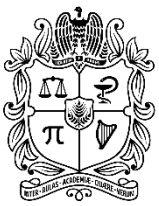


UNIVERSIDAD
NACIONAL
DE COLOMBIA

Lineamiento técnico para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS)

Mauricio Alexander Vargas Rodríguez

Universidad Nacional de Colombia

Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial

Bogotá, Colombia

2021

Lineamiento técnico para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS)

Mauricio Alexander Vargas Rodríguez

Tesis de investigación presentada como requisito parcial para optar al título de:

Magister en Telecomunicaciones

Directora:

Ph.D. Ingrid Patricia Páez Parra

Codirector:

Ph.D. Ernesto Cadena Muñoz

Línea de Investigación:

Redes y Sistemas de Telecomunicaciones

Universidad Nacional de Colombia

Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial

Bogotá, Colombia

2021

Dedicado a mi madre y a mi familia, combustible que me mantiene siempre adelante.

Declaración de obra original

Yo declaro lo siguiente:

He leído el Acuerdo 035 de 2003 del Consejo Académico de la Universidad Nacional. «Reglamento sobre propiedad intelectual» y la Normatividad Nacional relacionada al respeto de los derechos de autor. Esta disertación representa mi trabajo original, excepto donde he reconocido las ideas, las palabras, o materiales de otros autores.

Cuando se han presentado ideas o palabras de otros autores en esta disertación, he realizado su respectivo reconocimiento aplicando correctamente los esquemas de citas y referencias bibliográficas en el estilo requerido.

He obtenido el permiso del autor o editor para incluir cualquier material con derechos de autor (por ejemplo, tablas, figuras, instrumentos de encuesta o grandes porciones de texto).

Por último, he sometido esta disertación a la herramienta de integridad académica, definida por la universidad.

_____

Mauricio Alexander Vargas Rodríguez

Fecha 08/06/2021

Agradecimientos

Quiero expresar mis agradecimientos especiales al Ing. Ernesto Cadena Muñoz, por su apoyo, motivación y consejos en la realización de este trabajo.

A la Dra. Ingrid Patricia Páez por toda su colaboración, disposición y asesoría para la culminación de esta tesis.

A la Dra. Zoila Ramos de Flórez por la inspiración y ejemplo a seguir en la vida académica.

A Xavier Marichal y Telecapp por las asesorías, disposición y aportes en las temáticas desarrolladas en la presente investigación.

A la Universidad Nacional de Colombia – Sede Bogotá y su cuerpo docente, por la oportunidad de cursar esta maestría y el apoyo brindado a lo largo de la misma, particularmente en la participación en la V Conferencia científica de Telecomunicaciones, Tecnologías De La Información Y Comunicaciones realizada en la Isla Santa Cruz - Galápagos - Ecuador.

A Cintel, el SENA y el grupo de investigación GICS por permitir hacer uso de la infraestructura necesaria para la realización de las pruebas técnicas necesarias en el desarrollo de esta tesis y la oportunidad de poner en práctica mis conocimientos adquiridos en mi vida profesional.

A mi familia y a mi madre por su apoyo incondicional, paciencia y consejos para lograr todos mis objetivos trazados.

Resumen

Lineamiento técnico para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS)

Esta tesis de investigación busca generar un lineamiento técnico para la provisión de Calidad de Servicio (QoS) en interconexión de extremo a extremo bajo IP Multimedia Subsystem (IMS), revisando los estándares, normas, procedimientos, metodologías, recomendaciones, lineamientos y buenas prácticas, encontradas en organismos internacionales e industria, sustentadas en la normativa vigente, caracterizando los parámetros de calidad de los servicios convergentes (voz, datos y video) y evaluando el impacto técnico de la negociación de los parámetros de QoS interdominio de dichos servicios en un entorno emulado, mediante el desarrollo de una metodología sistemática, sustentada en el enfoque cuantitativo.

Se plantea que el problema central radica en brindar QoS consistente extremo a extremo en un servicio IP, de tal manera que se establezcan los requisitos de QoS solicitados por el cliente, cumpliendo con la normativa vigente cuando en el despliegue de infraestructura de servicio se involucran dos o más operadores, siendo redes autónomas, cuyos dominios administrativos se gestionan de acuerdo con sus políticas, sus topologías internas y mecanismos de QoS que dependen de sus dispositivos y otros requisitos de gestión que no son técnicos. En este sentido, el lineamiento brinda las herramientas necesarias para el diseño, implementación, mantenimiento y optimización de redes de telecomunicaciones relacionadas con QoS, dada la complejidad de las tecnologías subyacentes y su integración en el proceso de interconexión.

Palabras clave: BGP, DiffServ, IMS, Interconexión, MPLS, QoS, VPN.

Abstract

Technical guideline for the provision of end-to-end Quality of Service (QoS) in interconnection under IP Multimedia Subsystem (IMS)

This research thesis seeks to generate a technical guideline for the provision of end-to-end Quality of Service (QoS) in interconnection under IP Multimedia Subsystem (IMS), reviewing the standards, norms, procedures, methodologies, the recommendations, guidelines, and good practices, found in international organizations and industry, supported by current regulations, by characterizing the quality parameters for convergent services (voice, data, and video) and evaluating the technical impact of negotiation of the inter-domain QoS parameters of said services in an emulated environment, through the development of a systematic methodology supported by the quantitative approach.

It is posed that the central problem lies in providing consistent end-to-end QoS in an IP service in such a way that the QoS requirements requested by the client are set, complying with current regulations when the deployment of service infrastructure is involved between two or more operators, being autonomous networks, whose administrative domains are managed according to their policies, their internal topologies, and QoS mechanisms that depend on their devices and other non-technical management requirements. In this sense, the guideline provides the necessary tools in the design, implementation, maintenance, and optimization of telecommunications networks related to QoS, given the complexity of the related technologies and their integration in the interconnection processes.

Keywords: BGP, DiffServ, IMS, Interconnection, MPLS, QoS, VPN.

Esta tesis de maestría se sustentó el 16 de septiembre de 2021 a las 09:00am,
y fue evaluada por los siguientes jurados:

Jorge Eduardo Ortiz Triviño Ph.D.
Universidad Nacional de Colombia

Diego Fernando Rueda Pepinosa Ph.D.
Universitat de Girona

Contenido

Pág.

Lista de figuras ..... **XVII**

Lista de tablas ..... **XXIII**

Lista de abreviaturas ..... **XXVI**

Introducción **1**
Descripción del problema 2
Objetivos 3
a. Objetivo general 3
b. Objetivos específicos 3
Alcances y limitaciones 3
Metodología 3
Estructura del documento 5

1. Antecedentes y fundamentos teóricos **7**
1.1 Redes de próxima generación (NGN) 8
1.2 IP Multimedia Subsystem 9
1.3 Interconexión 13
1.3.1 Interconexión en IMS 13
1.3.2 Roaming en IMS 16
1.4 Consideraciones respecto a la QoS 17
1.4.1 Puntos de vista de la QoS 20
1.4.2 Métricas de desempeño en QoS 22
1.4.3 Mean Opinion Score (MOS) 22
1.5 Parámetros de desempeño para servicios IP en redes de extremo a extremo 23
1.5.1 Concatenación de secciones de la red y sus valores de QoS 24
1.5.2 Definiciones de clases de QoS de las redes IP 26
1.6 Marcos de referencia para la QoS 29
1.6.1 Marco de referencia de la IETF 29
1.6.2 Marco de referencia de la UIT 31
1.7 Calidad de Servicio en IMS 32
1.7.1 Arquitecturas de QoS basadas en políticas 33
1.8 Trabajos relacionados en el área de investigación 36
1.9 Herramientas de emulación 39
1.9.1 Virtualización 39
1.9.2 Emuladores de red 40
1.9.3 Entornos de núcleo IMS 40
1.9.4 Servidores IPTV 41

1.9.5 Tecnologías de contenedores 42
1.9.6 Monitores de tráfico SIP 42
1.9.7 Softphone 43
1.9.8 Herramientas de medición de tráfico de red 43

2. Caracterización de los parámetros de QoS para el despliegue de servicios convergentes bajo la arquitectura IMS en interconexión 44
2.1 Necesidad de la QoS en la prestación de servicios 45
2.2 Requerimientos en redes de transporte (IP Backhaul) 45
2.2.1 Equipos de Routing & Switching 48
2.2.2 Enlaces de transmisión de alta capacidad 48
2.2.3 Protocolos de transporte, gestión y monitoreo 48
2.2.4 Elementos de la red de acceso radio IP (IP RAN) 49
2.3 Protocolos de enrutamiento dinámico 51
2.3.1 Sistemas autónomos (AS) 52
2.3.2 Consideraciones para el diseño de redes convergentes 54
2.3.3 Funcionamiento desde las capas de enlace (L2) hasta la capa de red (L3) 54
2.3.4 Protocolo OSPF (Open Shortest Path First) 56
2.3.5 Protocolo BGP (Border Gateway Protocol) 57
2.3.6 BGP Route Reflector (RR) 57
2.4 Protocolo MPLS (Multiprotocol Label Switch) 59
2.4.1 Arquitectura MPLS 60
2.4.2 Operaciones y distribución de etiquetas 62
2.4.3 Distribución de etiquetas con LDP 62
2.5 Arquitectura MPLS VPN 63
2.5.1 Conceptos y tipos de VPN basadas en MPLS 63
2.5.2 Comparativo entre L2VPN y L3 basadas en MPLS 65
2.5.3 Conceptos relacionados con VPN de capa 2 (L2VPN) basada en MPLS 66
2.5.4 Conceptos relacionados con VPN de capa 3 (L3VPN) basada en MPLS 67
2.6 Arquitectura seamless MPLS 68
2.6.1 Tipos de configuración seamless MPLS 69
2.7 Modelos de QoS en MPLS 71
2.7.1 Modelo de Servicios Integrados (IntServ) 71
2.7.2 Modelo de servicios diferenciados (DiffServ) 72
2.7.3 Elementos de DiffServ 73
2.7.4 Campo de Servicios Diferenciados 75
2.8 Tipos de tráfico 78
2.8.1 Elasticidad de una aplicación 79
2.8.2 Aplicaciones no interactivas o por lotes 79
2.8.3 Aplicación interactiva 80
2.8.4 Aplicaciones de voz y video 80
2.9 QoS en IP RAN 81
2.9.1 4G LTE QoS Identifier (QCI) 81
2.9.2 5G NR QoS Identifier (5QI) 82
2.10 Herramientas para el manejo de QoS 83
2.10.1 Clasificación y marcado 84
2.10.2 Encolamiento (queuing) y organización del tráfico (scheduling) 85
2.10.3 Vigilancia de tráfico (Policing) 86
2.10.4 Modelado de tráfico (Shaping) 88
2.10.5 Evasión de la congestión 89

2.10.6 Ecuaciones para el acondicionamiento del tráfico 90

3. Evaluación del impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video 93
3.1 Diseño de red para la interconexión de redes IMS entre proveedores para la prestación de servicios interdominio 94
3.2 Conectividad de extremo a extremo 96
3.2.1 Conectividad VPN intra-AS seamless MPLS en interconexión 96
3.2.2 Conectividad VPN inter-AS seamless MPLS en interconexión 96
3.3 Análisis del diseño propuesto 97
3.4 Caracterización del tráfico de la red 98
3.5 Implementación de escenarios en el entorno emulado 99
3.6 Metodología de evaluación de parámetros de QoS para la conectividad intra-AS e inter-AS seamless MPLS L2VPN y L3VPN 105
3.7 Evaluación de la conectividad intra-AS e inter-AS seamless MPLS L2VPN sin QoS 106
3.7.1 Conectividad L2VPN intra-AS sin QoS 107
3.7.2 Conectividad L2VPN inter-AS sin QoS 113
3.7.3 Análisis comparativo de los escenarios L2VPN intra-AS e inter-AS sin QoS 118
3.8 Evaluación de la conectividad intra-AS e inter-AS seamless MPLS L3VPN sin QoS 119
3.8.1 Conectividad L3VPN intra-AS sin QoS 119
3.8.2 Conectividad L3VPN inter-AS sin QoS 126
3.8.3 Análisis comparativo de los escenarios L3VPN intra-AS e inter-AS sin QoS 132
3.9 Diseño e implementación de políticas de QoS 133
3.9.1 Clasificación y marcado del tráfico 134
3.9.2 Encolamiento y organización del tráfico 135
3.9.3 Acondicionamiento del tráfico 137
3.10 Evaluación de políticas de QoS 139
3.10.1 Conectividad L2VPN intra-AS con QoS 139
3.10.2 Conectividad L2VPN inter-AS con QoS 146
3.10.3 Análisis comparativo de los escenarios L2VPN intra-AS e inter-AS con QoS 152
3.10.4 Conectividad L3VPN intra-AS con QoS 153
3.10.5 Conectividad L3VPN inter-AS con QoS 160
3.10.6 Análisis comparativo de los escenarios L3VPN intra-AS e inter-AS con QoS 166

4. Definición de los lineamientos técnicos para la provisión de QoS extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios de voz, datos y video 169
4.1 Actores del negocio y relaciones 170
4.1.1 Actores del negocio 170
4.1.2 Relaciones entre los actores del negocio 171
4.2 Aspectos de la QoS en interconexión en NGN 172
4.2.1 Desafíos técnicos 172
4.2.2 Desafíos comerciales 173
4.2.3 Desafío regulatorio 174
4.3 Entorno regulatorio 174
4.3.1 Regulación de la QoS definida por la UIT 175
4.3.2 Documentos de la CRC relacionados con los indicadores de calidad 176

4.4 Metodologías para el aseguramiento de la QoS y la QoE 178
4.4.1 Sistemas de medición de QoS/QoE 179
4.4.2 Modelo de red para mediciones de la QoS 180
4.4.3 Metodologías de evaluación de la calidad 181
4.5 Proceso para la provisión de QoS extremo a extremo 182
4.6 Lineamiento técnico 184

5. Conclusiones, recomendaciones y contribuciones 189
5.1 Conclusiones 189
5.2 Recomendaciones 192
5.3 Contribuciones 193

A. Valores recomendados de PHB y DSCP 197

B. Anexo: Configuración de la red de transporte L2VPN 199

C. Anexo: Configuración de la red de transporte L3VPN 216

D. Anexo: Configuración del servidor SIP Kamailio IMS 235

Bibliografía 247

Lista de figuras

Pág.

Figura 0-1 Metodología propuesta para el desarrollo del proyecto de tesis. 4
Figura 1-1 Arquitecturas de telecomunicaciones horizontales y verticales [12]..... 8
Figura 1-2 Arquitectura IMS por capas y redes de acceso [16]..... 11
Figura 1-3 Componentes de la arquitectura IMS por capas [21]..... 12
Figura 1-4 Modelo IPX [26]..... 14
Figura 1-5 Arquitectura de referencia Inter IMS NNI [27] 15
Figura 1-6 Ejemplo de alto nivel de comunicación de voz y video basada en VoIMS [29] 15
Figura 1-7 Roaming en IMS [26]..... 16
Figura 1-8 Criterios de funcionamiento de la QoS [31]..... 17
Figura 1-9 Puntos de vista técnicos y no-técnicos de la calidad de servicio [25]..... 18
Figura 1-10 Calidad de servicio extremo a extremo [25] 19
Figura 1-11 Puntos de vista sobre QoS [25] 21
Figura 1-12 Trayecto de referencia para la QoS de UNI a UNI [25], [42]..... 24
Figura 1-13 Método de mejor esfuerzo [43] 29
Figura 1-14 Transmisión de información al aplicar mecanismos de QoS [43] 30
Figura 1-15 Marco de referencia de QoS de la UIT-T [25] 31
Figura 1-16 Gestión de QoS entre dominios [16]..... 33
Figura 1-17 Arquitectura IETF de Control de Admisión basada en políticas [53] 34
Figura 1-18 Arquitectura ETSI TISPAN RACS [53] 35
Figura 1-19 Arquitectura 3GPP PCC [53] 36
Figura 2-1 IP Backhaul [94] 46
Figura 2-2 Interconexión regional entre diversos backbone IP [94] 46
Figura 2-3 Modelo de red jerárquico [98] 47
Figura 2-4 Tipos de enlaces de transmisión [96] 48
Figura 2-5 Arquitectura de la red de telefonía móvil [96] 49
Figura 2-6 Elementos de la red de acceso radio IP (IP RAN) [96] 50
Figura 2-7 Estructura de la IP RAN móvil [96] 50
Figura 2-8 Protocolos de enrutamiento dinámico [98] 51
Figura 2-9 Sistemas autónomos y su interconexión [94] 53
Figura 2-10 Sistema autónomo en IP RAN [96]..... 53
Figura 2-11 Funcionamiento desde las capas de enlace (L2) hasta la capa de red (L3) [96] 55
Figura 2-12 Configuración de topología en malla [99] 57

Figura 2-13 Configuración con Route Reflector [99] 58
Figura 2-14 Una ruta aprendida de un cliente que no es RR se anuncia a los clientes RR pero no a los clientes que no son RR [99] 58
Figura 2-15 Una ruta aprendida de un cliente RR se anuncia tanto a clientes RR como a clientes no RR [99] 59
Figura 2-16 Una ruta aprendida de un vecino eBGP se anuncia tanto a clientes RR como a clientes no RR [99] 59
Figura 2-17 Cabecera MPLS [100] 59
Figura 2-18 Arquitectura MPLS [97] 61
Figura 2-19 Arquitectura MPLS VPN [97] 63
Figura 2-20 Sites [96] 64
Figura 2-21 Arquitectura seamless MPLS [96] 68
Figura 2-22 Intra-AS seamless MPLS [96] 69
Figura 2-23 Inter-AS seamless MPLS [96] 70
Figura 2-24 Inter-AS seamless MPLS HVPN [96] 70
Figura 2-25 QoS en IP RAN [96] 71
Figura 2-26 Arquitectura BGP MPLS-TE IP-VPN [95] 74
Figura 2-27 Cabecera IPv4 [97] 75
Figura 2-28 Campo ToS parámetros equivalentes [95], [106] 76
Figura 2-29 Valores de DSCP y PHB según el RFC 4594 [95], [106], [107] 78
Figura 2-30 Aquitectura para QoS en IP RAN [96] 81
Figura 2-31 Proceso de aplicación de políticas de QoS en Diffserv en un router [106] 83
Figura 2-32 Clasificación y marcado del tráfico [106] 84
Figura 2-33 Encolamiento (queuing) y organización del tráfico (scheduling) [108] 85
Figura 2-34 Comportamiento típico del tráfico generado por un usuario [108] 87
Figura 2-35 Vigilancia de tráfico (Policing) [108] 88
Figura 2-36 Modelado de tráfico (shaping) [108] 89
Figura 2-37 Evasión de la congestión [108] 89
Figura 3-1 Diseño de red para la interconexión de redes IMS entre proveedores para la prestación de servicios interdominio 94
Figura 3-2 Conectividad VPN intra-AS seamless MPLS en interconexión 96
Figura 3-3 Conectividad VPN inter-AS seamless MPLS en interconexión 97
Figura 3-4 Diseño de interconexión propuesto a emular 98
Figura 3-5 Topología de red para L2VPN 101
Figura 3-6 Topología de red para L3VPN 101
Figura 3-7 Core IMS en Kamailio emulado en QEMU 102
Figura 3-8 Configuración de usuarios en el HSS de Fokus 103
Figura 3-9 Configuración de UE en Zoiper 104
Figura 3-10 Canal de streaming en IPTV creado en Wowza Streaming Server 104
Figura 3-11 Detalles de los códecs de audio y video utilizados por el canal de streaming IPTV en Wowza Streaming Engine 105
Figura 3-12 Registro SIP UE con conectividad intra-AS seamless MPLS L2VPN sin QoS 109

Figura 3-13 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS 109
Figura 3-14 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS 110
Figura 3-15 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS en HOMER SIP 111
Figura 3-16 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine 111
Figura 3-17 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine . 112
Figura 3-18 Pérdidas de cuadros del video, congelamiento de imagen y sonido entrecortado del servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine 112
Figura 3-19 Registro SIP UE con conectividad inter-AS seamless MPLS L2VPN sin QoS 115
Figura 3-20 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS 115
Figura 3-21 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS 116
Figura 3-22 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS en HOMER SIP 116
Figura 3-23 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine 117
Figura 3-24 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine . 117
Figura 3-25 Pérdidas de cuadros, congelamiento en las imágenes y cortes en el sonido del servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine 118
Figura 3-26 Registro SIP UE con conectividad intra-AS seamless MPLS L3VPN sin QoS 122
Figura 3-27 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS 122
Figura 3-28 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS 123
Figura 3-29 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS en HOMER SIP 124
Figura 3-30 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine 124
Figura 3-31 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine . 125
Figura 3-32 Pérdidas de cuadros y congelamiento en las imágenes del servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine 125

Figura 3-33 Registro SIP UE con conectividad inter-AS seamless MPLS L3VPN sin QoS 128
Figura 3-34 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS 128
Figura 3-35 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS 129
Figura 3-36 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS en HOMER SIP 130
Figura 3-37 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine 130
Figura 3-38 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine . 131
Figura 3-39 Pérdidas de cuadros, congelamiento en las imágenes y cortes en el sonido del servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine 131
Figura 3-40 Sitio de aplicación de políticas de QoS 134
Figura 3-41 Organización del tráfico y distribución del ancho de banda en colas 136
Figura 3-42 Registro SIP UE con conectividad intra-AS seamless MPLS L2VPN con QoS 142
Figura 3-43 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS 142
Figura 3-44 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN con QoS 143
Figura 3-45 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN con QoS en HOMER SIP 144
Figura 3-46 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 144
Figura 3-47 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 145
Figura 3-48 Reproducción de video en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 145
Figura 3-49 Registro SIP UE con conectividad inter-AS seamless MPLS L2VPN con QoS 148
Figura 3-50 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS 149
Figura 3-51 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS 149
Figura 3-52 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS en HOMER SIP 150
Figura 3-53 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 151
Figura 3-54 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 151

Figura 3-55 Reproducción de video en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine 152
Figura 3-56 Registro SIP UE con conectividad intra-AS seamless MPLS L3VPN con QoS 156
Figura 3-57 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS 156
Figura 3-58 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS 157
Figura 3-59 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS en HOMER SIP 158
Figura 3-60 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 158
Figura 3-61 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 159
Figura 3-62 Reproducción de video en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 159
Figura 3-63 Registro SIP UE con conectividad inter-AS seamless MPLS L3VPN con QoS 162
Figura 3-64 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS 163
Figura 3-65 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS 163
Figura 3-66 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS en HOMER SIP 164
Figura 3-67 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 165
Figura 3-68 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 165
Figura 3-69 Reproducción de video en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine 165
Figura 4-1 Actores del negocio y relaciones [26] 170
Figura 4-2 Aspectos de la QoS en interconexión en NGN [63] 172
Figura 4-3 Actividades de regulación de la QoS definidas por la UIT [25] 175
Figura 4-4 Modelo de red para mediciones de QoS [25] 181
Figura 4-5 Percepciones del cliente y el proveedor de servicio [25] 182
Figura 4-6 Proceso para la provisión de QoS extremo a extremo [119] 183
Figura 4-7 Lineamiento técnico 184

Lista de tablas

Pág.

Tabla 1-1 Recomendaciones relevantes de la UIT-T sobre QoS y QoE [25] 19
Tabla 1-2 Mean Opinion Score (MOS) [25] 23
Tabla 1-3 Definiciones de clases de QoS de las redes IP [42] 27
Tabla 1-4 Clases de QoS para el transporte en redes [16] 32
Tabla 1-5 Trabajos relacionados en el área de investigación 36
Tabla 1-6 Soluciones de hipervisores 40
Tabla 1-7 Herramientas de emulación de red 40
Tabla 1-8 Entornos de núcleo IMS 41
Tabla 1-9 Servidores IPTV 42
Tabla 1-10 Tecnologías de contenedores 42
Tabla 1-11 Monitores de tráfico SIP 42
Tabla 1-12 Softphone 43
Tabla 1-13 Herramientas de medición de tráfico en red 43
Tabla 2-1 Costo para las interfaces en OSPF [94] 56
Tabla 2-2 Comparativo entre el plano de control y el plano de datos [97], [101] 62
Tabla 2-3 Comparativo entre L2VPN y L3 basadas en MPLS [100] 65
Tabla 2-4 Funcionamiento de VPLS en el plano de control en el plano de datos [100] ... 67
Tabla 2-5 Ejemplos de BA [95] 74
Tabla 2-6 Valores de precedencia [106] 77
Tabla 2-7 Valores de probabilidad de descarte del campo ToS [106] 77
Tabla 2-8 Valores del campo EXP y PHB asociados [95], [106] 78
Tabla 2-9 Valores representativos de QCI según el 3GPP TS 23.203 [109] 81
Tabla 2-10 Valores representativos de 5QI según el 3GPP TS 23.501 [110] 82
Tabla 3-1 Caracterización del tráfico de la red 99
Tabla 3-2 Herramientas de emulación seleccionadas 99
Tabla 3-3 Especificaciones del equipo de trabajo 100
Tabla 3-4 Características técnicas de la máquina virtual PNetLab 100
Tabla 3-5 Características técnicas del core IMS en QEMU 101
Tabla 3-6 Distribución de sockets IP del core IMS en Kamailio 102
Tabla 3-7 Usuarios creados en el HSS para los UE correspondientes 103
Tabla 3-8 Comandos para pruebas de medición en iPerf3 106
Tabla 3-9 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3 107

Tabla 3-10 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3..... 108
Tabla 3-11 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 114
Tabla 3-12 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3..... 114
Tabla 3-13 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 120
Tabla 3-14 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3..... 121
Tabla 3-15 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 127
Tabla 3-16 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3..... 127
Tabla 3-17 Valores calculados para el acondicionamiento del tráfico mediante un modelador 138
Tabla 3-18 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 140
Tabla 3-19 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3 140
Tabla 3-20 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3 141
Tabla 3-21 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 147
Tabla 3-22 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3 147
Tabla 3-23 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3 148
Tabla 3-24 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 154
Tabla 3-25 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3 155
Tabla 3-26 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3 155
Tabla 3-27 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3..... 161

Tabla 3-28 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3 161
Tabla 3-29 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3 162
Tabla 3-30 Resumen de valores obtenidos de RTT en prueba ping y Saltos de red en prueba traceroute para L2VPN y L3VPN sin y con QoS 166
Tabla 4-1 Documentos de la CRC relacionados con los indicadores de calidad e interconexión [118]..... 177
Tabla 4-2 Intervalo de confianza y tamaños de las muestras para las mediciones [25] 180

Lista de abreviaturas

Abreviatura	Término
3GPP	*3rd Generation Partnership Project*
5QI	*5G NR QoS Identifier*
ABR	*Area Border Router*
AC	*Attachment Circuit*
ACL	*Access Control List*
AF	*Assured Forwarding*
AGG	*Aggregation*
AS	*Application Server, Autonomous System*
ASBR	*Autonomous System Border Router*
ATM	*Asynchronous Transfer Mode*
BA	*Behavior Aggregates*
BE	*Best Effort*
BGP	*Border Gateway Protocol*
BW	*Bandwidth*
CBS	*Committed Burst Size*
CBWFQ	*Class-based Weighted Fair Queueing*
CE	*Customer Edge*
CIDR	*Classless Inter-Domain Routing*
CIR	*Committed Information Rate*
COPS	*Common Open Policy Service*
C-RAN	*Centralized/Cloud Radio Access Network*
CRC	*Comisión de Regulación de Comunicaciones*
CS	*Class Selector*
CSCF	*Call Sesion Control Function*
CSG	*Cell Site Gateway*
DF	*Default Forwarding*
DHCP	*Dynamic Host Configuration Protocol*
DiffServ	*Differentiated Services*
DNS	*Domain Name System*
DSCP	*Diffetentiated Service Code Point*
DSL	*Digital Subscriber Line*
e2e	*end-to-end*
eBGP	*External BGP*
EF	*Expedited Forwarding*
EGP	*Exterior Gateway Protocol*
EIGRP	*Enhanced Interior Gateway Routing Protocol*

Abreviatura	Término
ENUM	*Electronic Numbering*
E-LSR	*Egress LSR*
ETSI	*European Telecomunication Standards Institute*
E-UTRAN	*Evolved Universal Terrestrial Radio Access Network*
FCS	*Frame Check Sequence*
FIFO	*First In - First Out*
FNO	*Fixed Network Operator*
FTP	*File Transfer Protocol*
GBR	*Guaranteed Flow Bit Rate*
GERAN	*GSM EDGE Radio Access Network*
GSMA	*GSM Association*
HSI	*High Speed Internet*
HSS	*Home Subscriber Server*
IANA	*Internet Assigned Numbers Authority*
IBCF	*Interconnection Border Control Function*
iBGP	*Internal BGP*
I-CSCF	*Interrogating-CSCF*
IETF	*Internet Engineering Task Force*
HSRP	*Hot Standby Router Protocol*
IGP	*Interior Gateway Protocol*
I-LSR	*Ingress LSR*
IM	*Instant Messaging*
IMS	*IP Multimedia Subsystem*
IntServ	*Integrated Services*
IP	*Internet Protocol*
IP-CAN	*IP Connectivity Access Network*
IPDV	*IP Packet Delay Variation*
IPER	*IP Packet Error Ratio*
IPLR	*IP Packet Loss Ratio*
IPTD	*IP Packet Transfer Delay*
IPTV	*Internet Protocol Television*
IPX	*IP Exchange*
IS-IS	*Intermediate System to intermediate System*
ISP	*Internet Service Provider*
KPI	*Key Performance Indicator*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LL	*Low Latency*
LLQ	*Low-latency Queuing*
LSP	*Label Switched Path*
LSR	*Label Switch Router*
LTE	*Long Term Evolution*
L2	*Layer 2 OSI*

Abreviatura	Término
L3	*Layer 3 OSI*
MAN	*Metropolitan Area Network*
MASG	*Mobile Aggregate Service Gateway*
MNO	*Mobile Network Operator*
MOS	*Mean Opinion Score*
MP-BGP	*Multi-protocol BGP*
MPLS	*Multi-protocol Label Switching*
MSTP	*Multiple Spanning Tree Protocol*
NASS	*Network Attachment Subsystem*
NBAR	*Network Based Application Recognition*
NGN	*Next Generation Networks*
NNI	*Network-to-Network Interface*
NP	*Perfomance*
NR	*New Radio*
NRA	*National Regulatory Authority*
O&M	*Operations and Maintenance*
OS	*Operating System*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
P	*Provider*
PBS	*Peak Burst Size*
PC	*Personal Computer*
PCEF	*Policy and Charging Execution Function*
PCRF	*Policy and Charging Rules Function*
P-CSCF	*Proxy-CSCF*
PDF	*Policy Decision Function*
PDN	*Packet Data Network*
PDP	*Policy Decision Point*
PE	*Provider Edge*
PEP	*Policy Enforcement Point*
PES	*PSTN Emulation Subsystem*
PHB	*Per-hop behaviour*
PIR	*Peak Information Rate*
PLR	*Packet Loss Ratio*
PPC	*Policy and Charging Control*
PSTN	*Public Switched Telephone Network*
PTDN	*Public Telecom Packet Data Network*
PW	*Pseudowire*
QoE	*Quality of Experience*
QoS	*Quality of Service*
RACS	*Resource Admission Control Subsystem*
RAN	*Radio Access Network*

Abreviatura	Término
RD	*Route Distinguisher*
RR	*Route Reflector*
RRC	*Route Reflector Client*
RRnC	*Route Reflector non Client*
RRPP	*Rapid Ring Protection Protocol*
RSVP	*Resource Reservation Protocol*
RT	*Route Target*
RTCP	*Real Time Control Protocol*
RTSP	*Real Time Streaming Protocol*
RTP	*Real Time Transport Protocol*
RTT	*Round Trip Time*
S-CSCF	*Serving-CSCF*
SDP	*Session Description Protocol*
SSH	*Secure SHell*
SIP	*Session Initiation Protocol*
SLA	*Service Level Agreement*
SP	*Service Provider*
STP	*Spanning Tree Protocol*
TC	*Traffic Class*
TCP	*Transmission Control Protocol*
TDP	*Tag Distribution Protocol*
TE	*Traffic Engineering*
Telnet	*Teletype Network*
TISPAN	*Telecommunications and Internet converged Services and Protocol for Advanced Networking*
ToS	*Type of Service*
TrGW	*Transition Gateway*
UDP	*User Datagram Protocol*
UE	*User Equipment*
UIT	*Unión Internacional de Telecomunicaciones*
UNI	*User Network Interface*
UTRAN	*UMTS Terrestrial Radio Access Network*
VC	*Virtual Circuit*
VLSM	*Variable Length Subnet Mask*
VoD	*Video on Demand*
VoIMS	*Voice over IMS*
VoIP	*Voice over IP*
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VRF	*VPN Routing and Forwarding, VPN Routing and Forwarding*
VSI	*Virtual Switch Instance*
WAN	*Wide Area Network*
WRED	*Weighted Random Early Detection*

Introducción

El sector de las telecomunicaciones está adoptando el subsistema multimedia IP (IMS, por sus siglas en inglés) como la arquitectura de referencia para la evolución de todos los servicios de telecomunicaciones a NGN (Next Generation Networks, por sus siglas en inglés), soportando los servicios de telecomunicaciones actuales y futuros. Una de las ventajas de IMS radica en que integra el concepto de convergencia de servicios soportados por redes heterogéneas, es decir, redes de naturaleza distinta como lo son las redes fijas, móviles o la Internet, sin embargo, IMS no estandariza las aplicaciones, pero si facilita el acceso de las aplicaciones multimedia y de voz a los distintos tipos de terminales y tecnologías de acceso [1].

Uno de los aspectos más importantes en cuanto a la convergencia de servicios radica en la calidad de servicio (QoS, por sus siglas en inglés) debido a que las redes IP originalmente carecían de mecanismos de control de QoS. Estas redes fueron diseñadas para ofrecer la entrega de servicios sin garantizar la fiabilidad de la información, en dependencia de la cantidad de ancho de banda requerido sobre todo en servicios que requieren conexiones en tiempo real como lo son la voz y el streaming de video [2].

En Colombia la evolución de la infraestructura de los operadores ha comenzado con la implementación de Softswitches que permiten la migración hacia una red All-IP. Sin embargo, la industria está adoptando la arquitectura IMS debido a sus interfaces abiertas para el despliegue de servicios convergentes ya que les permite mejorar el nivel de servicio que se presta actualmente, así como implementar nuevos productos. De igual manera, se observa el interés mostrado por la CRC (Comisión de regulación de Comunicaciones) en materia de regulación con la conformación del grupo de industria para el despliegue y desarrollo de las NGN con el objetivo de establecer una discusión con los actores del sector sobre las perspectivas tecnológicas y económicas derivadas del despliegue de redes de nueva generación [3].

