunicación, que tienen una visión de control exhaustiva sobre los datos de suscriptor y políticas de uso, además de complementarse con información de la red y de las aplicaciones.

Para su usabilidad completa requieren conocer de forma detallada el tipo de tráfico que está fluyendo por la red, y aquí es donde entra en juego la tecnología DPI/DFI. En principio, si se hiciese un uso acorde a los 'well-known port', no habría necesidad de incluir esta tecnología de análisis profundo, pero la realidad es tal que para poder aplicar un servicio de QoS diferenciadas según la aplicación se hace necesaria su implementación.

- **La tecnología existente en materia de provisión de QoS permite diversificar planes tarifarios en función del tráfico o servicio cursado de modo exhaustivo.**

- **La tecnología DPI/DFI es necesaria para que las arquitecturas NGN puedan clasificar el tráfico según sus requerimientos de QoS debido a que muchas aplicaciones no hacen un uso en acorde a los 'well-known port'.**

Para la detección y clasificación de tráfico existen dos técnicas avanzadas de análisis. La primera es DPI, que ha sido causante de cierta polémica. Esto se debe básicamente a que DPI tiene la capacidad de analizar e incluso de comprender el contenido de una comunicación que no esté cifrada, por lo que en ciertas condiciones su uso puede atentar contra la privacidad de los usuarios. No obstante, se podría considerar que los paquetes que no van cifrados no responden a las necesidades que la criptografía ofrece. El empleo de Internet como medio de comunicación lo sitúa en el punto de mira de posibles ataques o espionaje para la obtención de información, con lo que cualquier dato importante debe, y en efecto, suele ser tratado de forma segura. Visto desde esta perspectiva, el hecho de que un paquete pueda ser analizado mediante DPI implica que es porque su emisor no ha querido evitarlo, ya que si así fuera existen mecanismos que posibilitan establecer una comunicación de forma privada.

- **DPI es una técnica de inspección avanzada que puede analizar el contenido de un paquete no cifrado, por lo que ha sido criticado por su potencial violación de privacidad.**

En cualquier caso, el empleo de DPI para la gestión de tráfico tiene como fin identificar el protocolo del nivel 7 ya que es éste el que contiene la información sobre el tipo de tráfico que se está analizando. Si el fin de cifrar una comunicación es su fin legítimo, entendiendo como tal el de otorgar privacidad, con el empleo de DPI se debería poder detectar el protocolo (ver apartados 5.1 y 5.2 del capítulo V).

En este sentido, se debe resaltar que el empleo de DPI en la gestión de tráfico no tiene intención, o al menos la necesidad, de comprender el contenido de una comunicación, sino que solo el tipo de tráfico o protocolo. Los fabricantes y operadores afirman que DPI se centra no en leer o entender el contenido de las comunicaciones, sino en la búsqueda de ciertos marcadores o patrones para una clasificación según el protocolo o aplicación que genera los paquetes. El ejercicio realizado en el apartado 5.2 del capítulo V pretende corroborar en cierta medida este hecho.

- **DPI en su aplicación para la gestión de tráfico no tiene necesidad de comprender el contenido de una comunicación, tan solo la detección del protocolo de nivel 7.**

Si bien DPI se puede considerar una herramienta agresiva en contra de los derechos de usuario y su privacidad, hay que considerar también que el tráfico que suele perseguir no respeta algunas reglas establecidas en Internet (en referencia a los 'well-known ports'). Se suele vincular DPI a la detección de tráfico para su posterior bloqueo o limitación, pero se debe considerar también su capacidad de posibilitar un trato especial para aquellos servicios que así lo requieran, en línea con las especificaciones de la arquitectura PCC de la 3GPP (ver sección 4.1.2 del capítulo IV). También son destacables otras de las aplicaciones a las que se destina esta tecnología, como por ejemplo posibles mejoras de seguridad. Dicho todo esto, se quiere resaltar la idea de que DPI tan sólo es una herramienta y debe ser tratada como tal. No es ético etiquetar DPI como bueno o malo, sino que lo que hay que catalogar como tal es el uso que se le dé.

- **DPI no debe ser visto tan solo como una herramienta agresiva en contra de los usuarios, ya que puede aportar mejoras en varios aspectos.**
- **DPI debe ser valorado como una herramienta sin más, las aplicaciones posteriores son varias y dependerá de éstas que su uso sea beneficioso o no.**

Cuando el contenido de un paquete se encuentra ofuscado o cifrado de modo que no se puede comprender la información referente al nivel 7 del modelo OSI, el empleo de DPI queda completamente anulado. Esto ha derivado en otro tipo de análisis de tráfico llamado DFI, basado en el estudio del comportamiento a nivel de flujo de paquetes. Precisamente por esto, DFI no supone un problema en el aspecto de la privacidad. DFI no atenta contra la privacidad de los usuarios, ya que no analiza el contenido de ningún paquete. Esta característica, junto con la capacidad de detectar protocolos ofuscados, posiciona a esta tecnología como la que realmente adquirirá un peso importante para la detección y clasificación de paquetes.

- **DFI tiene la capacidad de detectar y clasificar tráfico incluso cuando éste ha sido cifrado y no es posible su análisis mediante DPI.**
- **Debido a su modo de llevar a cabo el análisis, DFI no acarrea polémica en cuanto a cuestiones de privacidad.**
- **El hecho de que cada vez más tráfico sea cifrado, hace pensar que DFI es la tecnología de análisis que más se empleará.**

Lo que resulta muy importante en cualquiera de los casos son la transparencia y el estímulo de la competencia. La primera porque el hecho de saber cómo están siendo tratados los datos supone un elemento fundamental, aunque no suficiente, para que exista un buen transcurso de esta situación. Sean cuales sean las medidas que se acaben adoptando, el derecho a conocer por parte de los usuarios que medidas adoptan los ISPs con sus datos es algo fundamental para poder valorar y escoger a su ISP con un fundamento sobre las diferencias existentes entre las ofertas disponibles. En este ámbito se intuye un gran desafío, como se puede deducir de los pasos ya dados en Chile, que ha trabajado este aspecto de modo exhaustivo.

La competencia resulta importante porque si a raíz de esta transparencia no existe la posibilidad de cambiar de proveedor, la transparencia deja de cobrar algo de fuerza. Esto representa un serio problema en el modelo de los EEUU, pero no tanto en el mercado europeo donde se trabaja para conseguir una competencia efectiva.

- **La aplicación de gestión de tráfico mediante DPI/DFI debe ir acompañada de transparencia a los usuarios y de estímulo de la competencia por parte de los Estados o ANRs.**
- **Las medidas de transparencia suponen un gran desafío de implantación, como se intuye en los pasos ya dados por Chile.**
- **La competencia representa un problema notable en el mercado de los EEUU, en Europa este hecho no es tan preocupante ya que se ha logrado un mayor nivel de competencia.**

Los méritos para llevar a cabo DPI/DFI residen básicamente en el nivel hardware, que debe afrontar el desafío de tratar y procesar grandes cantidad des de datos a tiempo real. Esto no implica que a nivel software sea una tarea sencilla, pero el uso de 'Regular Expressions' no es nuevo y por ello se trata de una cuestión de escalabilidad. En el campo DFI la dificultad radica en la capacidad de actualización que deben ofrecer los proveedores de soluciones, ya que como se ha visto, DFI se basa en la búsqueda de parámetros deterministas de los protocolos que pueden variar según diferentes versiones o configuraciones.

La tecnología existente a día de hoy es capaz de cumplir con los requisitos que exigen el análisis DPI/DFI y la gestión de tráfico sin que apenas sea perceptible su impacto. Se ha visto en el apartado 4.1 del capítulo V que existen componentes hardware específicamente diseñados para este fin y que la ingeniería en este campo está en un constante proceso de innovación para dar cabida a las crecientes necesidades.

- **La tecnología DPI/DFI, está lo suficientemente madura para ser aplicada.**

- **El mayor desafío para que el impacto de emplear DPI/DFI sea el menor posible radica en el diseño hardware, aunque también en la necesidad de actualización a nivel software (sobre todo en el análisis DFI).**

La previsión de un notable aumento del campo DPI/DFI ha llevado a la aparición de numerosas empresas que ofrecen soluciones de este tipo para ISPs, pero también para cualquier otro tipo de organizaciones. Tal y como hemos visto en el apartado 3.2 del capítulo V, la previsión de un aumento de este sector es fuerte y esto hace aumentar el número de ofertantes. Pero no solo aparecen nuevas propuestas y elementos para la gestión de tráfico, también los fabricantes clásicos de telecomunicaciones participan en el desarrollo de elementos que sean capaces de gestionar el tráfico a niveles sofisticados, bien a través de equipos dedicados o bien integrándolos en equipos tradicionales de telecomunicaciones.

- **La tendencia de la industria y el mercado hacia un modelo gestión de tráfico mediante DPI/DFI queda plasmada en las previsiones de aumento del sector, y en la inclusión de estas técnicas por parte de proveedores de equipos de telecomunicaciones tradicionales.**

3 Recomendaciones

La gestión de tráfico mediante DPI/DFI implica una serie de medidas a tomar en relación a varios aspectos, muchos de ellos relacionados con la Neutralidad de Red. Una vez se han analizado las bases técnicas y con ello las posibilidades que éstas pueden ofrecer, se quiere en este subcapítulo hacer una propuesta sobre lo que, bajo juicio del autor, debería ser un buen modelo futuro de Internet.

1. **Se debe garantizar que Internet siga manteniendo su carácter abierto para que sirva como plataforma a la innovación, por lo que en ningún caso se debe llegar a dar un bloqueo sobre ningún tipo de servicio, contenido o aplicación sobre éste, ni otras prácticas con efectos similares.**

2. **Esto no debe suponer que los diferentes agentes del mercado no tengan libertad para experimentar con los modelos tarifarios que se ajusten a sus necesidades, dentro de un entorno competitivo que maximice el bienestar común.**

3. **Se debe incentivar a la inversión en capacidad de red en la medida en que la demanda lo exija, lo cual está relacionado con el punto anterior.**

4. **El nivel de regulación se tiene que determinar según el escenario existente. Las ANR deben trabajar para otorgar niveles de transparencia y competencia altos, ya que a mayor nivel de éstos, menor nivel de intervención será necesario en lo que a Neutralidad de Red se refiere.**

5. **El uso de técnicas de gestión de tráfico para la diferenciación de servicios según sus requerimientos no debe ser prohibido ya que puede aumentar la eficiencia en Internet. No obstante, se deberían tener en consideración para su aplicación aspectos que lo justifiquen, por lo que debería ser:**

    i. **Particularizado al tipo de red, tecnología o tráfico.**
    ii. **Proporcional con el conjunto del tráfico**
    iii. **Eficiente en términos de QoE para el conjunto de los usuarios.**

Así, en base a estos principios, un modelo que podría cumplir con estos principios y podría representar una solución al debate de Neutralidad de Red se basaría en una evolución hacia un Internet con niveles de QoS desde un modelo base 'best effort', que respetaría de acuerdo varios de los principios más relevantes de la Neutralidad de Red y permitiría no obstante la aplicación de nuevos modelos a operadores e ISPs.

En este modelo hipotético, debería existir un formato base 'best effort' de acceso a Internet, similar al que se oferta a día de hoy. Partiendo de esta base, así no se limitaría el acceso a ningún contenido, servicio o aplicación. A partir de este servicio base, el usuario podría

contratar diferentes niveles de QoS para atender a los diferentes tipos de servicios según sus requisitos de QoS. Es decir, el usuario que quisiera garantías de calidad, debería pagar por ellas.

Sobre esta base se podrían articular varias opciones más, pero siempre partiendo de un modelo básico 'best effort' para todos los usuarios. En momentos de poca demanda, todos los usuarios percibirían una QoE similar, siendo en momentos de congestión cuando los abonados a planes de QoS se beneficiarían de este servicio.

Este modelo, aunque con toda probabilidad sería criticado por el hecho de reservar un ancho de banda y discriminar contenidos sobre Internet, se adaptaría a las necesidades de cada usuario y sería por tanto más eficiente en términos económicos. Por otro lado, el hecho de basarse en un modelo base 'best effort' solucionaría el problema del bloqueo, que es uno de los puntos más nocivos en el trato de contenidos de servicios, aplicaciones o contenidos sobre Internet.

Como desafío más notable para esta posible vía se debería tener un control el trato que diesen los ISPs al contrato base 'best effort', pudiéndole asignar unos niveles de QoS por debajo de sus posibilidades para incentivar así la contratación de servicios superiores. Para subsanar este factor, se podrían fijar unos requisitos mínimos de QoS para éste, aspecto ya previsto en la normativa Europea.

Anexo A – Contexto regulatorio internacional

1 Unión Europea

La regulación europea de las telecomunicaciones se inicia en el año 1987 con el Libro Verde de la Convergencia. El 1 de enero de 1998 finalizó la liberalización total de todas las redes y servicios de telecomunicaciones en prácticamente todos los Estados miembros de la Unión Europea. El propósito general fue el de estimular la competencia en el mercado para empujar el avance en el sector de las TIC. Desde ese momento la Comisión Europea fue la encargada de marcar las pautas a seguir por los países miembros en materia de comunicaciones electrónicas.

1.1 Marco Legislativo

En 7 de marzo de 2002 se aprobaron un conjunto de disposiciones legislativas destinadas a regular el sector de las comunicaciones electrónicas y a modificar a la normativa existente en el sector de las telecomunicaciones. Sin pretensión de entrar en grandes detalles, a continuación se listan las diferentes Directivas que forman el marco regulatorio:

- 2002/21/CE (Directiva marco): Directiva relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.
- 2002/20/CE (Directiva autorización): Directiva relativa a la autorización de redes y servicios de comunicaciones electrónicas.
- 2002/19/CE (Directiva acceso): Directiva relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión.
- 2002/22/CE (Directiva servicio universal): Directiva relativa al servicio universal.
- 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas): Directiva relativa al tratamiento de los datos personales.

Se establecieron así las bases para una reglamentación armonizada, para una mayor competencia libre de influencias externas, y en general para una mejora en el acceso y servicio de contenidos de cara al usuario.

Años más tarde, en noviembre de 2009, tras varios meses de debate legislativo desde las propuestas iniciales de la Comisión Europea, se aprobaron reformas respecto al marco comunitario con objeto de ampliar los derechos de los consumidores y de actualizar la regulación de las telecomunicaciones a la realidad del mercado. La fecha límite para la aplicación por parte de los estados miembro se marcó a 25 de mayo de 2011. En concreto, respecto al tema que nos ocupa, se establecen las Directivas:

- 2009/140/CE (Directiva mejor regulación), por la que se modifican las citadas anteriormente: 2002/21/CE, 2002/19/CE, 2002/20/CE.

- 2009/136/CE (Directiva derechos de los ciudadanos), por la que se modifican las citadas anteriormente: 2002/22/CE, 2002/58/CE.

Los puntos relevantes de las citadas Directivas en cuanto a Neutralidad de Red se basan sobre todo en la transparencia y en la posibilidad de establecer obligaciones por parte de las ANR en relación a la calidad mínima del servicio. En este aspecto, se pueden extraer tres ejes principales de acción.