Mundialmente la QoS es una de las áreas más investigadas en la actualidad ya que es de interés para los usuarios, los operadores y el ente regulador, y a que IMS es una arquitectura basada en IP, en constante evolución y heterogeneidad en las redes de los operadores, caracterizada por la gran variedad de protocolos utilizados en sus infraestructuras, el control de políticas de QoS se convierte en un tema de investigación [4], [5].

Descripción del problema

El problema central está en proveer una calidad de servicio consistente de extremo a extremo en un servicio IP de manera que se satisfagan los requerimientos de QoS solicitados, cuando en el despliegue de un servicio interviene la infraestructura de dos o más operadores, siendo redes autónomas y cuyos dominios administrativos son gestionados de acuerdo con sus propias políticas. Aunque los operadores deben estar de acuerdo en los requerimientos de QoS para un servicio particular entre un conjunto de servicios IP, los operadores no configuran sus dispositivos de red de la misma manera puesto que tienen sus propias topologías internas y mecanismos de QoS que dependen de sus dispositivos, así como otros requerimientos de gestión que no son técnicos. Es por eso por lo que se hace necesario desarrollar un lineamiento que les permita a los operadores mantener un nivel consistente de QoS en las interconexiones sin depender de la complejidad de la red [6], [7].

Debido a que no existe una metodología estándar para el manejo de la calidad de servicio en interconexión bajo la arquitectura IMS, un lineamiento técnico para el manejo de metodologías permitiría la mejora del desempeño en el manejo de servicios convergentes, que soporten la priorización de paquetes y la ubicuidad del usuario sin afectar el nivel de servicio ofrecido. Un proyecto con estas características, además optimizar el desempeño en la red puede mejorar los ingresos de los operadores, ya que pueden establecer de una manera más eficiente las métricas de nivel de servicio como los niveles de experiencia, satisfacción de los usuarios ante los servicios que ellos ofrecen, disponibilidad de la red y así establecer las correspondientes acciones de mejora.

Objetivos

a. Objetivo general

Generar un lineamiento técnico para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS).

b. Objetivos específicos

- Caracterizar los parámetros de QoS para el despliegue de servicios convergentes bajo la arquitectura IMS en interconexión.
- Evaluar el impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video, en un entorno IMS emulado.
- Definir los lineamientos técnicos para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios de voz, datos y video.

Alcances y limitaciones

Los aspectos que restringen el alcance de este proyecto son:

- Las limitaciones propias de las herramientas de emulación.
- Las pruebas realizadas tienen en cuenta un modelo de red virtualizado, cuyo desempeño está determinado por el rendimiento del hardware del equipo huésped.

Metodología

Para el desarrollo del proyecto de tesis se plantea el siguiente enfoque sistémico soportado en la metodología cuantitativa vista en [8] y [9], en el cual, se parte de una etapa de planeación en la que se definen los objetivos y requerimientos de acuerdo con la recolección de la información bibliográfica; una etapa de diseño del modelo emulado, en la que se realiza una especificación del entorno de pruebas y configuración; una etapa de desarrollo cuyo objetivo es realizar la emulación y obtención de los resultados; una etapa de análisis en la que se consolidan los resultados para la realización y evaluación de las

conclusiones y finalmente, la realización de la documentación respectiva donde se presentan los resultados del desarrollo del proyecto para lograr la consecución de los objetivos propuestos (ver Figura 0-1).

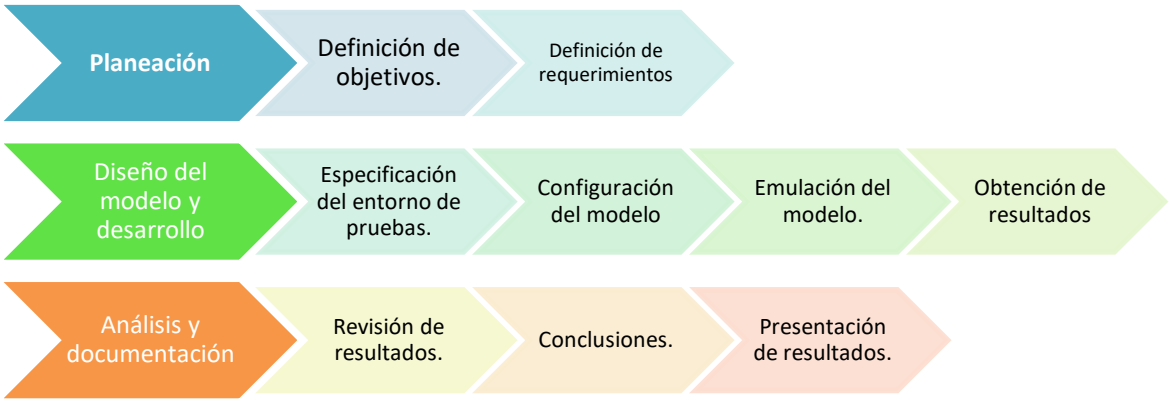


Figura 0-1 Metodología propuesta para el desarrollo del proyecto de tesis.

La metodología propuesta se llevó a cabo a través de las siguientes fases:

- **Fase de Planeación:** En esta fase se realizó la revisión bibliográfica de la información relevante acerca de los mecanismos de control de QoS bajo la arquitectura IMS, se analizaron las diferentes recomendaciones técnicas dadas por diferentes organismos internacionales y se realizó el estudio de la arquitectura IMS y la señalización SIP, de igual manera se definieron los requerimientos de QoS para el despliegue de servicios multimedia (voz, datos y video) en redes IP.
- **Fase de diseño y desarrollo:** En esta fase se planteó el diseño del modelo de emulación inter-dominio bajo IMS para el entorno de pruebas, así como la generación de diferentes métricas de QoS que permitieron obtener una serie de resultados acerca del comportamiento del sistema ante situaciones en las que se requiere establecer los parámetros de negociación de QoS en el establecimiento de una sesión extremo a extremo.
- **Fase de análisis y documentación:** Luego de obtener los resultados de los experimentos se realizó una evaluación de los parámetros de QoS de acuerdo con los requerimientos planteados, estos resultados permitieron establecer los lineamientos técnicos para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios

de voz, datos y video. Por otro lado, se realizó un análisis del estado de avance en la implementación de las redes NGN y su reglamentación en Colombia.

Estructura del documento

La presente investigación está dividida en los siguientes capítulos:

- Capítulo 1: Presenta los antecedentes y fundamentos teóricos de la investigación.
- Capítulo 2: Presenta la caracterización de los parámetros de QoS para el despliegue de servicios convergentes bajo la arquitectura IMS en interconexión.
- Capítulo 3: Presenta la evaluación del impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video en un entorno emulado.
- Capítulo 4: Presenta la definición de los lineamientos técnicos para la provisión de QoS extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios de voz, datos y video.
- Capítulo 5: Presenta las conclusiones y recomendaciones de la investigación.

1. Antecedentes y fundamentos teóricos

En este capítulo se abordan los antecedentes y fundamentos teóricos de la investigación, donde se abordan los conceptos relacionados con las redes de próxima generación (NGN), el IP Multimedia Subsystem (IMS), los fundamentos de interconexión, las consideraciones respecto a la QoS, los parámetros de desempeño para servicios IP en redes de extremo a extremo, los marcos de referencia para la QoS, la calidad de servicio en IMS, un análisis en el área de investigación y las herramientas de emulación que se pueden encontrar actualmente para la implementación de un entorno de pruebas o testbed.

1.1 Redes de próxima generación (NGN)

El concepto de redes de próxima generación (NGN) se introdujo para enfrentar el contexto actual de la industria de las telecomunicaciones, caracterizado por una competencia abierta entre los operadores debido a la desregulación de los mercados, la convergencia entre redes y servicios y la creciente demanda de aplicaciones multimedia [10]. Este escenario crea desafíos para los operadores tanto en su infraestructura como en su cartera de servicios; los operadores deben adoptar rápidamente nuevas tecnologías y la capacidad de desarrollar servicios en poco tiempo, a bajo costo, para satisfacer las necesidades del mercado [11].

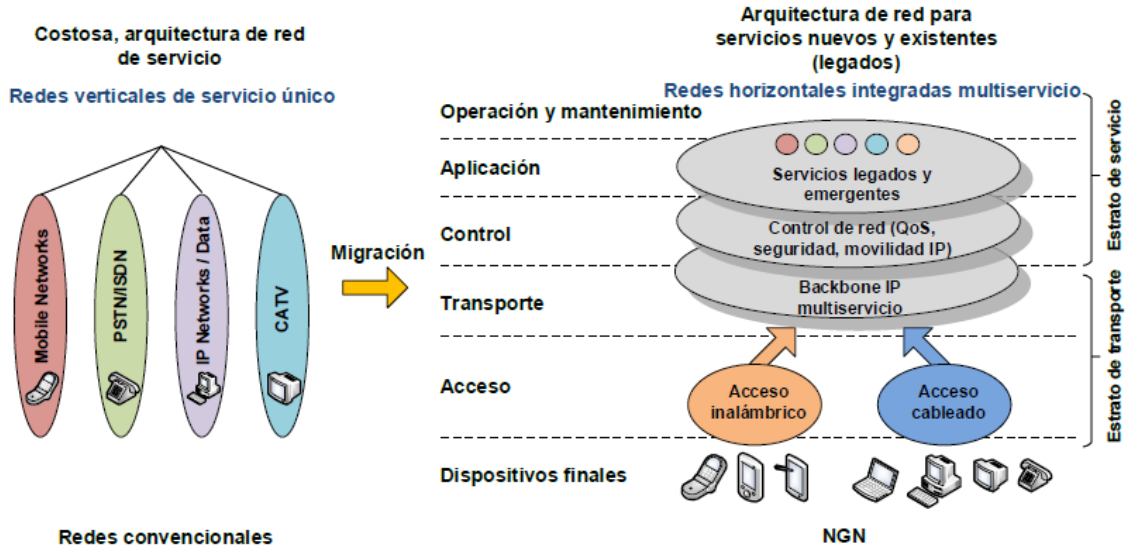


Figura 1-1 Arquitecturas de telecomunicaciones horizontales y verticales [12]

Las crecientes necesidades de movilidad y la personalización de los servicios prestados a los consumidores han dado lugar a formas más eficientes de proporcionar servicios utilizando cualquier tecnología disponible en cualquier momento; por lo tanto, las infraestructuras de red deben proporcionar recursos suficientes para ofrecer servicios de valor agregado. Las NGN proporcionan un modelo que permite al operador mejorar la provisión de recursos para integrar todos los tipos de servicios de telecomunicaciones en una única infraestructura de red que adopta el protocolo de Internet (IP); este modelo se conoce como All-IP [11]. Por lo tanto, los operadores pueden pasar de un modelo de arquitectura vertical, en el que cada servicio que prestan tiene una infraestructura separada (teléfonos móviles, telefonía conmutada, redes de datos, redes de televisión, etc.), con los

correspondientes tipos de infraestructura de acceso, transporte, control y aplicación, a una arquitectura independiente horizontal en la que estos servicios están integrados como se observa en la Figura 1-1.

La industria de las telecomunicaciones está adoptando el subsistema multimedia IP (IMS) como arquitectura de referencia para el desarrollo de todos los servicios de telecomunicaciones para las NGN, que pueden soportar los servicios de telecomunicaciones actuales y que serán útiles en el futuro. Una ventaja de IMS es que integra el concepto de convergencia de servicios soportados por redes heterogéneas, es decir, redes de diferentes tipos, tales como fijo, móvil o internet. Sin embargo, IMS no estandariza las aplicaciones, sino que facilita el acceso a las aplicaciones multimedia y el acceso de voz a diferentes tipos de terminales y tecnologías de acceso [1].

Uno de los aspectos más importantes relacionados con la convergencia de servicios es la QoS, porque las redes IP originalmente carecían de mecanismos de control. Estas redes fueron diseñadas para proporcionar la prestación de servicios sin garantizar la confiabilidad de la información correspondiente, dependiendo de la cantidad de ancho de banda requerida, especialmente para los servicios que requieren conexiones en tiempo real [2]. Sobre la base de la recomendación Y.2001 de la Unión Internacional de Telecomunicaciones (UIT), se establecieron las características necesarias para garantizar la QoS de extremo a extremo (e2e) en las NGN, entre las que se encuentran el retardo, la variación del retador, la pérdida de paquetes y el ancho de banda [13].

A nivel mundial, la QoS es actualmente una de las áreas más investigadas debido a su interés para los usuarios, operadores y reguladores [3]. IMS es una arquitectura basada en IP que evoluciona constantemente y es heterogénea en las redes de operadores; Se caracteriza por una variedad de protocolos utilizados en las infraestructuras de red del operador. Por lo tanto, el control de la política de QoS se ha convertido en un importante tema de investigación [4], [5].

1.2 IP Multimedia Subsystem

IMS es una arquitectura de referencia para la provisión de servicios de próxima generación estandarizada por el 3rd Generation Partnership Project (3GPP) e introducida en las

versiones 5 y 6 de UMTS (marzo de 2003). IMS permite a los operadores de telecomunicaciones ofrecer servicios multimedia, como voz, datos, video y combinaciones de estos, bajo la misma infraestructura a través de redes de conmutación de paquetes basadas en IP [14]. IMS se considera un subsistema porque es parte de una red completa en la que se requieren otros componentes, como una red de acceso, para funcionar completamente como un sistema de despliegue de servicios [15].

Este subsistema es importante porque permite integrar diferentes tipos de redes de acceso independientemente de la tecnología o los servicios de Internet que combinen redes fijas y móviles [16]; sin embargo, mientras que el 3GPP describe IMS desde el punto de vista de los operadores móviles (soporte de nuevas aplicaciones), un cuerpo de estandarización miembro de la European Telecomunication Standards Institute (ETSI) llamado Telecomunications and Internet converged Services and Protocol for Advanced Networking (TISPAN) agrega las especificaciones necesarias para compatibilizar IMS con las redes de los operadores fijos (convergencia). La flexibilidad de esta arquitectura permite modificaciones y extensiones en el subsistema [17], además simplifica el diseño de aplicaciones mediante la armonización del control de sesiones adoptando el protocolo Session Initiation Protocol (SIP) [18].

En la Figura 1-2 se observa la arquitectura IMS y sus tres niveles principales que son: la capa de Servicios Multimedia, la capa de Control de Sesión y la capa de Transporte IP en la que una red basada en la arquitectura IMS permite la convergencia de diferentes tecnologías de redes de acceso como las redes de telefonía fija PSTN, banda ancha xDSL, Wireless LAN, junto con redes de telefonía móvil celular de 2G, 3G, 4G y 5G, entre otras [16].

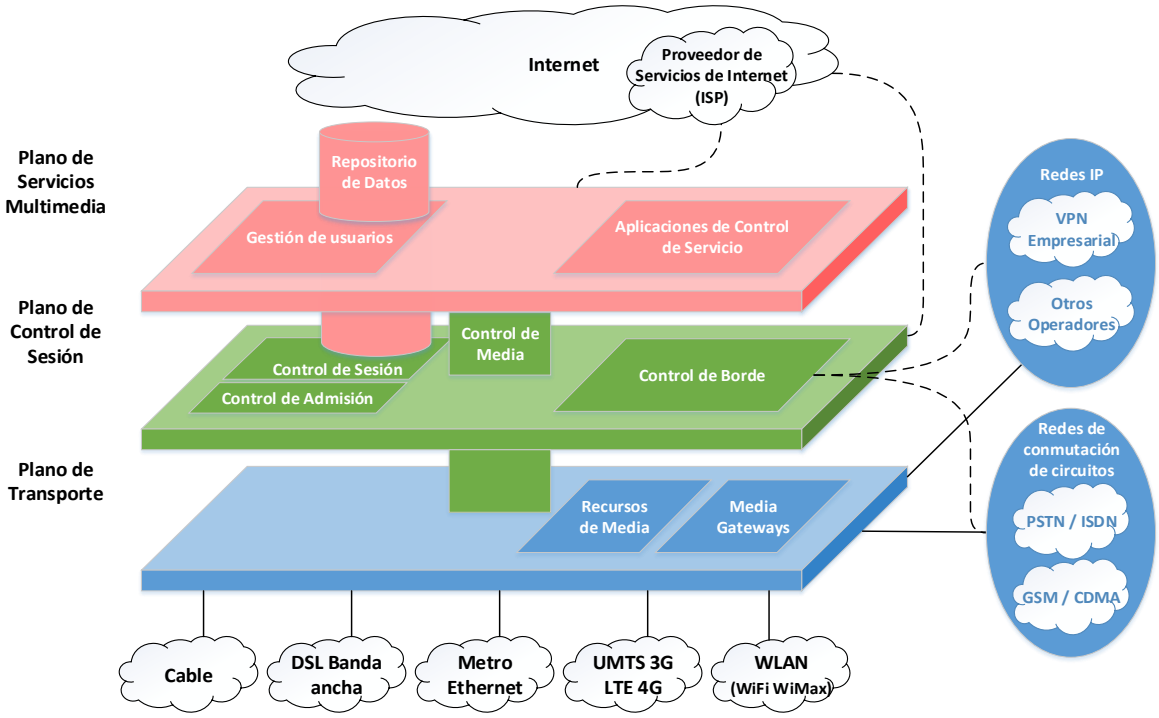


Figura 1-2 Arquitectura IMS por capas y redes de acceso [16]

Se debe hacer distinción entre “núcleo IMS” e “IMS”, ya que la arquitectura IMS se refiere a un “núcleo” o “Core IMS” (definido por el 3GPP), más el agregado de un número de subsistemas no IMS (definidos por TISPAN) como por ejemplo el Network Attachment Subsystem (NASS), el Resource Admission Control Subsystem (RACS) y el PSTN Emulation Subsystem (PES) [19]. Los componentes centrales de la arquitectura IMS son las entidades de Control de Sesión de Llamadas (Call Sesion Control Function - CSCF) que en realidad son servidores SIP. Estas entidades tienen funciones específicas para la señalización y enrutamiento del tráfico, entre las cuales se encuentran a nivel de núcleo el Proxy-CSCF (P-CSCF), el (I-CSCF), el Serving-CSCF (S-CSCF), el Home Subscriber Server (HSS) y los Aplication Server (AS) [20].

La Figura 1-3 muestra los diferentes tipos de componentes que se utilizan en una arquitectura IMS, entre los principales elementos que se encuentran en una solución básica están las entidades CSCF. De igual manera se definen diversas entidades funcionales para el manejo de redes fijas y móviles, algunas entidades están encargadas de comunicarse con la red de transporte para asegurar la QoS y evitar el mal uso de los servicios provistos [21].

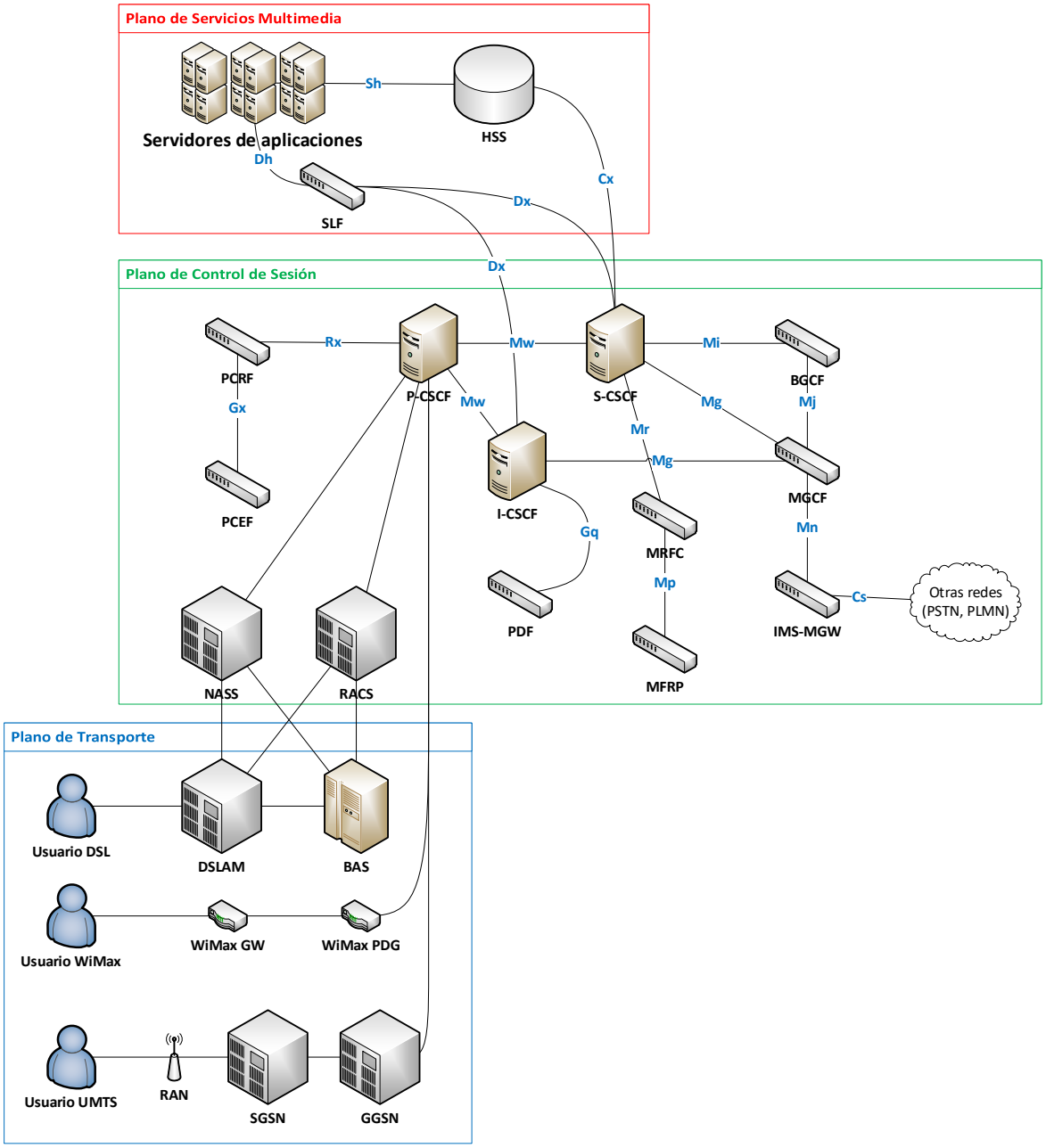


Figura 1-3 Componentes de la arquitectura IMS por capas [21]

Los diferentes protocolos utilizados por estos componentes de acuerdo a su función en la señalización, como el control de sesiones a través del Session Initiation Protocol (SIP), control de autenticación por medio de Diameter o el control de políticas mediante el modelo Open Policy Service (COPS), entre otros, han sido estandarizados por la Internet Engineering Task Force (IETF) con el propósito de adoptar los protocolos abiertos utilizados en la arquitectura TCP/IP, para de esta manera crear una plataforma flexible que

pueda ser escalable y compatible con las redes legadas [22]. La especificación de la arquitectura funcional del subsistema IMS se puede consultar en el documento 3GPP 23.228 [23] donde se definen las interfaces, los protocolos y las aplicaciones que pueden ofrecerse a los usuarios bajo la red IMS.

1.3 Interconexión

La Resolución CRC 5050 de 2016 [27] "Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones" en concordancia con el Manual de reglamentación de las telecomunicaciones [24] define la interconexión como *"la vinculación de recursos físicos y soportes lógicos de las redes de telecomunicaciones, incluidas las instalaciones esenciales, necesarias para permitir el inter-funcionamiento de redes y la interoperabilidad de plataformas, servicios y/o aplicaciones que permite que usuarios de diferentes redes se comuniquen entre sí o accedan a servicios prestados por otro proveedor. La interconexión de las redes implica el uso de estas y se constituye en un tipo especial de acceso entre proveedores de redes y servicios de telecomunicaciones."*

Desde el punto de vista técnico la interconexión se relaciona con enlaces de conexión entre dominios de red autónomos [25] (es decir, diferentes sistemas autónomos[1]), que pueden pertenecer a diferentes proveedores de red u operadores, que proporcionan acceso y/o tránsito a los usuarios de dichas redes.

1.3.1 Interconexión en IMS

Los operadores que migran a IMS deben recurrir al modelo de interconexión de intercambio IP [26] (IP Exchange o IPX, por sus siglas en inglés) como lo describe el documento IR.65. de la asociación GSM (GSMA) o un punto de conectividad directa [27]. IPX es una red IP privada y global que admite la QoS de extremo a extremo, está completamente separado

[1] Sistema autónomo (AS, por sus siglas en inglés) se define como un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de enrutamiento, tomada de Distribución de Números de Sistema Autónomo (ASN), LACNIC, https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomo-asn (consultada 05-03-2019)

de la Internet pública. En la Figura 1-4 se observa la arquitectura IPX, que consta de diferentes proveedores de IPX que se conectan entre sí, a través de un punto de interconexión para el intercambio de tráfico. Tanto la señalización (por ejemplo, SIP) como media (ej. RTP) se transportan dentro de la red IPX. En IPX, todas las partes están vinculadas por el SLA (Service Level Agreement, por sus siglas en inglés) de extremo a extremo. IPX se puede utilizar para transportar cualquier servicio IP entre proveedores de servicios, tanto en roaming como en escenarios de interfuncionamiento [28].

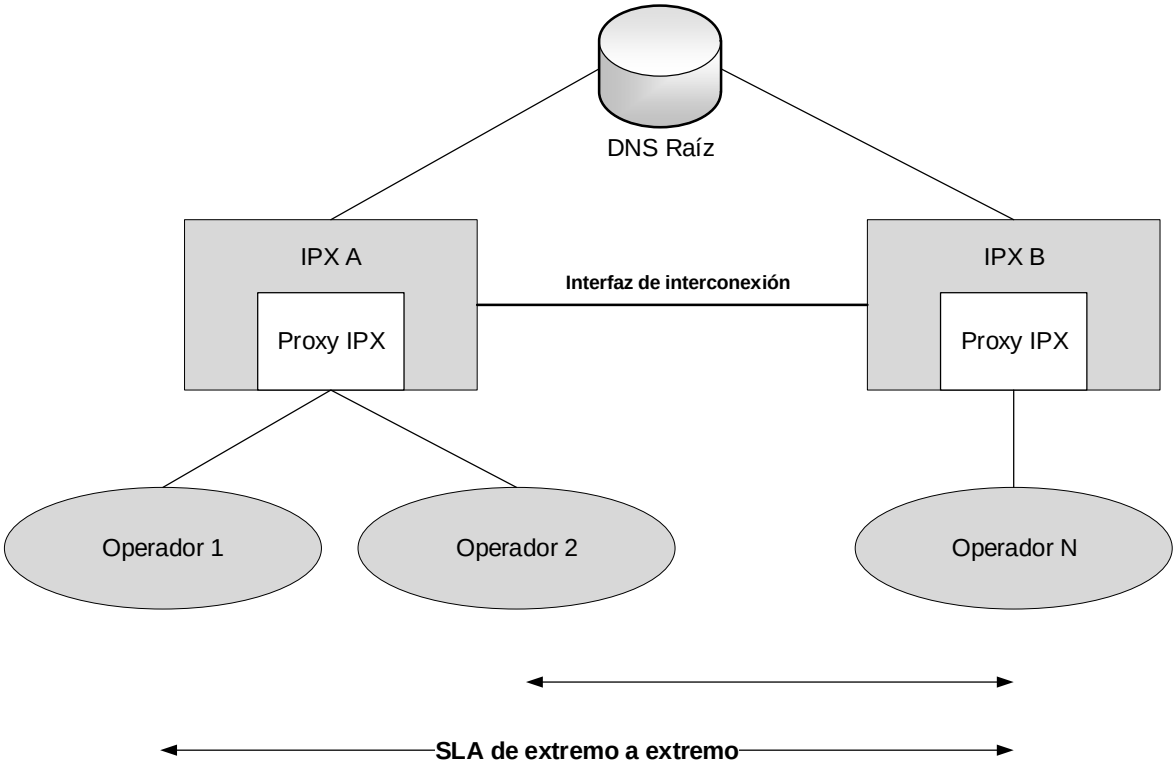


Figura 1-4 Modelo IPX [26]

En el documento oficial IR.95 se ilustra la interconexión en IMS (ver Figura 1-5) mediante la interfaz red a red (NNI) la cual consta de los puntos de referencia Ici e Izi entre los IBCF pares ((Interconnection Border Control Function) y TrGW (Transition Gateway) en los planos de control y medios, respectivamente [27].

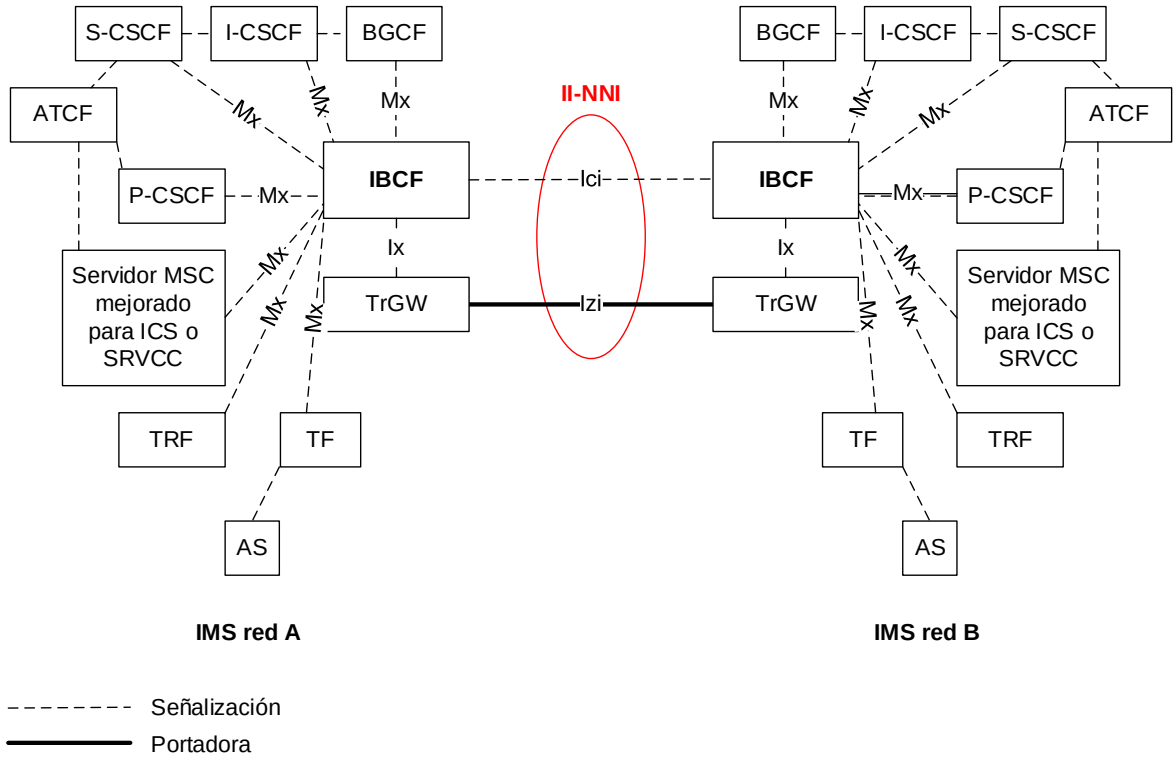


Figura 1-5 Arquitectura de referencia Inter IMS NNI [27]

En la Figura 1-6 se observa un ejemplo de interconexión de un usuario fijo y móvil mediante la Interfaz de usuario a red (UNI) de una red de acceso LTE (Long Term Evolution) a otras redes IMS, utilizando una red troncal IPX entre la red de un operador móvil (MNO) y la red de un operador fijo (FNO) con una red de acceso ADSL (Asymmetric Digital Subscriber Line) para el intercambio de un servicio de voz y video sobre IMS (VoIMS) utilizando la IMS NNI. El concepto representado en la figura también podría extrapolarse a más de un nodo de red troncal IPX al que están conectadas las redes IMS, lo que permite la interconexión inmediata a aquellas redes que tienen acuerdos con el IPX [29].

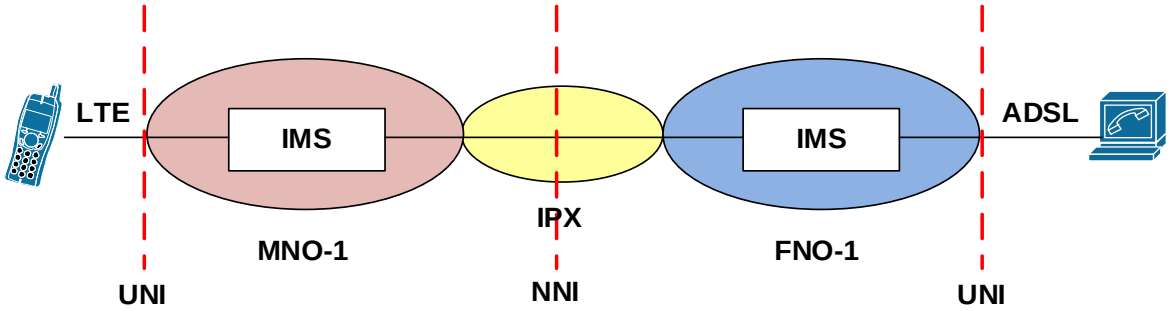


Figura 1-6 Ejemplo de alto nivel de comunicación de voz y video basada en VoIMS [29]

Desde el punto de vista del sistema central de IMS, IPX es solo una red IP que ofrece las características de QoS, seguridad y alcance global para cualquier servicio basado en IP entre diferentes proveedores de servicios. No es necesario realizar modificaciones ni en las especificaciones 3GPP IMS, ni en las implementaciones de nodos IMS debido a la inclusión de IPX [28].

1.3.2 Roaming en IMS

El término roaming o itinerancia se define por la GSMA como *"la capacidad de un cliente de una red celular para consumir servicios de forma automática, tales como, hacer y recibir llamadas, enviar y recibir datos, o acceder a otros servicios, incluyendo servicios de datos locales, cuando se viaja fuera de la cobertura geográfica de la red local, lo que significa que se utiliza una red visitada"* [26].

En [26] se observa que para la entrega de servicios en IMS, utilizando el escenario de itinerancia, se tienen las siguientes opciones:

- Mediante el uso de un P-CSCF visitado, conectado al dominio IMS local.
- Ser conectado a un P-CSCF local.

La Figura 1-7 muestra un escenario en el que un UE se conecta a un P-CSCF visitado y los mensajes de señalización, son manejados por este y no por un P-CSCF local. De igual manera los flujos de media son tratados por la red visitada. Las políticas y cargos deben ser negociadas entre ambos dominios [26].

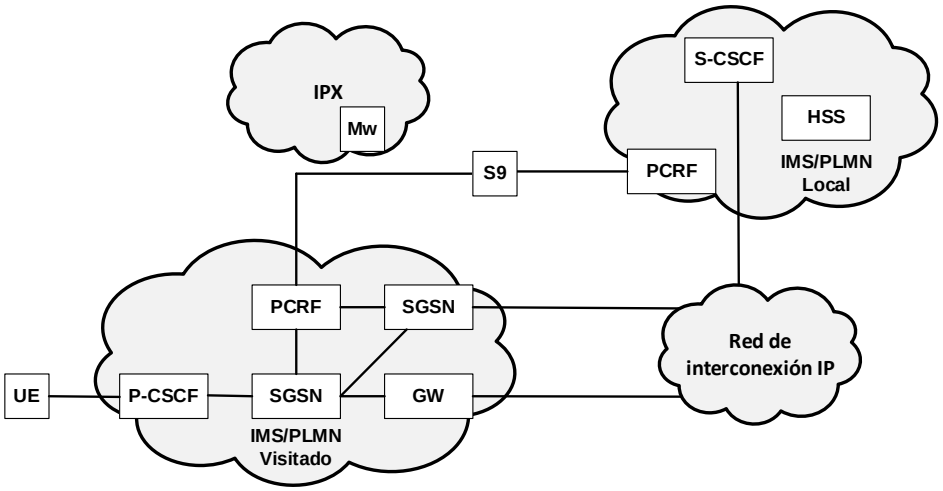


Figura 1-7 Roaming en IMS [26]

1.4 Consideraciones respecto a la QoS

Uno de los criterios esenciales para la evaluación de un sistema radica en la medición del desempeño de la red desde los puntos de vista del despliegue, la operación y la satisfacción del cliente. Para la evaluación de la calidad se tienen dos aproximaciones, las cuales son la Calidad de Servicio (QoS) y la Calidad de la Experiencia (QoE) [30]:

- La QoS se define por la UIT como la totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio [31], En Colombia, la Resolución CRC 5050 de 2016 [21] define la QoS como "*El efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción del servicio por parte de un usuario"*. Como muestra la recomendación E.800 la QoS comprende tanto la calidad del funcionamiento o el rendimiento de la red (Network Perfomance, NP) como la calidad de funcionamiento independiente de la red. Dentro del NP se incluyen la tasa de errores en los bits, la latencia, etc., y en la calidad de desempeño independiente de la red se cuentan el tiempo de prestación, el tiempo de reparación, la gama tarifaria y el tiempo de resolución de quejas, entre otros y por lo tanto se establecen métricas objetivas de evaluación de una red. La lista de criterios de QoS para un servicio concreto dependerá del servicio y su importancia podrá variar de un segmento de la clientela a otro, como se observa en la Figura 1-8.

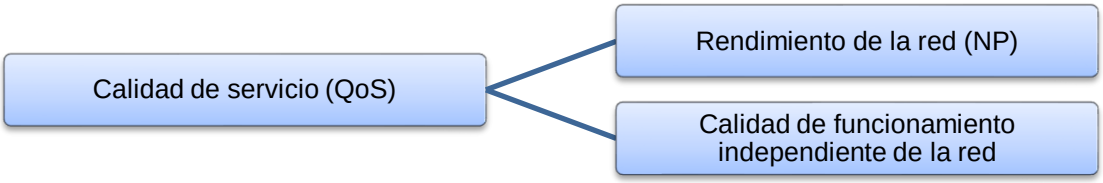


Figura 1-8 Criterios de funcionamiento de la QoS [31]

- La QoE se relaciona con los niveles de satisfacción centrada en el usuario de acuerdo a sus expectativas, percepción e impacto subyacente a la QoS y en consecuencia, evalúan de manera subjetiva el comportamiento de una red [32]. El impacto de estos factores tiene una evaluación subjetiva que puede variar entre porcentajes bajo, medio o alto [33]. Debido a que estos parámetros se centran en el usuario son de gran interés en investigación [34]. Dentro de los parámetros definidos por la QoE se encuentra la puntuación media de opinión (MOS) [25].

En resumen, se observa respecto a la calidad, que se evalúan aspectos que son técnicos y otros que no lo son, la Figura 1-9 muestra la dependencia de la QoS, en la cual se incluye el NP y el desempeño de los terminales, así como los aspectos no-técnicos que incluyen el cuidado del cliente y el punto de venta, las cuales influyen en la QoE relacionadas a los contextos y expectativas de los clientes [25].

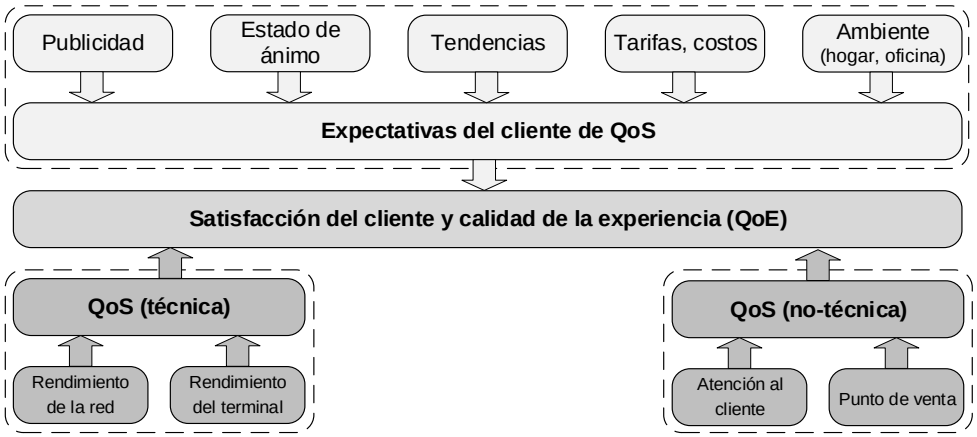


Figura 1-9 Puntos de vista técnicos y no-técnicos de la calidad de servicio [25]

En la

Figura **1-10** se observan los diferentes aspectos relacionados con la calidad del funcionamiento de la red del proveedor de servicios, los cuales incluyen la planeación, la implementación, la operación y el mantenimiento de los elementos que la componen. La QoS siempre será una característica de extremo a extremo en la que influye el usuario final, el dispositivo de usuario o terminal (smartphone, computador, etc), las redes de acceso (fija o móvil), redes de transporte IP, de núcleo, y las contribuciones de los demás dispositivos entre los extremos de la red (como por ejemplo internet) [25].

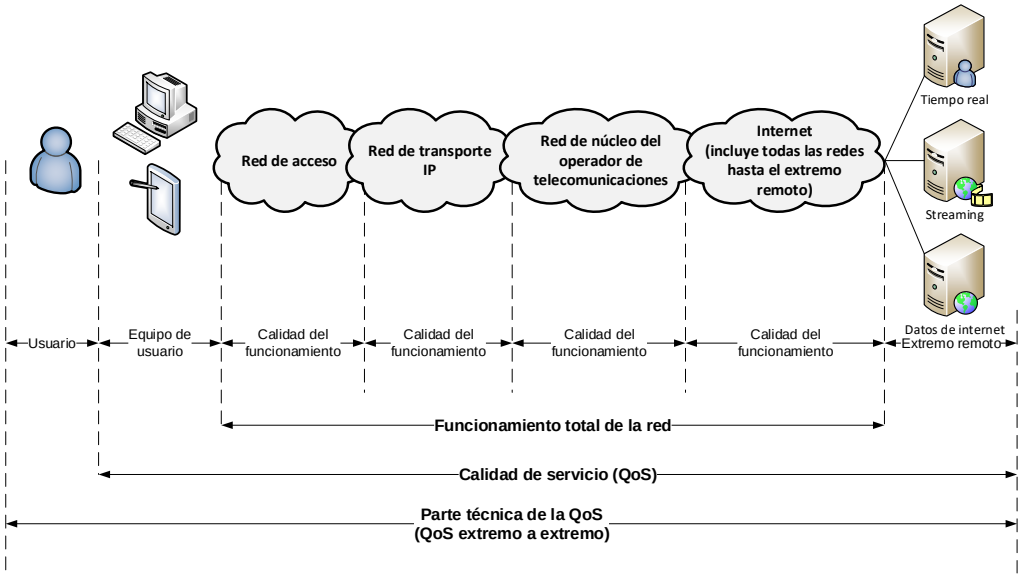


Figura 1-10 Calidad de servicio extremo a extremo [25]

Con relación a la QoS extremo a extremo, en la Tabla 1-1 se observan las recomendaciones de la UIT-T más relevantes sobre la QoS y la QoE referente a los tipos de redes de telecomunicaciones y sus correspondientes servicios.

Tabla 1-1 Recomendaciones relevantes de la UIT-T sobre QoS y QoE [25]

Recomendación UIT	Ejemplo de recomendación UIT-T sobre QoS/ QoE
Serie E: Operación general de la red, servicio telefónico, operación telefónica y factores humanos.	• E.800: Definición de términos relacionados con la calidad del servicio. • E.802: Marco y metodologías para la determinación y aplicación de parámetros QoS • E.803: Parámetros de calidad de servicio para soportar aspectos de servicio • E.804: aspectos de QoS para servicios populares en redes móviles • E.807: Definiciones y métodos de medición asociados de parámetros centrados en el usuario para el manejo de llamadas en el servicio de voz móvil celular • Suplemento 9 de la serie E: Directrices sobre aspectos regulatorios de QoS
Serie G: Sistemas y medios de transmisión, sistemas y redes digitales	• G.1000: Calidad de servicio de comunicaciones: un marco y definiciones • G.1010: Categorías de QoS multimedia para el usuario final • G.1011: Guía de referencia para metodologías de evaluación de la calidad de la experiencia

Recomendación UIT	Ejemplo de recomendación UIT-T sobre QoS/ QoE
Serie P: Terminales, métodos de prueba subjetivos y objetivos	• P.10/G.100: Vocabulario para el rendimiento y la calidad del servicio. • P.800: Métodos para la determinación subjetiva de la calidad de transmisión. • P.863: Evaluación objetiva perceptiva de la calidad de escucha • P.1200-P.1299: Modelos y herramientas para la evaluación de calidad de medios transmitidos
Serie Y: Infraestructura de información global, aspectos de protocolo de Internet y redes de próxima generación (NGN)	• Y.1540: Servicio de comunicación de datos de protocolo de Internet: transferencia de paquetes IP y parámetros de rendimiento de disponibilidad • Y.1541: objetivos de rendimiento de la red para servicios basados en IP • Y.1542: Marco para lograr objetivos de rendimiento de IP de extremo a extremo • Y.1543: Mediciones en redes IP para evaluación de desempeño entre dominios. • Y.1545.1: Marco para monitorear la calidad del servicio de los servicios de red IP

1.4.1 Puntos de vista de la QoS

De acuerdo con [25], el modelo de desempeño definido por la UIT-T en la recomendación UIT-T G.1000 establece cuatro puntos de vista sobre QoS entre el cliente y el proveedor de servicio los cuales son los siguientes de acuerdo con la Figura 1-11:

- **Necesidades de QoS del cliente:** Las necesidades de QoS del cliente definen el nivel de calidad que se exige en un determinado servicio, y se pueden expresar en lenguaje corriente. Al cliente no le interesa saber cómo se presta el servicio ni los aspectos del diseño interno de la red, pues sólo le importa la calidad total del servicio de extremo a extremo [35].
- **QoS ofrecida por el proveedor de servicio:** La QoS ofrecida por el proveedor de servicio es una declaración del nivel de calidad que él espera ofrecer al cliente, y que se expresa mediante valores atribuidos a los parámetros de calidad. Esta forma de calidad de servicio es especialmente útil para la planificación y para los acuerdos de nivel de servicio. Cada servicio tendrá su propio conjunto de parámetros de QoS (como en las clases de QoS de la Rec. UIT-T Y.1540 para los servicios IP). El

proveedor de servicio puede expresar la QoS ofrecida en lenguaje corriente para el cliente, y en lenguaje técnico para su uso en la industria [35].

- **QoS conseguida o entregada por el proveedor de servicio:** La QoS que consigue el proveedor de servicio es una declaración del nivel de calidad real alcanzado y entregado al cliente, y se expresa mediante valores asignados a parámetros, que deben ser idénticos a los especificados para la QoS ofrecida, de forma que se los pueda comparar para evaluar el nivel de calidad de funcionamiento logrado. Estos valores de calidad de funcionamiento se resumen para periodos específicos, por ejemplo, el mes anterior [35].
- **QoS percibida por el cliente:** La QoS percibida por los usuarios o clientes es una declaración en la que se expresa el nivel de calidad que ellos 'creen' haber experimentado, y que se expresa normalmente en función del grado de satisfacción y no en términos técnicos. Esta calidad de servicio se mide con encuestas a los clientes y sus comentarios sobre los niveles de servicio, y puede ser utilizada por el proveedor de servicio para determinar la satisfacción del cliente en cuanto a la calidad de servicio. Así, por ejemplo, un cliente puede decir que durante una cantidad inaceptable de ocasiones tuvo dificultad para realizar una llamada a través de la red y otorgar una calificación de 2 en una escala de 5, donde 5 corresponde a un servicio excelente. Idealmente, debería haber una correspondencia uno a uno entre la QoS entregada y la percibida [35].

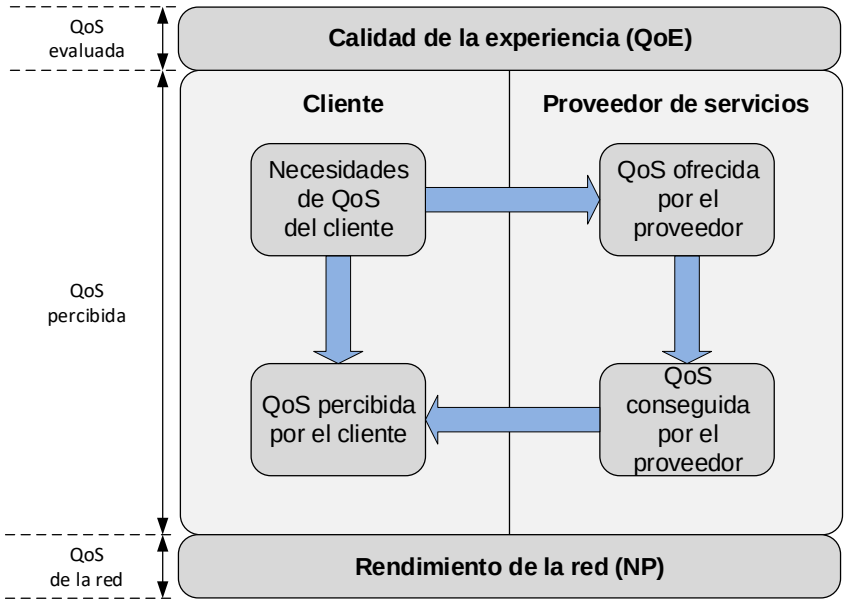


Figura 1-11 Puntos de vista sobre QoS [25]

1.4.2 Métricas de desempeño en QoS

La recomendación UIT-T Y.2617, define las métricas de QoS entre las que se encuentra el retardo, la variación del retardo (jitter) y la relación de pérdida de paquetes, especifica la asignación de rendimiento de extremo a extremo cuando una red pública de datos de telecomunicaciones por paquetes (PTDN) interactúa con otros PTDN o redes de paquetes de datos (PDN), describe la clasificación del servicio en términos de servicios de velocidad de bits constante y servicios de velocidad de bits variable, y define mecanismos de QoS garantizados en un PTDN [36]:

- **Rendimiento (throughput):** Definido por el RFC 1242 como la cantidad de información del usuario transferida en un período de tiempo [37], es la tasa máxima a la cual ninguna de las tramas enviadas es descartada por el dispositivo.
- **Latencia (delay)**: La latencia o retardo unidireccional, definida en la RFC 2679, es el tiempo entre el primer bit que ingresa a la red y el primer bit que llega al usuario a través de la red. Incluye tres factores: retraso de transmisión, retraso de propagación y retraso de procesamiento de nodo (incluido el retraso de espera).
- **Variación de latencia (jitter):** El jitter, definido en el RFC 3393 como la fluctuación unidireccional, es la diferencia entre la latencia máxima y la latencia mínima dentro de una ventana de tiempo específica.
- **Tasa de pérdida de paquetes (packet loss ratio):** Definida en el RFC 2680 y RFC 3357, la tasa de pérdida de paquetes (PLR) unidireccional, es el número total de paquetes que no se entregan a través de la red dividido por el número total de paquetes transmitidos dentro de una ventana de tiempo específica.

1.4.3 Mean Opinion Score (MOS)

En [25] se observa que la puntuación media de opinión o MOS, por sus siglas en inglés. Es un método de evaluación subjetivo de la QoE y actualmente es el método estandarizado más común para la evaluación de la calidad de un canal de voz. Se evalúa mediante un puntaje que varía de 1 (peor) a 5 (mejor), contemplado en la Tabla 1-2. Un puntaje en MOS entre 3.6 y 4 es aceptable para la mayoría de las redes, sin embargo, es deseable que se tenga un puntaje mayor a 4 en una red. La UIT ha definido el estándar P.862 para la evaluación del MOS en función del códec utilizado en una llamada.

Tabla 1-2 Mean Opinion Score (MOS) [25]

Puntaje	Definición	Descripción
5	Excelente	Una señal de voz perfecta grabada en una cabina silenciosa
4	Bueno	Inteligente y natural como la calidad del teléfono de larga distancia
3	Aceptable	Se requiere de algún esfuerzo para escuchar la comunicación
2	Pobre	Baja calidad y habla difícil de entender
1	Malo	Habla poco clara, entrecortada

1.5 Parámetros de desempeño para servicios IP en redes de extremo a extremo

La UIT en la recomendación Y.1540 define los parámetros que se pueden utilizar para especificar y evaluar la calidad de funcionamiento en cuanto a velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP servicios IP. Los parámetros definidos se aplican al servicio IP de extremo a extremo, punto a punto, y a tramos de la red que prestan, o contribuyen a prestar, ese servicio [38]. Los parámetros más importantes son los siguientes [3], [38], [39]:

- ***IPTD (IP Packet Transfer Delay):*** Corresponde al tiempo que tarda el paquete en pasar por un componente de la red (host, dispositivo de interconectividad o segmento de red). Este retardo se puede calcular en función de:
  - La distancia: Retardo de propagación (Propagation delay).
  - Procesamiento en los nodos: Retardo de transporte (Transport delay).
  - Conversión de la señal: Retardo del códec (Codec delay).
  - Suavizado de la variabilidad del retardo: Jitter Buffer Delay.

  El IPTD se puede calcular de acuerdo a la siguiente ecuación [40]:

$$IPTD = \frac{\sum_{i=1}^{n} x_i}{n} \tag{1-1}$$

Donde:

x_i: $Retardo\ de\ cada\ paquete$
n: $Número\ de\ paquetes$

- **IPDV (*IP Packet Delay Variation o jitter*):** es la variación de retardo entre los diferentes paquetes enviados desde el origen hacia el destino (medido durante un período de tiempo determinado, en milisegundos) [41], puede ser calculado como muestra la siguiente ecuación [40]:

$$IPDV = \frac{\sqrt{\sum_{i=1}^{n} x_i^{\,2} - n * IPTD^2}}{n-1} \quad (1\text{-}2)$$

Donde:

x_i: $Retardo\ de\ cada\ paquete$
n: $Número\ de\ paquetes$

- **IPLR (*IP Packet Loss Ratio*):** Tasa de pérdida de paquetes. Su valor se obtiene de la relación entre el total de paquetes perdidos y el total de paquetes transmitidos en un flujo de datos.
- **IPER (*IP Packet Error Ratio*):** Tasa de paquetes con errores; su valor se obtiene de la relación entre el total de paquetes con errores y el total de paquetes sin errores transmitidos en un flujo de datos determinado.

1.5.1 Concatenación de secciones de la red y sus valores de QoS

Con respecto a la comunicación de extremo a extremo, el modelo de red también se conoce como UNI a UNI (ver
Figura **1-12**). El rendimiento de extremo a extremo de un trayecto se puede estimar si se conoce el rendimiento de todas las subsecciones en el camino [25].

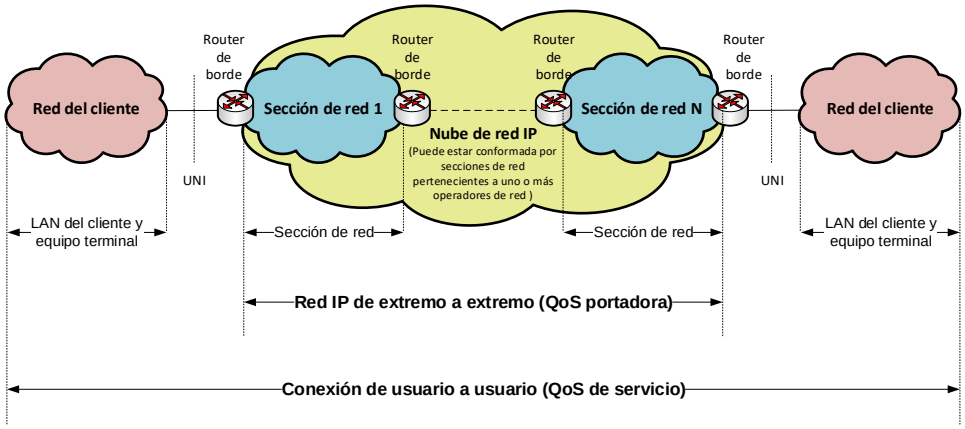


Figura 1-12 Trayecto de referencia para la QoS de UNI a UNI [25], [42]

En la recomendación Y.1541 se especifican los valores de calidad de funcionamiento IP de la red (UNI-UNI) para cada uno de los parámetros de calidad de funcionamiento definidos en la Rec. UIT-T Y.1540 [42]. Algunos parámetros para servicios IP se muestran a continuación:

- ***Retardo medio de transferencia (Mean transfer delay):*** En cuanto al parámetro de calidad de funcionamiento del retardo medio de transferencia de paquetes IP (IPTD), la calidad de funcionamiento UNI-UNI es la suma de los valores medios de las secciones de la red.

  Los valores del IPTD se expresan en segundos y su precisión mínima es de un microsegundo. Si la precisión de un valor es inferior, los dígitos no utilizados se ponen a cero [42].
- ***Tasa de pérdidas (Loss ratio):*** Para el parámetro de calidad de funcionamiento de tasa de pérdidas de paquetes IP (IPLR), la calidad de funcionamiento UNI-UNI se puede calcular mediante la probabilidad de la transferencia de paquetes con éxito a través de n secciones de red, del siguiente modo [42]:

$$IPLR_{UNI-UNI} = 1 - \prod_{i=1}^{n} 1 - IPLR_{NS_n} \tag{1-3}$$

Donde:

$$IPLR_{NSn}: Tasa\ de\ pérdidas\ de\ paquetes\ IP\ de\ la\ sección$$

Esta relación no impone límites sobre los valores de los parámetros, de modo que se prefiere a otras aproximaciones, como por ejemplo la suma simple de tasas de pérdidas. En todas las mediciones se utilizará el mismo valor de $T_{\text{máx}}$ (el tiempo de espera para declarar un paquete perdido). Las unidades de valores IPLR son paquetes perdidos por total de paquetes enviados, con una precisión mínima de 10^{-9}. Si la precisión de un valor es inferior, los dígitos no utilizados se ponen a cero [42].

- **Tasa de paquetes con errores (*Error packet ratio*):** Para el parámetro de calidad de funcionamiento de la tasa de errores en los paquetes IP (IPER), la calidad de funcionamiento UNI-UNI se puede calcular invirtiendo la probabilidad de transferencia de paquetes sin errores a través de n secciones de red, del siguiente modo [42]:

$$IPER_{UNI-UNI} = 1 - \prod_{i=1}^{n} 1 - IPER_{NS_n} \tag{1-4}$$

Donde:

$$IPER_{NSn}: Tasa\ de\ errores\ en\ los\ paquetes\ IP\ de\ la\ sección$$

Esta relación no impone límites sobre los valores de los parámetros, de manera que se prefiere a otras aproximaciones, como por ejemplo la suma simple de tasas de errores en los paquetes. Las unidades de valores de las IPER son paquetes con errores por total de paquetes enviados, con una precisión mínima de 10^{-9}. Si la precisión de un valor es inferior, los dígitos no utilizados se ponen a cero [42].

- **Relación provisional para la variación del retardo (*Delay variation*):** La relación para calcular la calidad de funcionamiento de variación de retardo (IPDV) UNI-UNI a partir de los valores de las secciones de la red debe reconocer la naturaleza subaditiva de estas últimas, por lo que será difícil calcular este parámetro con precisión sin disponer de suficiente información sobre la distribución de los retardos individuales. Si, por ejemplo, se conocen o miden todas las caracterizaciones de las distribuciones de retardo independientes, pueden convolucionarse para estimar la distribución combinada. No es frecuente que esta información detallada se comparta entre los operadores, y probablemente no esté disponible en forma de distribución continua. Por consiguiente, la estimación de la $IPDV_{\mathrm{UNI-UNI}}$ puede tener una precisión limitada. Habida cuenta de que existen estudios en curso sobre este tema, la relación de estimación que figura se ha especificado de manera provisional, y esta cláusula podría variar en el futuro al tomar en consideración nuevas conclusiones o experiencias operacionales reales [42].

1.5.2 Definiciones de clases de QoS de las redes IP

En la recomendación UIT-T Y.1541 se describen las clases de QoS de red definidas actualmente (ver Tabla 1-3). Cada clase de QoS de red crea una combinación específica de límites en los valores de la calidad de funcionamiento. De igual manera, se incluyen directrices sobre hasta cuándo se podría utilizar cada clase de QoS de red, pero no se obliga a utilizar ninguna en particular en ningún contexto especial [42].

En cada clase se definen los valores límites objetivo, estos valores se aplican a las redes IP públicas. Se considera que los objetivos son alcanzables en las implementaciones de la red IP comunes. El compromiso del proveedor de servicios de red ante el usuario es tratar de entregar los paquetes de modo que se alcancen cada uno de los objetivos aplicables. La gran mayoría de los trayectos IP que ofrecen conformidad con la

recomendación UIT-T Y.1541, deberían satisfacer estos objetivos. Para algunos parámetros, la calidad de funcionamiento en trayectos más cortos y/o menos complejos puede ser significativamente mejor siguiendo esta recomendación [42].

De acuerdo con la recomendación, se sugiere un intervalo de evaluación de un minuto para IPTD, IPDV e IPLR, y en todos los casos se debe registrar el intervalo con el valor observado. Cualquier minuto observado debe cumplir esos objetivos. Los proveedores de servicios de red pueden decidir ofrecer compromisos de calidad de funcionamiento mejores que los de estos objetivos [42].

En algunas clases de QoS de red se designa el valor de algunos parámetros de calidad de funcionamiento como "Sin especificar". En estos casos, la UIT-T no establece objetivos con relación a estos parámetros. Los operadores de red pueden elegir unilateralmente asegurar algún nivel mínimo de calidad para los parámetros no especificados, aunque la UIT-T no recomienda ningún mínimo de este tipo [42].

Los usuarios de estas clases de QoS deben ser conscientes de que la calidad de funcionamiento de los parámetros no especificados puede, a veces, ser arbitrariamente deficiente. Ahora bien, se espera que el IPTD medio no sea mayor de un segundo [42].

Tabla 1-3 Definiciones de clases de QoS de las redes IP [42]

Definiciones de clases de QoS de las redes IP	Servicio / Aplicación	IPTD	IPDV	IPLR	IPER
Clase 0	Tiempo real, sensibles a la fluctuación de fase, alta interacción (Voz sobre IP - VoIP, Videoconferencia - VTC)	$\leq 100ms$	$\leq 50ms$	$\leq 10^{-3}$	$\leq 10^{-4}$
Clase 1	Tiempo real, sensibles a la fluctuación de fase, alta interacción (Voz sobre IP - VoIP, Videoconferencia - VTC)	$\leq 400ms$	$\leq 50ms$	$\leq 10^{-3}$	$\leq 10^{-4}$
Clase 2	Datos transaccionales, altamente interactivas (señalización)	$\leq 100ms$	Sin especificar	$\leq 10^{-3}$	$\leq 10^{-4}$

Definiciones de clases de QoS de las redes IP	Servicio / Aplicación	IPTD	IPDV	IPLR	IPER
Clase 3	Datos transaccionales, interactivas	$\leq 400ms$	Sin especificar	$\leq 10^{-3}$	$\leq 10^{-4}$
Clase 4	Datos transaccionales, interactivas (Video streaming)	$\leq 1s$	Sin especificar	$\leq 10^{-3}$	$\leq 10^{-4}$
Clase 5	Aplicaciones tradicionales de redes IP por defecto	Sin especificar	Sin especificar	Sin especificar	Sin especificar
Clase 6	Sin especificar	$\leq 100ms$	$\leq 50ms$	$\leq 10^{-5}$	$\leq 10^{-6}$
Clase 7	Sin especificar	$\leq 400ms$	$\leq 50ms$	$\leq 10^{-5}$	$\leq 10^{-6}$

En general, se pueden usar las clases de QoS definidas para ciertos tipos de aplicaciones considerando sus requisitos de QoS, dados de la siguiente manera [25]:

- La clase 0 y clase 1 son apropiadas para aplicaciones en tiempo real que son sensibles al retardo medio y a las variaciones del retardo (por ejemplo, VoIP, servicios de video telefonía) donde la Clase-0 tiene un límite inferior en el parámetro IPTD y, por lo tanto, puede usarse para voz (sin video), juegos o algunos servicios inteligentes de tiempo crítico (por ejemplo, vehículos sin conductor).
- La clase 2 y clase 3 están dirigidas a datos de transacciones, de los cuales la clase-2 se utiliza para señalizar el tráfico, mientras que la clase 3 es para aplicaciones interactivas.
- La clase 4 está dirigida a transacciones cortas, transmisión de video o datos masivos.
- La clase 5 no está especificada (con respecto a todos los parámetros de rendimiento) y está dirigida a las aplicaciones tradicionales de Internet de mejor esfuerzo.
- Las clases 6 y 7 solo se especifican provisionalmente en la tabla. Estas clases se utilizan para ciertas aplicaciones nuevas o emergentes con un rendimiento estricto de QoS. También introducen en su definición un nuevo parámetro denominado tasa de reordenamiento de paquete IP (IP packet Reordering Ratio, IPRR).

1.6 Marcos de referencia para la QoS

Un cliente puede requerir servicios de conectividad tales como datos (internet de alta velocidad - HSI), de conectividad (redes privadas virtuales VPN de nivel 2 - L2 o nivel 3 - L3), voz (VoIP) o video (video por demanda - VoD), en los cuales cada uno de estos tiene diferentes demandas de los recursos de la red del proveedor para su entrega al usuario final. Si los recursos del proveedor de servicio contemplados en los SLA's no se administran, los usuarios tendrían problemas por congestión y en consecuencia una mala experiencia de servicio [43].

1.6.1 Marco de referencia de la IETF

La IETF define los siguientes mecanismos para la administración de la QoS [43]:

- **Mejor esfuerzo (Best effort)**: Es el modelo tradicional de la Internet sin garantías de QoS, donde las redes IP simplemente transportan la información entre un origen y un destino. Los paquetes siguen un esquema de encolamiento FIFO (First In – First Out), donde los paquetes se envían de forma aleatoria, sin tomar en cuenta las prioridades de los servicios ni el tipo de usuario, por lo que no hay manera de saber que clientes deben transmitir primero (ver Figura 1-13).

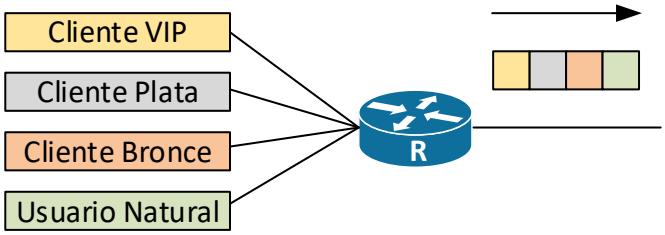


Figura 1-13 Método de mejor esfuerzo [43]

Los mecanismos descritos a continuación y trabajados en la ingeniería de tráfico (TE, por sus siglas en inglés) (ver Figura 1-14), propenden por establecer un orden en el que se transmite la información de forma adecuada, garantizando la experiencia del usuario al entregar los servicios según lo acordado en los SLA's establecidos ayudando a prevenir interrupciones, latencias o caídas repentinas del servicio [43].

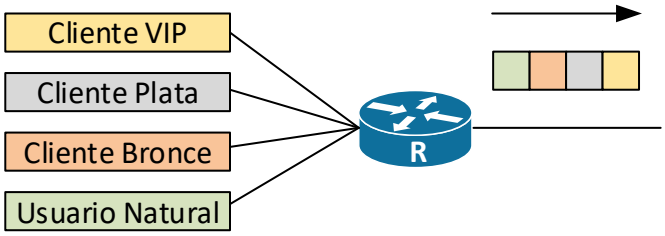


Figura 1-14 Transmisión de información al aplicar mecanismos de QoS [43]

- **Servicios integrados (IntServ):** Fue el primer mecanismo estandarizado por la IETF, implementa una reserva del canal y control de admisión de los paquetes a través de los nodos que conforman la red mediante el protocolo RSVP (Resource Reservation Protocol), por lo cual es un mecanismo e2e, consta de tres tipos de servicios los cuales son de carga controlada, garantizada y mejor esfuerzo [62], sin embargo, posee problemas de escalabilidad y complejidad por lo que actualmente no es el más implementado.
- **Servicios diferenciados (DiffServ):** Es el método más utilizado para la diferenciación de tráfico, mejora las limitaciones que tiene IntServ [63],en la cual los paquetes son clasificados en un número limitado de clases, por lo que los routers solo deben almacenar la información de la clase en lugar de las conexiones o flujos, por lo que es un mecanismo de QoS salto a salto (hop-by-hop) [25]. Todos los casos de interoperabilidad entre operadores se basan en el uso de los SLA que son una parte integral de la definición de DiffServ [64].
- **Multi-protocol Label Switching (MPLS):** Este es el enfoque "predeterminado" para el aprovisionamiento de QoS en redes IP de transporte, que se puede combinar con DiffServ y otros protocolos como BGP o protocolos VPN. En MPLS, los flujos se clasifican como diferentes tipos de tráfico. El flujo en cuestión se clasifica como una clase de tráfico de mayor prioridad por el proveedor de servicio (SP, por sus siglas en inglés), por lo que tiene menos retraso, más ancho de banda, etc [44].