- Objetivos generales y principios reguladores que han de regir la actividad de las ANR: Las ANR fomentarán los intereses de los ciudadanos de la Unión Europea promoviendo la capacidad de los usuarios finales para acceder y distribuir la información o utilizar las aplicaciones y los servicios de su elección. Se extiende la potestad de las ANR a la resolución de conflictos no sólo entre operadores, sino también entre operadores y otros agentes. Ello podría respaldar la intervención en los eventuales conflictos por cuestiones de priorización y gestión de tráficos que pudieran darse entre los operadores que ofrecen acceso a Internet y los agentes que ofrecen servicios y aplicaciones en Internet.

- Requisitos de transparencia relacionados con la Neutralidad de Red: En materia de transparencia e información, el contenido mínimo de los contratos habrán de incluir expresamente los siguientes datos: información sobre los límites al acceso o utilización de servicios y aplicaciones, niveles mínimos de QoS, medidas para la gestión del tráfico y restricciones relativas a terminales. Además, las ANR tendrán la competencia de obligar a los operadores e ISPs a: informar a los abonados sobre las limitaciones al acceso o utilización de servicios y aplicaciones y de proporcionar información sobre procedimientos de gestión de tráfico. La regulación de las mencionadas obligaciones de información y transparencia dan a entender que, en principio, no queda prohibido que los operadores establezcan condiciones que limiten el acceso o la utilización de servicios y aplicaciones.

- Competencias de las ANR en materia de calidad: Las ANR tendrán potestad para establecer requisitos mínimos de QoS a las empresas proveedoras de redes públicas de comunicaciones, si bien, informando debidamente a la Comisión y al BEREC y procurando que no afecte de forma negativa, aplicando requisitos coherentes. Esta previsión es la que más controversia y discusiones suscitó durante la tramitación legislativa del nuevo marco.

Cabe remarcar que el texto citado no proclama expresamente el principio de Neutralidad de Red como tal, ni exige un reconocimiento incondicional de la ésta. Se denota una cierta preocupación en relación con los efectos sobre la competencia de la transmisión de contenidos y, en ese sentido, se añade expresamente en lo relativo a los objetivos y principios de la regulación, que el fomento de la competencia incluya este aspecto.

Asimismo se estableció la instauración de un Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (BEREC) con la finalidad de reforzar la cooperación entre las Autoridades Reguladoras Nacionales (ANR) y mejorar su colaboración con el resto de instituciones europeas.

1.2 Declaración de la Comisión Europea sobre la Neutralidad de Red

Apenas un mes después de la aprobación de las dos nuevas directivas, la Comisión emitió un comunicado a fecha en diciembre de 2009 en el otorga gran importancia al mantenimiento del carácter abierto y neutral de Internet. La transparencia y la acción de las ANR se muestran como bases para fomentar estos principios. Se hace hincapié en la necesidad de tener un seguimiento al respecto, que se llevará a cabo por las ANR (138).

1.3 Consulta pública

Entre junio y septiembre de 2010 la Comisión realizó una consulta pública en la que participaron operadores, proveedores de contenidos, Estados miembro, consumidores y organizaciones de sociedad civil además de personas individuales, sobre el debate de la Neutralidad de Red. Se recibieron 318 respuestas (139).

La consulta se llevó a cabo para sentar las bases empíricas sobre la situación en la Neutralidad de Red en Europa y se estructura en torno a cinco bloques que pretenden tratar todos los aspectos de interés. A continuación se sintetizan las diferentes opiniones y datos proporcionados por los encuestados, manteniendo la estructura original.

Carácter abierto de Internet

1. Problemas con el carácter abierto de Internet y la Neutralidad de Red en la UE: Según ISPs, operadores de red y fabricantes de equipos e infraestructuras parece no haber ningún conflicto de grandes magnitudes en la actualidad. Se defiende que la gestión de tráfico existe con la finalidad de dar un servicio más eficiente y no perjudica negativamente al consumidor, además de reducir costes. Mantienen que no existe ningún tipo de discriminación. No obstante, según el BEREC se afirma que sí que ha habido casos de discriminación, si bien, aislados y no generalizados, relacionados básicamente con VoIP y P2P en operadores móviles, y que en la mayoría de casos se han solucionado voluntariamente.

2. Futuros problemas: Muchas respuestas coinciden en que será necesaria la intervención de las ANR en los nuevos modelos de negocio que pueden presentar problemas, como por ejemplo la IPTV. Algunos proveedores de contenidos opinan que los operadores podrían dar más prioridad a un tipo de tráfico en detrimento de otros

servicios. También afirman que aunque Internet se ha mantenido abierto hasta ahora, esto no tiene porqué suceder en el futuro, y que las nuevas estructuras de mercado puedan dañar la apertura de Internet y reducir los incentivos para invertir en contenidos. Por su parte los operadores de red opinan que estas preocupaciones no son justificadas y que un proceso competitivo y transparente que de opciones al consumidor no acarreará mayores problemas. En cuanto a la evolución futura, el BEREC prevé posibles problemas en tres áreas: discriminación que puedan llevar a efectos contrarios a la competencia; consecuencias potenciales posibles para la economía de Internet que afecten a la innovación y la libertad de expresión; y daños a los consumidores debido a la falta de transparencia

3. Capacidad de tratar con los problemas identificados: En general, todos los implicados consideran que el Marco de la UE es suficiente para tratar los posibles conflictos y que no será necesaria regulación adicional.

Gestión de tráfico

4. Necesidad de la gestión de tráfico como medida para hacer Internet eficiente: Existe un gran consenso respecto a este tema en cuanto a que las medidas de gestión de tráfico son legítimas para tratar congestión y por temas de seguridad, y que no son contrarias al concepto de Neutralidad de Red siempre que no se use de forma abusiva a favor o en contra de ciertos servicios, en especial cuando se tratan de servicios de la misma índole. No obstante, algunos participantes exigen salvaguardar la privacidad en cuanto a la gestión de tráfico aplicada mediante técnicas tales como DPI, que puede constituir una violación de derechos.

5. Suficiencia de la transparencia para garantizar la Neutralidad de Red: En términos generales todos los participantes coinciden en asegurar que a los clientes estén correctamente informados, aunque un amplio rango de encuestados consideran que esto no es suficiente.

6. Trato equivalente de gestión de tráfico en red fija y móvil: Los participantes consideran que se deben aplicar las mismas políticas y que el Marco debe quedar fuera de consideraciones tecnológicas. No obstante, algunas opiniones defienden que se deben considerar algunas distinciones debido a las diferencias inherentes entre estos tipos de red.

7. Otros modos de priorización: En cuanto a este aspecto se citan las CDN, que ayudan a los proveedores de contenido a ofrecer un acceso a mayor velocidad y calidad de servicio a sus consumidores. A nivel técnico, las CDN pueden ayudar a aliviar la carga de tráfico en la red y según BEREC no implican en sí mismas una violación de la Neutralidad de Red.

8. QoS en servicios dedicados e Internet: Operadores e ISPs argumentan que se les debería permitir determinar libremente sus modelos de negocio. Esto crea división entre los Estados miembro. Por otra parte, proveedores de contenidos declaran que no está clara la distinción entre servicios dedicados y los 'best effort', y consideran que se deben ofrecer ambos en las mismas condiciones y sin discriminación.

9. Necesidad de medidas regulatorias adicionales en servicios dedicados: En general se considera que no es necesario actualmente. Sin embargo, algunos piden a la Comisión que incluya una definición de servicios dedicados, mientras que otros apuestan por un liderazgo de la industria como medio para asegurar equidad y no discriminación.

Estructura del mercado

10. Modelo de acuerdos comerciales: Hay un acuerdo general en que los modelos actuales basados en peering y pago de tránsito han funcionado hasta ahora. En cambio, hay división de opiniones en las previsiones. Algunos citan ineficiencias debidas al mercado bilateral y apuestan por un nuevo modelo. Por el contrario, los proveedores de contenidos temen que un cambio en la estructura del mercado pueda perjudicarles y los operadores adquieran demasiado poder, preocupación compartida por organizaciones de consumidores.

Consumidores y QoS

11. Mínima QoS en los accesos a Internet: Muchos encuestados, entre ellos operadores y proveedores de contenidos, opinan que establecer un mínimo nivel de QoS sería contraproducente y frenaría la innovación. En su opinión un mercado competitivo con transparencia es suficiente para dar un mínimo de calidad.

12. Determinación de parámetros mínimos de QoS: Existen diversas opciones, como la propuesta por parte de la UE de la adopción de directrices sobre la base de un acceso a Internet por parte de la industria en base a un acuerdo sobre un código de conducta, y mediante disposición las normas internacionales.

13. Control sobre la QoS: De forma general se considera que es una tarea compleja dada la cantidad de parámetros que afectan a la velocidad y entrega de datos.

14. Transparencia para los consumidores: Se aportan sugerencias sobre como informar de forma clara sobre los términos y condiciones, sobre el derecho a usar cualquier aplicación legal y sobre los medios para cambiar de proveedor. Algunos defienden un modelo de dos niveles de transparencia, por el que todos los consumidores puedan conocer con información fácilmente comprensible el estado de su servicio.

Aspectos políticos, culturales y sociales

15. Libertad de expresión, pluralismo, y diversidad cultural: Algún operador que ha contestado hace referencia a que estas cuestiones están determinadas por los contenidos reales de Internet, sobre los que no tienen control.

1.4 Comunicado de la Comisión sobre la Neutralidad de Red

Comunicado publicado en abril de 2011 dónde la Comisión Europea se posiciona respecto al debate sobre la Neutralidad de Red en base a la consulta realizada a finales de 2010. Se manifiesta la intención de aguardar a la aplicación de las disposiciones de la Directiva Marco 2009 (fecha límite 25 de mayo de 2011) para ver cómo funcionan en la práctica (140).

En referencia a las problemáticas extraídas de la consulta pública de 30 de septiembre, la Comisión concluye que no existen evidencias para justificar las preocupaciones existentes respecto a bloqueo o limitación de tráfico, pero se deben tener en cuenta para un ejercicio de estudio más exhaustivo. En cuanto a la gestión de tráfico, la Comisión continuará con el seguimiento llevado a cabo por tal de que éste se gestione de forma transparente y razonable, de acuerdo con los objetivos del Marco.

Si se detectaran problemas significantes y persistentes de modo que no se asegure la calidad en los usuarios, se tomarán las medidas pertinentes, que pueden adoptar la forma de medidas de orientación o legislativas. La Comisión también solicitó al BEREC el estudio de ciertas cuestiones relacionadas con los procesos de cambio de operador, calidad de servicio, así como sobre el bloqueo y ralentización de servicios y otras prácticas equivalentes.

1.5 Recomendaciones del Parlamento Europeo

En mayo de 2011 el Parlamento Europeo se pronuncia respecto al debate que se está llevando a cabo, mediante la publicación de un dossier informativo dónde además incluye ciertas recomendaciones para los agentes implicados (141):

- No imponer ninguna obligación de Neutralidad de Red hasta que haya suficiente experiencia con las obligaciones ya impuestas a través de la modificación del marco normativo 2009, para hacer así un juicio razonado sobre su eficacia.

- Dar apoyo técnico a la investigación de políticas para mejorar la eficacia de las obligaciones respecto a los consumidores y la transparencia, y para asegurar que las obligaciones mínimas de QoS pueden ser efectivamente impuestas en caso de que llegar a ser necesario.

- Continuar con el estudio de los aspectos de la neutralidad de la red, donde las denuncias pueden tener algún fundamento, incluyendo los cargos y condiciones que

los operadores móviles puedan imponer a los proveedores de voz sobre IP (VoIP), y el deterioro de tráfico P2P.

- Juicio reservado sobre cualquier otra obligación hasta que haya una visión más clara de lo que se ve perjudicado el bienestar social y/o de consumo, hasta que las disposiciones del 2009 se apliquen plenamente.

2 EEUU

En Estados Unidos la FCC es el órgano independiente regulador de las comunicaciones y tiene a su cargo la reglamentación de las comunicaciones por radio, televisión, teléfono, satélite y cable. Pese a ello, por motivos legales no dispone de poderes suficientes para hacer cumplir sus determinaciones en relación a Internet ya que los servicios de banda ancha están catalogados (paradójicamente por decisión de la propia FCC) como servicios de información y no de comunicación (142).

Por este motivo, la FCC posee esencialmente dos opciones básicas para avanzar en la neutralidad de la red: se puede esperar a que el Congreso redactase un Proyecto de ley a favor de la Neutralidad de Red o se puede decidir la reclasificación de los servicios de banda ancha como de telecomunicaciones, en lugar de los servicios de información, para tener autoridad reguladora sobre ellos.

2.1 Internet Policy Statements

El 5 de agosto de 2005 la FCC adoptó unas medidas que sentaron las bases en su política en cuanto a la Neutralidad de Red. Estas medidas se conocen cómo 'Internet Policy Statements', y recogen cuatro derechos fundamentales que pretenden preservar y promover el carácter dinámico y abierto de Internet, así como el mercado de las telecomunicaciones; fomentar la creación, adopción y utilización de contenidos de Internet y asegurar que sus consumidores se beneficien de la innovación creada por la competencia (143).

Los cuatro principios adoptados fueron:

- Los consumidores tienen derecho a poder acceder a los contenidos legales de Internet de su elección.
- Los consumidores tienen derecho a ejecutar aplicaciones y servicios que deseen, dentro de los límites de seguridad que imponga el estado.
- Los consumidores tienen derecho a conectar los dispositivos legales que deseen, siempre que no dañen la red.
- Los consumidores tienen derecho a elegir en competencia entre proveedores de red, proveedores de aplicaciones y servicios, y proveedores de contenido.

Esta declaración de intenciones se vio desautorizada en abril de 2009 por la decisión de un tribunal del distrito de Columbia en relación al denominado caso Comcast que cuestionó la competencia de la FCC para imponer a los ISPs normas en relación a la neutralidad de la red.

Meses más tarde junio 2009, tras la elección de un nuevo presidente para la FCC (Julius Genachowski) nombrado por la administración Obama, se reaviva el debate. En octubre de ese mismo año se realiza una consulta para una propuesta de regulación que incluye obligaciones

concretas de neutralidad que se aplicarían a los prestadores de servicios de banda ancha. Además se añaden dos principios más a los cuatro anteriormente citados:

- Impedir que los proveedores de acceso a Internet discriminen por el contenido o las aplicaciones, aunque permitiéndoles que hagan una gestión razonable de la red.

- Garantizar que los proveedores de acceso a Internet sean transparentes con respecto a la manera en que gestionan las redes.

Finalmente, en 2010, la Corte de Apelaciones del Distrito de Columbia dictaminó que la FCC no tiene autoridad suficiente para obligar a los ISPs a mantener sus redes abiertas a cualquier contenido (144). Este hecho, frenó considerablemente el progreso de los principios de la Neutralidad de Red en los EEUU ya que a efectos prácticos se confirmó lo que muchos ya sabían, la FCC no disponía del refuerzo legal para hacer cumplir sus principios.

2.2 Report&Order : Preserving the Open Internet

Bajo esta situación de falta de respaldo legal para hacer cumplir sus decisiones, la FCC adoptó en diciembre de 2010 unas nuevas reglas bajo la idea de que la apertura de Internet promueve la innovación, inversión, competencia y la libertad de expresión. Estas reglas están en vigor des del 20 de noviembre de 2011, aunque la polémica acerca de su base legal sigue abierta.