  La implementación de una red IMS se vuelve más estructurada con el backbone IP/MPLS subyacente. La red IP/MPLS ofrece la facilidad de introducir nuevas clases de servicios IP con QoS diferenciado y enrutamiento de ingeniería de tráfico. Esto simplifica la implementación de la red IMS [15].

- **QoS basada en políticas:** Esto se usa típicamente para el aprovisionamiento de QoS entre proveedores de red (por ejemplo, las políticas BGP se usan para enrutar paquetes entre AS interconectados) [43].

1.6.2 Marco de referencia de la UIT

La UIT-T define los siguientes planos (ver Figura 1-15) para los mecanismos de QoS:

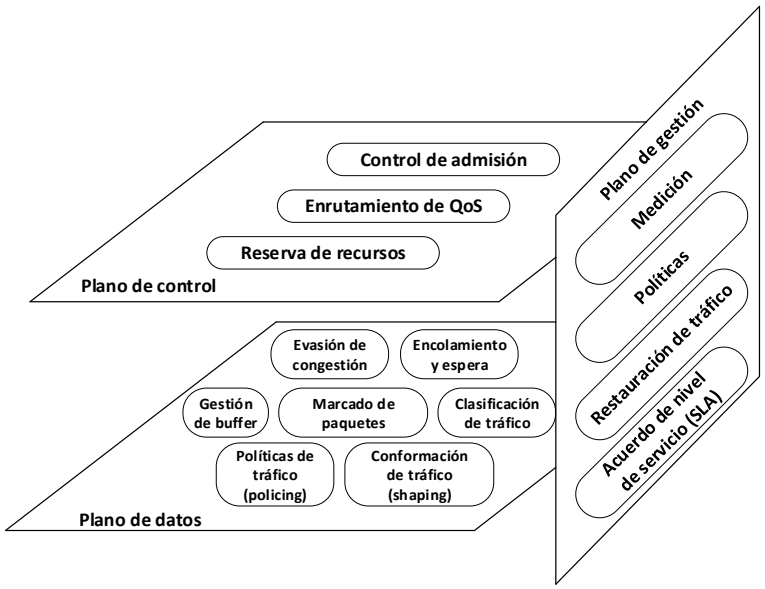


Figura 1-15 Marco de referencia de QoS de la UIT-T [25]

- **Plano de Control:** Incluye el control de admisión, el enrutamiento de QoS y la reserva de recursos.
- **Plano de datos:** Incluye varios aspectos de la gestión del tráfico, como la gestión del búfer, la prevención de la congestión, el marcado de paquetes, las colas y la programación, la clasificación del tráfico, la vigilancia del tráfico y la conformación del tráfico.
- **Plano de gestión:** Incluye el acuerdo de nivel de servicio (SLA), la restauración del tráfico, la medición y el registro, y las políticas.

El marco de la UIT-T incluye todos los estándares de la IETF en los tres planos mencionados, mostrando así la sinergia y esfuerzos entre ambas organizaciones en relación a la QoS [25].

1.7 Calidad de Servicio en IMS

La arquitectura IMS se centra en garantizar la QoS aplicando políticas entre peticiones específicas de las aplicaciones (Session Initiation Protocol - SIP/Session Description Protocol - SDP) y los flujos multimedia (Real-time Transport Protocol - RTP), las políticas son definidas por los operadores de la red según el tipo de negocio y requerimientos de servicios a nivel de aplicaciones, las cuales son utilizadas para gestionar los recursos de la red y mejorar la QoS [45].

En IMS el control de QoS juega un papel importante a través de una serie de indicadores a evaluar según el tipo de servicio (como el ancho de banda, el retardo e2e (delay), la variación del retardo (jitter), la velocidad de datos y la tasa de error de bit, etc.). En el contexto de una red IP un servicio es una descripción del tratamiento global de tráfico de un cliente a través de un dominio particular, un servicio solo es útil si cumple con los requerimientos del usuario final. Las organizaciones 3GPP y TISPAN definen un conjunto de cuatro clases de QoS para el transporte en redes, correspondiente a los servicios IMS, estos requerimientos también corresponden a la interconexión de las redes de acceso basadas en IP (IP-CAN) y las redes IMS. Estas cuatro clases se describen en la Tabla 1-4 [16], [21], [46], [47].

Tabla 1-4 Clases de QoS para el transporte en redes [16]

Clase de QoS	Característica	Ejemplo
Conversacional	Sensible a la variación el retardo, tolerancia limitada a la pérdida de paquetes	Conversación Audio/Video
Streaming	Tolerante pero sensible a la variación del retardo, tolerancia limitada a la pérdida de paquetes	Streaming de video
Interactivo	Sensible al retardo de ida y vuelta, paquetes transferidos de forma transparente con baja tasa de error de bit.	Colaboración, conferencia
Background	Insensible al retardo, de forma transparente con baja tasa de error de bit.	Email, Mensajería instantánea, Chat

Al establecer una sesión multimedia e2e, esta puede atravesar una serie de dominios administrativos heterogéneos en la NGN, en la cual el sistema de control de las políticas debe ser capaz de garantizar los recursos de calidad de servicio en todos los dominios implicados, como se puede ver en la Figura 1-16. Cada dominio define sus propios mecanismos y políticas para la provisión de QoS dependiendo de las tecnologías

de cada operador; sin embargo, en una sesión e2e es necesaria una negociación mutua de SLA entre los dominios implicados. El SLA es un contrato formal, negociado entre dos partes, que define el compromiso en los niveles del rendimiento de la red de servicio y capacidad de respuesta [48]. Las dos partes pueden ser un usuario y un operador, o dos operadores en donde alguno toma el papel de cliente para la compra de servicios de otro proveedor de servicios [49].

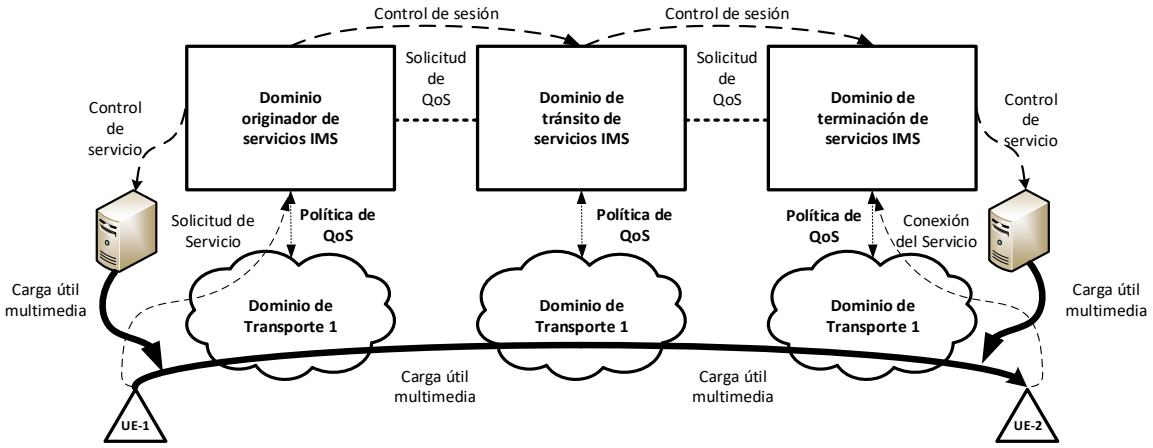


Figura 1-16 Gestión de QoS entre dominios [16]

Con relación a los puntos mencionados anteriormente se observan las siguientes limitaciones respecto a la QoS en interconexión [50]:

- Las aplicaciones tienen diversas necesidades de ancho de banda y rendimiento.
- Los dispositivos de usuario tienen capacidades mejoradas pero variadas respecto a los servicios consumidos y desempeños esperados.
- Se utilizan diferentes tecnologías de acceso.
- Múltiples proveedores u operadores están involucrados de extremo a extremo.

1.7.1 Arquitecturas de QoS basadas en políticas

Para proveer QoS en NGN se han definido diferentes arquitecturas para el control de los flujos de datos, estas arquitecturas han sido definidas por las organizaciones IETF, ETSI TISPAN y 3GPP. La IETF describe un marco de políticas a través del RFC 2753 [51] como se puede ver en la Figura 1-17, en el que los conjuntos de reglas de políticas definidos en forma de modelos se convierten en configuraciones de red o dispositivos en un dominio administrativo. Estas reglas son almacenadas en repositorios de políticas denominados Policy Decision Point (PDP) o Policy Decision Function (PDF), estos

repositorios recuperan las reglas de políticas apropiadas en respuesta a las peticiones de políticas que se generan por los requerimientos de QoS de los servicios [52], el Policy Enforcement Point (PEP) es el lugar en un servidor que hace cumplir las políticas de control de admisión y las decisiones de política en respuesta a una petición de transacción de un usuario que quiera acceder a un recurso en un servidor de red.

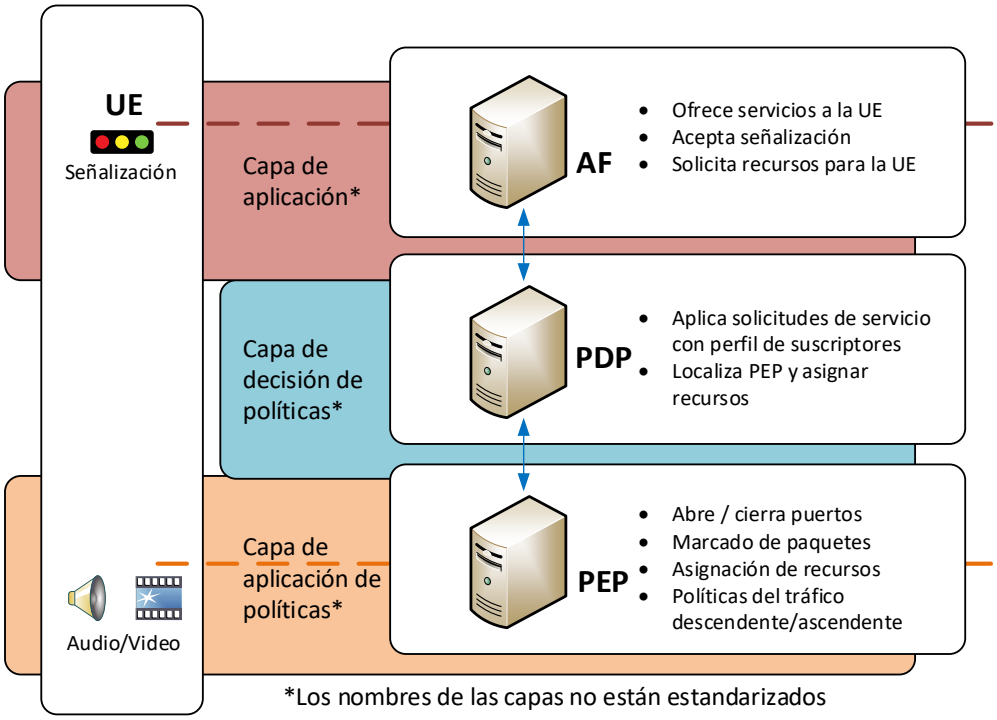


Figura 1-17 Arquitectura IETF de Control de Admisión basada en políticas [53]

ETSI TISPAN ha desarrollado su propia arquitectura de aseguramiento de QoS a través del estándar ETSI ES 282 003 [54] que se denomina Resource and Admission Control Subsystem (RACS, ver Figura 1-18), el cual es un subsistema NGN responsable de los elementos de control de la política, la reserva de recursos y control de admisión. Es el principal componente que interactúa con la red de acceso, así como el núcleo de la red que transporta un servicio, puede influir en las prioridades de los paquetes mediante el protocolo DiffServ, también puede reservar recursos con RSVP [55]. El RACS es el elemento lógico de la red más importante para la interacción entre la capa de servicio y las funciones de transferencia de los recursos de control y soporte de QoS dentro de la respectiva NGN [56].

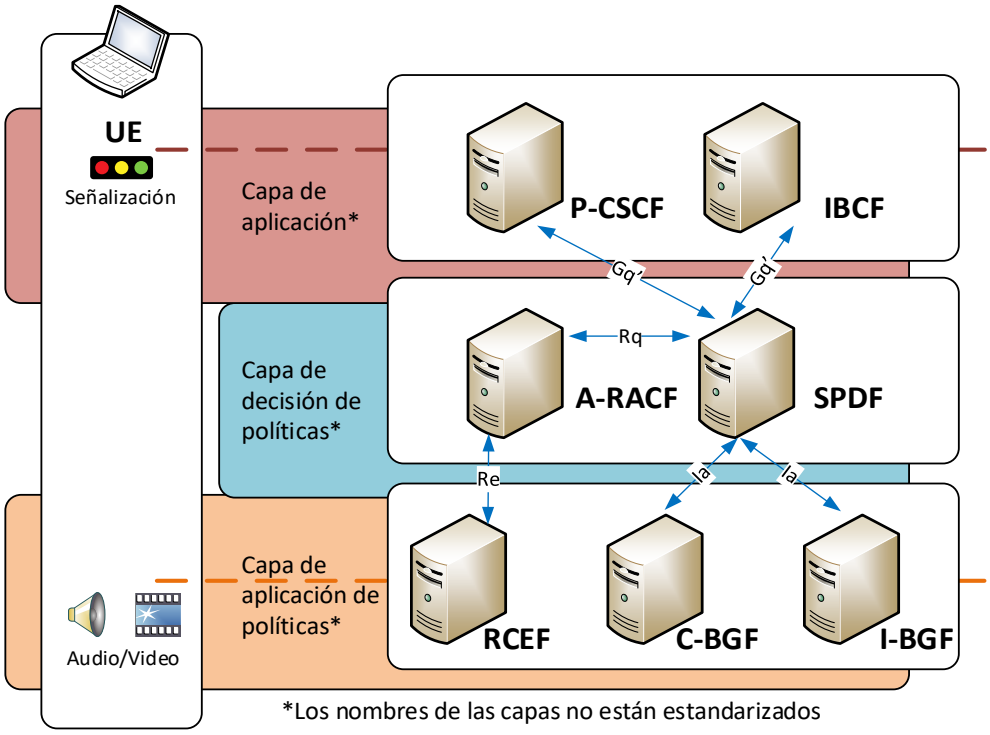


Figura 1-18 Arquitectura ETSI TISPAN RACS [53]

El 3GPP define en la especificación TS 23.203 [57] una arquitectura basada en políticas de QoS denominada PPC (Policy and Charging Control, ver Figura 1-19) desde el punto de vista de la movilidad, fue introducido en el 3GPP R7 [58], en ella se define la entidad PCRF (Policy and Charging Rules Function) la cual está encargada del control de políticas y carga, así como la entidad de Policy and Charging Execution Function (PCEF) y los puntos de referencia asociados a éstas [59]. El concepto y la arquitectura de QoS utilizada por el 3GPP se detallan en la especificación 3GPP TS 23,107 [60]. El concepto de QoS extremo a extremo y la arquitectura utilizada por el 3GPP se describe en la especificación 3GPP TS 23.207 [61]. La arquitectura PCC es flexible y aplicable a una variedad de servicios, redes de acceso y modelos de carga, sin embargo, no está bien adaptada a servicios multimedia con requisitos de QoS negociables de forma dinámica de acuerdo a las condiciones variables en la red [62].

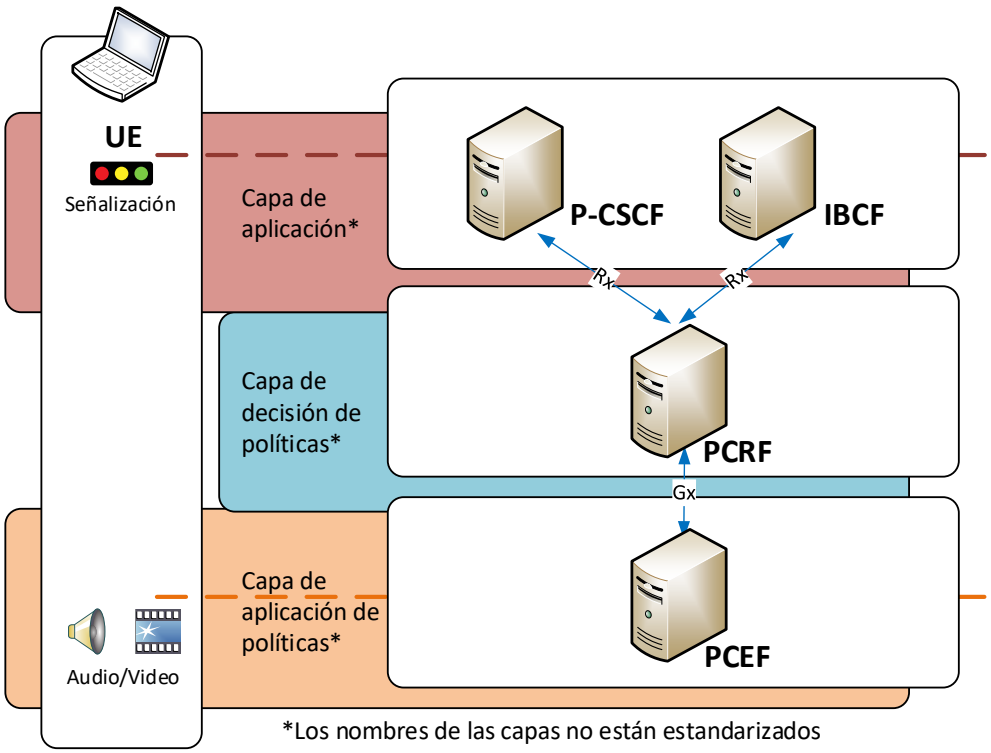


Figura 1-19 Arquitectura 3GPP PCC [53]

1.8 Trabajos relacionados en el área de investigación

La QoS es un tema complejo, donde convergen diversidad de tecnologías a nivel de transporte de datos. La Tabla 1-5, muestra algunos trabajos representativos realizados con la QoS en redes NGN, en los que se soporta la problemática de este proyecto de investigación.

Tabla 1-5 Trabajos relacionados en el área de investigación

Alcance	Método	Conclusión representativa	Herramienta software	Referencia
Proponer un modelo para evaluar la calidad de servicio (QoS) de un servicio de video llamada implementado sobre la red virtualizada IMS.	Evaluación de QoS en un Core IMS intra-operador, utilizando el hipervisor VMWare ESXi, red de transporte basada en un switch HP 5500. No se aplican políticas de QoS a nivel de la red de transporte. Se realiza un análisis de tiempos de respuesta	La variable que más afecta el rendimiento de Open IMS Core es el número de usuarios, ya que a medida que esta variable aumenta afecta el tiempo de respuesta y la perdida de información. De la misma forma se puede observar que	Open IMS Core VMWare ESXi	[6]

Alcance	Método	Conclusión representativa	Herramienta software	Referencia
	del tráfico SIP en función de la escalabilidad horizontal y vertical del ISP IMS.	el promedio de concurrencia de conexiones también afecta el rendimiento ya que este se satura a medida que más usuarios desean conectarse en un determinado tiempo.		
Mapeo de los requisitos de QoS a nivel de red en IMS	Para proporcionar QoS de extremo a extremo, es necesario administrar la QoS dentro de cada dominio a lo largo de la ruta. Para resolver los desafíos de QoS en IMS, las emulaciones y simulaciones deben realizarse. OPNET Modeler es la herramienta de simulación de software que permite la investigación e investigación del comportamiento de la red. Un objetivo parcial de este artículo es averiguar si las capacidades de este simulador de red son suficientes para analizar y diseñar redes IMS y monitorear la calidad del servicio.	Se configuraron dos mecanismos de QoS para asegurar la QoS: Servicios Integrados y Servicios Diferenciados. También se consideró como comparación el mecanismo de Mejor Esfuerzo, que no incluye ningún tipo de notificación de control de calidad. La posibilidad de emplear tecnologías DiffServ e IntServ en el entorno IMS con el fin de lograr un soporte completo de QoS para aplicaciones en tiempo real fue el objeto de interés porque la arquitectura IMS no aborda todos los problemas relacionados con redes heterogéneas.	OPNET	[7]
QoS en la interconexión de redes de próxima generación	El documento tiene en cuenta las estipulaciones actuales para la comunicación intra e interdominio en redes inalámbricas, alámbricas y de banda ancha en la India. Las métricas desarrolladas se prueban con datos de campo e informes	Mantener la QoS de E2E requeriría asegurar la QoS en las interconexiones además de cuidar la QoS intradominio. La arquitectura NGN en capas, las redes heterogéneas con diferentes clases de QoS y parámetros de QoS y la falta de disponibilidad de estándares	No utiliza, se demuestra utilizando datos de campo e informes proporcionados por el operador	[63]

Alcance	Método	Conclusión representativa	Herramienta software	Referencia
	proporcionados por el operador y se demuestra su utilidad.	universalmente aceptados para QoS entre dominios dificultan esta tarea. Si bien se pueden aprender algunas lecciones de las redes de voz y datos existentes, se requiere mucho trabajo para definir las clases de servicio y su mapeo en las clases de red y definir conjuntos de parámetros para diferentes servicios.		
Estado del arte sobre las herramientas para la implementación de redes 4G y 5G basadas es software	Revisión de los marcos, hardware y software basado en código abierto relacionado con las redes 4G y 5G en el que se brinda una perspectiva crítica sobre el estado de la técnica.	La “softwarización de todo” está en las tendencias actuales en informática, redes y comunicaciones, cómo no solo ha revolucionado la cuarta generación, sino que también ha establecido una forma radicalmente nueva, tanto técnica como comercial, para marcar el comienzo de la era 5G con éxito. Se ha centrado en los avances más recientes en el ecosistema 5G de código abierto y reprogramable. A pesar de que los operadores, proveedores y científicos están prestando mucha atención a las nuevas tecnologías definidas por software, estas soluciones aún no están listas para su implementación en redes comerciales 5G.	Diversas herramientas basadas en código libre para los elementos de acceso radio y core 4G y 5G	[64]

En el análisis comparativo de estos trabajos, se encuentra que es necesario realizar un estudio de las políticas de QoS aplicadas a tráfico de servicios convergentes (voz, datos y video) en un entorno emulado, debido a la complejidad de la red y a la variedad de tecnologías involucradas en las redes NGN heterogéneas. Cabe resaltar que así como a pesar de que los operadores, proveedores y científicos están prestando mucha atención a las nuevas tecnologías definidas por software, estas soluciones aún no están listas para su implementación en redes comerciales 5G [64].

Se observa la necesidad de establecer un lineamiento técnico que permita la provisión de QoS en interconexión, estudiando la red de transporte, que implemente políticas mediante DiffServ bajo MPLS, dado que los estudios revisados se enfocan en modelos simulados bajo OPNET [7] y en los casos en los que se ha implementado la red de forma emulada, estos estudios se enfocan en el rendimiento del Core IMS, dejando de lado la red de transporte [6].

1.9 Herramientas de emulación

Las herramientas de emulación permiten ejecutar mediante software un entorno que recrea los recursos de una plataforma física u otro software, en un entorno diferente para el cual fue diseñado originalmente. Tiene como ventajas la reducción de costos de operación y mantenimiento, sin embargo, al estar basado en software, tiene como limitaciones los recursos de hardware del equipo en el que se ejecute, tales como procesador, memoria RAM, memoria ROM, entre otros y la optimización que se haga en el uso los mismos en el sistema anfitrión.

1.9.1 Virtualización

La virtualización es una tecnología que permite crear una representación basada en software (o virtual) de una entidad física a través de un hipervisor, el cual permite crear, administrar y ejecutar máquinas virtuales, aislando el sistema operativo huésped (conocido como host) de los sistemas virtualizados (guest) [65], [66]. Actualmente, se pueden encontrar las siguientes soluciones de hipervisores como se puede ver en la Tabla 1-6.

Tabla 1-6 Soluciones de hipervisores

Hipervisor	Licencia	Desarrollador	Sistema Operativo	Referencia
Hyper-V	Propietaria	Microsoft	Windows	[67]
VMware Workstation	Propietaria	VMware	Multiplataforma	[68]
Oracle VM VirtualBox	Privativa / GPLv2	Oracle Corporation	Multiplataforma	[69]
QEMU	Varias (código abierto)	Fabrice Bellard	Multiplataforma	[70]
Kernel-based Virtual Machine o KVM	GPL y LGPL	Open Virtualization Alliance	Linux	[71]

1.9.2 Emuladores de red

Existen diferentes herramientas de emulación de entornos de red como se observa en la Tabla 1-7 que permiten crear ambientes de laboratorio de diferentes tecnologías de redes de datos, de fabricantes como Cisco, Huawei, Juniper, Nokia, Arista, Aruba, Fortinet, entre otros. Soluciones como GNS3, EVE-ng y su derivado (fork) PNETLab, presentan soporte de imágenes de equipos multivendor. En el caso de VIRL y eNSP, solo soportan las tecnologías del fabricante respectivo (Cisco y Huawei) [72], [73].

Tabla 1-7 Herramientas de emulación de red

Emulador	Licencia	Desarrollador	Sistema Operativo	Soporte Multivendor	Referencia
GNS3	GPLv3	Equipo de desarrollo GNS3	Multiplataforma	Si	[74]
Cisco VIRL 2.0	Propietaria	Cisco	Máquina virtual (imagen OVA)	No	[72]
eNSP	Privativa / GPLv2	Huawei	Windows	No	[73]
EVE-ng	Varias (código abierto)	Equipo de desarrollo EVE-ng	Máquina virtual (imagen OVA)	Si	[75]
PNETLab	Varias (código abierto)	Equipo de desarrollo PNETLab	Máquina virtual (imagen OVA)	Si	[76]

1.9.3 Entornos de núcleo IMS

En la Tabla 1-8 se pueden observar diferentes implementaciones basadas en software del núcleo IMS, estos desarrollos se denominan bancos de pruebas o testbeds [77]. El Instituto Fraunhofer FOKUS desarrolló el proyecto OpenIMSCore para crear un banco de pruebas en NGN, con el objetivo de crear servicios en IMS. En esta solución se encuentran las entidades del núcleo IMS P/S/I/CSCF y HSS. El proyecto inició basándose en el servidor

SIP Open SIP Express Router (También conocido como OpenSER) [78], del cual se desprende el proyecto Kamailio que implementa los módulos P/S/I/CSCF en el servidor SIP, donde para completar el núcleo IMS, es necesario conectarlos con HSS externos, que pueden ser propietarios o de código abierto como el desarrollado por el instituto Fraunhofer FOKUS [77].

El proyecto Clearwater IMS, desarrollado por la empresa Metaswitch, inició como un proyecto de código abierto; sin embargo, fue descontinuado y actualmente solo se ofrece soporte de manera comercial. Implementa las entidades P/S/I/CSCF a nivel del core IMS, y ofrece otras como el HSS, BGCF y TAS [79].

Tabla 1-8 Entornos de núcleo IMS

Testbed	Licencia	Desarrollador	Sistema Operativo	Entidades	Referencia
OpenIMSCore	GPLv2	Fraunhofer FOKUS	Linux	P-CSCF S-CSCF I-CSCF HSS	[77]
Kamailio SIP Server	GPL	The Kamailio SIP Server Project	Linux	P-CSCF S-CSCF I-CSCF	[78]
Clearwater IMS	GNU GPLv3	Metaswitch	Linux Máquina virtual (imagen OVA)	P-CSCF S-CSCF I-CSCF HSS BGCF TAS	[79]

1.9.4 Servidores IPTV

La Tabla 1-9 muestra algunos de los servidores IPTV que se encuentran en el mercado. VLC Media player es un reproductor multimedia libre y de código abierto multiplataforma y un “framework” que reproduce la mayoría de los archivos multimedia. Este reproductor puede configurarse a manera de servidor IPTV [80].

Wowza Streaming Engine es un software de servidor de medios de transmisión unificado desarrollado por Wowza Media Systems bajo JAVA, como solución comercial. El servidor se utiliza para la transmisión de video en vivo y bajo demanda, audio y aplicaciones de Internet enriquecidas a través de redes IP a computadoras de escritorio, portátiles y tabletas, dispositivos móviles, decodificadores de IPTV, televisores conectados a Internet, consolas de juegos, y otros dispositivos conectados a la red [81].

Tabla 1-9 Servidores IPTV

Entorno	Licencia	Desarrollador	Sistema Operativo	Soporte Multicast	Referencia
VLC Media player	GPLv2.1+	VideoLAN Jean-Baptiste Kempf	Multiplataforma	Si	[80]
Wowza Streaming Engine	Propietaria	Wowza Media Systems	Multiplataforma	Si	[81]

1.9.5 Tecnologías de contenedores

En lugar de virtualizar la pila de hardware como en el enfoque de las máquinas virtuales, los contenedores realizan la virtualización en el nivel del sistema operativo, se ejecutan directamente en el kernel del sistema operativo (OS). Esto significa que los contenedores son mucho más livianos: comparten el kernel del OS, se inician con más rapidez y usan una fracción de la memoria en comparación con el arranque de todo el OS [82]. La Tabla 1-10 muestra algunas de las tecnologías más representativas para el manejo de contenedores, entre los que se encuentran los entornos Docker, Rocket y Apache Mesos.

Tabla 1-10 Tecnologías de contenedores

Entorno	Licencia	Desarrollador	Sistema Operativo	Kernel	Referencia
Docker	Apache License 2.0	Docker, Inc.	Multiplataforma	Linux	[83]
Rocket - rkt	Apache License 2.0	Cloud Native Computing Foundation	Multiplataforma	Linux	[84]
Apache Mesos	Apache License 2.0	Apache Software Foundation	Multiplataforma	Linux	[85]

1.9.6 Monitores de tráfico SIP

La Tabla 1-11 muestra los monitores de tráfico SIP HOMER y VoIP Monitor, utilizados para la captura, diagnóstico, generación de registros de llamadas y medición de parámetros de QoS en tráfico de voz IP en entornos de producción.

Tabla 1-11 Monitores de tráfico SIP

Entorno	Licencia	Desarrollador	Sistema Operativo	Referencia
HOMER SIP Capture	GNU GPLv3	QXIP Team	Linux	[86]
VoIP Monitor	Código abierto	Martin Vít	Linux	[87]

1.9.7 Softphone

La Tabla 1-12 muestra los softphone con soporte de IMS, para la realización de llamadas, videollamadas y mensajería instantánea (IM) en VoIP con señalización SIP. Entre los softphone comerciales se encuentran Zoiper y Bria Solo. Como proyectos de código abierto están Boghe IMS Client e IMS Droid.

Tabla 1-12 Softphone

Entorno	Licencia	Desarrollador	Sistema Operativo	Referencia
Zoiper	Propietaria	Securax Ltd.	Multiplataforma	[88]
Bria Solo	Propietaria	Counterpath	Multiplataforma	[89]
Boghe IMS Client	GNU GPL v3	Doubango	Windows	[90]
IMS Droid	GNU GPL v3	Doubango	Android	[91]

1.9.8 Herramientas de medición de tráfico de red

La Tabla 1-13 muestra las herramientas de medición de tráfico de red más utilizadas en los entornos profesionales debido a que son proyectos de código abierto, donde se observan Wireshark para el monitoreo de tráfico de red e iPerf3 para la realización de pruebas de ancho de banda, jitter y pérdida de paquetes en protocolos TCP y UDP [92], [93].

Tabla 1-13 Herramientas de medición de tráfico en red

Entorno	Licencia	Desarrollador	Sistema Operativo	Referencia
Wireshark	GNU GPL v2	The Wireshark team	Multiplataforma	[92]
iPerf3	BSD	Jon Dugan, Seth Elliott, Bruce A. Mah, Jeff Poskanzer, Kaustubh Prabhu	Multiplataforma	[93]

2. Caracterización de los parámetros de QoS para el despliegue de servicios convergentes bajo la arquitectura IMS en interconexión

En este capítulo se presentan los conceptos técnicos que permiten el despliegue de servicios convergentes bajo la arquitectura IMS en interconexión con QoS, donde se observan los requerimientos de las redes de transporte, los protocolos de enrutamiento dinámico, los conceptos del protocolo MPLS, la arquitectura para la conectividad VPN bajo MPLS, los modelos de QoS en MPLS, los tipos de tráfico, la QoS en IP RAN y las herramientas para el manejo de la QoS.

2.1 Necesidad de la QoS en la prestación de servicios

Un ISP (Internet Service Provider, por sus siglas en inglés) debe gestionar los recursos de infraestructura de manera eficiente, dado que estos son limitados, para garantizar los niveles de calidad establecidos en los SLA´s en la entrega de servicios convergentes a sus clientes, brindando claridad sobre la forma en que los servicios son transmitidos, mantenidos y consumidos durante el período de tiempo acordado. Un cliente puede requerir servicios de voz, datos o video de manera síncrona o asíncrona. Si el proveedor no administra los recursos de red contemplados en los SLA's, el usuario final podría tener problemas por congestión y en consecuencia una mala percepción de la experiencia [94]–[97].

El comportamiento por defecto de las redes IP se identifica bajo el esquema de mejor esfuerzo (Best Effort), en el cual, la información es enviada en la modalidad de encolamiento FIFO (First in – First Out) donde los paquetes envían de forma desordenada, por lo que se requieren mecanismos de QoS. Los paquetes son enviados de forma aleatoria sin tomar en cuenta las prioridades, y en consecuencia no hay manera de saber que cliente transmitirá primero, así que el modelo de mejor esfuerzo no es el más efectivo al no tener en cuenta la prioridad de los paquetes en función de un determinado tipo de servicio consumido. Por otro lado, para garantizar la entrega de la información entre un origen y destino, es necesario contemplar mecanismos diferentes a los protocolos de enrutamiento convencionales dado que estos no discriminan la información de voz, datos o video. El objetivo del ISP en este sentido es asegurar la correcta entrega de los servicios mientras se acuerde un conjunto de SLA's con los clientes o incluso otros ISP's [94]–[97].

2.2 Requerimientos en redes de transporte (IP Backhaul)

La red IP Backhaul es la red de telecomunicaciones utilizada por un ISP (Internet Service Provider) para brindar servicios a los clientes (usuarios naturales o corporativos). Su principal función es la de transportar la información desde el núcleo hacia la red de acceso, donde pueden estar contempladas diferentes tipos de tecnologías de red de acceso radio (RAN) tales como redes 3G, 4G, 5G, Wifi, entre otras tecnologías inalámbricas o usuarios fijos (PC's, teléfonos IP, impresoras, etc.) (ver Figura 2-1) [94].