En cualquier caso, estas reglas se publicaron con el objeto de promulgar y salvaguardar el carácter abierto de Internet, proteger a los consumidores y garantizar que Internet continúa creciendo en base a una inversión sólida del sector privado. Las tres reglas aprobadas se describen a continuación (145).

- **Transparencia:** Los proveedores de redes tanto fijas como móviles deben divulgar las prácticas de gestión, las características de funcionamiento y los términos y condiciones de sus servicios de acceso de banda ancha.

- **No bloqueo:** Los proveedores de red fija no pueden bloquear ningún contenido legal, ni aplicaciones o servicios que no sean nocivos. Los proveedores móviles no pueden bloquear sitios web legítimos ni aplicaciones que compitan con sus servicios de voz o video.

- **No discriminación:** Los proveedores de redes fijas no pueden discriminar de forma no razonable la transmisión de contenidos legales.

Además de las citadas reglas se desarrollan una serie de ideas, algunas de ellas dignas de mención. En primer lugar, se aprecia una diferenciación en cuanto a las redes fijas y móviles. En cuanto a fijas se establece que los servicios especializados que se ofrecen sobre el mismo acceso que Internet no deben suponer un riesgo para el carácter abierto de Internet. En cuanto a las redes móviles se decide tomar medidas precavidas debido a que es un campo que

está en proceso de crecimiento e implantación, no obstante, sí que se prohíbe el bloqueo de aplicaciones que pueden competir con sus servicios de voz o video. Es de destacar que se limita la negativa de bloqueo a sitios web, a diferencia de la red fija que niega el bloqueo a cualquier tipo de tráfico legal. Esto implica que el uso de aplicaciones independientes puede verse perjudicado en los dispositivos móviles, alegando a que la gestión de este tipo de tráfico es de mayor complejidad que el trafico web.

Aunque existe la opinión de que las reglas para mantener la Neutralidad de Red pueden perjudicar a los ISPs a la hora de ofrecer diferentes niveles de tarifas el marco no les prohíbe tarificar según consumos. Se aceptarían ciertos casos de discriminación razonable que no atente contra los principios de Neutralidad de Red, siempre que no se discrimine según usos o categorías. Ejemplo de ello sería, en casos de congestión, la provisión por parte de un ISP de un mayor ancho de banda a un usuario que ha consumido menos tráfico ante otro que ha consumido más, técnica que se cita como 'discriminación agnóstica'. En cualquier caso, respecto a la gestión de tráfico, la FCC afirma que el margen que tienen los operadores es suficientemente amplio para gestionar sus redes de forma flexible.

No se prohíben de forma expresa los acuerdos entre proveedores de contenidos e ISP, aunque se sobreentiende que un pago que atente contra las medidas expuestas podría ser investigado y sancionable.

3 Chile

En julio de 2010, el Parlamento Chileno aprobó de forma unánime la modificación de su Ley de telecomunicaciones, convirtiéndose así el primer país que ha contemplado en su legislación la Neutralidad de Red. La legislación se encuentra en activo desde julio de 2011, y esto permite que sea un referente en cuanto a aplicación de las medidas propuestas.

3.1 Proyecto de Ley

Las diferentes modificaciones en la Ley de telecomunicaciones imponen unas ciertas obligaciones a los ISPs y operadores (146):

- No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios.

- No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.

- Deberán ofrecer, a expensas de los usuarios que lo soliciten, servicios de controles parentales para contenidos que atenten contra la ley, la moral o las buenas costumbres, siempre y cuando el usuario reciba información por adelantado y de manera clara y precisa respecto del alcance de tales servicios.

- Deberán publicar en su sitio web, toda la información relativa a las características del acceso a Internet ofrecido, su velocidad, calidad del enlace, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio.

- Articulo 24 J. - Un reglamento establecerá las condiciones mínimas que deberán cumplir los prestadores de servicio de acceso a Internet en cuanto a la obligatoriedad de mantener publicada y actualizada en su sitio web información relativa al nivel del servicio contratado, que incorpore criterios de direccionamiento, velocidades de acceso disponibles, nivel de agregación o sobreventa del enlace, disponibilidad del enlace en tiempo, y tiempos de reposición de servicio, uso de herramientas de administración o gestión de tráfico, así como también aquellos elementos propios del

tipo de servicio ofrecido y que correspondan a estándares de calidad internacionales de aplicación general.

En relación a la gestión de tráfico los ISPs podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia además de procurar preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red.

Las infracciones a las obligaciones legales o reglamentarias asociadas a la implementación, operación y funcionamiento de la Neutralidad de Red que impidan, dificulten o de cualquier forma amenacen su desarrollo o el legítimo ejercicio de los derechos que de ella derivan, serán sancionables.

3.2 Requisitos de transparencia

En noviembre de 2011, meses después de entrar en vigor la legislación y el posterior reglamento del articulo 24 J que se publicaba en marzo de 2011, y se puede consultar en (147), la Subsecretaría de Telecomunicaciones (SUBTEL) estandarizó la información mínima que por Ley deben entregar las compañías a los usuarios cuando contratan un servicio de Internet, de la que se extraen los puntos más destacados (148).

Artículo 1º. De la Información sobre Planes y Servicios Ofertados a los Usuarios

Los servicios de Internet ofertados deberán contener como mínimo la siguiente información, en el orden que se indica:

a) El nombre y precio del plan.

b) La velocidad publicitada en cada plan que deberá expresarse como un rango de velocidad, informando una velocidad máxima y una velocidad mínima. Además en forma separada la velocidad de subida y bajada, indicando claramente en el caso que existan diferencias para accesos nacionales e internacionales.

c) Para tecnologías inalámbricas o redes móviles, en la oferta de los servicios deberá expresarse claramente que los rangos de velocidad están sujetos a la variabilidad y comportamiento probabilístico del servicio de acceso inalámbrico a Internet, inherentes a este tipo de tecnologías, para ello deberán entregar la siguiente información: mapas de cobertura por tipo de tecnología, propagación de señales, velocidades medias esperadas y toda aquella información que permita un cabal conocimiento de los usuarios cuando optan a este tipo de servicios.

d) La tasa de agregación, especificando expresamente la tasa de reventa para servicios de internet en accesos nacionales o internacionales. Esta tasa corresponderá al cociente entre la suma de las velocidades contratadas por todos los usuarios y la capacidad real contratada en Mbps en el enlace nacional o internacional, según corresponda.

e) Límites de Descarga y condiciones del Servicio de Roaming.

Artículo 2º. De la Información común a los Planes y Servicios Ofertados a los Usuarios

En caso de existir medidas de gestión de tráfico y administración de red, se deberán especificar las características y la forma en que impactan a la totalidad o a un grupo de planes específicos. La aplicación de dichas medidas, deberán ser no discriminatorias entre usuarios de los mismos servicios y deberán ajustarse a lo siguiente:

- Deberán ser estáticas y no pueden ser modificadas unilateralmente.
- Se deberán publicar en el sitio web, con acceso desde la descripción de cada plan que comercialice el ISP.
- Dichas medidas deberán quedar consignadas expresamente en el contrato de suministro respectivo.
- Se deberá indicar claramente el impacto que tienen estas medidas en el o los planes, en especial su impacto en las aplicaciones, en los contenidos y en la velocidad o plan de servicios respectivo.
- Para los casos de ofertas, en que existan elementos de red que impliquen restricciones o concentraciones del tráfico, que afecten la velocidad u otros indicadores, los ISP deberán establecer en sus planes u ofertas específicas que la velocidad ofertada contempla las restricciones que imponen los elementos de red, lo que además deberá ser consignado en los contratos de suministro respectivo.
- Las medidas de administración de congestiones podrán ser ejecutadas solo con carácter excepcional y de manera no discriminatoria entre usuarios. Ellas podrán ser implementadas, ante situaciones de fuerza mayor o caso fortuito no imputables a los ISP que generen congestión de red. Cada vez que un ISP aplique una práctica de este tipo deberá comunicarla, en forma destacada en su sitio Web, describiendo sus características, duración, zonas y servicios afectados, y en especial los potenciales efectos en el servicio prestado a los usuarios finales.

Artículo 3º. De la Información Técnica y de Calidad de los Servicios Ofertados

Toda información técnica que debe publicarse por cada ISP, deberá contener como mínimo la siguiente información y bajo los formatos señalados a continuación:

a) Los indicadores técnicos de calidad que debe informarse deberán representarse en gráficos en base a la medición definida, información que deberá ser actualizada trimestralmente. La velocidad de transmisión efectiva será expresada en Mbps y debe al menos la siguiente información: velocidad máxima, mínima, promedio y desviación estándar. Se debe establecer la ubicación de los puntos de medición distantes.

b) Tiempo de reposición para los percentiles 80% y 95%y el porcentaje de fallas reparadas dentro del tiempo objetivo de cada ISP.

c) Calidad y disponibilidad de los enlaces nacionales e internacionales, con sus respectivos puntos de interconexión, precisándose según enlace:

- Tasa de ocupación en porcentaje, indicando tráfico de bajada y subida.
- Latencia en milisegundos.
- Pérdida de paquetes en porcentaje.

d) Los ISPs deberán disponer de una aplicación reconocida, de fácil acceso para los usuarios, que permita a estos medir las velocidades de los accesos nacionales e internacionales a Internet, especificando claramente la localización de él o los puntos de medición del extremo distante. El usuario debe tener la posibilidad de imprimir el resultado de la medición.

e) Finalmente, el sitio Web del ISP deber tener un link para el acceso al sitio Web de la SUBTEL con el nombre “Ley de Neutralidad”.

4 Holanda

El Parlamento holandés votó el 22 de junio de 2011, por gran mayoría, la prohibición de la diferenciación del tráfico de datos de Internet. De este modo, Holanda pasó a ser el primer país europeo (el segundo del mundo, después de Chile) que adoptó medidas para preservar la Neutralidad de Red.

4.1 Enmienda de Ley

Las propuestas se engloban en cinco puntos, que se añaden a continuación (149):

1. Los proveedores de redes públicas de comunicaciones electrónicas a través de los cuales se ofrecen servicios de Internet y los proveedores de servicios de Internet, no podrán obstaculizar o retrasar los servicios o aplicaciones en Internet, excepto en la medida en que los servicios o aplicaciones se vean obstaculizados o demorados, cuando:

    a) se combata la reducción de congestión, tratando por igual todo el tráfico;

    b) por motivos de integridad y seguridad de la red del proveedor de servicios o del terminal del usuario final;

    c) se transmitan comunicaciones no consentidas por un usuario, siempre que el usuario final antes de autorización expresa, o

    d) en virtud de una disposición legal u orden judicial.

2. En caso de violación del sub-apartado b) del apartado anterior sea causada por parte del dispositivo de usuario, el proveedor antes de tomar una medida de restricción o retraso en la comunicación, deberá informar al usuario y darle la posibilidad de detener dicha infracción.

3. Los proveedores de servicios de acceso a Internet no deben modificar el precio de las tarifas de acceso a Internet dependiendo de los servicios o aplicaciones que sean ofrecidos o utilizados.

4. En virtud de Orden del Consejo se podrán establecer normas específicas en relación con lo dispuesto en el párrafo primero y tercero.

5. En virtud de una orden administrativa para impedir la degradación del servicio y la obstaculización o ralentización del tráfico en las redes de comunicaciones electrónicas públicas se deben detallar los requisitos mínimos para la calidad de las comunicaciones electrónicas públicas que lleven a cabo los proveedores de redes públicas de comunicaciones electrónicas.

Se puede extraer de la misma propuesta de Ley varios aspectos relevantes. Se afirma que los proveedores de servicios de Internet tenderán cada vez más a tomar medidas para bloquear o retrasar Internet, ya sea por iniciativa propia o bajo la presión de terceros, a menos que esté prohibido. Bajo esta argumentación, la enmienda tiene por objeto facilitar la elección y la libertad de expresión en Internet para los usuarios finales. Internet no está destinado a la reserva de ancho de banda para servicios basados en IP ni a la prohibición de ningún servicio o aplicación en Internet. Se afirma también que el mejor método para evitar congestión es evitarla, y la mejor forma d hacerlo es mediante la inversión en mayor capacidad de red.

Es importante resaltar también que los proveedores en conformidad con este artículo están autorizados para ofrecer servicios VoIP sobre el mismo acceso a Internet. Esto permite al proveedor ofrecer una suscripción separada para llamadas VoIP móviles en lugar del servicio de telefonía móvil regular (refiriéndose al modelo LTE donde todos los servicios son sobre IP).

5 Francia

La ARCEP (Autorité de Régulation des Communications Électroniques et des Postes) es la ANR encargada de las telecomunicaciones en Francia. Su actividad en el debate de Neutralidad de Red ha desembocado en una declaración de propuestas y recomendaciones muy elaborada que contempla varios aspectos de interés.

5.1 Consulta pública sobre propuesta de directrices

En noviembre de 2009 la ARCEP llevó a cabo una serie de consultas con agentes del sector. Tras una conferencia que organizó en abril de 2010, lanzó en mayo de 2010 una consulta pública sobre una propuesta de directrices sobre la Neutralidad de Red. Dichas directrices se estructuran en 6 puntos que se resumen a continuación (150):

- Los usuarios tienen derechos de acceso para enviar y recibir contenidos, utilizar las aplicaciones y conectar los equipos que desee.
- Se reconoce la necesidad de la gestión de tráfico de forma eficaz, transparente y no discriminatoria.
- Las conexiones a Internet deben disfrutar de una QoS suficiente y transparente.
- Los operadores deben disponer de la posibilidad de configurar los servicios gestionados que deseen, destinados a los usuarios finales o a los proveedores de contenidos y aplicaciones, siempre que dichos servicios no degraden la calidad del servicio de acceso a Internet.
- Los mercados de la interconexión IP se caracterizan por una opacidad que justifica que ARCEP proceda a requerir periódicamente información sobre estos mercados y la posibilite en un futuro a implementar regulación en éstos si fuera necesario.
- Se debe mejorar la transparencia para el usuario final respecto de los servicios accesibles, gestión de tráficos, calidad de servicio y de cualquier limitación, incluyendo la publicación periódica de indicadores de calidad. La denominación 'servicio de acceso a Internet' no debe aplicarse a las ofertas con restricciones de servicios o protocolos (habituales en redes móviles) y la denominación 'ilimitado' no debe aplicarse a las ofertas con restricciones.

5.2 Propuestas y recomendaciones

En base a las respuestas obtenidas en la consulta pública, el ARCEP elabora en septiembre de 2010 un documento en el que lista 10 propuestas y recomendaciones para preservar la neutralidad de Internet. Se trata de un conjunto de recomendaciones que abarcan casi todos

los aspectos del debate de Neutralidad de Red, y que prioriza los derechos de los usuarios en el acceso a Internet (5).

Neutralidad en los accesos a Internet

1. Libertad y calidad en el acceso: Los ISPs deben proveer a sus clientes con la capacidad de recibir y enviar el contenido que deseen, usar los servicios de su elección y conectar el hardware y usar los programas que escojan, además de ser transparentes.

2. No discriminación entre flujos de datos: Como norma general no se debe diferenciar en el tratamiento de flujos según ningún criterio (contenidos, servicios, aplicaciones, equipos o direcciones IP) en ningún punto de la red, incluyendo los puntos de interconexión. Pueden aplicarse excepciones a esta regla, siempre que cumplan con la propuesta nº 3.

3. Marco para regular las prácticas de gestión: Cuando se empleen técnicas de gestión de tráfico para asegurar el acceso a Internet, se deberá cumplir con unos criterios de relevancia, proporcionalidad, eficiencia, no discriminación y transparencia.

4. Servicios dedicados: Para preservar la capacidad de innovación de todos los implicados, todos los operadores deben ser capaces de comercializar los servicios dedicados al margen del acceso a Internet, tanto para usuarios como para proveedores de contenidos, de modo que estos servicios no degraden la QoS del acceso a Internet por debajo de un nivel satisfactorio.

5. Mayor transparencia para los usuarios finales: Los ISPs deben proporcionar a los usuarios finales en los términos y condiciones contractuales, de forma clara y precisa información acerca de los servicios y aplicaciones a los que pueden acceder, la QoS, posibles limitaciones y las prácticas de gestión de tráfico que les puedan afectar. Para ello, ARCEP recomienda que cualquier desviación de lo propuesto en las propuestas 1) y 2) se especifique con claridad en las condiciones contractuales. El término 'Internet', no podrá ser usado si alguna de estas restricciones no cumple con los requisitos de la cláusula 3). El término 'ilimitado' no podrá ser usado para servicios con cualquier tipo de limitación en cuanto al acceso, a la QoS o a la velocidad, así como tampoco para servicios que puedan implicar una facturación adicional.

6. Seguimiento de las prácticas de gestión de tráfico: ARCEP solicitará a ISPs, proveedores de contenidos y asociaciones de consumidores que trabajen juntos para identificar y calificar los tipos de prácticas de gestión de tráfico para tener respuesta en el primer trimestre de 2011. Entretanto se monitorizarán las técnicas actuales que los operadores emplean.

7. Control de la QoS del acceso a Internet: Para asegurar una calidad suficiente y transparente, se trabajará en identificar la calidad de los principales parámetros de

acceso a Internet y en establecer los indicadores adecuados. Se exigirá a los ISPs la publicación de dichos parámetros en los accesos minoristas tanto para redes fijas como móviles.

8. Monitorización del mercado de interconexión de datos: Se recomienda que las partes que proveen al usuario final sean capaces de responder a cualquier petición cuyo propósito sea dar acceso a servicios o aplicaciones. En cuanto a las que proveen a los proveedores de contenidos, deben garantizar que estos contenidos sean accesibles a los usuarios de Internet. Para acabar con la falta de claridad existente en la interconexión, ARCEP tomará unas normas para la recolección periódica de información de este mercado.

Otros aspectos de neutralidad

9. El papel de los proveedores de contenido en la Neutralidad de Red: Para que los usuarios puedan ejercer su libertad de elegir entre contenidos, los proveedores de contenidos deben no discriminar entre operadores que acceden a éstos. Además deberán ser transparentes con los usuarios en cuanto a las norma empleadas cuando los proveedores de contenido seleccionan contenidos de terceros, como en el caso de motores de búsqueda.

10. Aumentar la neutralidad en los dispositivos: En base a una revisión de la Directiva RTTE (Radio and Telecommunications Terminal Equipment) se recomienda examinar la situación en los diferentes dispositivos, en especial la relación entre las capas de software de los dispositivos con los proveedores de contenido.

6 Reino Unido

La ANR del Reino Unido, OFCOM, lanzó en junio de 2010 una consulta pública con objeto de generar un debate de cara a la revisión de la legislación y su integración en el Marco Europeo, que además incluye algunas valoraciones del organismo. OFCOM consultó acerca de la gestión de tráfico a los interesados tanto sobre sus posibles aspectos positivos (generación de valor) y problemas potenciales (discriminación injustificada, desincentivo a la innovación, perjuicio al consumidor, etc.), y solicitó también aportaciones sobre cómo mejorar la transparencia para los usuarios (151).

De las valoraciones que hace OFCOM, hay varios aspectos a destacar:

- No hay necesidad, por el momento, de regulación adicional destinada a proteger la Neutralidad de Red ni a prohibir la gestión de tráfico, debido a que no ha habido pruebas en cuanto a comportamientos contrarios a la competencia.

- En lugar de introducir nuevas obligaciones como las de QoS se propone aplicar las herramientas ya disponibles de fomento de la competencia y las posibilidades de mejorar la transparencia para los usuarios.

- No hay justificación para prohibir la remuneración a los operadores por los proveedores de servicios, siempre que no se haga uso de técnicas anti-competitivas. Esto puede beneficiar al consumidor final.

- Es importante la transparencia y la información completa de cualquier degradación o bloqueo, aunque se considera que el mero hecho de dar información no es suficiente para los usuarios.

El resultado de dicha consulta salió a la luz en noviembre de 2011, y en él se reposicionan en la misma línea, afirmando que una gestión de tráfico puede resultar beneficiosa. Se resalta la necesidad de que exista transparencia de modo que le usuario sea capaz de comprender y comprobar los parámetros contratados. Se aboga por un modelo de coexistencia entre el modelo ‘best effort’ y los servicios dedicados, haciendo hincapié en salvaguardar el modelo ‘best effort’ por su aporte a la sociedad, llegando incluso a imponer un mínimo de QoS (152).

7 Suecia

El 30 de noviembre de 2009, el regulador Sueco PTS (Post and Telecom Swedish-Authority) emitió un amplio informe encargado por el Gobierno de Suecia sobre el estado de redes y servicios abiertos (153). Este trata muchas cuestiones, además de incluir una síntesis de las respuestas de la consulta realizada como parte del mismo Proyecto a operadores, proveedores de contenido, fabricantes de equipos y usuarios de Internet, con el fin de conseguir una visión amplia de que entienden estos grupos acerca de redes abiertas.

El informe desarrolla una serie de ideas, algunas de ellas no directamente relacionadas con la Neutralidad de Red, y llega a las siguientes conclusiones de carácter general:

- El carácter abierto de redes y servicios crea oportunidades para la innovación y la competitividad, no obstante, debe ser equilibrado con otros intereses dignos de protección como los incentivos a la inversión y la seguridad de la red.

- El carácter abierto de redes y servicios se promueve garantizando la no discriminación y la competencia efectiva.

- Es de gran importancia que los ISPS sean transparentes sobre los periodos de permanencia, restricciones en el acceso y en la accesibilidad a los servicios que comercializan.

Debido a que no se consideran situaciones concretas que pongan de manifiesto la violación de estos principios, PTS no considera necesaria una regulación de la Neutralidad de Red. Sin embargo, consideran que en un futuro se deberá determinar en qué medida las herramientas de gestión y priorización son pertinentes si hay limitación en la capacidad de las redes.

8 Canadá

La CRTC es la agencia reguladora en Canadá y se encarga de todos los aspectos de radiodifusión y telecomunicaciones. El contexto regulatorio en Canadá es similar al existe en la UE. Existen unos mercado finales liberalizados y regulación en los servicios mayoristas de banda ancha en redes fijas (27).

8.1 Telecom Decision 2008-108

El 20 de noviembre de 2008, la CRTC publica la resolución acerca de la denuncia puesta en abril de ese mismo año por la CAIP en contra de Bell Canada por prácticas de gestión de tráfico discriminatoria a sus clientes mayoristas, fallando a favor del operador por considerar que las medidas empleadas no resultaban discriminatorias (32).

La CRTC, a la luz de que las partes en este proceso mostraron preocupaciones serias en cuanto a la gestión del tráfico de Internet, e inició un procedimiento para revisar las actuales y potenciales prácticas de gestión de tráfico por parte de los ISPs. Como muestra de ello, lanza el mismo día que hace pública esta decisión, un documento de consulta pública (154) con la intención de sentar las bases para iniciar dicha revisión.

8.2 Telecom Regulatory Policy CRTC 2009-657

El 21 de diciembre de 2009, casi un año después del lanzamiento de la consulta pública, la CRTC emite este documento en el que se establecen los principios que pretenden equilibrar adecuadamente la libertad de los canadienses para utilizar Internet, con independencia de los intereses legítimos de los ISPs para gestionar el tráfico (155).

Las determinaciones tomadas se articulan en torno a cuatro aspectos:

Transparencia

- Si se usan técnicas de gestión de tráfico, los ISPs deben ser transparentes al respecto.
- Si se aplican medidas económicas en cuanto relaciones entre precio y consumo, estas deben ser bien conocidas por el usuario.

Innovación

- Si bien se afirma que la inversión en la red es fundamental para combatir, como medida principal, posibles problemas de congestión, se reconocen ciertas medidas de gestión de tráfico como solución a problemas puntuales.
- El uso de técnicas de gestión debe llevarse a cabo sólo para necesidades justificadas.

Imparcialidad

- El uso de gestión de tráfico por los ISPs no puede ser discriminatorio o preferencial.

Neutralidad en la competencia

- En cuanto a servicios minoristas, los ISPs podrán hacer uso de las técnicas de gestión sin necesidad de la aprobación de la CRTC. Estas prácticas serán revisadas y evaluadas ante el marco expuesto, en base a posibles quejas de consumidores.

- En los servicios mayoristas se aplicará una revisión más exhaustiva. Si un ISP pretende hacer uso de técnicas de gestión más restrictivas para sus servicios mayoristas que para el minorista, deberá cumplir con el marco y se requerirá la aprobación de la CRTC.

En caso de uso de prácticas discriminatorias, el operador denunciado a tal efecto, deberá demostrar que la práctica en cuestión está diseñada para conseguir solamente el objetivo prefijado, que resulta en el mínimo grado de discriminación posible, y que el daño causado a cualquier otro operador o usuario es el menor posible. En el caso de una práctica de tipo técnico, se deberá justificar que no se podría solucionar el problema con cualquier otra práctica económica o con la inversión en capacidad de red. Así pues, la CRTC acepta la aplicación de mecanismos de gestión de tráfico pero la restringe a los casos claramente justificados.

Respecto de la ralentización de los servicios P2P, la CRTC considera que, por tratarse de servicios no sensibles al retardo, resulta aceptable siempre que no implique en la práctica un bloqueo de estos servicios. La CRTC entiende asimismo que las prácticas de gestión de tráfico que traten de mantener la integridad y seguridad de las redes ante ataques o amenazas de éstos (como el spam, aplicaciones dañinas o la distribución de contenido ilícito) son permisibles y son parte de la gestión corriente de las redes de los operadores.

9 Noruega

Agentes del sector en Noruega reunidos en un foro encabezado por el regulador Norway Post and Telecommunication-Authority (NPT) acordaron unas directrices sobre 'Internet neutrality' (156).

En febrero de 2009 se publicó un informe realizado con la participación de ISPs, organizaciones de consumidores, organizaciones industriales y proveedores de contenidos. En él se establecen una serie de directrices enfocadas a preservar la neutralidad de Internet, que están basadas en tres principios.

- Los usuarios de Internet tienen derecho a una conexión a Internet con capacidad y calidad predefinidas.

- Los usuarios de Internet tienen derecho a una conexión a Internet que les permita enviar y recibir el contenido de su elección, utilizar los servicios y ejecutar las aplicaciones de su elección, y conectar el hardware y usar el software de su elección que no dañen la red.

- Los usuarios de Internet tienen derecho a una conexión a Internet que esté libre de discriminación en relación con el tipo de aplicación, servicio o contenido o que esté basada en la dirección del emisor o receptor.

Las citadas directrices reconocen expresamente que algunos de sus principios se basan en referencias internacionales. Concretamente, el segundo principio se deriva de la declaración de la FCC de 2005 antes mencionada y que el tercer principio se fundamenta en las conclusiones del grupo de trabajo formado en Japón.

10 Japón

El 15 de noviembre de 2006, el Ministerio de Asuntos Interiores y Comunicaciones (MIC) de Japón estableció un grupo de trabajo sobre Neutralidad de Red. El trabajo realizado por el grupo de trabajo se publicó el 20 de septiembre de 2007. Dicho Informe recoge tres principios (157):

- Los usuarios tienen derecho a usar las redes IP de manera flexible y a acceder libremente a la capa de contenido y aplicaciones.
- Los usuarios tienen derecho a conectarse libremente a las redes IP por medio de terminales normalizados y dichos terminales podrán conectarse mutuamente de manera flexible.
- Los usuarios tienen derecho a utilizar la capa de comunicaciones y la capa de plataformas de forma no discriminatoria y a un precio razonable.

Anexo B – Análisis de tráfico real

1 OpenDPI

OpenDPI constituye una versión no comercial del motor de búsqueda PACE de Ipoque. Carece de muchas de las características de su versión completa, como por ejemplo que no soporta detección en flujos unidireccionales, su rendimiento es hasta cinco veces menor que la versión comercial y no soporta IPv6. Además, OpenDPI no soporta el análisis de tráfico cifrado ya que no emplea análisis heurístico o DFI. Pese a estas limitaciones cabe decir que la tasa de error en la detección que proporciona el fabricante es del orden de $< 2^{-64}$ ($= 5 * 10^{-18}$ %) por flujo, y el número de protocolos que es capaz de detectar es notable (158):

- **P2P:** BitTorrent, eDonkey, KaZaa / Fasttrack, Gnutella, WinMX, DirectConnect, AppleJuice, Soulseek, XDCC, Filetopia, Manolito, iMesh, Pando
- **VoIP:** SIP, IAX, RTP
- **IM (Instant Messaging):** Yahoo, Oscar, IRC, unencrypted Jabber, Gadu!Gadu, MSN
- **Streaming:** ORB, RTSP, Flash, MMS, MPEG, Quicktime, Joost, WindowsMedia, RealMedia, TVAnts, SOPCast, TVUPlayer, PPStream, PPLive, QQLive, Zattoo, VeohTV, AVI, Feidian, Ececast, Kontiki, Move, RTSP, SCTP, SHOUTcast
- **Tunneling:** IPsec, GRE, SSL, SSH, IP in IP
- **Protocolos estándar:** HTTP, Direct download links (1 click file hosters), POP, SMTP, IMAP, FTP, BGP, DHCP, DNS, EGP, ICMP, IGMP, MySQL, NFS, NTP, OSPF, pcAnywhere, PostgresSQL, RDP, SMB, SNMP, SSDP, STUN, Telnet, Usenet, VNC, IPP, MDNS, NETBIOS, XDMCP, RADIUS, SYSLOG, LDAP
- **Juego On-line:** World of Warcraft, Halflife, Steam, Xbox, Quake, Second Life

2 Capturas de tráfico

El método empleado para realizar un análisis mediante OpenDPI es el siguiente. En primer lugar se debe realizar una captura de tráfico mediante Wireshark y se guarda en formato *.pcap*. Posteriormente se procesa por el motor OpenDPI sobre una máquina Linux. Para más detalle sobre la operación seguida, consúltese el "OpenDPI Integration Manual" en (158).