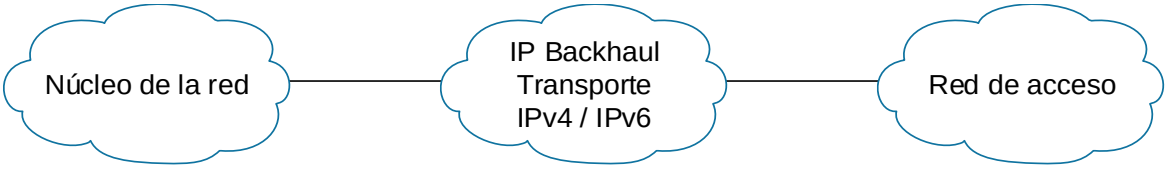


Figura 2-1 IP Backhaul [94]

El IP Backhaul utiliza la pila de protocolos del modelo TCP/IP, en la interconexión de redes a nivel regional forman un backbone basado en IP que trabaja con protocolos de enrutamiento y MPLS como se puede ver en la Figura 2-2 [94].

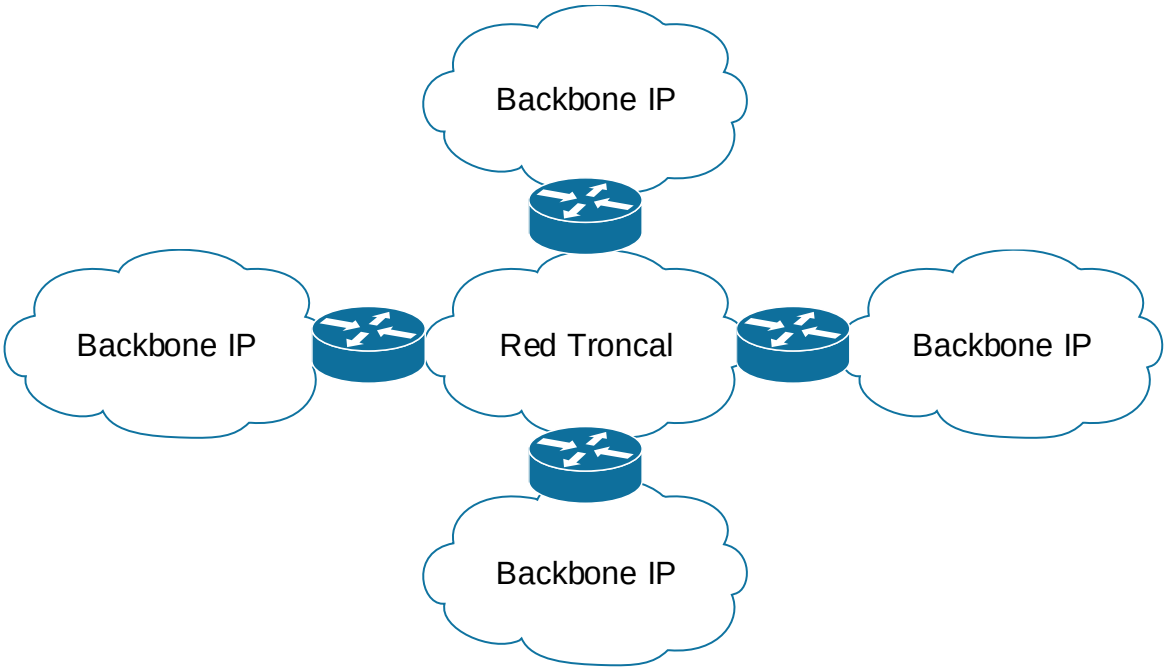


Figura 2-2 Interconexión regional entre diversos backbone IP [94]

Esta red debe cumplir con los requerimientos de flexibilidad, robustez, tolerancia a fallas, seguridad, disponibilidad y calidad de servicio. De acuerdo con estas necesidades, Cisco plantea el modelo jerárquico para el diseño de redes (ver Figura 2-3), el cual aplica para las redes en la capa de transporte del modelo NGN, donde la red de transporte se segmenta en varias capas, según el tráfico y las funciones de red de los equipos de transporte, para que su diseño, configuración, mantenimiento, escalabilidad y gestión sean eficientes en relación con las necesidades presentadas [98].

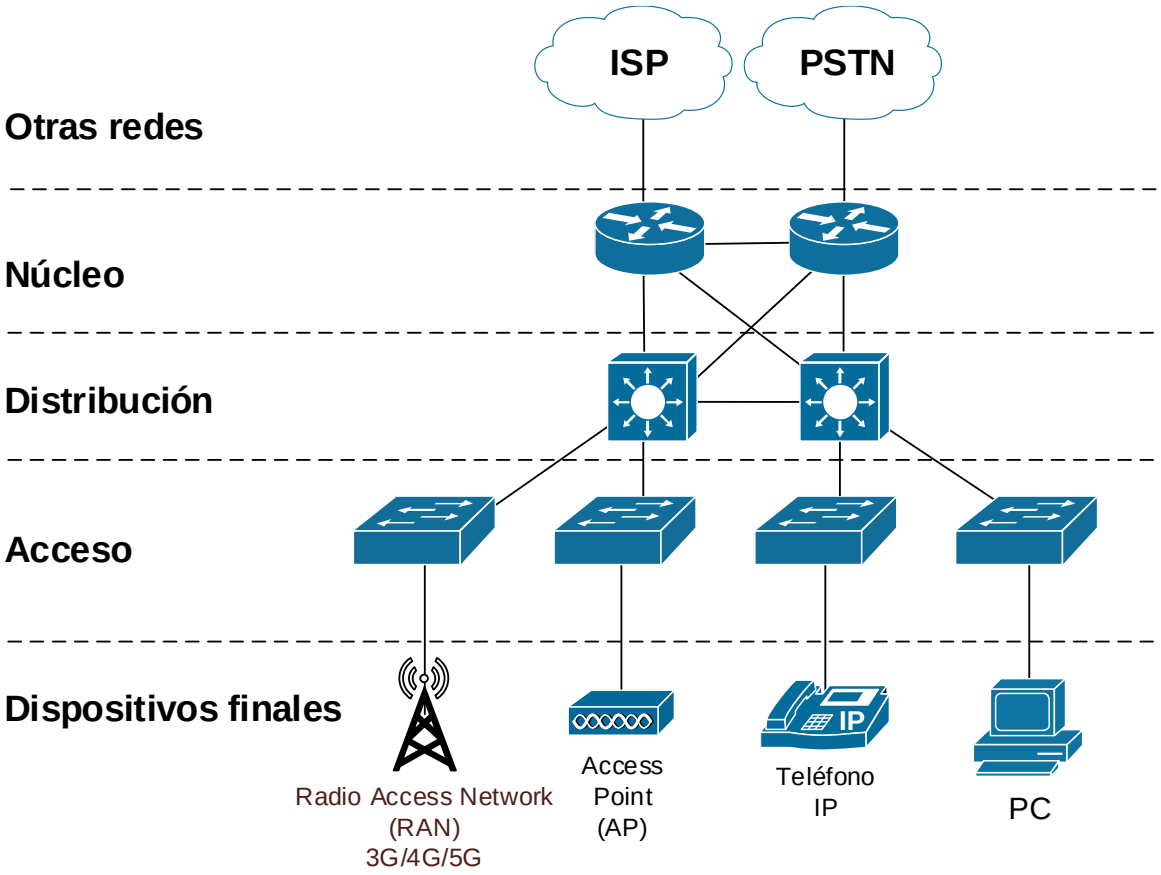


Figura 2-3 Modelo de red jerárquico [98]

Las capas del modelo de red jerárquico son las siguientes:

- **Acceso:** Conectividad a usuarios finales.
- **Distribución:** Transporte de información entre capas.
- **Núcleo**: Conmuta la información Intra e Inter dominio.

Adicionalmente a estas capas, es necesario tener presente los elementos a nivel de infraestructura, los cuales garantizan las condiciones necesarias para la operatividad de la red, entre las cuales se encuentran los elementos de alimentación eléctrica, refrigeración, temperatura, entre otros.

Los requerimientos de las redes de transporte se pueden definir en función de las tecnologías relacionadas en cuanto a equipos de Routing & Switching, enlaces de transmisión de alta capacidad y enlaces de transmisión de alta capacidad [94].

2.2.1 Equipos de Routing & Switching

De acuerdo con [94], los equipos de routing y switching deben cumplir con los siguientes requerimientos:

- Deben contar con alta capacidad en recursos de hardware y software.
- Deben contar con la capacidad para manejar multiservicios de forma integrada.
- Deben poseer funcionalidades avanzadas para la gestión y automatización de la red, es decir brindar eficiencia en operación y mantenimiento (O&M).
- Deben brindar alta escalabilidad y modularidad en el transcurso del tiempo.

2.2.2 Enlaces de transmisión de alta capacidad

- En función del tipo de enlace se pueden encontrar los siguientes (ver Figura 2-4):

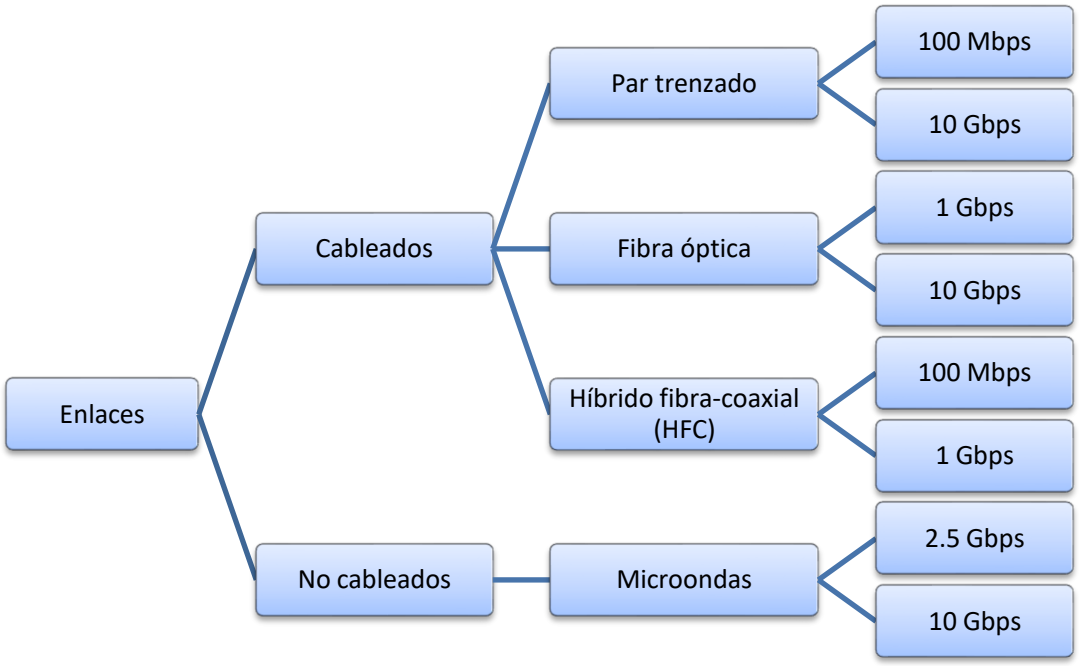


Figura 2-4 Tipos de enlaces de transmisión [96]

2.2.3 Protocolos de transporte, gestión y monitoreo

Con relación a los protocolos de transporte, gestión y monitoreo, en [96] se observan los siguientes requerimientos para la implementación en IP RAN:

- Transporte unificado de distintas tecnologías entre las que se encuentran el direccionamiento IP en las interfaces lógicas o físicas de los routers (IPv4/IPv6), protocolos de enrutamiento IGP (OSPF/IS-IS), protocolo de enrutamiento EGP (iBGP, eBGP, MP-BGP), protocolo para el manejo de etiquetas y distribución dinámica (MPLS, VPN, IP QoS, Ingeniería de tráfico - TE).
- Capacidad para optimizar el uso de ancho de banda, aunque existan distintas tecnologías de transporte.
- Capacidad para aplicar mecanismos de Calidad de Servicio (QoS) tales como la asignación de prioridades de servicio (voz, video por demanda (VoD), datos, etc.), mecanismos de reducción de latencia, mecanismos para asegurar el ancho de banda mínimo para determinados servicios y mecanismos para evitar la pérdida significativa de paquetes.

2.2.4 Elementos de la red de acceso radio IP (IP RAN)

La red de acceso radio IP o IP RAN (por sus siglas en inglés) es la parte de una red móvil de telecomunicaciones que proporciona al usuario los mecanismos y elementos para el acceso a la utilización de servicios de voz datos y video en dispositivos móviles, cuyas redes poseen una infraestructura compuesta de tres capas, que consisten en la red de acceso, la red troncal, y la red de núcleo (ver Figura 2-5) [96].

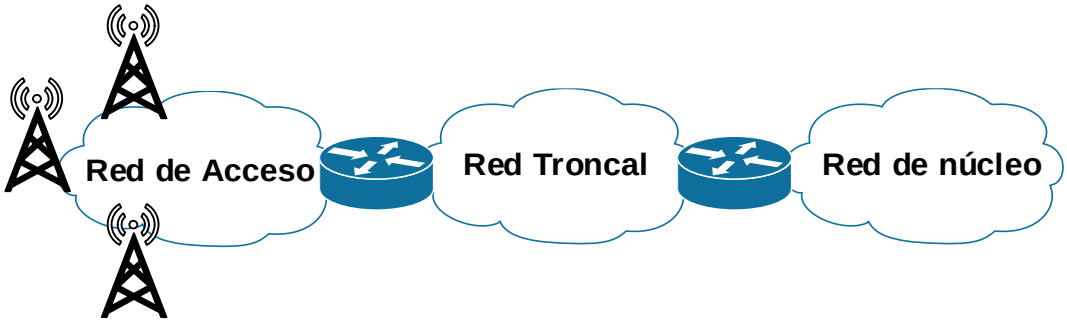


Figura 2-5 Arquitectura de la red de telefonía móvil [96]

La IP RAN se compone como mínimo de dos etapas, el fronthaul que incluye los nodos de acceso, torres y antenas, y el backhaul (ver Figura 2-6).

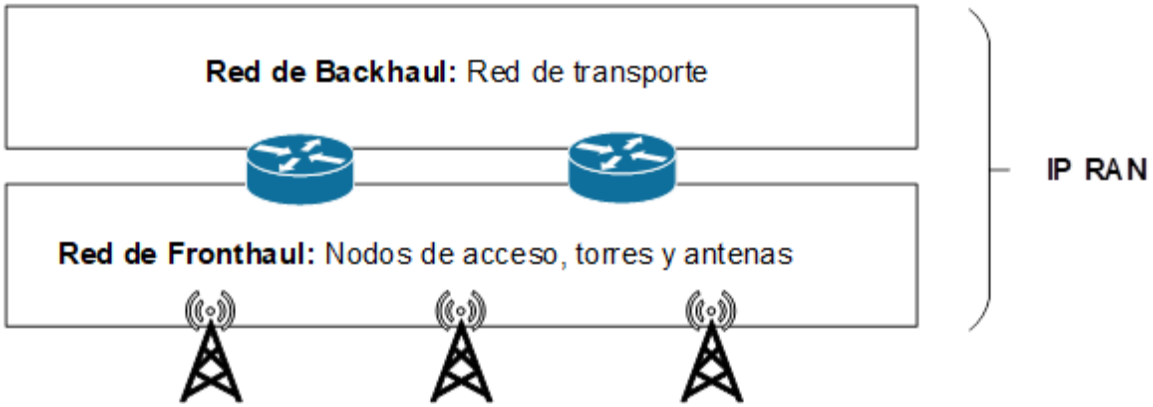


Figura 2-6 Elementos de la red de acceso radio IP (IP RAN) [96]

Dependiendo de la generación de telefonía móvil se pueden encontrar diferentes tipos de tecnologías, o generaciones, entre los que se encuentran:

- 2G: GERAN (GSM EDGE Radio Access Network).
- 3G: UTRAN (UMTS Terrestrial Radio Access Network).
- 4G: E-UTRAN (Evolved Universal Terrestrial Radio Access Network).
- 5G: C-RAN (Centralized/Cloud Radio Access Network).

Entre las características a destacar las IP RAN poseen nodos de acceso (BTS, Node B, eNodeB, gNB dependiendo de la generación de telefonía móvil), poseen interfaces lógicas para interconectarse con otros elementos de la red de telefonía móvil, utilizan la interfaz aire para comunicarse con los dispositivos de los usuarios (UE), utilizan métodos de acceso al medio para organizar el tráfico de baja y de seguridad los usuarios, y los nodos de acceso entregan la información del tráfico de los usuarios una red de transporte que puede estar conformada de múltiples tecnologías (ver Figura 2-7) [96].

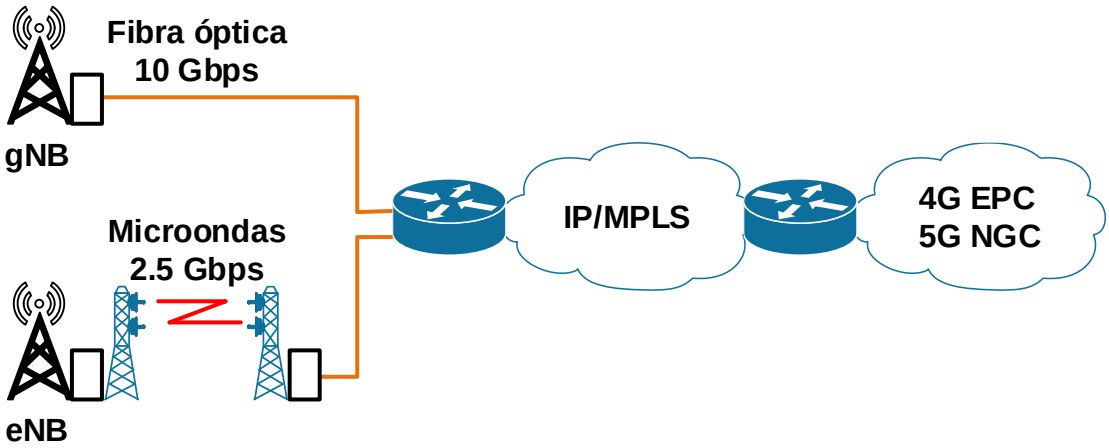


Figura 2-7 Estructura de la IP RAN móvil [96]

La red de transporte estará basada en IP/MPLS, utilizará routers o switches multicapa de alta capacidad y tecnologías de transmisión que proporcionen el ancho de banda adecuado para cubrir el tráfico entrante desde la red de acceso y saliente hacia el núcleo o core de la red y con capacidad de transporte multiservicios, y con capacidades que cubran calidad de servicio extremo a extremo (e2e QoS) y bajo costo [96].

Dentro de los beneficios de este tipo de implementación se encuentran la cobertura de la demanda de tráfico de forma eficiente, el bajo costo de implementación, la alta disponibilidad del servicio la optimización del uso de recursos (ancho de banda y hardware de los equipos) a través de la implementación de ingeniería de tráfico (MPLS TE) y QoS [96].

2.3 Protocolos de enrutamiento dinámico

Los protocolos de enrutamiendo dinámico se utilizan para facilitar el intercambio de información de enrutamiento entre equipos de capa tres del modelo OSI. Estos protocolos permiten a los routers compartir información de manera dinámica sobre las redes remotas, y a su vez, agregar la información automáticamente sus propias tablas de enrutamiento, determinando la mejor ruta para llegar desde una red de origen nacional red destino [98].

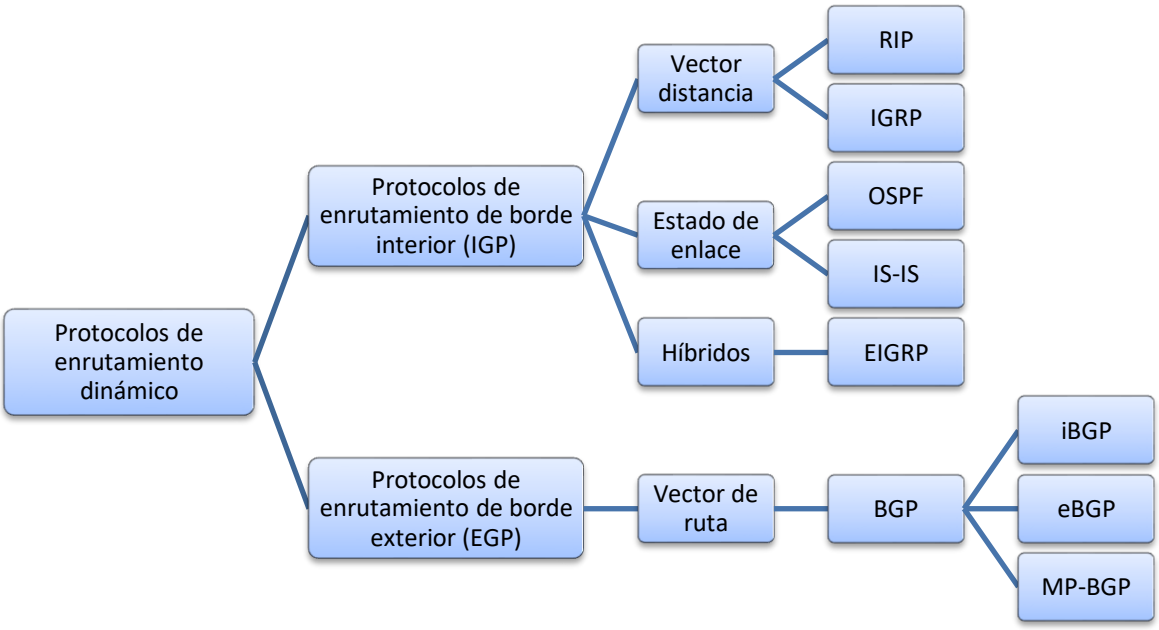


Figura 2-8 Protocolos de enrutamiento dinámico [98]

En la Figura 2-8 se observa la clasificación de los protocolos de enrutamiento dinámico, que se dividen en dos tipos, en protocolos de enrutamiento de borde interior (IGP) y protocolos de enrutamiento de borde exterior (EGP). Los IGP´s son utilizados para intercambiar la información de enrutamiento en el mismo sistema autónomo (AS), mientras que los EGP´s son utilizados para comunicar AS entre sí [98].

Un ejemplo de protocolo EGP es el protocolo de vector de ruta BGP (Border Gateway Protocol), el cual se puede configurar a nivel interno y externo, así como el soporte multiprotocolo para aplicaciones en MPLS [94].

Los IGP se clasifican en tres clases [98]:

- **Vector distancia:** la mejor ruta hacia una red de destino se establece en función de la distancia, donde se define en el momento en que un paquete atraviesa un router, estableciendo una métrica que es llamada “salto”. La ruta con el menor número de saltos será la mejor para conectar un origen común destino. Dentro de los protocolos de vector distancia se encuentran los protocolos IGP RIP e IGRP.
- **Estado de enlace:** Permiten a los routers la construcción de la topología de la red al manejar un registro de la información de los enlaces de un router con sus vecinos, de tal manera que, al ocurrir un cambio en la red, el protocolo permite enviar una actualización del estado de los enlaces de un router hace sus vecinos, y dado que un router se encuentra monitoreando estas notificaciones, las tablas de enrutamiento se actualizan constantemente. Dentro de los protocolos de estado de enlace se encuentran los protocolos IGP OSPF e IS-IS.
- **Híbridos:** utilizan características tanto de vector distancia como estado de enlace, por ejemplo, el protocolo EIGRP.

2.3.1 Sistemas autónomos (AS)

Un sistema autónomo define una red o conjunto de redes que pueden ser administradas por uno o más operadores de red, en la que se utiliza una misma política de enrutamiento. Los sistemas autónomos se comunican entre sí a través del protocolo de enrutamiento BGP, cada uno tiene un número de identificación el cual es asignado por la IANA definido bajo la RFC 5396. Normalmente dentro de un sistema autónomo se utiliza un protocolo de

enrutamiento de tipo IGP, y para la comunicación entre los sistemas autónomos diferentes se utiliza un EGP (ver Figura 2-9) [94].

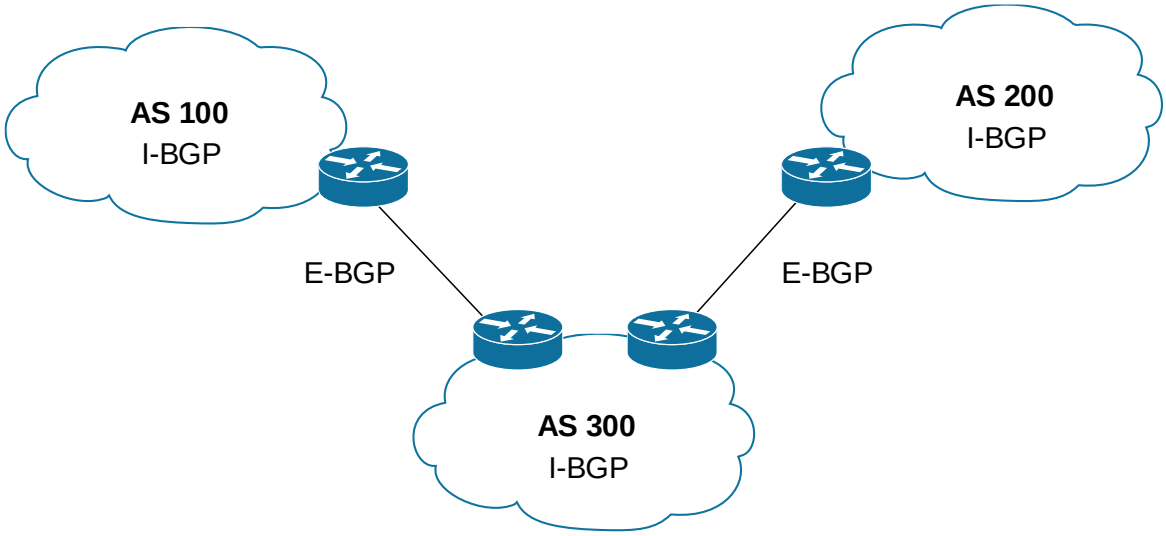


Figura 2-9 Sistemas autónomos y su interconexión [94]

Los sistemas autónomos se pueden clasificar en los siguientes tipos:

- Conectividad única (stub).
- Tránsito.
- Múltiples conexiones sin tránsito (multihomed).

La red de acceso radio basada en IP, puede haber uno o más subsistemas autónomos como se observa en la Figura 2-10, esto se hace con el objetivo de administrar mejor el despliegue de redes de telefonía móvil en las cuales se pueden desplegar diferentes nodos de acceso en función de la cobertura geográfica, a su vez esta estructura permite reducir las tablas de enrutamiento optimizando los recursos de hardware del proveedor de servicios [96].

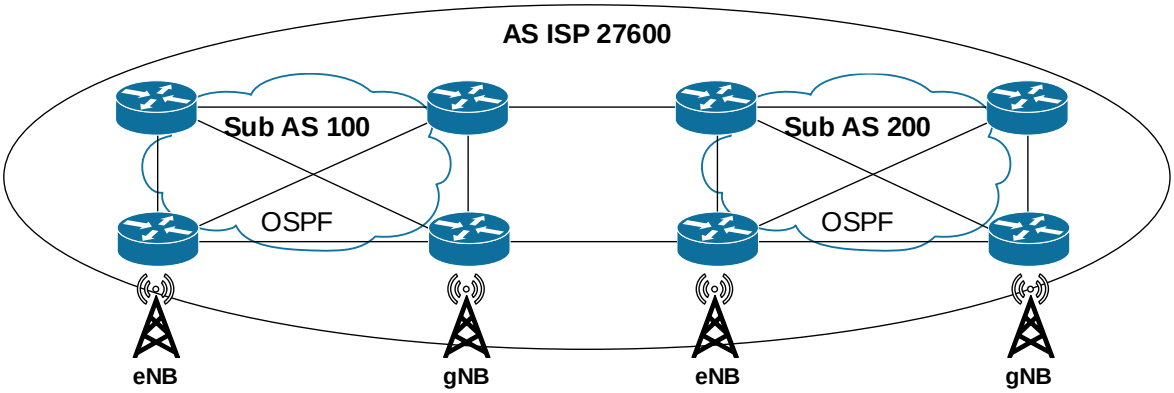


Figura 2-10 Sistema autónomo en IP RAN [96]

2.3.2 Consideraciones para el diseño de redes convergentes

Se deben tener en cuenta las siguientes consideraciones para el diseño de una red convergente (multiservicios) [43]:

- La infraestructura física para la implementación de la red.
- Protocolos de enrutamiento IGP / EGP.
- Conmutación de etiquetas mediante MPLS.
- Características de redes remotas bajo la arquitectura MPLS/VPN.
- Aplicación de técnicas de QoS en MPLS.
- Aplicación de técnicas de ingeniería de tráfico en MPLS TE.

Con relación a los protocolos a trabajar se deben tener en cuenta lo siguiente [43]:

- Los routers intermediarios y los nodos de acceso 4G o 5G trabajarán con IPv4 o IPv6, los protocolos de enrutamiento permiten crear las tablas de enrutamiento y conocer la información de la topología de la red.
- BGP y MP-BGP permitirán crear adyacencias entre los routers externos una red IP/MPLS.
- La información proporcionada por los protocolos de enrutamiento será utilizada por MPLS para la entrega etiquetas con MPLS LDP.
- Las funciones de la capa de red en IP RAN son informativas dado que la conmutación de las tramas se realizará mediante las etiquetas de MPLS.

2.3.3 Funcionamiento desde las capas de enlace (L2) hasta la capa de red (L3)

En la **Figura 2-11** se describe el proceso de funcionamiento desde la capa de enlace hasta la capa de red:

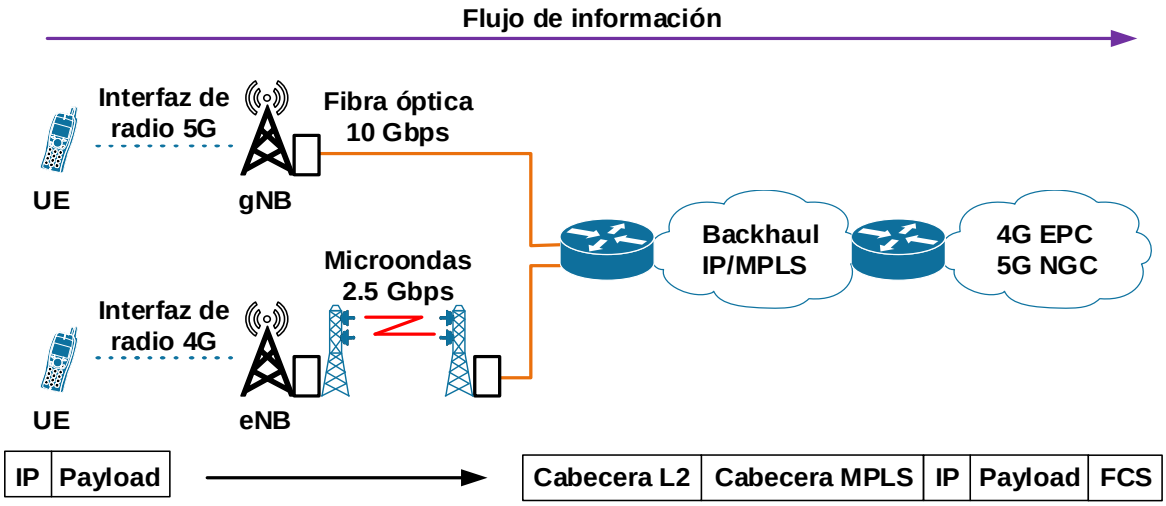


Figura 2-11 Funcionamiento desde las capas de enlace (L2) hasta la capa de red (L3) [96]

Los UE se conectarán al nodo de acceso a través de la interfaz de radio correspondiente a la tecnología móvil utilizada, el nodo de acceso les otorgará una dirección IP mediante DHCP. Las tramas generadas por los usuarios (L2) estarán encapsuladas por el protocolo IP (L3) con las direcciones de origen y destino que correspondan de acuerdo con el servicio de interés, el cual puede estar dentro de la red del operador o en una red externa. En cuanto al funcionamiento de la capa de red se puede utilizar el protocolo IPv4 o IPv6 tanto en los dispositivos terminales de usuario, como en los nodos de acceso o en los routers de borde de la red, sin importar la versión del protocolo IP [96].

A nivel de transporte se utilizará MPLS (L2,5) conmutando por etiquetas las tramas generadas en sentido ascendente por los usuarios, o en sentido descendente desde el núcleo 4G o 5G desde el operador. El router de borde y de la red encapsulara las tramas generadas por el usuario con las etiquetas MPLS, que le permitirán a los demás routers que se encuentran dentro de la nube del backhaul IP establecer el camino de etiquetas, por otro lado, se le aplicará un código de detección de error (Frame Check Sequence, FCS). Con base en esta información generada se podrán aplicar las técnicas de calidad de servicio correspondientes que permitan establecer prioridades, y más allá del alcance de esta tesis se podrán aplicar técnicas de ingeniería de tráfico para optimizar la red en conexiones L2VPN o L3VPN [96].

2.3.4 Protocolo OSPF (Open Shortest Path First)

OSPF es un protocolo enrutamiento dinámico estándar abierto, definido por el RFC 2338, que utiliza el costo como métrica para evaluar el mejor camino es una red de destino, como se puede ver en la ecuación (2-1) [94]:

$$\text{Costo}_{OSPF} = \frac{10^{18}}{BW\left[bps\right]} \tag{2-1}$$

Donde:

BW: $Ancho\ de\ banda\ del\ enlace$

El costo se calcula en función del ancho de banda, en donde la ruta que tiene el menor costo será aquella que tenga el mayor ancho de banda en la interfaz de un router (ver Tabla 2-1).

Tabla 2-1 Costo para las interfaces en OSPF [94]

Tipo de interfaz	Costo
Fast Ethernet/Giga Ethernet	1
Ethernet	10
E1	48
T1	64
128 Kbps	781
64 Kbps	1562
56 Kbps	1785

Dentro de las características de OSPF se encuentran:

- Soporte de escalabilidad.
- Número ilimitado de conteo de saltos.
- Soporte de VLSM/CIDR.
- Manejo sistemas autónomos.
- Permite la segmentación de la red en áreas, con lo cual se confina la inestabilidad de la red.
- Mejora la velocidad de convergencia (actualizaciones de la tabla de enrutamiento).
- Minimiza las actualizaciones de tráfico de enrutamiento.
- Permite la implementación de redes multi-vendor al ser un estándar abierto.
- Utiliza algoritmos de cifrado de paquetes como MD5.

2.3.5 Protocolo BGP (Border Gateway Protocol)

Es un protocolo de enrutamiento de sistemas inter autónomos de vector distancia que fue diseñado como EGP, definido por el RFC 1771. BGP define dos clases de vecinos que son interno (iBGP) y externo (eBGP), estos términos se utilizan desde la perspectiva de un router donde un vecino BGP puede estar dentro del mismo sistema autónomo (iBGP) o en un sistema autónomo diferente (eBGP). BGP se encarga de divulgar, aprender y escoger el mejor camino en Internet. Cuando dos o más proveedores se interconectan, utilizan BGP para intercambiar la información de enrutamiento. A pesar de que fue diseñado como un protocolo EGP, puede utilizarse como protocolo IGP. Algunas de sus características son las siguientes [94]:

- Soporta VLSM, CIDR y sumarización.
- Se crean y mantienen las conexiones entre vecinos utilizando el puerto TCP 179.
- Actualmente se encuentra en la versión BGP-4.