Se muestran en todos los casos las capturas de pantalla de la información proporcionada por Wireshark (salvo en el apartado 2.3) y por OpenDPI, para su posterior comparación. En todos los casos, se han realizado las capturas de tráfico sin más aplicaciones conectadas a Internet para ver con más claridad que los paquetes transferidos provienen de los clientes empleados en cada caso.

2.1 P2P (Peer-To-Peer)

Para las diferentes simulaciones de tráfico P2P se ha cogido como muestra una captura de tráfico de unos 15000 paquetes IP, que representan un volumen de unos 7 MB (valor aproximado, véase más adelante este parámetro en las capturas de pantalla).

2.1.1 BitTorrent

***qBitorrent* sin cifrar**

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	15256	6098669	0,485	0	0	0,000
Ethernet	100,00 %	15256	6098669	0,485	0	0	0,000
Internet Protocol	99,95 %	15249	6098125	0,485	0	0	0,000
User Datagram Protocol	7,79 %	1188	140983	0,011	0	0	0,000
Domain Name Service	0,03 %	4	356	0,000	4	356	0,000
Data	7,75 %	1182	140413	0,011	1182	140413	0,011
ENTTEC	0,01 %	1	107	0,000	1	107	0,000
Quake III Arena Network Protocol	0,01 %	1	107	0,000	1	107	0,000
Internet Control Message Protocol	1,38 %	210	23456	0,002	210	23456	0,002
Transmission Control Protocol	90,79 %	13851	5933686	0,472	11173	4800919	0,382
BitTorrent	17,51 %	2672	1130775	0,090	2358	1012794	0,081
Data	0,04 %	6	1992	0,000	6	1992	0,000
Address Resolution Protocol	0,03 %	4	168	0,000	4	168	0,000
Logical-Link Control	0,01 %	1	126	0,000	0	0	0,000
802.1X Authentication	0,01 %	2	250	0,000	2	250	0,000

Ilustración 66: Análisis Wireshark sobre captura *qBitorrent* sin cifrar

```
pcap file contains
        ip packets:   15249         of 15256 packets total
        ip bytes:     6098125
        unique ids:   1714
        unique flows: 2035


detected protocols:
        unknown             packets: 3557          bytes: 810960          flows: 1584
        DNS                 packets: 4             bytes: 356             flows: 2
        Bittorrent          packets: 11478         bytes: 5703347         flows: 243
        ICMP                packets: 210           bytes: 23456           flows: 206
```

Ilustración 67: Análisis OpenDPI sobre captura *qBitorrent* sin cifrar

***qBitorrent* cifrado**

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100,00 %	15148	7032998	0,526	0	0	0,000
▼ Ethernet	100,00 %	15148	7032998	0,526	0	0	0,000
▼ Internet Protocol	99,83 %	15122	7028325	0,526	0	0	0,000
▼ Transmission Control Protocol	97,41 %	14756	6987743	0,523	6527	452345	0,034
Data	54,31 %	8227	6534465	0,489	8227	6534465	0,489
▼ TCP Encapsulation of IPsec Packets	0,01 %	1	343	0,000	0	0	0,000
Encapsulating Security Payload	0,01 %	1	343	0,000	1	343	0,000
▷ Session Traversal Utilities for NAT	0,01 %	1	590	0,000	0	0	0,000
▼ User Datagram Protocol	2,18 %	330	36601	0,003	0	0	0,000
Data	2,17 %	328	36421	0,003	328	36421	0,003
Domain Name Service	0,01 %	2	180	0,000	2	180	0,000
Internet Control Message Protocol	0,24 %	36	3981	0,000	36	3981	0,000
Address Resolution Protocol	0,01 %	2	84	0,000	2	84	0,000
▷ Logical-Link Control	0,16 %	24	4589	0,000	0	0	0,000

Ilustración 68: Análisis Wireshark sobre captura *qBitorrent* cifrado

```
pcap file contains
        ip packets:   15122         of 15148 packets total
        ip bytes:     7028325
        unique ids:   584
        unique flows: 811


detected protocols:
        unknown                 packets: 15084          bytes: 7024164          flows: 776
        DNS                     packets: 2              bytes: 180              flows: 1
        ICMP                    packets: 36             bytes: 3981             flows: 34
```

Ilustración 69: Análisis OpenDPI sobre captura *qBitorrent* cifrado

µTorrent sin cifrar

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100,00 %	15316	8815501	0,441	0	0	0,000
▼ Ethernet	100,00 %	15316	8815501	0,441	0	0	0,000
▼ Internet Protocol	99,96 %	15310	8815249	0,441	0	0	0,000
▼ User Datagram Protocol	9,86 %	1510	272107	0,014	0	0	0,000
Data	9,58 %	1467	265743	0,013	1467	265743	0,013
NAT Port Mapping Protocol	0,03 %	5	260	0,000	5	260	0,000
Hypertext Transfer Protocol	0,09 %	14	3202	0,000	14	3202	0,000
Domain Name Service	0,14 %	22	2648	0,000	22	2648	0,000
Microsoft Media Server	0,01 %	1	109	0,000	1	109	0,000
Internet Security Association and Key Management Protocol	0,01 %	1	145	0,000	1	145	0,000
Internet Control Message Protocol	1,00 %	153	18235	0,001	153	18235	0,001
▼ Transmission Control Protocol	89,10 %	13647	8524907	0,426	10166	5714604	0,286
Data	0,25 %	38	33360	0,002	38	33360	0,002
▷ Hypertext Transfer Protocol	0,16 %	24	7009	0,000	19	4823	0,000
▷ BitTorrent	22,24 %	3407	2756098	0,138	3172	2704525	0,135
▷ X11	0,08 %	12	13836	0,001	1	59	0,000
Address Resolution Protocol	0,04 %	6	252	0,000	6	252	0,000

Ilustración 70: Análisis Wireshark sobre captura *µTorrent* sin cifrar

```
pcap file contains
        ip packets:   15310         of 15316 packets total
        ip bytes:     8815249
        unique ids:   1057
        unique flows: 1338


detected protocols:
        unknown                 packets: 2646           bytes: 339868           flows: 1118
        DNS                     packets: 22             bytes: 2648             flows: 11
        HTTP                    packets: 64             bytes: 33607            flows: 5
        SSDP                    packets: 3              bytes: 525              flows: 1
        Bittorrent              packets: 12422          bytes: 8420286          flows: 68
        ICMP                    packets: 153            bytes: 18235            flows: 135
```

Ilustración 71: Análisis OpenDPI sobre captura *µTorrent* sin cifrar

µTorrent cifrado

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100,00 %	15122	7984878	0,430	0	0	0,000
▼ Ethernet	100,00 %	15122	7984878	0,430	0	0	0,000
▼ Internet Protocol	99,97 %	15118	7984710	0,430	0	0	0,000
▼ User Datagram Protocol	9,75 %	1474	275001	0,015	0	0	0,000
NAT Port Mapping Protocol	0,07 %	10	520	0,000	10	520	0,000
Hypertext Transfer Protocol	0,24 %	36	8370	0,000	36	8370	0,000
Domain Name Service	0,12 %	18	2244	0,000	18	2244	0,000
Data	9,30 %	1407	263284	0,014	1407	263284	0,014
Microsoft Media Server	0,01 %	1	109	0,000	1	109	0,000
Network Service Over IP	0,01 %	2	474	0,000	2	474	0,000
Internet Control Message Protocol	1,06 %	160	19119	0,001	160	19119	0,001
▼ Transmission Control Protocol	89,17 %	13484	7690590	0,414	5634	362720	0,020
Data	51,73 %	7823	7317513	0,394	7823	7317513	0,394
▶ Hypertext Transfer Protocol	0,16 %	24	6996	0,000	19	4810	0,000
▶ DCE RPC	0,01 %	1	1474	0,000	0	0	0,000
▶ Sinec H1 Protocol	0,01 %	1	413	0,000	0	0	0,000
Universal Computer Protocol	0,01 %	1	1474	0,000	1	1474	0,000
Address Resolution Protocol	0,03 %	4	168	0,000	4	168	0,000

Ilustración 72: Análisis Wireshark sobre captura *µTorrent* cifrado

```
pcap file contains
        ip packets:   15118          of 15122 packets total
        ip bytes:     7984710
        unique ids:   994
        unique flows: 1278


detected protocols:
        unknown              packets: 14697        bytes: 7877296        flows: 1110
        DNS                  packets: 18           bytes: 2244           flows: 9
        HTTP                 packets: 129          bytes: 60092          flows: 10
        SSDP                 packets: 9            bytes: 1575           flows: 1
        Bittorrent           packets: 105          bytes: 15384          flows: 14
        ICMP                 packets: 160          bytes: 19119          flows: 134
```

Ilustración 73: Análisis OpenDPI sobre captura *µTorrent* cifrado

2.1.2 eDonkey

eMule sin ofuscar

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100,00 %	15000	13337193	0,540	0	0	0,000
▼ Ethernet	100,00 %	15000	13337193	0,540	0	0	0,000
▼ Internet Protocol	99,89 %	14983	13335949	0,540	0	0	0,000
▼ User Datagram Protocol	0,63 %	95	11272	0,000	0	0	0,000
Hypertext Transfer Protocol	0,19 %	28	7256	0,000	28	7256	0,000
Data	0,41 %	61	3656	0,000	61	3656	0,000
eDonkey Protocol	0,04 %	6	360	0,000	6	360	0,000
▼ Transmission Control Protocol	98,75 %	14813	13320235	0,539	5023	273958	0,011
Data	65,17 %	9776	13042571	0,528	9776	13042571	0,528
eDonkey Protocol	0,08 %	12	1414	0,000	12	1414	0,000
Universal Computer Protocol	0,01 %	1	1474	0,000	1	1474	0,000
▶ Short Message Peer to Peer	0,01 %	1	818	0,000	0	0	0,000
Internet Control Message Protocol	0,50 %	75	4442	0,000	75	4442	0,000
Address Resolution Protocol	0,08 %	12	504	0,000	12	504	0,000
▶ Internet Protocol Version 6	0,03 %	5	740	0,000	0	0	0,000

Ilustración 74: Análisis Wireshark sobre captura *eMule* sin ofuscar

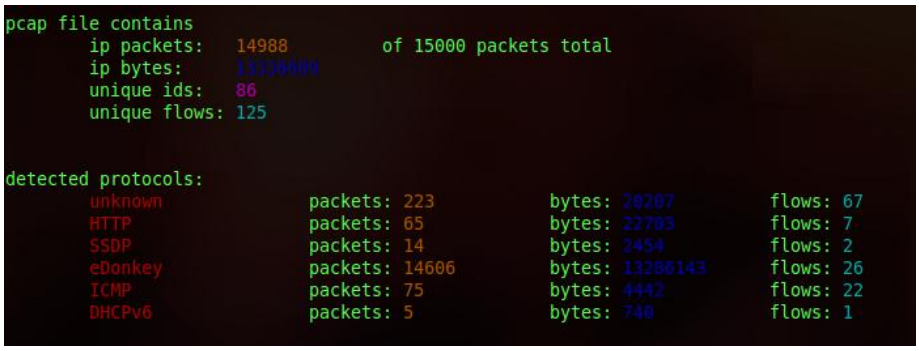

Ilustración 75: Análisis OpenDPI sobre captura *eMule* sin ofuscar

***eMule* ofuscado**

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	15027	10980878	0,134	0	0	0,000
Ethernet	100,00 %	15027	10980878	0,134	0	0	0,000
Internet Protocol	99,56 %	14961	10975794	0,134	0	0	0,000
User Datagram Protocol	8,60 %	1292	152427	0,002	1	85	0,000
Hypertext Transfer Protocol	0,56 %	84	21180	0,000	84	21180	0,000
Data	6,94 %	1043	112193	0,001	1043	112193	0,001
eDonkey Protocol	1,02 %	153	17140	0,000	153	17140	0,000
FOUNDATION Fieldbus	0,03 %	4	957	0,000	0	0	0,000
Microsoft Media Server	0,01 %	1	85	0,000	1	85	0,000
Logical-Link Control	0,04 %	6	787	0,000	0	0	0,000
Transmission Control Protocol	86,34 %	12975	10783992	0,131	4385	237834	0,003
Data	57,16 %	8590	10546158	0,128	8590	10546158	0,128
Internet Control Message Protocol	4,61 %	693	37869	0,000	693	37869	0,000
Data	0,01 %	1	1506	0,000	1	1506	0,000
Internet Protocol Version 6	0,13 %	20	3152	0,000	0	0	0,000
Address Resolution Protocol	0,31 %	46	1932	0,000	46	1932	0,000

Ilustración 76: Análisis Wireshark sobre captura *eMule* ofuscado

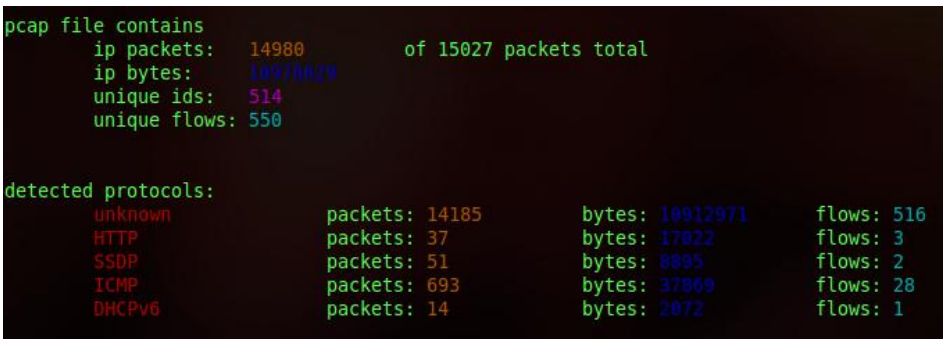

Ilustración 77: Análisis OpenDPI sobre captura *eMule* ofuscado

2.2 VoIP (SIP + RTP)

Blink **sin cifrar**

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▽ Frame	100,00 %	1097	234295	0,099	0	0	0,000
▽ Ethernet	100,00 %	1097	234295	0,099	0	0	0,000
▽ Internet Protocol	99,00 %	1086	232865	0,099	0	0	0,000
▽ User Datagram Protocol	98,54 %	1081	231655	0,098	0	0	0,000
Domain Name Service	2,55 %	28	3166	0,001	28	3166	0,001
Session Initiation Protocol	0,82 %	9	5759	0,002	9	5759	0,002
Data	0,18 %	2	342	0,000	2	342	0,000
▷ Real-time Transport Control Protocol	0,46 %	5	470	0,000	3	218	0,000
Real-Time Transport Protocol	94,53 %	1037	221918	0,094	1037	221918	0,094
Internet Control Message Protocol	0,46 %	5	1210	0,001	5	1210	0,001
▷ Internet Protocol Version 6	0,46 %	5	1040	0,000	0	0	0,000
▷ Logical-Link Control	0,09 %	1	93	0,000	0	0	0,000
Address Resolution Protocol	0,36 %	4	204	0,000	4	204	0,000
▷ MDS Header	0,09 %	1	93	0,000	0	0	0,000