2.3.6 BGP Route Reflector (RR)

En BGP se utiliza el Route Reflector (RR) con el objetivo de optimizar la utilización de los recursos de hardware de los routers y el ancho de banda, al reducir el tamaño de las tablas de enrutamiento. Dentro de un sistema autónomo el RR permite que los router participantes en iBGP aprendan las rutas de sus vecinos sin introducir bucles en una topología en configuración de malla (ver Figura 2-12) [99].

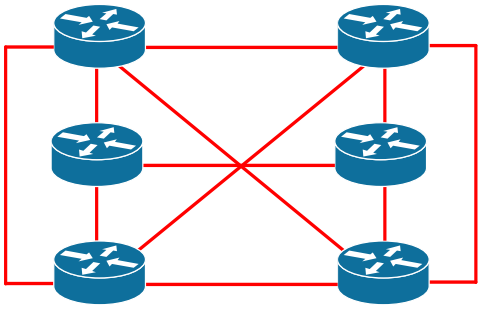


Figura 2-12 Configuración de topología en malla [99]

El número de relaciones entre vecinos (adyacencias) iBGP se puede establecer mediante la siguiente ecuación [99]:

$$Adyacencias_{iBGP} = \frac{N(N-1)}{2} \quad (2\text{-}2)$$

Donde:

N: $Número\ de\ routers\ iBGP$

Para el ejemplo de la Figura 2-12 con $N = 6$, se tiene que $Adyacencias_{iBGP} = 15$. Al introducir un RR se tiene la siguiente configuración resultante (ver **Figura 2-13**) manteniendo la misma cantidad de routers:

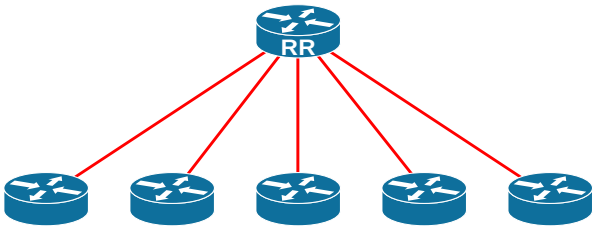


Figura 2-13 Configuración con Route Reflector [99]

Un RR puede establecer tres tipos de relaciones de adyacencias:

- Vecino eBGP (eBGP RRC)
- Vecino iBGP cliente (iBGP RRC)
- Vecino iBGP no cliente (iBGP RRnC)

Para que un RR comparta una ruta con sus vecinos se deben seguir las siguientes condiciones:

- Una ruta aprendida de un cliente que no es RR se anuncia a los clientes RR, pero no a los clientes que no son RR (ver Figura 2-14).

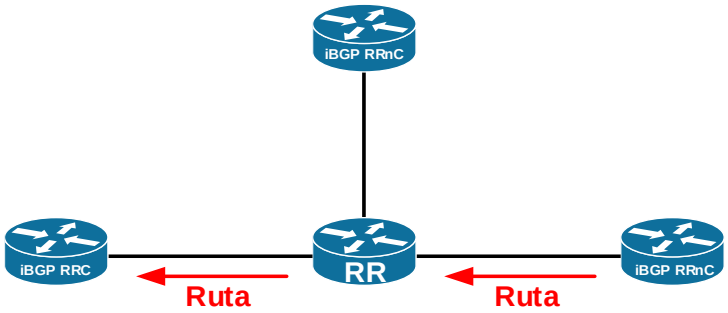


Figura 2-14 Una ruta aprendida de un cliente que no es RR se anuncia a los clientes RR pero no a los clientes que no son RR [99]

- Una ruta aprendida de un cliente RR se anuncia tanto a clientes RR como a clientes no RR (ver Figura 2-15). Incluso el cliente RR que anunció la ruta recibirá una copia y la descartará porque se ve a sí mismo como el origen.

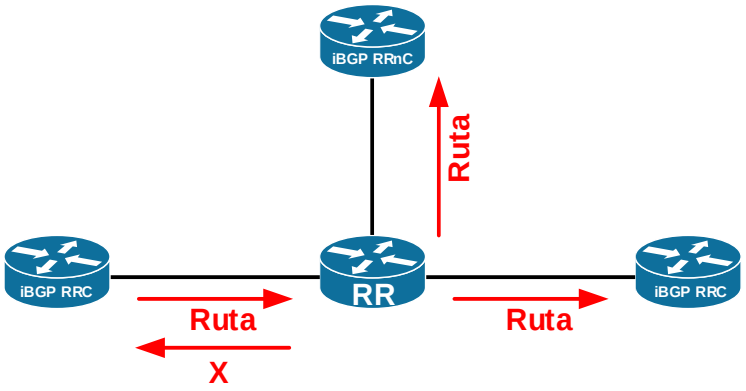


Figura 2-15 Una ruta aprendida de un cliente RR se anuncia tanto a clientes RR como a clientes no RR [99]

- Una ruta aprendida de un vecino eBGP se anuncia tanto a clientes RR como a clientes no RR (ver Figura 2-16).

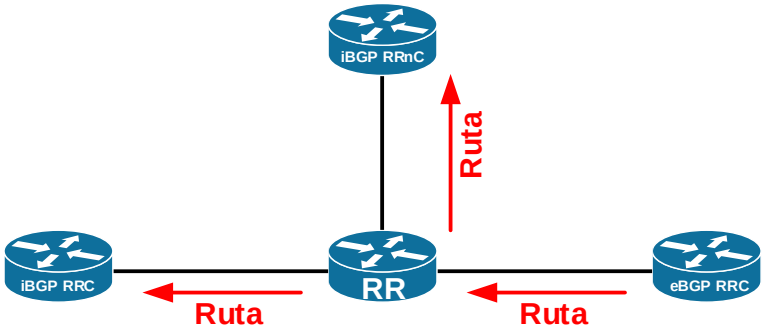


Figura 2-16 Una ruta aprendida de un vecino eBGP se anuncia tanto a clientes RR como a clientes no RR [99]

2.4 Protocolo MPLS (Multiprotocol Label Switch)

Es una tecnología utilizada en redes IP para el reenvío de paquetes mediante la utilización de etiquetas, se encuentra definido en la RFC 3031. La Figura 2-17 muestra la cabecera MPLS y sus correspondientes campos.

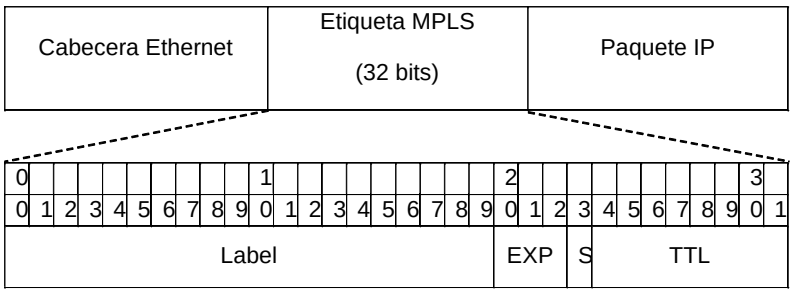


Figura 2-17 Cabecera MPLS [100]

Los campos que conforman la cabecera MPLS son los siguientes:

- **Label (20 bits):** Este campo representa el valor de la etiqueta MPLS.
- **EXP (3 bits):** Bits experimentales utilizados para QoS.
- **S (1 bit):** Bottom of Stack, es cero a menos que sea la etiqueta inferior de la pila, en cuyo caso es 1.
- **TTL (8 bits):** Time to live - tiempo de vida, es un valor que decrece en uno en cada salto.

En los últimos años ha adquirido gran popularidad y ha comenzado a repasar rápidamente otras tecnologías como Frame Relay y ATM. El objetivo de esta tecnología es permitir que los routers construyan un mapa topológico de la red mediante etiquetas, sin necesidad de ver la dirección IP destino, lo que implica una reducción importante de la latencia. MPLS opera entre las capas dos y tres del modelo OSI, entre sus características se encuentran [100]:

- Permite la utilización de infraestructuras de red unificadas (redes de conmutación de circuitos y de paquetes), para el envío de paquetes de voz, datos y video.
- Mejora la integración de tecnologías como ATM sobre redes IP.
- MPLS permite administrar los recursos de la red de manera eficiente al integrar ingeniería de tráfico sobre la esta, para controlar el balanceo de carga, QoS y una mejor distribución de paquetes.
- Permite la utilización dinámica y controlada de redes privadas virtuales sitio (VPN site-to-site).
- Tiene un óptimo control de flujo de tráfico en la red IP Backhaul.
- Es fundamental para la calidad de servicio en redes de telefonía móvil 3G, 4G y 5G.

2.4.1 Arquitectura MPLS

En MPLS los routers conmutan los paquetes mediante etiquetas, definiendo el término LSR (Label Switch Router) para su identificación en la red (ver Figura 2-18).

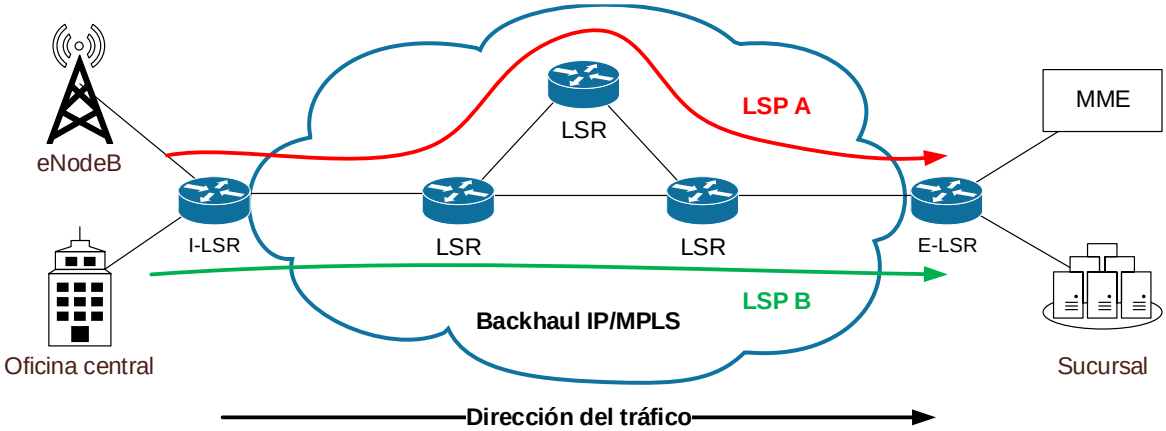


Figura 2-18 Arquitectura MPLS [97]

En MPLS los LSR deben ser únicos y por lo tanto deben estar identificados, comúnmente se utiliza la interfaz Loopback 0 como identificador del router. Dependiendo de la posición del router en la red, este tiene una función específica. Los routers se clasifican en los siguientes [97]:

- **Ingress LSR (I-LSR):** Son los routers de entrada a la red, reciben un paquete que entra la red (sin etiquetas) y le coloca la primera etiqueta para reenviarlo hacia otro router del backbone MPLS. Es un router de borde del backbone MPLS.
- **Intermediate LSR:** Son los routers MPLS que se encuentran en el medio de la red, normalmente reciben un paquete con una o más etiquetas a través de una interfaz de entrada y proceden a reenviarlas hacia su destino a través de una interfaz de salida. En este proceso, es probable que el router LSR intermedio le coloque otra etiqueta antes de reenviarlo.
- **Egress LSR (E-LSR):** Es el router final, su función es retirar las etiquetas que posee el paquete IP para poder entregarlo su destino final. Es un router de borde del backbone MPLS.
- **Label Switched Path (LSP):** A la secuencia de routers de una red MPLS que definen un camino conmutado por etiquetas se le conoce como LSP (Label Switched Path). Los LSP comienzan con un I-LSR y terminan en un E-LSR, pasando por diversos LSR intermedios. Dentro de las ventajas que permite MPLS se encuentra en que el ISP para interconectar los sitios de uno o varios clientes asignándoles un LSP distinto, es de resaltar que MPLS sólo tiene sentido en el dominio definido entre los routers I-LSR y E-LSR.

2.4.2 Operaciones y distribución de etiquetas

Cuando un paquete ingresa una ruta LSP, los routers LSR pueden realizar tres tipos de operaciones para conmutar el paquete a través de la red entre las que se encuentran:

- **PUSH:** Agrega una o más etiquetas en la pila de etiquetas del paquete.
- **SWAP:** Se realiza cuando un LSR recibe un paquete etiquetado y cambia la etiqueta del tope de la pila por una nueva.
- **POP:** Consiste en remover una o más etiquetas en el tope de la pila etiquetas del paquete IP.

Para la distribución de etiquetas se utilizan protocolos para crear y mantener la asociación de estas a lo largo de un LSP, estos protocolos se encargan de señalizar el camino informar a los LSR las etiquetas que se están utilizando entre los puntos de ingreso y egreso. Para que la distribución de etiquetas pueda funcionar correctamente, la red IP del proveedor de servicio debe tener implementado un protocolo de enrutamiento como OSPF, IS-IS o EIGRP [97], [101]. Dentro de los protocolos de distribución de etiquetas se encuentran los siguientes:

- Tag Distribution Protocol (TDP), el cual se encuentra obsoleto.
- Label Distribution Protocol (LDP), formalizado por el IETF.
- Resource Reservation Protocol (RSVP), utilizado en ingeniería de tráfico MPLS.

MPLS divide sus funciones en los planos de control y de datos de la siguiente manera (ver Tabla 2-2):

Tabla 2-2 Comparativo entre el plano de control y el plano de datos [97], [101]

Plano de control (Control plane)	Plano de datos (Data plane)
Es donde la información de enrutamiento y de gestión, como las vinculaciones de etiqueta se intercambian entre LSR.	Es donde se realiza el reenvío de paquetes entre los diferentes LSR que conforman la red IP MPLS

2.4.3 Distribución de etiquetas con LDP

El protocolo LDP permite obtener y reenviar paquetes a través de un camino LSP en una red MPLS, para esto los routers LSR de la red deben habilitarlo, el protocolo tiene las siguientes funciones [97]:

- Descubrimiento de los routers LSR de la red.
- Establecimiento y mantenimiento de las sesiones.
- Comunicación del mapeado utilizado para las etiquetas.

- Envío de mensajes de notificación cuando haya errores en la red.

2.5 Arquitectura MPLS VPN

Una red privada virtual (VPN, por sus siglas en inglés) es una tecnología que permite la interconexión remota de dos o más ubicaciones de red, mediante un túnel o conexión que provee una conexión segura a través una red WAN. En MPLS, esta tecnología la utilizan los ISP para brindar conectividad P2P a uno o más clientes al pasarlos por su backhaul IP basado en MPLS permitiendo la interconexión de sucursales u otros sitios entre sí [97].

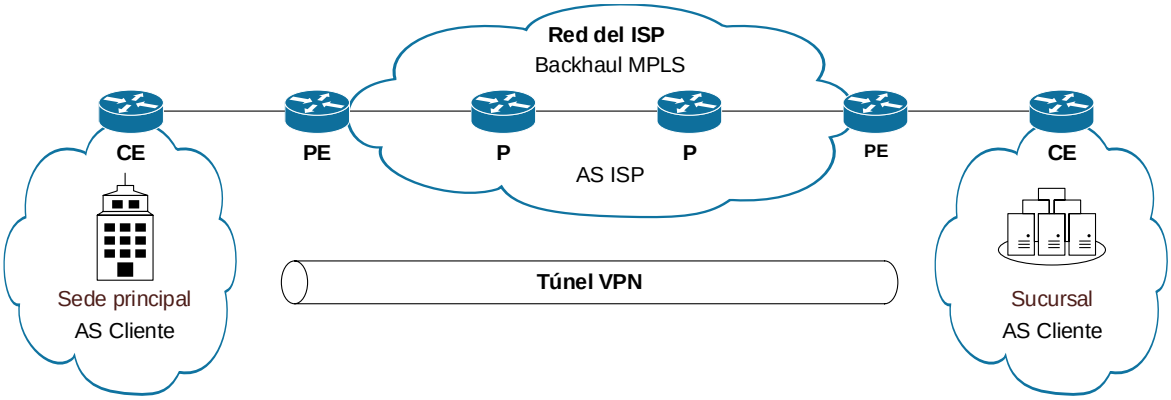


Figura 2-19 Arquitectura MPLS VPN [97]

La arquitectura MPLS VPN (ver Figura 2-19) considera la siguiente terminología:

- **Customer Edge (CE):** Son los routers del cliente, se conectan directamente a los PE.
- **Provider Edge (PE):** Son los routers de borde de la red del ISP.
- **Provider (P):** Son los routers intermediarios que se encuentran dentro de la red del ISP.

Tanto el ISP como los clientes, pueden pertenecer a sistemas autónomos diferentes, por lo que es necesario la utilización los correspondientes protocolos de enrutamiento.

2.5.1 Conceptos y tipos de VPN basadas en MPLS

- **Sites:** Un conjunto de sistemas se denomina “sitio” (site, en inglés) dentro de la arquitectura MPLS VPN (ver Figura 2-20), si tiene una interconectividad IP mutua que no requiere el uso de la red troncal [96].

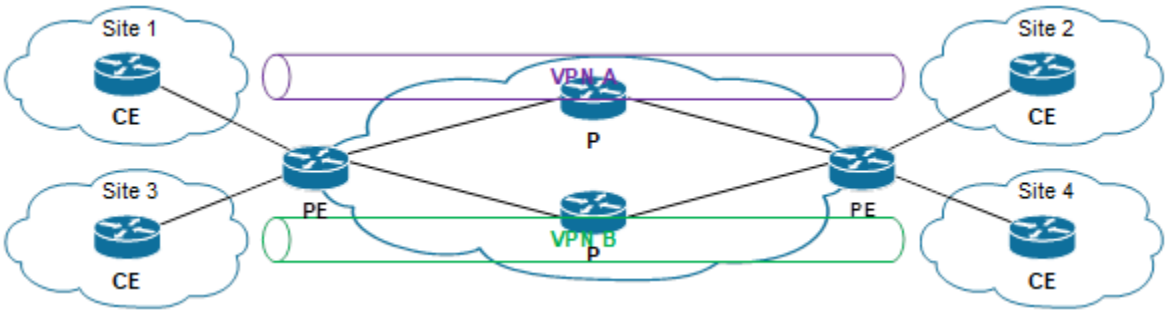


Figura 2-20 Sites [96]

- **VPN de capa 2 (L2VPN) basada en MPLS:** En una VPN de capa 2 basada en MPLS, el switch (o router) CE reenvía el tráfico al PE en un formato de capa 2. MPLS lo transmite a través de la red del proveedor de servicios y luego se convierte de nuevo al formato de Capa 2 en el sitio de recepción [96].

  En una VPN de capa 2, el enrutamiento se produce en los CE. El CE conectado a un proveedor de servicios en una VPN de capa 2 debe seleccionar el circuito apropiado en el cual enviar tráfico. El PE que recibe el tráfico lo envía a través de la red del proveedor de servicios al PE conectado al sitio receptor. Los PE no almacenan ni procesan las rutas del cliente; los switches multicapa o routers deben configurarse para enviar datos al túnel adecuado [96].

  Para una VPN de capa 2, los clientes deben configurar sus propios equipos para transportar todo el tráfico de capa 3. El proveedor de servicios debe detectar solo cuánto tráfico deberá transportar la VPN de capa 2. Los equipos del proveedor de servicios transportan tráfico entre los sitios del cliente mediante interfaces VPN de capa 2. La topología de VPN está determinada por las políticas configuradas en los PE. Los clientes solo deben saber qué interfaces VPN se conectan a cuál de sus propios sitios [96].
- **VPN de capa 3 (L3VPN) basada en MPLS:** En una VPN de capa 3, el enrutamiento se realiza en los routers del proveedor de servicios. Por lo tanto, las VPN de capa 3 requieren más configuración por parte del proveedor de servicios, porque los PE del proveedor de servicios deben almacenar y procesar las rutas del cliente [96].

  Las VPN de capa 3 se basan en RFC 4364, redes privadas virtuales IP BGP/MPLS. Esta RFC define un mecanismo mediante el cual los proveedores de servicios pueden utilizar sus redes troncales IP para proporcionar servicios VPN de capa 3

a sus clientes. Los sitios que componen una VPN de capa 3 están conectados a través de la red troncal de Internet pública existente de un proveedor [96].

Las VPN basadas en RFC 4364 también se conocen como BGP/MPLS VPN porque BGP se usa para distribuir información de enrutamiento VPN a través de la red troncal del proveedor y MPLS se usa para reenviar el tráfico VPN a través de la red troncal a sitios VPN remotos [96].

Las redes de clientes, debido a que son privadas, pueden usar direcciones públicas o privadas, como se define en RFC 1918, Asignación de direcciones para Internet privado. Cuando las redes de clientes que utilizan direcciones privadas se conectan a la infraestructura pública de Internet, las direcciones privadas pueden superponerse con las direcciones privadas utilizadas por otros usuarios de la red. Las VPN BGP/MPLS resuelven este problema prefijando un identificador de VPN a cada dirección de un sitio VPN en particular, creando así una dirección que es única tanto dentro de la VPN como dentro de la Internet pública [96].

2.5.2 Comparativo entre L2VPN y L3 basadas en MPLS

En la Tabla 2-3 se pueden observar las diferencias entre los dos tipos de VPN:

Tabla 2-3 Comparativo entre L2VPN y L3 basadas en MPLS [100]

VPN de capa 2	VPN de capa 3
Los sitios de los clientes parecen estar en la misma LAN incluso si están dispersos geográficamente.	La experiencia técnica del proveedor de servicios garantiza un enrutamiento eficiente de sitio a sitio. Los proveedores de servicios pueden proporcionar servicios de valor agregado adicionales a través de la convergencia de redes que abarca voz, video y datos.
El proveedor de servicios no requiere información sobre la topología de la red del cliente, las políticas, la información de enrutamiento, etc.	Los clientes deben compartir información sobre la topología de su red.
El cliente tiene un control total sobre las políticas y el enrutamiento.	El proveedor de servicios determina las políticas y el enrutamiento.
El CE reenvía el tráfico al PE del proveedor de servicios en formato de Capa 2.	El CE del cliente debe estar configurado para usar BGP u OSPF para comunicarse con el PE del proveedor de servicios para transportar prefijos IP a través de la red. No se admiten paquetes otros protocolos.

2.5.3 Conceptos relacionados con VPN de capa 2 (L2VPN) basada en MPLS

En MPLS se trabajan con VPLS (Virtual Private LAN Service), que consisten en una conexión virtual multipunto basada en Ethernet que pasa a través del vagón MPLS de un proveedor de servicios. Normalmente un cliente corporativo contrata el servicio de una VPLS cuando quiere interconectar varios sitios alejados geográficamente entre sí, como si se conectarán a través de una misma red LAN. Los sitios ven a la red del proveedor de servicios como si se tratara de un switch. Por tal motivo las VPLS son muy utilizadas en redes de área metropolitana (MAN) y redes de área amplia (WAN). Dentro de las VPN de capa dos se considera la siguiente terminología [97]:

- **PW (Pseudowire):** Es una conexión virtual utilizada para el envío de tramas entre dos nodos PE de manera bidireccional.
- **VSI (Virtual Switch Instance):** Son instancias que permiten separar a las VPLS entre sí.
- **VC (Virtual Circuit):** Representan circuito lógico unidireccional entre dos nodos. Se dice que dos VC direccionalmente opuestos constituyen una PW.
- **AC (Attachment Circuit):** Puede ser lógico o físico, la función del AC es permitir la comunicación entre el equipo de borde CE y el PE. Los nodos PE reenvían la información de las VPLS mediante el uso de las VSI. Las tramas Ethernet se reenvían entre dos PE a través de una PW.

Las VPLS tienen las siguientes ventajas:

- Son rentables para clientes corporativos porque le permiten conectar múltiples sitios entre sí.
- Al ser conexiones virtuales de capa 2 del modelo OSI permiten el reenvío de tráfico de alta prioridad en aplicaciones de tiempo real tales como VoIP o IPTV.
- Al ser conexiones virtuales de capa 2 se reducen tiempos y latencias relacionadas con el procesamiento de capa 3.
- La comunicación se realiza directamente entre los PE involucrados.
- Los bucles no pueden ocurrir porque los protocolos como STP (Spanning Tree Protocol), MSTP (Multiple Spanning Tree Protocol) o RRPP (Rapid Ring Protection Protocol) no son estrictamente requeridos.

- En cuanto al funcionamiento de VPLS en el plano de control en el plano de datos se tiene lo siguiente (ver Tabla 2-4):

Tabla 2-4 Funcionamiento de VPLS en el plano de control en el plano de datos [100]

Plano de control	Plano de datos
Descubrimiento de miembros: Encontrar todos los PE relacionados una misma VPLS. **Señalización:** Establecer, mantener y remover la PW entre los PE relacionados a una misma VPLS	**Encapsulación:** al recibir las tramas provenientes de un CE, el nodo PE las encapsulara antes de reenviarlas al backbone. **Reenvío:** conmutación de los paquetes basados en la dirección MAC de destino. **Desencapsulación:** antes de entregar una trama a un CE, el nodo PE remueve la encapsulación.

2.5.4 Conceptos relacionados con VPN de capa 3 (L3VPN) basada en MPLS

A diferencia de las VPN de capa 2, las VPN de capa 3 son más complejas, cuando se agrega un nuevo sitio a una VPN existente, es necesario modificar la configuración de todos los nodos de borde que acceden al sitio VPN. Esto agrega complejidad de la red y aumenta el tiempo de procesamiento. Se considerar la siguiente terminología cuando se trabaja con VPN de capa 3 [97].

- **Instancia VPN:** Son los nombres que se le da a una VPN en particular. Cada VPN debe tener un nombre que la identifique en el backbone IP/MPLS.
- **Route Distinguisher (RD):** El RD es un valor de 8 bytes que sirve para distinguir las direcciones IPv4 de VPN y no descartar información de otras VPN cuyos prefijos de red sean similares. Para esto se usa MP-BGP.
- **Route Target (RT):** El RT es un parámetro de 32 bits que sirve para el control de las notificaciones de las rutas VPN en la red.
- **VPN Routing and Forwarding (VRF):** Una VRF es una tabla especial que poseen los PE dentro del backbone IP MPLS del proveedor. Cada router PE mantiene varias tablas de reenvío separadas de esta manera los routers saben a dónde deben reenviar un paquete relacionado con una L3VPN en específico.
- **Multiprotocol BGP (MP-BGP):** Es una extensión de BGP que se utilizan la implementación de L3VPN para el intercambio de etiquetas VPN extremo a extremo entre los equipos PE. Está definido bajo la RFC 4760. Soporta IPv4 e IPv6 y es capaz de separar distintas topologías de red.

2.6 Arquitectura seamless MPLS

La arquitectura seamless MPLS (ver Figura 2-21), también conocida como unificada o jerárquica se define en el documento [102] del IETF. Consiste en extender las funcionalidades y beneficios de MPLS hacia la red de acceso o agregación debido a la necesidad de aumentar el rango de cobertura de las redes móviles en una región, que conlleva a un incremento en el despliegue de los nodos de acceso, esto lleva al incremento de las tablas de enrutamiento, el incremento en la dificultad de la gestión de etiquetas de MPLS y en consecuencia la afectación en el rendimiento a nivel del plano de control en MPLS [103].

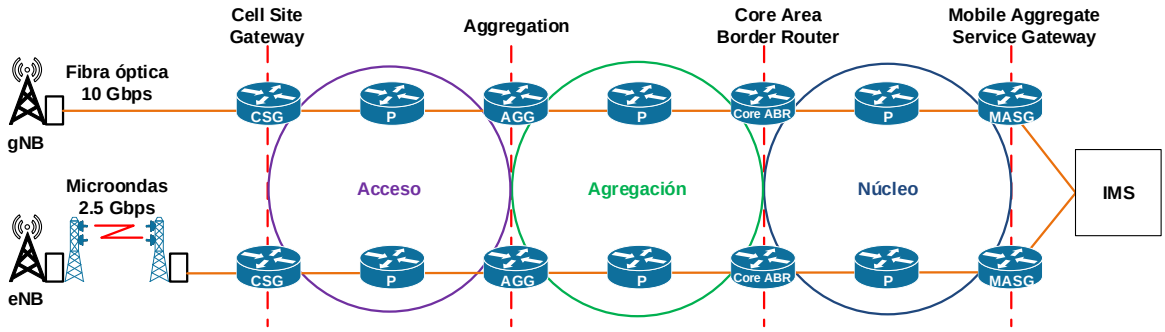


Figura 2-21 Arquitectura seamless MPLS [96]

Los routers PE, de la arquitectura MPLS convencional son reemplazados por los routers CSG (Cell Site Gateway) que se conecta a los nodos de acceso 4G o 5G a través de las interfaces lógicas correspondientes y el router MASG (Mobile Aggregate Service Gateway), se conecta al core 4G o 5G por las interfaces lógicas de las entidades correspondientes. Los routers CSG y MASG mantienen la funcionalidad de borde del proveedor (PE). Para efectos de esta tesis, dado que la arquitectura IMS provee el control de la señalización SIP a las redes 4G y 5G, el MASG estará conectado a las entidades P/S/I-CSCF y HSS. En los routers CSG y MASG se implementarán las VPN de capa 2 o 3, según sea la configuración implementada por el proveedor de servicio [96].

Los routers P mantienen su funcionalidad, y pueden haber o no, tantos como sean necesarios geográficamente para lograr la cobertura necesaria. Los routers AGG (Aggregation) y Core ABR (Core Area Border Router) implementan la funcionalidad del RR de BGP.

Al implementar la arquitectura seamless MPLS se tienen los siguientes beneficios [96]:

- Encapsula los servicios y los transmite a través de un LSP e2e.
- Se simplifica la operación de los nodos de acceso.
- Se segmenta la red al introducir las capas de acceso, agregación y núcleo en IP RAN.
- La segmentación de la red permite aislar las subredes en secciones específicas, reduciendo la carga de consumo de recursos de hardware en los equipos de la red IP MPLS.
- Se reduce la complejidad de los escenarios en donde la configuración de la arquitectura tradicional de MPLS hace difícil la gestión de la red, por lo que se simplifican los procesos de O&M.
- Permite crear servicios VPN de capas 2 y 3 de forma mucho más flexible, lo que reduce los costos de O&M.

2.6.1 Tipos de configuración seamless MPLS

Dependiendo de la interconectividad de sistemas autónomos del proveedor, la arquitectura seamless MPLS se puede clasificar de la siguiente manera:

- **Intra-AS seamless MPLS:** Las capas de acceso, agregación y núcleo de la red IP RAN están dentro del mismo AS. Se establecen sesiones iBGP y MPLS LDP entre cada par de equipos adyacentes, esto permite el intercambio de rutas etiquetadas a través de BGP, es la configuración más utilizada por los proveedores de servicio. Se establece entonces un LSP e2e BGP (ver Figura 2-22) [96].

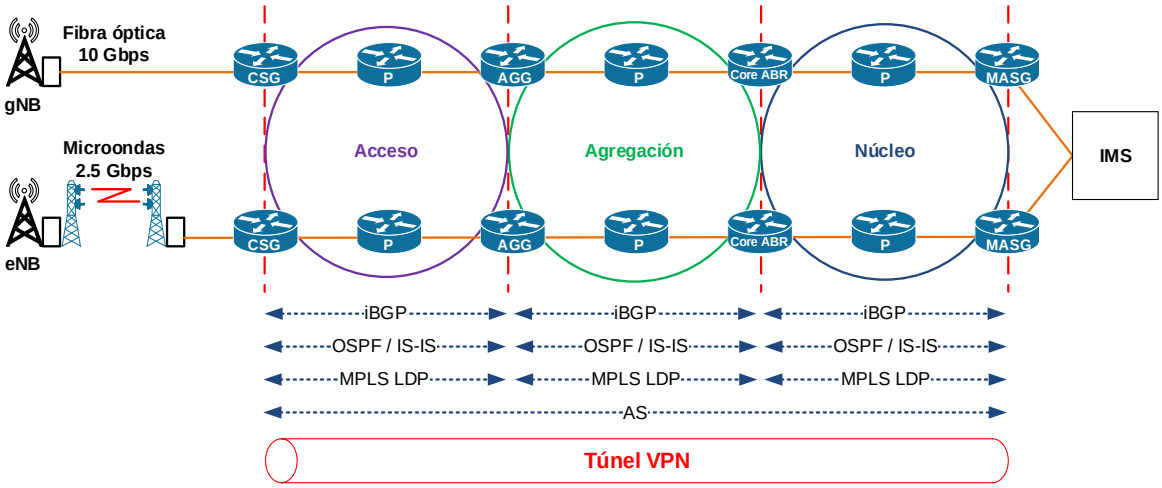


Figura 2-22 Intra-AS seamless MPLS [96]

- **Inter-AS seamless MPLS:** Las capas de acceso y agregación pertenecen a un AS y la capa de núcleo está en un AS distinto. Se establecen sesiones iBGP y MPLS LDP entre cada par de equipos adyacentes en cada AS, exceptuando los routers de borde de cada AS (AGG ASBR y Core ASBR). Posteriormente se interconectan ambos AS mediante eBGP. Los mensajes de eBGP entre los routers de borde de la capa de agregación u núcleo incluyen información de etiquetas MPLS (ver Figura 2-23) [96].

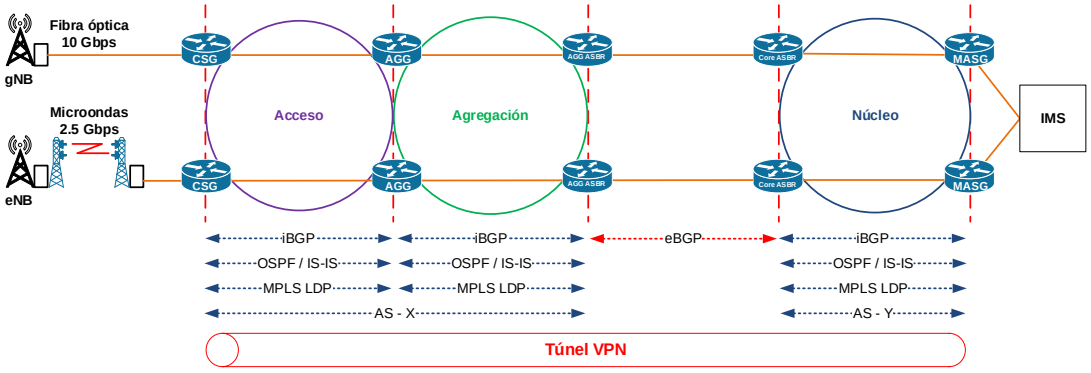


Figura 2-23 Inter-AS seamless MPLS [96]

- **Inter-AS seamless MPLS HVPN:** Se establecen sesiones iBGP y MPLS LDP entre cada par de equipos adyacentes intra-AS. Se establece una HVPN entre la capa de acceso y agregación. Luego seamless MPLS entre el AGG y el MASG. Se establece una relación de eBGP entre los routers de borde de agregación (AGG ASBR) y núcleo (Core ASBR). Se establece una relación MP-iBGP entre CSG y AGG y una relación MP-eBGP entre AGG y MASG. Se establecen sesiones iBGP y MPLS LDP entre cada par de equipos adyacentes en cada AS, exceptuando los routers de borde de cada AS (AGG ASBR y Core ASBR) (ver Figura 2-24) [96].