Ilustración 78: Análisis Wireshark sobre captura de *Blink* sin cifrar

```
pcap file contains
        ip packets:   1091          of 1097 packets total
        ip bytes:     233905
        unique ids:   9
        unique flows: 21


detected protocols:
        unknown             packets: 10          bytes: 1454          flows: 3
        DNS                 packets: 28          bytes: 3166          flows: 14
        SSDP                packets: 5           bytes: 1040          flows: 1
        ICMP                packets: 5           bytes: 1210          flows: 1
        RTP                 packets: 1034        bytes: 221276        flows: 1
        SIP                 packets: 9           bytes: 5759          flows: 1
```

Ilustración 79: Análisis OpenDPI sobre captura de *Blink* sin cifrar

Blink **cifrado**

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▽ Frame	100,00 %	1069	239567	0,116	0	0	0,000
▽ Ethernet	100,00 %	1069	239567	0,116	0	0	0,000
▷ Internet Protocol Version 6	0,75 %	8	1608	0,001	0	0	0,000
▽ Internet Protocol	98,69 %	1055	237569	0,115	0	0	0,000
▽ User Datagram Protocol	98,32 %	1051	236561	0,114	0	0	0,000
Domain Name Service	1,31 %	14	1583	0,001	14	1583	0,001
Session Initiation Protocol	0,65 %	7	5060	0,002	7	5060	0,002
▷ Real-time Transport Control Protocol	0,47 %	5	540	0,000	4	476	0,000
Real-Time Transport Protocol	95,51 %	1021	228704	0,110	1021	228704	0,110
Data	0,19 %	2	342	0,000	2	342	0,000
Hypertext Transfer Protocol	0,19 %	2	332	0,000	2	332	0,000
Internet Control Message Protocol	0,37 %	4	1008	0,000	4	1008	0,000
▷ MDS Header	0,19 %	2	186	0,000	0	0	0,000
Address Resolution Protocol	0,37 %	4	204	0,000	4	204	0,000

Ilustración 80: Análisis Wireshark sobre captura de *Blink* cifrado

```
pcap file contains
        ip packets:   1063          of 1069 packets total
        ip bytes:     238177
        unique ids:   10
        unique flows: 15

detected protocols:
        unknown             packets: 10          bytes: 1554          flows: 3
        DNS                 packets: 14          bytes: 1583          flows: 7
        SSDP                packets: 10          bytes: 1940          flows: 2
        ICMP                packets: 4           bytes: 1008          flows: 1
        RTP                 packets: 1018        bytes: 228032        flows: 1
        SIP                 packets: 7           bytes: 5060          flows: 1
```

Ilustración 81: Análisis OpenDPI sobre captura de *Blink* cifrado

2.3 Email (SMTP + IMAP)

Email sin cifrado

```
pcap file contains
        ip packets:   45            of 45 packets total
        ip bytes:     4703
        unique ids:   4
        unique flows: 4

detected protocols:
        unknown             packets: 10          bytes: 778           flows: 0
        Mail_SMTP           packets: 20          bytes: 2195          flows: 1
        Mail_IMAP           packets: 11          bytes: 1270          flows: 1
        DNS                 packets: 4           bytes: 460           flows: 2
```

Ilustración 82: Análisis OpenDPI sobre captura de envío (SMTP) sin cifrado

```
pcap file contains
        ip packets:   31            of 31 packets total
        ip bytes:     5087
        unique ids:   2
        unique flows: 1

detected protocols:
        unknown             packets: 3           bytes: 226           flows: 0
        Mail_IMAP           packets: 28          bytes: 4861          flows: 1
```

Ilustración 83: Análisis OpenDPI sobre captura de recepción (IMAP) sin cifrado

Email cifrado

```
pcap file contains
        ip packets:   49            of 49 packets total
        ip bytes:     10210
        unique ids:   4
        unique flows: 4

detected protocols:
        unknown             packets: 11          bytes: 1482          flows: 1
        DNS                 packets: 4           bytes: 460           flows: 2
        SSL                 packets: 34          bytes: 8274          flows: 1
```

Ilustración 84: Análisis OpenDPI sobre captura de envío (SMTPS) cifrado

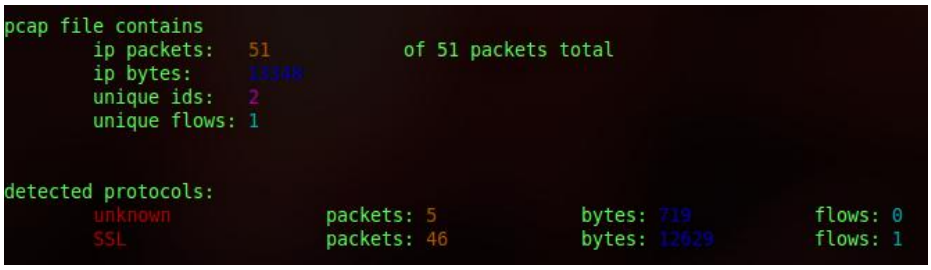

Ilustración 85: Análisis OpenDPI sobre captura de recepción (IMAPS) cifrado

Referéncias

1. **Arbor Networks, Inc.; University of Michigan; Merit Network, Inc. .** ATLAS Internet Observatory 2009 Annual Report. [En línea] 2009. [Citado el: 01 de Diciembre de 2011.] http://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf.

2. **Bendrath, Ralf.** Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection. [En línea] 2009. [Citado el: 01 de Diciembre de 2011.] http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf.

3. **J. H. Saltzer; D. P. Reed; D. D. Clark.** End-To-End Arguments in System Design. [En línea] 1981. [Citado el: 02 de Diciembre de 2011.] http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

4. **Lessig, Lawrence.** The Future of Ideas. The Fate of the Commons in a Connected World. [En línea] 2001. [Citado el: 02 de Diciembre de 2011.] http://www.the-future-of-ideas.com/download/lessig_FOI.pdf.

5. **ARCEP.** Internet and network neutrality: Proposals and recommendations. [En línea] 2010. [Citado el: 02 de Diciembre de 2011.] http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010-eng.pdf.

6. **Kearney, A.T.** A viable future for the Internet. [En línea] 2011. [Citado el: 02 de Diciembre de 2011.] http://www.atkearney.com/images/global/pdf/Viable_Future_Model_for_Internet.pdf.

7. **Kenny, Robert.** Are traffic charges needed to avert a coming capex catastrophe? [En línea] [Citado el: 19 de Diciembre de 2011.] https://869789182725854870-a-commcham-com-s-sites.googlegroups.com/a/commcham.com/www/traffic-charges/TrafficChargesATKReview.pdf?attachauth=ANoY7coN_eiJ58KT3bPB9U_xeVgQprC6SDXKu1eKCCyOKvIHxkvIdPUGHKKN6GxIULIq0Sd4cr9IET_RHfjtUewwyMJp3sV2ZBpljj0pZessRs7maZ.

8. **El País.** ElPais.com. *Telefónica abre fuego contra los buscadores.* [En línea] 2010. [Citado el: 26 de Ocutbre de 2011.] http://www.elpais.com/articulo/tecnologia/Telefonica/abre/fuego/buscadores/elpeputec/20100207elpeputec_1/Tes.

9. **Varios.** Carta de proveedores de servicio a la FCC. [En línea] 19 de Octubre de 2009. [Citado el: 14 de Diciembre de 2011.] http://online.wsj.com/public/resources/documents/netneutrality20091018.pdf.

10. **Cisco.** Cisco Visual Networking Index: Forecast and Methodology, 2010–2015. [En línea] 2011. [Citado el: 02 de Diciembre de 2011.] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf.

11. **Nicholas Economides; Joacim Tåg.** Net Neutrality on the Internet: A Two-sided Market Analysis. [En línea] 2009. [Citado el: 02 de Diciembre de 2011.] http://www.stern.nyu.edu/networks/Economides_Tag_Net_Neutrality.pdf.

12. **Arbor Networks.** Security To The Core. *Google Sets New Internet Traffic Record.* [En línea] 2010. [Citado el: 2011 de Octubre de 2011.] http://asert.arbornetworks.com/2010/10/google-breaks-traffic-record/.

13. **Varios.** The Flattening Internet Topology: Natural Evolution, Unsightly Barnacles or Contrived Collapse? [En línea] 2008. [Citado el: 02 de Diciembre de 2011.] http://www.hpl.hp.com/techreports/2008/HPL-2008-47.pdf.

14. **Movistar Colombia.** Movistar. *Paquetes de Internet.* [En línea] http://www.movistar.co/Personas/Internet_movil/Planes/Paquetes_de_internet/.

15. **The Economist.** The Economist. *A tangled web.* [En línea] 2010. [Citado el: 20 de Diciembre de 2011.] http://www.economist.com/node/17800141.

16. **Wu, Tim.** Network Neutrality, Broadband Discrimination. [En línea] 2003. [Citado el: 02 de Diciembre de 2011.] http://campus.murraystate.edu/faculty/mark.wattier/Wu2003.pdf.

17. —. Tim Wu. *Network Neutrality FAQ.* [En línea] [Citado el: 02 de Noviembre de 2011.] http://www.timwu.org/network_neutrality.html.

18. **Sandvine.** Global Internet Phenomena Report Fall 2011. [En línea] 2011. [Citado el: 16 de Diciembre de 2011.] http://www.sandvine.com/downloads/documents/10-26-2011_phenomena/Sandvine%20Global%20Internet%20Phenomena%20Report%20-%20Fall%202011.PDF.

19. **BEREC.** BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe. [En línea] 2010. [Citado el: 02 de Diciembre de 2011.] http://www.irg.eu/streaming/BoR%20(10)%2042%20BEREC%20response_ECconsultation_Net%20neutrality_final.pdf?contentId=546969&field=ATTAC.

20. **Financial Times Deutschland.** Financial Times Deutschland. *Netzbetreiber blocken Skype auf Handys.* [En línea] 2009. [Citado el: 27 de Octubre de 2011.] http://www.ftd.de/it-medien/it-telekommunikation/:streit-um-internettelefondienst-netzbetreiber-blocken-skype-auf-handys/494337.html.

21. **Brian Williamson; David Black; Thomas Punton.** The open Internet - A platform for growth. [En línea] 2011. [Citado el: 02 de Diciembre de 2011.] http://www.bbc.co.uk/aboutthebbc/reports/pdf/plumbriefing_oct2011.pdf.

22. **Wagner, Ben.** Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'. [En línea] 2009. [Citado el: 03 de Diciembre de 2011.] http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf.

23. **White, Bobby.** Watching What You See on the Web. [En línea] 2007. [Citado el: 16 de Diciembre de 2011.] http://online.wsj.com/article/SB119690164549315192.html.

24. **Clayton, Richard.** The Phorm "Webwise" System. [En línea] 2008. http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

25. **Sterling, Toby.** Boston.com. *Dutch parliament approves mobile 'net neutrality'.* [En línea] 2011. [Citado el: 27 de Ocutbre de 2011.] http://articles.boston.com/2011-06-22/business/29684368_1_net-neutrality-skype-messaging.

26. **FCC.** CONSENT DECREE. [En línea] 2005. [Citado el: 12 de Diciembre de 2011.] http://www.steptoe.com/assets/attachments/1311.pdf. DA 05-543.

27. **Mueller, Milton.** Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States. [En línea] 2011. [Citado el: 12 de Diciembre de 2011.] http://www.tprcweb.com/images/stories/2011%20papers/miltonmueller_2011.pdf.

28. **TorrentFreak.** TorrentFreak. *Comcast Throttles BitTorrent Traffic, Seeding Impossible.* [En línea] 2007. [Citado el: 27 de Octubre de 2011.] http://torrentfreak.com/comcast-throttles-bittorrent-traffic-seeding-impossible/.

29. **Cheng, Jacqui.** Ars Technica. *Comcast settles P2P throttling class-action for $16 million.* [En línea] 2010. [Citado el: 27 de Ocutbre de 2011.] http://arstechnica.com/tech-policy/news/2009/12/comcast-throws-16-million-at-p2p-throttling-settlement.ars.

30. **FCC.** MEMORANDUM OPINION AND ORDER. [En línea] 2008. [Citado el: 03 de Diciembre de 2011.] http://cyberlaw.stanford.edu/system/files/FccComcastOrder.pdf. FCC 08-183.

31. **CRTC.** Canadian Radio-television and Telecommunications Commission. *Canadian Association of Internet Providers (CAIP) - Application requesting certain orders directing Bell Canada to cease and desist from throttling its wholesale ADSL Access Services.* [En línea] [Citado el: 28 de Octubre de 2011.] http://www.crtc.gc.ca/PartVII/eng/2008/8622/c51_200805153.htm.

32. —. Telecom Decision CRTC 2008-108. [En línea] 2008. [Citado el: 03 de Diciembre de 2011.] http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm.

33. **BEREC.** BEREC report on the public consultation on the draft BEREC Guidelines on Transparency in the scope of Net Neutrality . [En línea] Diciembre de 2011. [Citado el: 28 de Diciembre de 2011.] http://www.erg.eu.int/doc/berec/bor/bor11_66_transparencyinput.pdf. BoR (11) 66.

34. —. A framework for Quality of Service in the scope of Net Neutrality. [En línea] Diciembre de 2011. [Citado el: 28 de Diciembre de 2011.] http://www.erg.eu.int/doc/berec/bor/bor11_53_qualityservice.pdf. BoR (11) 53.

35. **Mueller, Milton.** DPI Technology from the standpoint of Internet governance studies: An introduction. [En línea] 2011. [Citado el: 12 de Diciembre de 2011.] http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

36. **Finnie, Graham.** ISP Traffic Management Technologies: The State of the Art. [En línea] 2009. [Citado el: 12 de Diciembre de 2011.] http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

37. **Sandvine.** The Evolution of Network Traffic Optimization: Providing Each User Their Fair Share. [En línea] 2011. [Citado el: 12 de Diciembre de 2011.] http://www.sandvine.com/downloads/documents/Evolution_of_Traffic_Optimization.pdf.

38. **Klaus Mochalski; Hendrik Schulze.** Deep Packet Inspection Technology, Applications & Net Neutrality. [En línea] 2009. [Citado el: 12 de Diciembre de 2011.] http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf.

39. **ITU-T.** Network performance objectives for IP-based services. [Online] Febrero 2006. [Cited: Diciembre 23, 2011.] http://www.google.es/url?sa=t&rct=j&q=itu-t%20y.1541%202006&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fwftp3.itu.int%2Fpacket%2FBackground%2520Docs%2FY_1541-200602-prepub.doc&ei=psn1TsmmN4KZhQfJqYDMAQ&usg=AFQjCNEVhMANXl7z81K7k6zGgl8ySCz6MA&sig2=IXcWDS. Y.1541.

40. **Ixia.** Quality of Service (QoS) and Policy Management in Mobile Data Networks. [En línea] 2011. [Citado el: 08 de Diciembre de 2011.] http://www.ixiacom.com/pdfs/library/white_papers/policy_management.pdf.

41. **IETF.** IETF. *Integrated Services in the Internet Architecture: an Overview.* [En línea] Junio de 1994. [Citado el: 21 de Ocutubre de 2011.] http://www.ietf.org/rfc/rfc1633.txt. RFC 1633.

42. —. IETF. *Resource ReSerVation Protocol.* [En línea] Septiembre de 1997. [Citado el: 03 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc2205.txt. RFC 2205.

43. **Oram, Andy.** A Nice Way to Get Network Quality of Service? [En línea] 2002. [Citado el: 13 de Diciembre de 2011.] http://tim.oreilly.com/pub/a/network/2002/06/11/platform.html?page=1.

44. **IETF.** IETF. *An Architecture for Differentiated Services.* [En línea] Diciembre de 1998. [Citado el: 21 de Octubre de 2011.] http://www.ietf.org/rfc/rfc2475.txt. RFC 2475.

45. —. IETF. *Multiprotocol Label Switching Architecture.* [En línea] Enero de 2001. [Citado el: 2011 de Octubre de 2011.] http://www.ietf.org/rfc/rfc3031.txt. RFC 3031.

46. —. IETF. *A Framework for Policy-based Admission Control.* [En línea] Enero de 2000. [Citado el: 07 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc2753.txt. RFC 2753.

47. **Ericsson.** LTE – an introduction. [En línea] 2009. [Citado el: 13 de Diciembre de 2011.] http://lteuniversity.com/industry_resources1/m/ltewhitepapers/107.aspx.

48. **Cisco & Starent.** LTE Simplifying the Migration to 4G Networks. [En línea] 2010. [Citado el: 13 de Diciembre de 2011.] http://www.cisco.com/en/US/solutions/ns341/ns973/starent/whitepaper_c11-577763_v1.pdf.

49. **Inspira.** Introduction to the GGSN Node: a Building Block of Mobile Data Networks. [En línea] 2001. [Citado el: 13 de Diciembre de 2011.] http://student.ing-steen.se/IPv6/MIX/ggsn.intro.en.pdf.

50. **3GPP.** 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 1999). [En línea] 2002. [Citado el: 13 de Diciembre de 2011.] http://www.arib.or.jp/IMT-2000/V800Apr10/5_Appendix/R99/23/23107-390.pdf. 3GPP TS 23.107 V3.9.0 (2002-09).

51. **Mottishaw, Peter.** Policy control and charging for LTE networks. [En línea] 2009. [Citado el: 13 de Diciembre de 2011.] http://downloads.lightreading.com/wplib/openet/Openet_Policy_control_LTE.pdf.

52. **Alcatel-Lucent.** Introduction to Evolved Packet Core. [En línea] 2009. [Citado el: 13 de Diciembre de 2011.] http://lte.alcatel-lucent.com/locale/en_us/downloads/wp_evolved_packet_core.pdf.

53. **Ericsson.** Traffic inspection for visibility, control and new business opportunities. [En línea] 2010. [Citado el: 13 de Diciembre de 2011.] http://www.ericsson.com/res/docs/whitepapers/traffic_inspection.pdf.

54. **S. M. Chadchan ; C. B. Akki.** 3GPP LTE/SAE: An Overview. [En línea] 2010. [Citado el: 13 de Diciembre de 2011.] http://www.ijcee.org/papers/232-E271.pdf.

55. **Motorolla.** Long Term Evolution (LTE): A Technical Overview. [En línea] 2007. [Citado el: 13 de Diciembre de 2011.] http://www.motorola.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20Operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf.

56. **Brown, Gabriel.** LTE/SAE & the Evolved Packet Core: Technology Platforms & Implementation Choices. [En línea] [Citado el: 13 de Diciembre de 2011.] http://lte.alcatel-lucent.com/locale/en_us/downloads/wp_platform_and_implementation.pdf.

57. **3GPP.** 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 10). [En línea] 2010. [Citado el: 12 de Diciembre de 2011.] http://3gppprotocol.com/web_documents/23203-a00-policy-chrg-arch.doc. 3GPP TS 23.203 V10.0.0 (2010-06).

58. **Brown, Gabriel.** Evolved Packet Core & Policy Management for LTE. [En línea] 2010. [Citado el: 14 de Diciembre de 2011.] http://www.cisco.com/en/US/solutions/collateral/ns341/ns973/Cisco_LTE_Policy_Management_WP.pdf.

59. **ETSI.** Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control over Gx reference point (3GPP TS 29.212 version 9.4.0 Release 9). [En línea] 2010. [Citado el: 14 de Diciembre de 2011.] http://www.etsi.org/deliver/etsi_ts/129200_129299/129212/09.04.00_60/ts_129212v090400p.pdf. RTS/TSGC-0329212v940.

60. **Martin Ljungberg ; Aldo Bolle.** Mobile broadband second wave – differentiated offerings. [En línea] 2011. [Citado el: 20 de Diciembre de 2011.] http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2011/er_mobile_broadband_2nd_wave.pdf.

61. **SETSI.** Tecnologías de Banda Ancha y Convergencia de Redes. [En línea] 2009. [Citado el: 2011 de 12 de 21.] http://oa.upm.es/2697/2/BERROCAL_LIBRO_2009_01.pdf.

62. **Sandvine.** Sandvine Network Policy Control Architecture for Cable. [En línea] 2009. [Citado el: 14 de Diciembre de 2011.] http://www.sandvine.com/downloads/documents/Sandvine%20Policy%20Control%20for%20Cable.pdf.

63. **CableLabs.** Quality-of-Service: A DOCSIS/ PacketCable™ Perspective—Part I. [En línea] 2000. [Citado el: 24 de Diciembre de 2011.] http://www.cablelabs.com/news/newsletter/SPECS/MayJune2000/news.pgs/story5.html.

64. **Mohammed Hawa ; David W. Petr.** QoS Scheduling in Cable and Broadband Wireless Networks. [En línea] 2002. [Citado el: 14 de Diciembre de 2011.] http://129.237.125.27/publications/documents/Hawa2002_iwqos_paper.pdf.

65. **Cable Television Laboratories, Inc.** PacketCable™ 2.0 Quality of Service Specification. [En línea] 2008. [Citado el: 14 de Diciembre de 2011.] http://www.cablelabs.com/specifications/PKT-SP-QOS-I02-080425.pdf. PKT-SP-QOS-I02-080425.

66. **White, Gerry.** DEPLOYING ENHANCED IP SERVICES USING PACKETCABLETM MULTIMEDIA QOS CONTROL. [En línea] [Citado el: 14 de Diciembre de 2011.] http://www.motorola.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Cable%20Operators/Residential%20Access%20for%20Cable%20Operators%20(CH)/_Documents/static%20files/IP_PacketCable_Svcs-II_New.pdf.

67. **I. Vidal; J. Garcia ; F. Valera ; I. Soto ; A. Azcorra.** Integration of a QoS aware end user network within the TISPAN NGN solutions. [En línea] 2006. [Citado el: 24 de Diciembr de 2011.] http://www.it.uc3m.es/jgr/publicaciones/07-ividal-QoSNGNRGW.pdf.

68. **ETSI.** TISPAN Defining the Next Generation Network. [En línea] 2008. [Citado el: 24 de Diciembre de 2011.] http://docbox.etsi.org/Workshop/2008/200805_TISPANWORKSHOP/02_TISPAN_Muench.pdf.

69. **Brennan, Richard.** ETSI NGN Work: TISPAN Status. [En línea] 2006. [Citado el: 14 de Diciembre de 2011.] http://www.itu.int/ITU-T/worksem/h325/200605/presentations/s1p4-brennan.pdf.

70. **ETSI.** Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture. [En línea] 2011. [Citado el: 14 de Diciembre de 2011.] http://www.etsi.org/deliver/etsi_es/282000_282099/282003/03.05.01_60/es_282003v030501p.pdf. 282 003 V3.5.1 (2011-04).

71. **Daid, Cathal Mc.** Palo Wireless. *Overview and Comparison of QoS Control in Next Generation Networks.* [En línea] 2005. [Citado el: 24 de Octubre de 2011.] http://www.palowireless.com/3g/qos2.asp.

72. **Christian Esteve Rothenberg ; Andreas Roos.** A Review of Policy-Based Resource and Admission Control Functions in Evolving Access and Next Generation Networks. [En línea] 2008. [Citado el: 15 de Diciembre de 2011.] http://www.dca.fee.unicamp.br/~chesteve/pubs/review-racf-ngn-jnsm08.pdf.

73. **Wikipedia.** Wikipedia. *Deep Packet Inspection.* [En línea] [Citado el: 28 de Septiembre de 2011.] http://es.wikipedia.org/wiki/Deep_Packet_Inspection.

74. **Parsons, Christopher.** Deep Packet Inspection in Perspective:Tracing its lineage and surveillance potentials. [En línea] 2008. [Citado el: 19 de Diciembre de 2011.] http://christopher-parsons.com/Academic/WP_Deep_Packet_Inspection_Parsons_Jan_2009.pdf.

75. **Alok Madhukar ; Carey Williamson.** A Longitudinal Study of P2P Traffic Classification. [En línea] 2006. [Citado el: 15 de Diciembre de 2011.] http://biblioteca.universia.net/html_bura/ficha/params/title/longitudinal-study-of-p2p-traffic-classification/id/47809251.html.

76. **Allot Communications.** dpacket.org. *Digging Deeper Into Deep Packet Inspection (DPI).* [En línea] 2007. [Citado el: 05 de Octubre de 2001.] https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi.

77. **Erik Hjelmvik ; Wolfgang John.** Breaking and Improving Protocol Obfuscation. [En línea] 2010. [Citado el: 15 de Diciembre de 2011.] https://www.iis.se/docs/hjelmvik_breaking.pdf. TR No. 2010-05, ISSN 1652-926X.

78. **eMule.** eMule. *Protocol Obfuscation.* [En línea] [Citado el: 15 de Noviembre de 2011.] http://www.emule-project.net/home/perl/help.cgi?l=1&rm=show_topic&topic_id=848.

79. **Vuze.** Vuze Wiki. *Message Stream Encryption.* [En línea] [Citado el: 2011 de Noviembre de 2011.] http://wiki.vuze.com/w/Message_Stream_Encryption#Protocol_Objectives.

80. **Skype.** Skype. *Privacidad y seguridad.* [En línea] [Citado el: 15 de Noviembre de 2011.] https://support.skype.com/es/faq/FA31/Usa-Skype-cifrado.

81. **Gil, Miguel.** Deep Packet Inspection & Co: la preocupación por el control de Internet. [En línea] 2010. [Citado el: 16 de Diciembre de 2011.] http://www.davara.com/documentos/relacionados/sociedad/Nota_Enter_155.pdf.

82. **Jonathan Zittrain ; Benjamin Edelman.** Empirical Analysis of Internet Filtering in China. [En línea] 2003. [Citado el: 16 de Diciembre de 2011.] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-02.pdf. Research Publication No. 2003-02 4/2003.

83. **Network Strategy Partners.** The Business Case for an Integrated Policy and Charging Control (PCC) Solution in the Multimedia Core. [En línea] 2010. [Citado el: 16 de Diciembre de 2011.] http://www.cisco.com/en/US/solutions/collateral/ns341/ns973/ns1081/PCC_TCO__Whitepaper.pdf.

84. **Cisco.** Cisco ASR 5000 Multimedia Core Platform Data Sheet. [En línea] 2010. [Citado el: 16 de Diciembre de 2011.] http://www.cisco.com/en/US/prod/collateral/wireless/ps11035/ps11047/ps11072/data_sheet_c78-606223.pdf.

85. **Allot Communications.** Intelligent PCEF: Pure-play versus Embedded Solutions. [En línea] 2011. [Citado el: 16 de Diciembre de 2011.] http://www.maxtec.co.za/wp-content/uploads/2011/06/WP_PurePlay-vs-Embedded-PCEF_06-2011496428750.pdf.

86. **Schneider, Edward.** Seeking Alpha. *Deep Packet Inspection: An Interesting Investment Theme.* [En línea] Ocutbre de 2011. [Citado el: 07 de Noviembre de 2011.] http://seekingalpha.com/article/303715-deep-packet-inspection-an-interesting-investment-theme?source=yahoo.

87. **Sandvine.** Sandvine. *Sandvine Customers.* [En línea] [Citado el: 15 de Octubre de 2011.] http://www.sandvine.com/customers/.

88. —. Sandvine. *Policy Traffic Switch.* [En línea] [Citado el: 14 de Octubre de 2011.] http://www.sandvine.com/products/policy_traffic_switch.asp.

89. —. Sandvine Service Delivery Engine (SDE) Platform. [En línea] 2011. [Citado el: 16 de Diciembre de 2011.] http://www.sandvine.com/downloads/documents/Sandvine%20Service%20Delivery%20Engine%20Platform.pdf.

90. **Allot Communications.** Allot Communications. *Press Releases.* [En línea] [Citado el: 17 de Octubre de 2011.] http://www.allot.com/Press_Releases.html.

91. —. Allot Communications. *Allot Product Portfolio.* [En línea] [Citado el: 17 de Ocutbre de 2011.] http://www.allot.com/Products_Overview.html.

92. **Procera Networks.** Procera. *Company Background.* [En línea] [Citado el: 17 de Ocutbre de 2011.] http://www.proceranetworks.com/en/about-procera/company-background.html.

93. —. Procera. *PacketLogic Real-Time Enforcement.* [En línea] [Citado el: 17 de Octubre de 2011.] http://www.proceranetworks.com/en/products/plr-packetlogic-real-time-enforcement.html.

94. —. Procera. *PacketLogic Subscriber Manager.* [En línea] [Citado el: 17 de Octubre de 2011.] http://www.proceranetworks.com/en/psm-packetlogic-subscriber-manager.html.

95. **Ipoque.** Ipoque. *Products.* [En línea] [Citado el: 08 de Noviembre de 2011.] http://www.ipoque.com/en/products.

96. **Ericsson.** Ericsson. *Ericsson to acquire Redback Networks.* [En línea] 20 de Diciembre de 2006. [Citado el: 05 de Ocutbre de 2011.] http://www.ericsson.com/thecompany/press/releases/2006/12/1094314.

97. **Cisco.** Cisco. *Cisco has Acquired Starent Networks.* [En línea] Diciembre de 2009. [Citado el: 05 de Ocutbre de 2011.] http://www.cisco.com/web/about/ac49/ac0/ac1/ac259/starent.html.

98. —. Cisco SCE 8000 Service Control Engine Data Sheet. [En línea] 2008. [Citado el: 16 de Diciembre de 2011.] http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps9591/ps9613/data_sheet_c78-492987.pdf.

99. **Ericsson.** THIS IS ERICSSON. [En línea] 2011. [Citado el: 16 de Diciembre de 2011.] http://www.ericsson.com/res/thecompany/docs/this_is_ericsson_v5.pdf.

100. —. Ericsson. *Service Aware Support Node (SASN).* [En línea] [Citado el: 18 de Octubre de 2011.] http://www.ericsson.com/ourportfolio/products/service-aware-support-node-sasn?nav=fgb_101_256.

101. —. Ericsson. *GGSN-MPG, Evolved Packet Gateway.* [En línea] [Citado el: 18 de Octubre de 2011.] http://www.ericsson.com/ourportfolio/products/ggsn-mpg,-evolved-packet-gateway?nav=fgb_101_256.

102. **Infonetics Research.** Infonetics Research. *Mobile operators fueling hockey-stick growth in standalone deep packet inspection (DPI) market.* [En línea] [Citado el: 19 de Octubre de 2011.] http://www.infonetics.com/pr/2011/1H11-DPI-Deep-Packet-Inspection-Market-Highlights.asp.