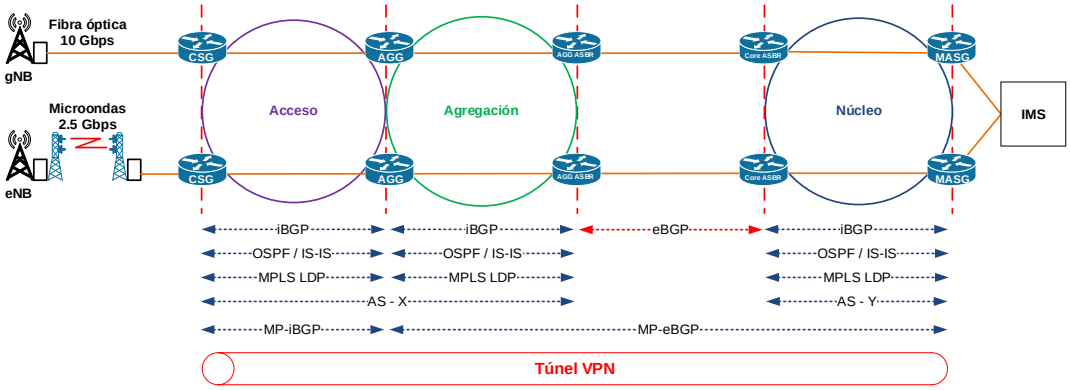


Figura 2-24 Inter-AS seamless MPLS HVPN [96]

2.7 Modelos de QoS en MPLS

Por defecto, las redes basadas en TCP-IP manejan el tráfico bajo el esquema de mejor esfuerzo, transportando la información con el esquema de encolamiento FIFO (Sin prioridades). En IP RAN (ver Figura 2-25), las políticas de QoS se establecen desde el nodo de acceso 4G o 5G hacia la red del proveedor de servicio. Estas políticas permiten definir las prioridades de los paquetes según los servicios que el usuario quiera consumir [95].

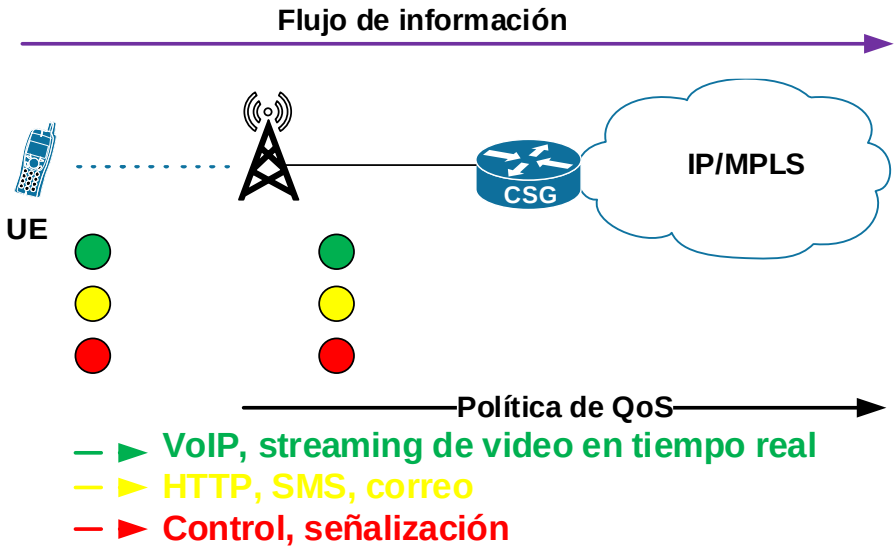


Figura 2-25 QoS en IP RAN [96]

Para garantizar la correcta interoperabilidad y convergencia de redes a nivel de red para la provisión de QoS IP extremo a extremo la IETF ha definido el modelo de reserva de recursos basados en Servicios Integrados (IntServ) y el modelo de priorización de tráfico basado en Servicios Diferenciados (DiffServ) [33,34].

- Servicios Integrados (IntServ).
- Servicios Diferenciados (DiffServ).

2.7.1 Modelo de Servicios Integrados (IntServ)

Surge en 1994 gracias al IETF como una alternativa de solución efectiva el modelo de mejor esfuerzo. Está definido bajo el RFC 1633. Entre sus características se encuentran [43]:

- Utiliza RSVP como protocolo de señalización.
- Reserva recursos de red para flujos de tráfico unidireccionales.

- Para flujos de tráfico bidireccionales, la señalización RSVP se realiza de manera independiente en cada dirección.
- Integra todos los servicios de manera controlada a través de los enlaces. Parte funciona tanto para comunicaciones unicast como multicast.

IntServ funciona de la siguiente manera [43]:

- Cada host o enrutador que usa RSVP puede especificar requisitos de recursos o calidad de servicios requeridos para la ruta de extremo a extremo, para cada flujo o secuencia de datos individual.
- Cada nodo en la ruta que recibe el mensaje RSVP verifica si tiene recursos suficientes para aceptar el flujo. Si la verificación falla, se envía una notificación de error al remitente que originó el RSVP.
- Si la señalización de RSVP es exitosa, entonces cada nodo en la ruta hace la reserva solicitada para la conexión y comienza la transmisión de datos. Para cada flujo con QoS se establece “un canal” con reserva de recursos, por lo que es difícilmente escalable y en consecuencia es poco utilizado.

El modelo de servicios integrados (IntServ) a su vez define dos tipos de modelos que son [43]:

- **Servicios garantizados:** emula BE. Misma garantía de QoS para los paquetes habiendo uno congestión. No es efectivo para el manejo de tráfico y retardos.
- **Servicios de carga controlada:** garantía sólo a nivel de Delay, no ofrece garantías en cuanto al Jitter. No es eficiente para servicios en tiempo real (VoIP o streaming de video en tiempo real). Se utiliza cuando se requieren garantías a nivel de recursos de red relacionadas con el ancho de banda para transmitir la información de manera integral.

2.7.2 Modelo de servicios diferenciados (DiffServ)

Está definido bajo el RFC 2475. En este modelo, el tráfico que ingresa se clasifica y posiblemente se condiciona en los límites de la red, asignando diferentes agregados de comportamiento conocidos como Behavior Aggregates (BA). Se le asigna un comportamiento los paquetes dependiendo del servicio que representan. Este modelo introduce la posibilidad de separar el tráfico de voz, datos y video para darles tratamientos y prioridades relacionadas a las necesidades de proveedor de servicios. Entre sus mayores

ventajas se encuentra el hecho de que puede ser implementado en una red que trabaja con MPLS [97].

2.7.3 Elementos de DiffServ

El modelo DiffServ contempla los siguientes elementos, que se ilustran en la Figura 2-26 [95]:

- **BA (Behavior Aggregate):** Es el comportamiento de un agregado dentro de un DS Domain.
- **DSCP (Differentiated Service Code Point):** Es un valor definido en el campo ToS (Type of Service) de la cabecera IPv4. Este campo indica el comportamiento del rotor de borde del DS deberá asignarle.
- **PHB (Per-Hop Behavior):** Comportamiento por salto, es el tratamiento de QoS el modelo DiffServ y aplica una clase de tráfico en concreto cuando se mueve entre distintos nodos que forman parte de un mismo DS Domain. El modelo DiffServ define cuatro tipos de PHB:
    - **EF (Expedited Forwarding):** reenvío acelerado para aquellos paquetes cuya importancia es muy alta.
    - **AF (Assured Forwarding):** reenvío asegurado, para aquellos paquetes que requieren un mínimo de ancho de banda para su entrega.
    - **CS (Class Selector):** selector de clases, clasifica los paquetes de segunda clase.
    - **BE (Best Effort) o DF (Default Forwarding):** envío tradicional basada mejor esfuerzo.

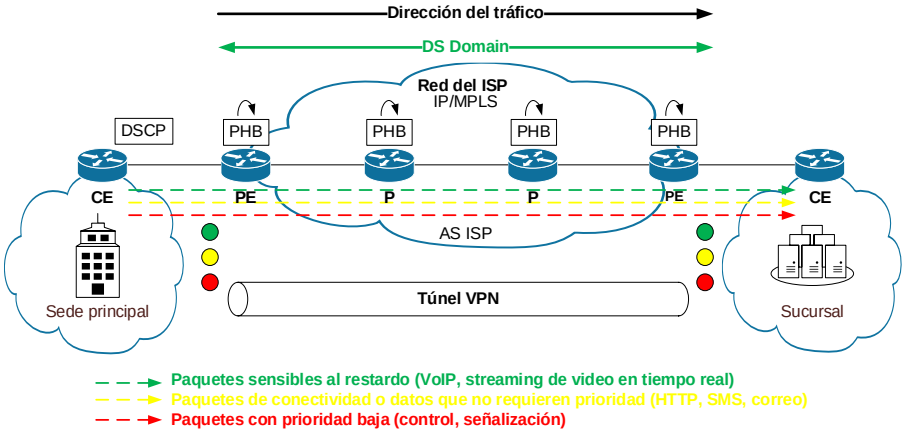


Figura 2-26 Arquitectura BGP MPLS-TE IP-VPN [95]

Los paquetes marcados con DSCP los equipos clientes son recibidos por el router de borde del DS, quien los clasifica dentro de distintos BA. Luego en el núcleo de la red del SP, los paquetes se reenvían de acuerdo con el comportamiento definido por los routers de borde. Se asignan "colores" para determinar el tipo de tratamiento de los paquetes (ver Tabla 2-5), por ejemplo:

Tabla 2-5 Ejemplos de BA [95]

Behavior Aggregate (BA)	Descripción
Verde	Paquetes sensibles al retardo y que requieren ancho de banda mínimo (VoIP o streaming de video en tiempo real).
Amarillo	Paquetes de conectividad o datos que no requieren tanta prioridad (HTTP, correo, SMS).
Rojo	Paquetes con prioridad baja (control o señalización).

El router de borde clasifica los paquetes en los BA y los reenvía a los router intermediarios quienes los verifican, reenviándolos según el comportamiento establecido, a esto se le conoce como comportamiento por salto (per-hop-behavior).

El Dominio de Servicios Diferenciados (DS Domain) se define como toda red IP que utiliza el modelo de Servicios Diferenciados. SIP utiliza el backbone IP/MPLS como un DS Domain para controlar de forma más eficiente el tráfico entrante a la red, para cumplir con los SLA's acordados con sus clientes. En tal sentido de acuerdo con [95]:

- Cada sistema autónomo que utilice en su backbone IP el modelo de DiffServ será considerado como un DS Domain.

- Dentro de una red corporativa, pueden existir varios DS Domain siempre que el administrador de la red así lo decida.
- La red IP/MPLS con QoS del SP se considerará un DS Domain.

En la práctica, el objetivo es diferenciar los distintos tipos de servicios entrantes al dominio, para luego reenviarlos de acuerdo con el tratamiento que cada uno requiere (PHB). El modelo presenta una arquitectura en donde el cliente puede ser uno de los siguientes elementos [95]:

- Un router de un cliente corporativo.
- Un switch de un cliente corporativo.
- Un router de la red del mismo proveedor de servicios de Internet nodo de red de acceso radio (eNode B de 4G o un gNode B de 5G).
- Un dispositivo de VoIP.

Cuando se habla de un equipo cliente, se habla de un equipo que introduce distintos tipos de tráfico a dicho dominio, esos equipos pueden ser externos al proveedor o internos.

2.7.4 Campo de Servicios Diferenciados

En cada tecnología se utiliza su cabecera en un campo específico para QoS [97]:

- En la cabecera de IPv4, se utiliza el campo Type of Service (ToS).
- En la cabecera de IPv6, se utiliza el campo Traffic Class (TC).
- En Ethernet se utiliza el campo 802.1p.
- En la cabecera de MPLS se utiliza el campo EXP.

MPLS permite la integración de diferentes tecnologías, el campo EXP es el más relevante. Campo ToS de IPv4: RFC 791 cabecera IPv4 (ver Figura 2-27).

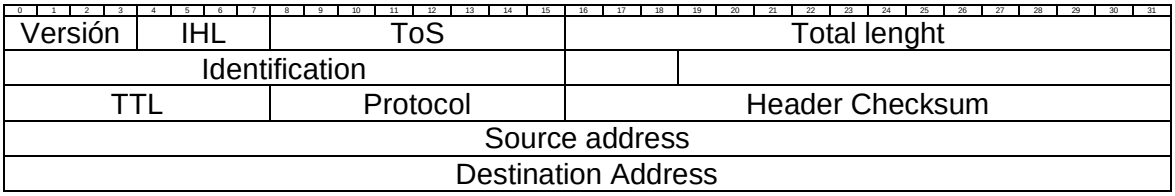


Figura 2-27 Cabecera IPv4 [97]

La descripción de los campos de la cabecera IPv4 es la siguiente:

- **Versión (4 bits):** indica la versión del paquete (IPv4 o IPv6).
- **IHL (4 bits):** indica el tamaño de la cabecera del paquete IP.
- **Type of Service-ToS (8 bits):** Indica la QoS deseada para el paquete.

- **Total lenght (16 bits):** indica el tamaño del paquete.
- **Identification (16 bits):** usado para identificar los fragmentos de un datagrama.
- **Flags (3 bits):** usado para la información de los fragmentos.
- **Fragment offset (13 bits):** indica la posición de la carga útil al comienzo del segmento de datos no fragmentado.
- **TTL (8 bits):** indica el tiempo de vida del paquete. Se decrementa en uno con cada salto.
- **Protocol (8 bits):** indica el protocolo de capa superior utilizado.
- **Checksum (16 bits):** utilizado para verificar la correcta validez de la cabecera del paquete.
- **Source Address (32 bits):** IP de origen.
- **Destination (32 bits):** IP de destino.

El campo ToS, en la Figura 2-28, indica una serie de parámetros que combinados entre sí representarán la QoS deseada para el paquete, en el cual se usan 6 bits para asignar lo que se conoce como el DSCP (Diffetentiated Service Code Point). El tratamiento del tráfico en IP MPLS se realiza en el dominio de servicios diferenciados de acuerdo con el valor del DSCP en el campo ToS de la cabecera IPv4 [95], [106].

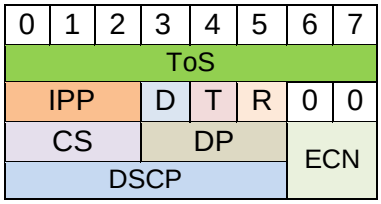


Figura 2-28 Campo ToS parámetros equivalentes [95], [106]

A continuación, se describen los diferentes parámetros del campo ToS:

- **IPP:** Valor de precedencia IP, selector de clase (CS, por sus siglas en inglés) o Clase de Servicio (CoS, por sus siglas en inglés). Identifica el tipo de servicio que se está transportando en el paquete. La prioridad se escribe de manera descendente, la red dará prioridad a aquellos paquetes cuyo valor de presencia sea más alto. La Tabla 2-6 muestra los posibles valores de precedencia:

Tabla 2-6 Valores de precedencia [106]

Precedencia				Uso	Comentario
Valor decimal	Valor binario				
7	1	1	1	Control de red	Reservados para el control de tráfico
6	1	1	0	Control de interred	
5	1	0	1	Crítico / ECP	Disponibles para el usuario
4	1	0	0	Flash override	
3	0	1	1	Flash	
2	0	1	0	Inmediato	
1	0	0	1	Prioridad	
0	0	0	0	Rutina	

- **DP:** Probabilidad de descarte (3 bits), está con formado por los valores de los bits D, T y R (Tabla 2-7).

  Tabla 2-7 Valores de probabilidad de descarte del campo ToS [106]

DP			Probabilidad
D	T	R	
0	1	0	Baja
1	0	0	Media
1	1	0	Alta

- **ECN:** Notificación de congestión explícita, se utilizan de forma opcional para notificar la congestión, se asume que siempre están en estado 0.
- **D:** Delay o latencia, el valor 0 indica que el paquete acepta un nivel normal de retardo. El valor 1 indica que el paquete es sensible al retardo. El retardo es el parámetro que sirve para identificar si el paquete es sensible o no a este.
- **T:** Throughput o rendimiento, el valor 0 indica que el paquete acepta un nivel normal de rendimiento. El valor 1 indica que el paquete requiere mayor ancho de banda.
- **R:** Reliability o confiabilidad, el valor 0 indica una probabilidad de descarte normal. El valor 1 indica baja probabilidad de caída o descarte. La confiabilidad indica si el paquete puede o no ser descartado por la red.

Los valores de precedencia se pueden asociar con los PHB y el campo EXP de la cabecera MPLS de la siguiente manera. Dependiendo del valor EXP en la cabecera MPLS del paquete, el router lo clasificará como un PHB en particular (ver Tabla 2-8):

Tabla 2-8 Valores del campo EXP y PHB asociados [95], [106]

EXP	Precedencia			PHB
Valor decimal	Valor binario			
7	1	1	1	CS7
6	1	1	0	CS6
5	1	0	1	EF
4	1	0	0	AF4
3	0	1	1	AF3
2	0	1	0	AF2
1	0	0	1	AF1
0	0	0	0	BE

La Figura 2-29 muestra los posibles valores de DSCP y PHB según el RFC 4594:

PHB	IPP = CoS = EXP	DP	DSCP decimal	ToS decimal	Aplicación
CS0	0		0	0	Mejor esfuerzo
CS1	1		8	32	Scavenger
AF11	1	Bajo	10	40	Datos masivos
AF12	1	Medio	12	48	
AF13	1	Alto	14	56	
CS2	2		16	64	Gestión de red
AF21	2	Bajo	18	72	Datos transaccionales
AF22	2	Medio	20	80	
AF23	2	Alto	22	88	
CS3	3		24	96	Señalización voz
AF31	3	Bajo	26	104	Misión crítica
AF32	3	Medio	28	112	Video streaming
AF33	3	Alto	30	120	
CS4	4		32	128	
AF41	4	Bajo	34	136	
AF42	4	Medio	36	144	
AF43	4	Alto	38	152	
CS5	5		40	160	
EF	5		46	184	Voz
CS6	6		48	192	Enrutamiento
CS7	7		56	224	

Figura 2-29 Valores de DSCP y PHB según el RFC 4594 [95], [106], [107]

2.8 Tipos de tráfico

Dentro de los servicios ofrecidos por un ISP se encuentran diferentes tipos de tráfico, los cuales se caracterizan por tener diferentes tipos de requerimientos de ancho de banda,

retardo, variación del retardo y pérdida de paquetes. En función de las necesidades del cliente, se establecerá la priorización de este tráfico dentro de la red. Dependiendo del tipo de RAN se utilizarán los parámetros definidos por el QCI o el 5QI de las redes 4G y 5G respectivamente [96].

2.8.1 Elasticidad de una aplicación

La elasticidad o inelasticidad de una aplicación se refiere a la capacidad que tiene una aplicación de reaccionar a las condiciones cambiantes de la red. Por ejemplo, las aplicaciones TCP reducirán su tasa de transmisión cuando los paquetes se pierden haciéndolos elásticos. La televisión en vivo y la voz por IP, a menudo basadas en UDP, no disminuyen su velocidad de transmisión y son consideradas inelásticas [106].

2.8.2 Aplicaciones no interactivas o por lotes

Dentro de las aplicaciones por lotes se pueden encontrar archivos o ficheros que proveen información a los usuarios de la red. En función de su tamaño, será necesario transmitir una determinada cantidad de paquetes, la cual puede ser calculada de la siguiente manera [108]:

$$Paquetes_{IP} = \frac{Peso_{Fichero}\left[bytes\right]}{Segmento_{TCP}\left[bytes\right]} \tag{2-3}$$

Donde:

$Paquetes_{IP}$: $Número\ de\ paquetes\ IP\ a\ transmitir$
$Peso_{Fichero}$: $Peso\ del\ fichero\ a\ transmitir$
$Segmento_{TCP}$: $Número\ de\ paquetes\ IP\ a\ transmitir$

El tiempo de descarga del fichero estará dado por el cociente entre el peso del fichero y la velocidad o ancho de banda de descarga contratada en el ISP [108]:

$$t_{descarga}[s] = \frac{Peso_{Fichero}\left[bits\right]}{BW\left[bps\right]} \tag{2-4}$$

Donde:

$t_{descarga}$: $Tiempo\ de\ descarga\ del\ fichero$
$Peso_{Fichero}$: $Peso\ del\ fichero\ a\ transmitir$
BW: $Ancho\ de\ banda\ de\ descarga\ contratado\ en\ el\ ISP$

Por lo tanto, se observa que, a mayor ancho de banda de descarga contratado, menor es el tiempo de descarga para el cliente.

Este tipo de aplicación no es sensible al retardo, ni a la variación del retardo, debido a que el usuario no está interactuando con el fichero. Una vez que inicia la descarga del fichero, debe esperar a que termine.

Por último, en el caso de la pérdida de paquetes, debido que se utiliza el protocolo TCP, en caso de pérdida los paquetes en el receptor, estos son retransmitidos por el origen.

2.8.3 Aplicación interactiva

Son aplicaciones que no requieren mucho ancho de banda, pero son algo sensibles al retraso y la pérdida de paquetes, como por ejemplo las conexiones Telnet o SSH al momento de gestionar un router o switch de forma remota [108].

2.8.4 Aplicaciones de voz y video

Las aplicaciones de voz y video son las que generan el tráfico más sensible en la red en términos de retardo, variación del retardo y pérdida de paquetes [108].

- **Voz:** En una red IMS, el protocolo de señalización es SIP para el establecimiento y mantenimiento de las sesiones, la voz se transporta mediante el protocolo RTP. Para la información de control se utiliza el protocolo RTCP (Real Time Transport Protocol). El tráfico de voz utiliza el protocolo UDP. En función del códec que se utilice se garantizan diferentes anchos de banda requeridos para codificar y decodificar la voz, la negociación de los códecs de voz se realiza mediante el protocolo SDP (Session Description Protocol). Los parámetros típicos que garantizan la QoS son los siguientes:
  - **Retardo de una vía:** < 150 ms.
  - **Jitter:** <30 ms.
  - **Pérdida de paquetes:** < 1%
- **Video:** El tráfico de video tiene requerimientos similares al tráfico de voz. El tráfico de video requiere más ancho de banda que el tráfico de voz, dependiendo del códec y del tipo de video que está transmitiendo (por ejemplo, un video con muchos cuadros por segundo requiere más ancho de banda). El tráfico de video interactivo es sensible al retardo, la variación del retardo y la pérdida de paquetes. Los parámetros típicos que garantizan la QoS son los siguientes:
  - **Retardo de una vía:** 200 – 400 ms.
  - **Jitter:** 30 – 50 ms.

- **Pérdida de paquetes:** Entre 0.1% – 1%

2.9 QoS en IP RAN

Para proveer QoS en IP RAN, se debe tener en cuenta que la QoS e2e depende del manejo de la QoS en la red de acceso 4G o 5G y el manejo de QoS en la red de transporte IP/MPLS. La Figura 2-30 describen las etapas de la arquitectura para QoS en IP RAN, en la que el UE procede enviar paquetes asociados a diferentes servicios. El nodo de acceso asigna un identificador de QoS dependiendo del tipo de servicio y luego los reenvía la red IP/MPLS [96].

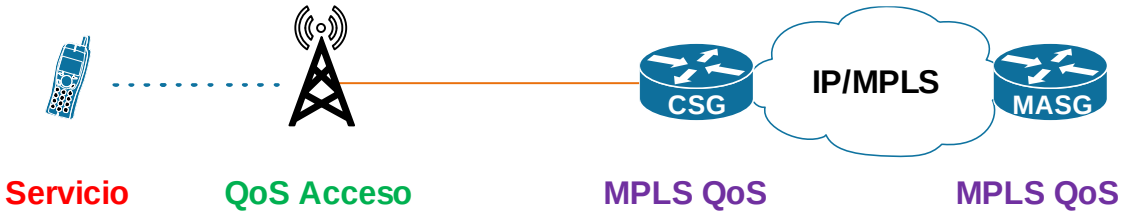


Figura 2-30 Aquitectura para QoS en IP RAN [96]

En la red IP RAN se mapean los identificadores de QoS de 4G LTE o 5G NR con un valor de DCSP. Luego en el DS Domain se mapea el valor de DSCP a un valor de EXP en la cabecera MPLS.

2.9.1 4G LTE QoS Identifier (QCI)

LTE utiliza un identificador para cada servicio de usuario con la QoS requerida, clasificándolo como GBR (Guaranteed Flow Bit Rate) o non-GBR (non Guaranteed Flow Bit Rate). Este procedimiento se realiza de acuerdo con la especificación del 3GPP TS 23.203 (ver Tabla 2-9).

Tabla 2-9 Valores representativos de QCI según el 3GPP TS 23.203 [109]

QCI	Tipo de recurso	Prioridad	Packet delay	Packet Error Loss Rate	Servicios
1	GBR	2	$100ms$	10^{-2}	Voz conversacional
2		4	$150ms$	10^{-3}	Video en tiempo real
3		3	$50ms$	10^{-3}	Juegos en tiempo real
4		5	$300ms$	10^{-6}	Video almacenado (buffer)
5	Non-BGR	1	$100ms$	10^{-6}	Señalización IMS
6		6	$300ms$	10^{-6}	Web, correo, FTP (usuarios con prioridad alta)

QCI	Tipo de recurso	Prioridad	Packet delay	Packet Error Loss Rate	Servicios
7		7	$100ms$	10^{-3}	Voz, video en tiempo real y juegos
8		8	$300ms$	10^{-6}	Web, correo, FTP (usuarios con prioridad media)
9		9	$300ms$	10^{-6}	Web, correo, FTP (usuarios con prioridad baja)

2.9.2 5G NR QoS Identifier (5QI)

5G utiliza un identificador para cada servicio de usuario con la QoS requerida, clasificándolo como GBR (Guaranteed Flow Bit Rate) o non-GBR (non Guaranteed Flow Bit Rate). Este procedimiento se realiza de acuerdo con la especificación del 3GPP TS 23.501 (ver Tabla 2-10).

Tabla 2-10 Valores representativos de 5QI según el 3GPP TS 23.501 [110]

5QI	Tipo de recurso	Prioridad	Packet delay	Packet Error Loss Rate	Servicios
1	GBR	20	$100ms$	10^{-2}	Voz conversacional
2		40	$150ms$	10^{-3}	Video conversacional
3		30	$50ms$	10^{-3}	Juegos en tiempo real, mensajes V2X, distribución de electricidad, monitoreo de procesos de automatización
4		50	$300ms$	10^{-6}	Video no-conversacional streaming almacenado (buffer)
65		7	$75ms$	10^{-2}	Voz push to talk de misión crítica en plano de usuario
66		20	$100ms$	10^{-2}	Voz push to talk de misión no crítica en plano de usuario
67		15	$100ms$	10^{-3}	Video de misión crítica en el plano de usuario
75		25	$50ms$	10^{-2}	Mensajes V2X
5	Non-BGR	10	$100ms$	10^{-6}	Señalización IMS
6		60	$300ms$	10^{-6}	Video (streaming almacenado), aplicaciones TCP (correo electrónico, chat, ftp, archivos compartidos p2p, video progresivo, etc.)
7		70	$100ms$	10^{-3}	Voz, video (streaming en vivo), juegos interactivos
8		80	$300ms$	10^{-6}	Video (streaming almacenado), aplicaciones TCP (correo electrónico,

5QI	Tipo de recurso	Prioridad	Packet delay	Packet Error Loss Rate	Servicios
					chat, ftp, archivos compartidos p2p, video progresivo, etc.)
9		90	$300ms$	10^{-6}	Video (streaming almacenado), aplicaciones TCP (correo electrónico, chat, ftp, archivos compartidos p2p, video progresivo, etc.)
69		5	$60ms$	10^{-6}	Señalización de misión crítica sensible al retardo
70		55	$200ms$	10^{-6}	Datos de misión crítica (mismos servicios de QCI 6/8/9)
79		65	$50ms$	10^{-2}	Mensajes V2X
80		68	$10ms$	10^{-6}	Aplicaciones eMBB de baja latencia, realidad aumentada

2.10 Herramientas para el manejo de QoS

La Figura 2-31 ilustra el proceso que se le debe aplicar al tráfico que atraviese un router para proveer QoS, tanto en IPv4 como en IPv6. No todos los pasos descritos deben ser configurados en un mismo router y en el mismo orden [106], sin embargo este es el proceso lógico.

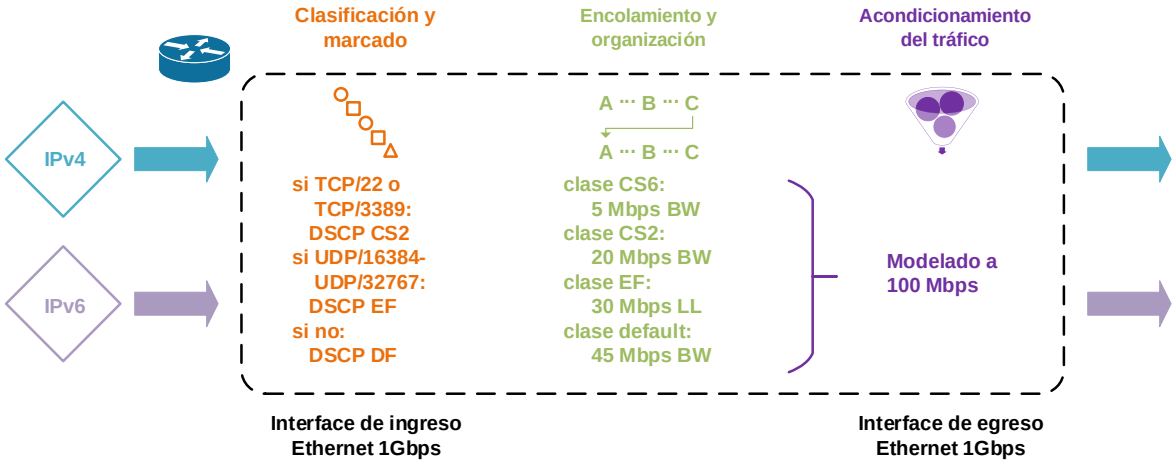


Figura 2-31 Proceso de aplicación de políticas de QoS en Diffserv en un router [106]

De acuerdo con los diferentes requerimientos de tráfico en la red, se deben utilizar las siguientes herramientas para el manejo de QoS [106], [108]:

- **Clasificación y marcado:** Para poder brindar un tratamiento diferenciado a los paquetes transmitidos según la prioridad requerida, es necesario identificar los paquetes y marcarlos con el valor de DSCP correspondiente.

- **Encolamiento (queuing) y organización del tráfico (scheduling):** Para manejar el tráfico en las interfaces de un router o switch multicapa, se utilizan buffers de memoria, en lugar de manejar una única cola que aplique el método FIFO. Se pueden crear diferentes colas que manejen diferentes prioridades según el marcado asignado.
- **Acondicionamiento del tráfico:** Se utiliza para reducir artificialmente la velocidad de transmisión del tráfico. Dado que en un ISP se poseen interfaces con velocidades de transmisión más altas que las velocidades contratadas por el cliente, el tráfico se debe adaptar a esta última, ya que de lo contrario el tráfico excedente sería descartado. Dentro del acondicionamiento del tráfico se encuentran las siguientes herramientas o mecanismos:
    - **Vigilancia (policing) y modelado (shaping) del tráfico:** Con estas herramientas se limita la tasa de transmisión del tráfico.
    - **Evasión de la congestión:** Sirve para evitar la pérdida de paquetes y reducir la congestión.

2.10.1 Clasificación y marcado

La Figura 2-32 describe el proceso de clasificación y marcado en el router R1.

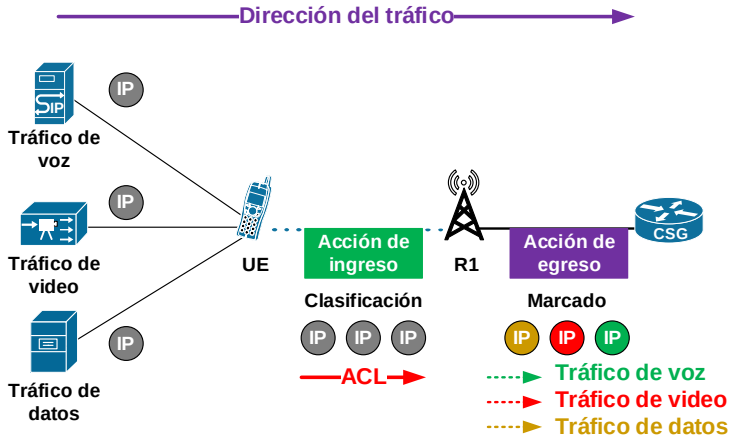


Figura 2-32 Clasificación y marcado del tráfico [106]

La clasificación consiste en identificar y caracterizar las aplicaciones en función de las direcciones IP, enlaces entre paquetes, protocolos, puertos y detalles de la capa de aplicación de los paquetes que ingresan a una interfaz del router [106], esta acción se puede lograr mediante la creación de listas de control de acceso (ACL), o en el caso de

equipos Cisco, mediante el reconocimiento de aplicaciones basado en red (NBAR). La diferencia entre estas dos alternativas radica en que la ACL es un método manual de reconocimiento de aplicaciones y NBAR es un método automático [108].

El marcado consiste en cambiar el campo ToS del encabezado de un paquete según el tipo de aplicación, es decir una vez que el tráfico fue clasificado. El valor del campo ToS se asigna según el valor DSCP de la aplicación correspondiente. El anexo A muestra los Valores recomendados de PHB y DSCP [106] con los que se diseñaran las políticas de QoS en el escenario planteado en la Figura 3-1 para el tráfico de voz, datos y video.