103. **ABI Research .** ABI Research. *Mobile Network Optimization's $4.5 Billion Opportunity is Ripe for M&A Activity.* [En línea] [Citado el: 19 de Octubre de 2011.] https://www.abiresearch.com/press/3788-Mobile+Network+Optimization%E2%80%99s+%244.5+Billion+Opportunity+is+Ripe+for+M%26A+Activity.

104. **Light Reading.** Heavy Reading. *Mobile Broadband & the Rise of Policy: Technology Review & Forecast* . [En línea] [Citado el: 19 de Octubre de 2011.] http://www.heavyreading.com/details.asp?sku_id=2718&skuitem_itemid=1339.

105. **Bryan Veal ; Annie Foong.** Performance Scalability of a Multi-core Web Server. [En línea] 2007. [Citado el: 2011 de 17 de Diciembre.] http://www.cse.wustl.edu/ANCS/2007/papers/p57.pdf.

106. **ISOCORE.** Validation of Cisco SCE8000 . [En línea] 2009. [Citado el: 19 de Diciembre de 2011.] https://mail-attachment.googleusercontent.com/attachment?ui=2&ik=3d1ad04e34&view=att&th=13441c50467a5792&attid=0.3&disp=inline&safe=1&zw&saduie=AG9B_P8i__S9hCUu1un1T_AyAP_V&sadet=1324309717977&sads=Mu8MzBJX9DzreBWG3ITzen_AnNY.

107. **The Tolly Group.** Allot Communicatiions Net Enforcer AC-1010 Throughput and Functinality Evalutaion. [En línea] [Citado el: 19 de Diciembre de 2011.] https://mail-attachment.googleusercontent.com/attachment?ui=2&ik=3d1ad04e34&view=att&th=13441c50467a5792&attid=0.1&disp=inline&safe=1&zw&saduie=AG9B_P8i__S9hCUu1un1T_AyAP_V&sadet=1324309712904&sads=d24mcilSS3fs5_VQQxTLnNJHEfU.

108. **Ipoque.** PRX-10G Traffic Manager. [En línea] 2011. [Citado el: 19 de Diciembre de 2011.] https://mail-attachment.googleusercontent.com/attachment?ui=2&ik=3d1ad04e34&view=att&th=13441c50467a5792&attid=0.2&disp=inline&safe=1&zw&saduie=AG9B_P8i__S9hCUu1un1T_AyAP_V&sadet=1324309715671&sads=a0b7Ohs1L4EnkROVNS8Zivn6VMk.

109. **RadiSys.** DPI: DEEP PACKET INSPECTION MOTIVATIONS, TECHNOLOGY, AND APPROACHES FOR IMPROVING BROADBAND SERVICE PROVIDER ROI. [En línea] 2010. [Citado el: 17 de Diciembre de 2011.] http://embedded.communities.intel.com/servlet/JiveServlet/previewBody/6748-102-1-1821/DPI_WP_Final_12_8.pdf.

110. **JumpGen Systems.** Whitepaper: Deploying Network Services: Network Appliances vs. AdvancedTCA. [En línea] 2011. [Citado el: 17 de Diciembre de 2011.] http://www.jumpgen.com/company/network-appliance-whitepaper/.

111. **Damouny, Nabil.** Security Journal. *The World of Secure, Virtualized Networking.* [En línea] 24 de Septiembre de 2010. [Citado el: 13 de Octubre de 2011.] http://security.sys-con.com/node/1543915?page=0,0.

112. **Smith, David.** RTC Magazine. *Communications Processors vs. Network Processors: Programmable Data Plane Approaches.* [En línea] Febrero de 2006. [Citado el: 13 de Octubre de 2011.] http://rtcmagazine.com/articles/view/100479.

113. **Terry Nelms ; Mustaque Ahamad.** Packet Scheduling for Deep Packet Inspection on Multi-Core Architectures. [En línea] 2010. [Citado el: 17 de Diciembre de 2011.] http://www.deepdyve.com/lp/association-for-computing-machinery/packet-scheduling-for-deep-packet-inspection-on-multi-core-ZBzRpbWvTI.

114. **Damouny, Nabil.** Adapting x86-based ATCA Platforms to High-speed Networking. [En línea] 2010. [Citado el: 17 de Diciembre de 2011.] http://www.advancedtcasummit.com/English/Collaterals/Proceedings/2010/20101111_SpecTutorial_Damouny.pdf.

115. **Netronome.** The Evolution to Network Flow Processing. [En línea] 2008. [Citado el: 17 de Diciembre de 2011.] http://www.netronome.com/files/file/The%20Evolution%20to%20Network%20Flow%20Processing%20(5-09).pdf.

116. **Cisco.** The Cisco QuantumFlow Processor: Cisco's Next Generation Network Processor. [En línea] 2008. [Citado el: 17 de Diciembre de 2011.] http://www.cisco.com/en/US/prod/collateral/routers/ps9343/solution_overview_c22-448936.pdf.

117. **Netronome.** NFP-3200 Network Flow Processor. [En línea] 2009. [Citado el: 17 de Diciembre de 2011.] http://www.netronome.com/files/file/Netronome%20NFP%20Product%20Brief%20(3-09).pdf.

118. **NetLogic.** NetLogic Microsystems. *XLP832 Processor Product Brief.* [En línea] [Citado el: 13 de Octubre de 2011.] http://www.netlogicmicro.com/Products/ProductBriefs/MultiCore/XLP832.htm.

119. **Cavium.** Cavium. *OCTEON II CN68XX Multi-Core MIPS64 Processors.* [En línea] [Citado el: 13 de Octubre de 2011.] http://www.caviumnetworks.com/OCTEON-II_CN68XX.html.

120. **Freescale.** Freescale. *QorIQ Advanced Multiporcessing (AMP) Series.* [En línea] [Citado el: 13 de Ocutbre de 2011.] http://www.freescale.com/webapp/sps/site/overview.jsp?code=QORIQ_AMP.

121. **Linux Foundation.** The Linux Foundation. *NAPI.* [En línea] 19 de Noviembre de 2009. [Citado el: 05 de Ocutbre de 2011.] http://www.linuxfoundation.org/collaborate/workgroups/networking/napi.

122. **Microsoft.** MSDN. *Receive-Side Scaling Enhancements in Window.* [En línea] 05 de Noviembre de 2008. [Citado el: 05 de Octubre de 2011.] http://msdn.microsoft.com/en-us/windows/hardware/gg463253.

123. **Wang Cong ; Joe Morris ; Wang Xiaojun.** HIGH PERFORMANCE DEEP PACKET INSPECTION ON MULTI-CORE PLATFORM. [En línea] 2009. [Citado el: 18 de Diciembre de 2011.] http://doras.dcu.ie/15525/1/wang2.pdf.

124. **Cisco.** Cisco ASR 5000 Series Poduct Overview Release 8.x and 9. [En línea] 2010. [Citado el: 18 de Diciembre de 2011.] http://www.cisco.com/en/US/docs/wireless/asr_5000/8_x_9.0/OL-22956-02_Change_Reference.pdf.

125. **Randy Smith ; Cristian Estan ; Somesh Jha ; Shijin Kong.** Deflating the Big Bang: Fast and Scalable Deep Packet Inspection with Extended Finite Automata. [En línea] 2008. [Citado el: 20 de Diciembre de 2011.] http://pages.cs.wisc.edu/~estan/publications/bigbang.pdf.

126. **Po-Ching Lin ; Ying-Dar Lin ; Tsern-Huei Lee ; Yuan-Cheng Lai.** Using String Matching for Deep Packet Inspection. [En línea] 2008. [Citado el: 20 de Diciembre de 2011.] http://speed.cis.nctu.edu.tw/~ydlin/string%20matching.pdf.

127. **Fang Yu ; Zhifeng Chen ; Yanlei Diao ; T. V. Lakshman ; Randy H. Katz.** Fast and Memory-Efficient Regular Expression Matching for Deep Packet Inspection. [En línea] 2006. [Citado el: 19 de Diciembre de 2011.] http://research.microsoft.com/en-us/people/fangyu/ancs06.pdf.

128. **J. E. Hopcroft, R. Motwani, J. D. Ullman.** Introduction to Automata Theory, Languages and Computation. [En línea] 2001. [Citado el: 20 de Diciembre de 2011.] http://es.scribd.com/doc/3528945/Introduction-to-automata-theory-languages-and-computation-part-1.

129. **Sailesh Kumar ; Jonathan Turner ; John Williams.** *Advanced Algorithms for Fast and Scalable Deep Packet Inspection.* s.l. : Washington University, Cisco Systems, 2006.

130. **Canvium.** OCTEON II CN68XX Multi-Core MIPS64 Processors Product Brief. [En línea] 2011. [Citado el: 06 de Octubre de 2011.] http://www.caviumnetworks.com/pdfFiles/CN68XX_PB_Rev1.pdf.

131. **IETF.** IETF. *Session Initiation Protocol.* [En línea] Junio de 2002. [Citado el: 29 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc3261.txt. RFC 3261.

132. —. IETF. *A Transport Protocol for Real-Time Applications.* [En línea] Julio de 2003. [Citado el: 29 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc3550.txt. RFC 3550.

133. —. IETF. *The TLS Protocol Version 1.0.* [En línea] Enero de 1999. [Citado el: 29 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc2246.txt. RFC 2246.

134. —. IETF. *The Secure Real-time Transport Protocol.* [En línea] Marzo de 2004. [Citado el: 29 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc3711.txt. RFC 3711.

135. —. IETF. *Simple Mail Transfer Protocol.* [En línea] Abril de 2001. [Citado el: 2011 de Noviembre de 29.] http://www.ietf.org/rfc/rfc2821.txt. RFC 2821.

136. —. IETF. *Ineternet Message Access Protocol - Version 4rev1.* [En línea] Diciembre de 1996. [Citado el: 29 de Noviembre de 2011.] http://tools.ietf.org/html/rfc2060. RFC 2060.

137. —. IETF. *Post Office Protocol - Version 3.* [En línea] Mayo de 1996. [Citado el: 29 de Noviembre de 2011.] http://www.ietf.org/rfc/rfc1939.txt. RFC 1939.

138. **Comisión Europea.** Declaración de la Comisión sobre la neutralidad de Internet. [En línea] 2009. [Citado el: 20 de Diciembre de 2011.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:308:0002:0002:ES:PDF. 2009/C 308/02.

139. —. Report on the public consultation on 'The open internet and net neutrality in Europe'. [En línea] 2010. [Citado el: 20 de Diciembre de 2011.] http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf.

140. —. The open internet and net neutrality in Europe. [En línea] 2011. [Citado el: 20 de Diciembre de 2011.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:EN:PDF.

141. **European Parlament.** Network Neutrality: Challenges and responses in the EU and in the U.S. [En línea] 2011. [Citado el: 20 de Diciembre de 2011.] http://www.europarl.europa.eu/document/activities/cont/201105/20110523ATT20073/20110523ATT20073EN.pdf. IP/A/IMCO/ST/2011-02.

142. **Tech Law Journal.** Tech Law Journal. *FCC Classifies DSL as Information Service.* [En línea] Agosto de 2005. [Citado el: 2011 de 09 de 2011.] http://www.techlawjournal.com/topstories/2005/20050805a.asp.

143. **FCC.** POLICY STATEMENT. [En línea] 2005. [Citado el: 20 de Diciembre de 2011.] http://www.plateautel.com/docs/FCC_05_151A1.pdf.

144. **United States Court of Appeals For The Disctrict Of Columbia Circuit.** COMCAST CORPORATION v. FEDERAL COMMUNICATIONS COMMISSION AND UNITED. [En línea] 2010. [Citado el: 20 de Diciembre de 2011.] https://www.eff.org/files/Comcast%20v%20FCC%20(DC%20Cir%202010).pdf.

145. **FCC.** REPORT AND ORDER: Preserving the Open Internet. [En línea] [Citado el: 20 de Diciembre de 2011.] http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf. FCC 10-201.

146. **MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES; SUBSECRETARÍA DE TELECOMUNICACIONES DE CHILE.** CONSAGRA EL PRINCIPIO DE NEUTRALIDAD EN LA RED PARA LOS CONSUMIDORES Y USUARIOS DE INTERNET. [En línea] 2010. [Citado el: 20 de Diciembre de 2011.] http://www.leychile.cl/Navegar?idNorma=1016570&buscar=NEUTRALIDAD+DE+RED. LEY NÚM. 20.453.

147. —. Regalmento que regula las características y condiciones de la Neutralidad de Red en el servicio de acceso a Internet. [En línea] 2010. [Citado el: 28 de Diciembre de 2011.] http://www.subtel.gob.cl/prontus_subtel/site/artic/20110311/asocfile/20110311195708/10d_0368.pdf. Decreto Nº 368.

148. **SUBTEL.** SUBTEL INSTRUYE Y EXIGE A EMPRESAS DE INTERNET MAYOR TRANSPARENCIA EN PLANES DE BANDA ANCHA POR LEY DE NEUTRALIDAD DE RED. *Resolución Exenta Nº 6267.* [En línea] Noviembre de 2011. [Citado el: 20 de Diciembre de 2011.] http://www.subtel.gob.cl/prontus_subtel/site/artic/20111102/asocfile/20111102160813/11r_6267.pdf.

149. **Gobierno de Holanda.** Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen. [En línea] 2011. [Citado el: 20 de Diciembre de 2011.] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/06/01/voorstel-van-wet-tot-wijziging-van-de-telecommunicatiewet-ter-implementatie-van-de-herziene-telecommunicatierichtlijnen.html.

150. Discussion points and initial policy directions on Internet and network neutrality. [En línea] Mayo de 2010. [Citado el: 28 de Diciembre de 2011.] http://www.arcep.fr/uploads/tx_gspublication/consult-net-neutralite-200510-ENG.pdf.

151. **OFCOM.** Traffic Management and 'net neutrality'. [En línea] Junio de 2010. [Citado el: 28 de Diciembre de 2011.] http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf.

152. —. Ofcom's approach to net neutrality. [En línea] Noviembre de 2011. [Citado el: 28 de Diciembre de 2011.] http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf.

153. **PTS.** Open networks and services. [En línea] 2009. [Citado el: 20 de Diciembre de 2011.] http://www.pts.se/en-gb/Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/.

154. **CRTC.** Telecom Public Notice CRTC 2008-19 Notice of consultation and hearing. [En línea] 2008. [Citado el: 19 de Diciembre de 2011.] http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm. 8646-C12-200815400.

155. —. Telecom Regulatory Policy. [En línea] 2009. [Citado el: 20 de Diciembre de 2011.] http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm. CRTC 2009-657.

156. **NPT.** Network neutrality Guidelines for Internet neutrality. [En línea] 2009. [Citado el: 19 de Diciembre de 2011.] http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf.

157. **Izumi Aizu ; Judit Bayer.** BEYOND NETWORK NEUTRALITY: THE STATE OF PLAY IN JAPANESE TELECOMMUNICATION COMPETITION. [En línea] 2009. [Citado el: 20 de Diciembre de 2011.] http://tja.org.au/index.php/tja/article/view/111.

158. **Ipoque.** OpenDPI Integration Manual. [En línea] 2009. [Citado el: 20 de Diciembre de 2011.] http://code.google.com/p/opendpi/downloads/detail?name=OpenDPI-Manual.pdf.