2.10.2 Encolamiento (queuing) y organización del tráfico (scheduling)

Todos los dispositivos intermediarios de red (L2/L3) reciben información desde un origen para reenviarlos y un destino, pero en ocasiones, las interfaces están ocupadas o congestionadas, motivo por el cual se usa el encolamiento (queue). La Figura 2-33 ilustra el proceso de encolamiento (queuing) y organización del tráfico (scheduling):

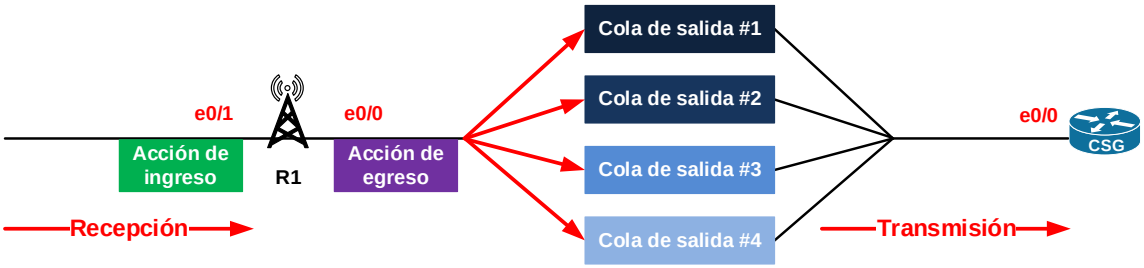


Figura 2-33 Encolamiento (queuing) y organización del tráfico (scheduling) [108]

Los equipos intermediarios reciben la información por distintas interfaces de red, teniendo interfaces de entrada de tráfico interfaces de salida y alguna realizarán ambas acciones. Por defecto, estos equipos manejan un esquema de encolamiento FIFO. En ocasiones las interfaces se pueden congestionar debido al tráfico que manejan, motivo por el cual manejan el encolamiento, para colocar la información en colas de espera para reenviar la información cuando la interfaz esté disponible. Cuando una cola se llena los paquetes son descartados, se conoce con el término ***queue starvation*** en inglés [108].

La congestión puede causar problemas a nivel de retardos, jitter, pérdida de paquetes y por tanto generar una mala experiencia en el usuario. Al hablar de manejo de congestión en QoS, se habla de un conjunto de herramientas encargadas de manejar las colas que

mantienen a los paquetes que están a la espera de ser enviados. La mayoría de los equipos de red poseen sistemas de encolamiento con diferentes colas para cada clase de servicio una vez ser ha realizado el proceso de clasificación y marcado de tráfico [95].

Se pueden utilizar diferentes algoritmos para el manejo de la congestión al organizar el tráfico en colas, tales como CBWFQ (Class Based Weighted Fair Queuing, por sus siglas en inglés) que garantiza un ancho de banda mínimo para cada clase cuando hay congestión y que funciona para aplicaciones de datos, ya que garantiza un cierto ancho de banda para cada cola. Sin embargo, esto no funciona para el tráfico sensible al retraso como VoIP. Otro algoritmo es LLQ (Low Latency Queuing) el cual prioriza una cola con reenvío inmediato mientras todas las demás colas deben esperar [108].

2.10.3 Vigilancia de tráfico (Policing)

Este mecanismo utilizado por los ISP se refiere a los paquetes que son descartados por los límites o las políticas operativas, descartando paquetes que tienen la prioridad más baja mientras se envían. Este mecanismo se utiliza en los routers y se aplica a los paquetes IP en las interfaces de entrada y salida [111], dependiendo de las siguientes variables de acuerdo con el RFC 2698 [112]:

- **PIR (Peak Information Rate):** Velocidad máxima de transmisión de un cliente en bits/s previamente acordada entre el cliente y el operador con cualquier tipo de contrato o acuerdo de nivel de servicio (SLA). El PIR nunca puede ser mayor que la capacidad de la línea provista por el operador [113].
- **CIR (Committed Information Rate):** Tasa promedio de tráfico a largo plazo que el operador se compromete a proporcionar a un cliente con un contrato o acuerdo de nivel de servicio (SLA). Este parámetro se mide en bits/s y generalmente es menor que PIR. En cualquier caso, el CIR nunca puede ser mayor que el PIR [113].
- **CBS (Committed Burst Size):** Tamaño máximo de ráfaga permitido en la red. Especifica el número máximo de bytes que pueden transmitirse al PIR, mientras cumple con el acuerdo del CIR [113].
- **PBS (Peak Burst Size):** Similar al CBS pero definido con respecto a PIR en lugar del parámetro CIR [113].

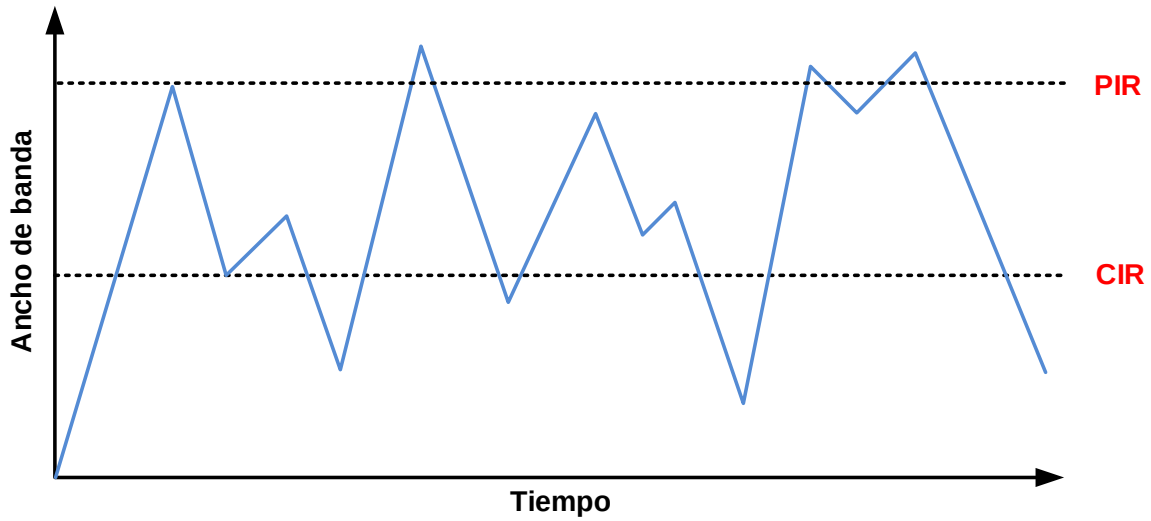


Figura 2-34 Comportamiento típico del tráfico generado por un usuario [108]

Para el análisis del comportamiento del tráfico al aplicar el mecanismo de policing se utilizará la Figura 2-34, como se observó, el parámetro CIR se refiere a la velocidad contratada por el cliente, mientras que el PIR se refiere a la velocidad pico que puede llegar a alcanzar, sin sobrepasar la velocidad de línea o a la capacidad de la interfaz del equipo del ISP.

Cuando se aplica policing, el tráfico observado en la Figura 2-34 es modificado, siendo descartados todos los paquetes que excedan el CIR. Solo se permite una ráfaga que supere este punto durante un breve periodo de tiempo luego de un tiempo de inactividad (ver Figura 2-35).

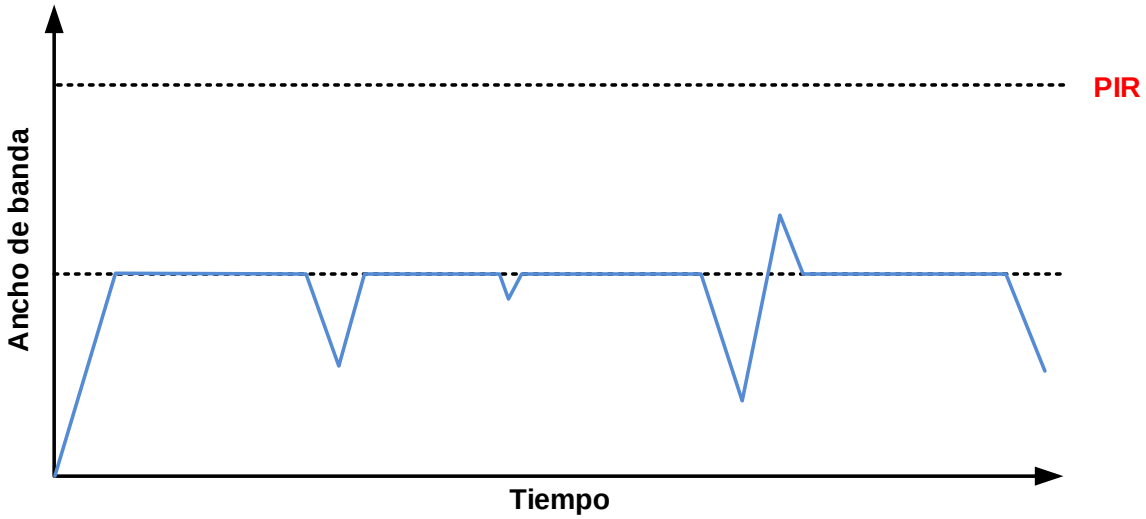


Figura 2-35 Vigilancia de tráfico (Policing) [108]

Cuando se trabaja con vigilancia, hay tres categorías que se pueden utilizar para podemos usar para saber si un paquete cumple con el tráfico contratado o no, entre las que están:

- Conforme
- Excesivo
- Violación

En función de cómo se trabaje con estas categorías, se pueden encontrar tres técnicas diferentes para el manejo del tráfico, que son:

- Tasa única, dos colores.
- Tasa única, tres colores.
- Tasa dual, tres colores.

2.10.4 Modelado de tráfico (Shaping)

El modelado del tráfico utiliza una política basada en el encolamiento y la posterior extracción de paquetes para mantener la velocidad del tráfico [113]. Es ampliamente utilizado por los proveedores de servicios y usuarios para garantizar siempre el ancho de banda contratado [111]. Tomando como referencia la Figura 2-34, al aplicar el modelado de tráfico se tiene el comportamiento resultante de la Figura 2-36, en la que el tráfico está en cola y retrasado, por lo que se supera el CIR. Esto evita el tráfico se caiga en el ISP. La desventaja de esta herramienta radica en que introduce retardos, lo que puede afectar a

las aplicaciones y servicios que sean sensibles a este parámetro, tales como la voz y el video en vivo [106], [108].

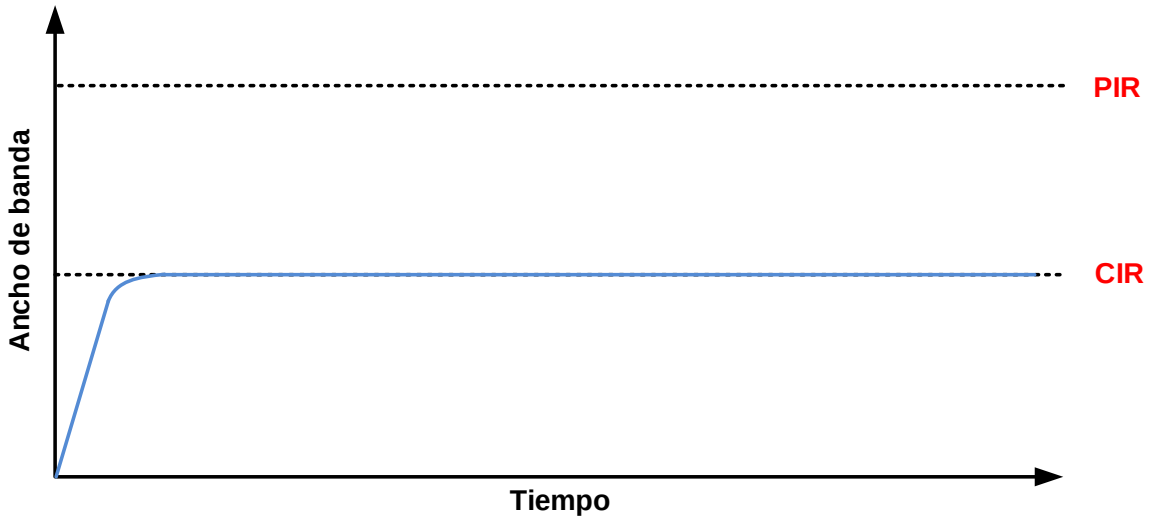


Figura 2-36 Modelado de tráfico (shaping) [108]

2.10.5 Evasión de la congestión

Este mecanismo sirve para modificar la ventana de congestión del protocolo TCP, utilizando algoritmos como WRED (Weighted Random Early Detection, por sus siglas en inglés). Estas herramientas monitorearán la cola de salida y una vez que esté en un cierto nivel, eliminarán los segmentos de TCP de manera aleatoria, con el objetivo de que, al reducir el tamaño de la ventana, las conexiones de TCP se ralentizarán para que se logre reducir la congestión y evitar la caída de la cola. Las variaciones de la velocidad de los flujos TCP/IP de tráfico repentino provoca la pérdida simultánea de paquetes en muchas sesiones TCP utilizando un solo enlace (congestionado), esto se conoce como sincronización global TCP [108].

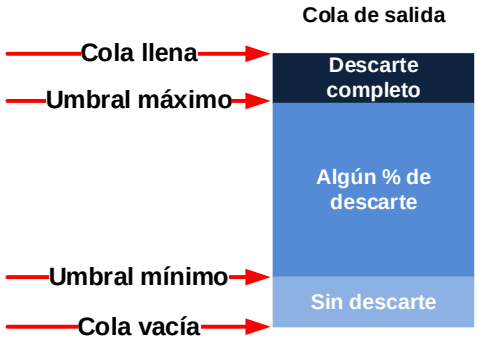


Figura 2-37 Evasión de la congestión [108]

La Figura 2-37 ilustra el manejo de los umbrales de descarte. Cuando la cola está vacía, no se descarta ningún paquete. Una vez que la cola se llena y está entre el umbral mínimo y máximo, se descarta un pequeño porcentaje de los paquetes. Una vez se supera el umbral máximo, se descartan todos los paquetes.

La herramienta para evitar la congestión puede descartar paquetes de forma aleatoria, o se puede configurar para dar a ciertos paquetes un tratamiento diferente en función de su marcado [108].

2.10.6 Ecuaciones para el acondicionamiento del tráfico

A continuación, se presentan las ecuaciones necesarias para el condicionamiento del tráfico, al diseñar políticas de QoS que apliquen vigilancia o modelado del tráfico.

Ecuaciones para el cálculo del retardo de serialización [107]:

$$S_d = \frac{F_{size}}{phy} \qquad F_{size} = S_d * phy \qquad phy = \frac{F_{size}}{S_d} \tag{2-5}$$

Donde:

S_d: $Retardo\ de\ serialización$ [s]
F_{size}: $Tamaño\ de\ la\ trama$ [bits]
phy: $Velocidad\ del\ puerto\ físico$ [bits/s]

Ecuaciones para el cálculo del CIR [107]:

$$T_c = \frac{B_c}{CIR} \qquad B_c = T_c * CIR \qquad CIR = \frac{B_c}{T_c} \tag{2-6}$$

Donde:

Tc: $Tiempo\ comprometido$ [s]
Bc: $Ráfaga\ comprometida$ [bits]
CIR: $Committed\ Information\ Rate$ [bits/s]

Ecuaciones para el cálculo del PIR [107]:

$$T_c = \frac{(B_c + B_e)}{PIR} \qquad PIR = \frac{(B_c + B_e)}{T_c} \qquad (2\text{-}7)$$

$$B_c = (T_c * PIR) - B_e \qquad B_e = (T_c * PIR) - B_c$$

Donde:

Tc: $Tiempo\ comprometido$ [s]

Bc: $Ráfaga\ comprometida$ [bits]

Be: $Exceso\ de\ ráfaga$ [bits]

PIR: $Peak\ Information\ Rate$ [bits/s]

3. Evaluación del impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video

En este capítulo se presenta la evaluación del impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video en los escenarios de conectividad en L2VPN y L3VPN en un entorno emulado, donde se realiza un diseño de red con base en la arquitectura seamless MPLS para la conectividad de dos dominios de red IMS. Se realiza la caracterización del tráfico de la red según los servicios de voz, datos y video a entregar a los usuarios finales, donde en función de estas características se procede a diseñar, implementar y evaluar las políticas de QoS necesarias para cumplir con las métricas de QoS para los servicios definidos.

3.1 Diseño de red para la interconexión de redes IMS entre proveedores para la prestación de servicios interdominio

Para evaluar los parámetros de QoS tales como el retardo, la variación del retardo, el ancho de banda y la pérdida de paquetes en un escenario de interconexión en IMS ,como el planteado en la

Figura **1-12**, se plantea el diseño de red que se observa en la Figura 3-1 utilizando la arquitectura seamless MPLS para la prestación de servicios convergentes de acuerdo con las especificaciones 3GPP TS 23.107, 3GPP TS 23.203 y 3GPP TS 23.207 [48], [49].

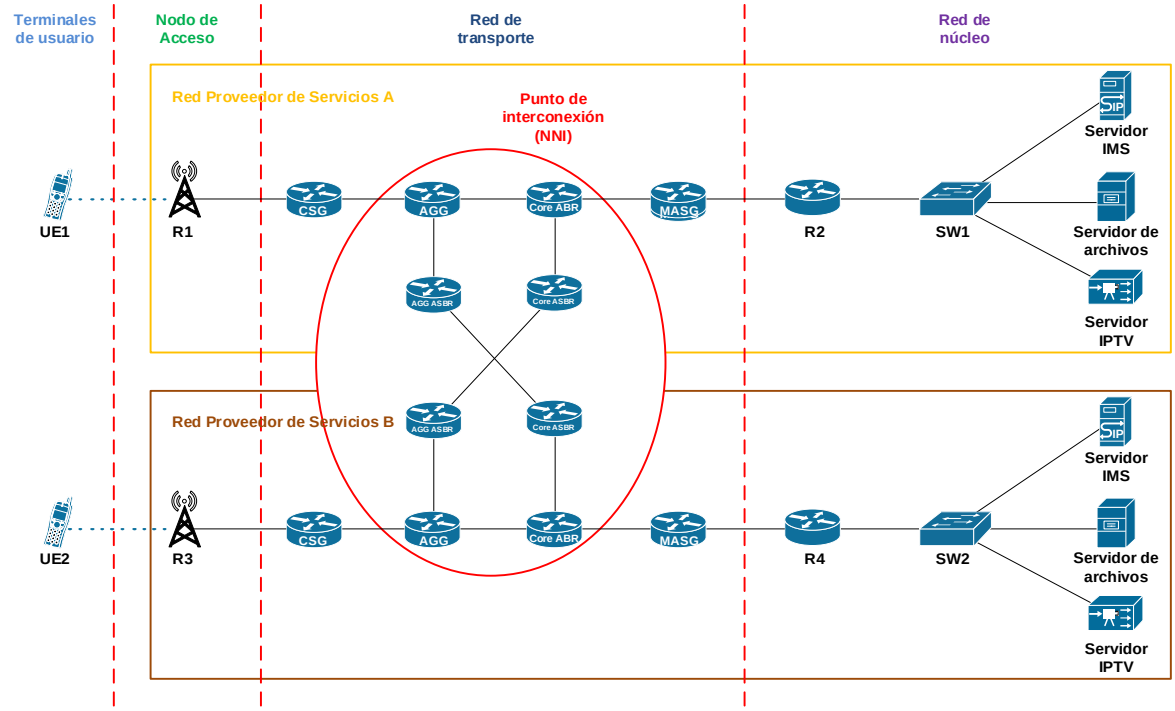


Figura 3-1 Diseño de red para la interconexión de redes IMS entre proveedores para la prestación de servicios interdominio

En la Figura 3-1 se plantea la interconexión de dos redes, entre los proveedores de servicio A y B, cada uno de ellos cuenta con un nodo de acceso (que puede ser un eNodeB o un gNodeB, para una red 4G o 5G respectivamente), el cual brinda conectividad a los UE que deseen conectarse a la red. Estos nodos de acceso deben brindar conectividad IP a los UE, por lo que, para efectos de las pruebas, se emularan mediante un router de acceso. El direccionamiento IP de los UE se asignará de forma dinámica mediante DHCP configurado en estos nodos.

En cuanto a la red de transporte, cada ISP cuenta con una red seamless MPLS intra-AS, como se observó en la sección 2.6, los nodos P de la arquitectura MPLS se pueden omitir para efectos de las pruebas. En un escenario real puede haber tantos nodos P como equipos se requieran para lograr la cobertura necesaria. De igual manera puede darse conectividad redundante entre todos los nodos de la red para garantizar la disponibilidad acordada en los SLA con los clientes. Cabe resaltar que se pueden implementar diferentes tecnologías en los router o switches multicapa para el manejo de enlaces redundantes, tales como HSRP (Hot Standby Router Protocol) o Etherchannel respectivamente en caso de que el ISP decida utilizar una configuración en malla. En la red de transporte se deberán configurar las políticas de QoS necesarias para garantizar la priorización del tráfico generado por los UE.

Para la red de núcleo de cada ISP se tiene en cuenta un servidor IMS, que provee el control de la señalización SIP para el establecimiento, mantenimiento y finalización de las sesiones de voz (llamadas) entre los UE. En este servidor se implementan las entidades P/I/S-CSCF y HSS del core IMS de forma virtualizada en un mismo equipo, como se observa en el procedimiento detallado en el Anexo: Configuración del servidor SIP Kamailio IMS. Los UE a su vez, deben conectarse entre sí mediante ENUM, por lo que debe haber un servidor DNS soportando el core IMS de acuerdo con lo observado en la Figura 1-4.

El servidor de IPTV se debe implementar de tal manera que brinde servicios de streaming en tiempo real a través de una multicast RTP, por lo que la red de transporte deberá soportar el enrutamiento multicast sobre una VPN MPLS. A su vez, el servidor estará en la capacidad de ofrecer el servicio de VoD y en directo mediante el protocolo RTSP (Real Time Streaming Protocol). El servidor de IPTV está limitado, debido a que no es un servidor de aplicaciones o proxy que soporte el protocolo SIP para iniciar/mantener y finalizar una sesión de video, el cual se utilizaría en un contexto real. Sin embargo, la plataforma es utilizada de forma comercial en contextos empresariales para la prestación de servicios reales.

El tráfico de datos se debe evaluar mediante la implementación de un servidor FTP o SSH, que almacene archivos a transferir hacia los UE que lo requieran. Mediante una prueba de

velocidad se podrá establecer la velocidad de subida y bajada desde los UE hacia este servidor.

3.2 Conectividad de extremo a extremo

Como se observó en la sección 2.5.1, en las redes MPLS se pueden configurar VPN de capa 2 o 3 para garantizar la conectividad entre los UE y los servidores de aplicaciones. Para el escenario planteado en la Figura 3-1 se tienen los siguientes casos de conectividad independientemente del tipo de VPN configurada.

3.2.1 Conectividad VPN intra-AS seamless MPLS en interconexión

En el caso de que los UE deseen consumir servicios intradominio, se tiene la conexión VPN para cada UE según lo observado en la Figura 3-2.

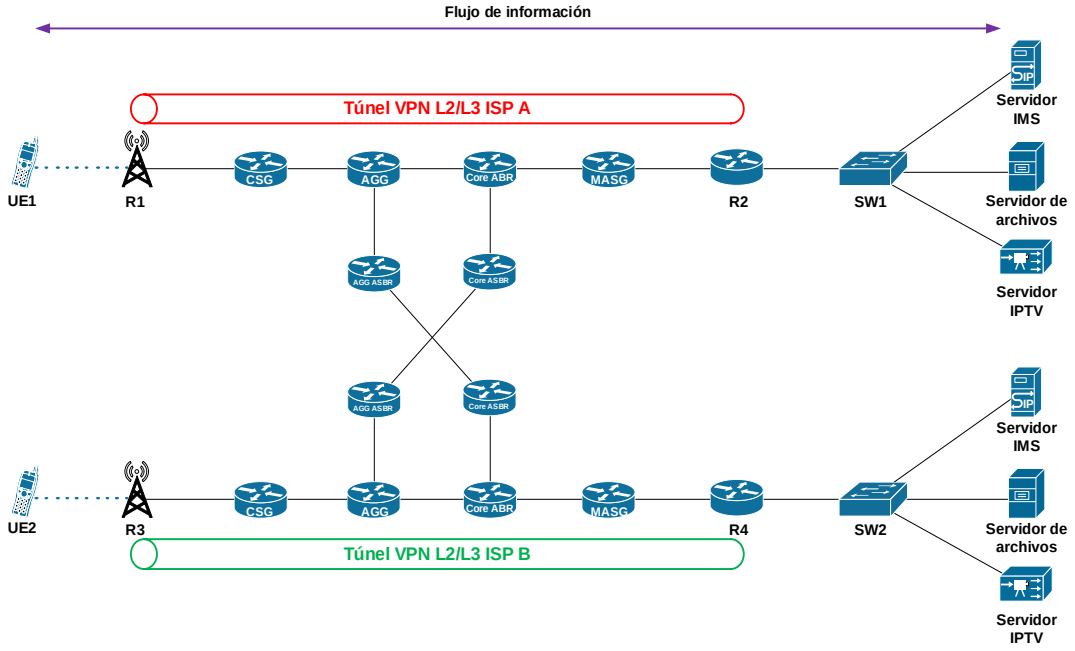


Figura 3-2 Conectividad VPN intra-AS seamless MPLS en interconexión

3.2.2 Conectividad VPN inter-AS seamless MPLS en interconexión

En el caso de que los UE deseen consumir servicios interdominio, se tiene la conexión VPN para cada UE de acuerdo con la Figura 3-3.

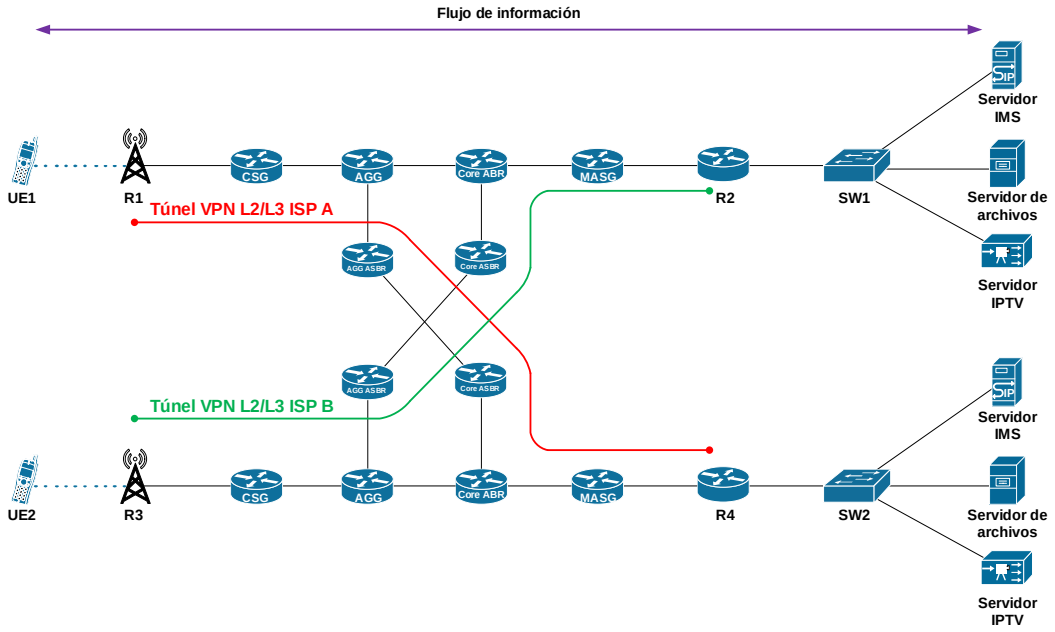


Figura 3-3 Conectividad VPN inter-AS seamless MPLS en interconexión

Para que los UE puedan consumir servicios de voz interdominio, los servidores IMS deben tener configurado el soporte de itinerancia (roaming) en el HSS. Los servicios de video (IPTV) y datos, solo dependen de la conectividad IP entre los UE y los servidores de aplicaciones [114].

3.3 Análisis del diseño propuesto

Al analizar el diseño planteado en la Figura 3-1, se observa que la topología resultante es la que se describe en la Figura 2-22 Intra-AS seamless MPLS [96], con los routers correspondientes a la topología inter-AS seamless MPLS, desde el punto de vista de un UE que quiera acceder a un servicio para el LSP correspondiente a su propio operador. En caso contrario, la topología resultante será la que se describe en la Figura 2-23 Inter-AS seamless MPLS [96], en la que los UE acceden a los servicios que provee un operador externo.

Por otro lado. Tomando como referencia lo observado en [103] y en la sección 2.5.1, el problema de la QoS en MPLS no radica principalmente en la cantidad de routers que se tengan conectados, pues a mayor cantidad de equipos en un LSP mayor es el procesamiento que se debe hacer respecto del enrutamiento de los paquetes (debido al

análisis de la tabla de enrutamiento) y análisis de las etiquetas MPLS, y en consecuencia el retardo generado por estos nodos es mayor.

La principal diferencia de la conectividad VPN entre la configuración intra-AS de la configuración inter-AS seamless MPLS, radica en la sección que configura el protocolo e-BGP entre los equipos de borde AGG ASBR y Core ASBR de los ISP, dado que debido al análisis que deben realizar estos nodos para enrutar los paquetes entre los sistemas autónomos de ambos ISP, generan un retardo adicional por lo visto en la ecuación (1-1) y (1-2) en los parámetros de retardo y variación del retardo. En consecuencia, para efectos de la evaluación de los parámetros de QoS en interconexión, se realizará la evaluación y validación de los parámetros de QoS comparando la conectividad entre L2VPN y L3VPN para los servicios de voz, datos y video, a través de la implementación del diseño de interconexión ilustrado en la Figura 3-4.

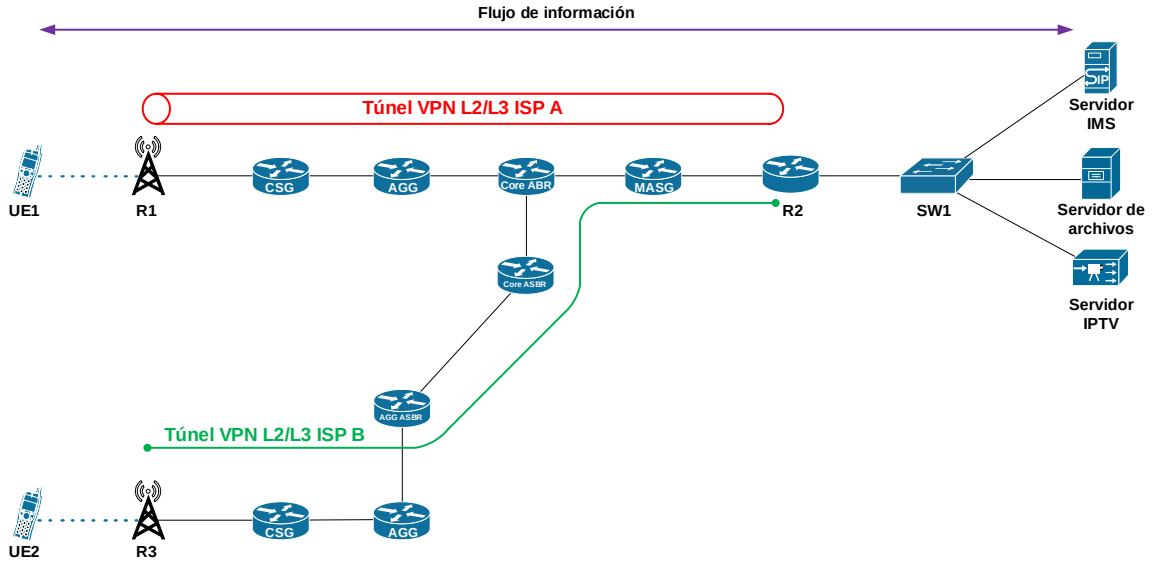


Figura 3-4 Diseño de interconexión propuesto a emular

3.4 Caracterización del tráfico de la red

La red propuesta debe transportar el tráfico de voz (Señalización SIP y transporte de RTP), datos (SSH, HTTP, DNS, DHCP) y video (video en streaming RTP/RTSP), así como el tráfico de control de la red, que contempla los protocolos de enrutamiento OSPF y BGP. La Tabla 3-1 presenta el tráfico identificado, con los detalles expuestos en el anexo A [106].

Tabla 3-1 Caracterización del tráfico de la red

Tipo de trafico	RFC 4594 DSCP	PHB	Latencia (ms)	Jitter (ms)	Pérdida de paquetes	Notas
Control de red	CS6	Reserva BW	No importa	No importa	Mínima	Protocolos de enrutamiento (OSP, BGP) y otro tráfico que mantiene unida a la red
Señalización	CS5	Reserva BW	No importa	No importa	Mínima	Señalización interactiva de voz (SIP) / video (configuración de llamadas, reenvío, etc.)
OAM	CS2	Reserva BW	No importa	No importa	Mínima	Operaciones de red: SSH
Voz	EF	Baja-latencia/prioridad	< 150	< 30	< 1%	Tráfico RTP y RTCP, muy sensible a la latencia, la fluctuación y la pérdida
Transmisión de video	CS3	LL/prioridad (posible)	No importa	No importa	< 0.1%	Normalmente tiene almacenamiento en búfer a nivel de aplicación. Incluye transmisiones de video en vivo, IPTV, CCTV
Mejor esfuerzo	CS0 / DF	DF + reserva BW (posible)	No importa	No importa	No importa	La mayoría de las aplicaciones encajan aquí, cualquier cosa no clasificada

3.5 Implementación de escenarios en el entorno emulado

Con el objetivo de evaluar los parámetros de QoS correspondientes al ancho de banda, retardo, jitter y pérdida de paquetes en el tráfico de servicios de voz, datos y video, se plantea establecer como línea base de comparación entre escenarios las topologías sin políticas de QoS, para luego aplicar las políticas de QoS y comparar los resultados en los servicios mencionados aplicados al diseño de la Figura 3-4. La Tabla 3-2 muestra las herramientas de emulación seleccionadas para la implementación de los escenarios planteados.

Tabla 3-2 Herramientas de emulación seleccionadas

Función	Herramienta	Versión
Virtualización	VMWare Workstation / QEMU	16.0.0 / 2.12.0
Emulador de red	PNetLab	4.2.8
Entornos de núcleo IMS	Kamailio IMS Core / FOKUS HSS (FHoSS)	4.3 / Rev. 1198
Servidor IPTV	Wowza Streaming Engine	4.8.0
Tecnologías de contenedores	Docker	19.03.6
Monitores de tráfico SIP	HOMER SIP Capture	7.7
Softphone	Zoiper	3.3.25608 64 bit
Herramientas de medición de tráfico de red	Wireshark / iPerf3	3.2.7 / 3.1.3

La Tabla 3-3 muestra las especificaciones técnicas del equipo de trabajo en el que se ejecuta el entorno emulado con las herramientas seleccionadas en la Tabla 3-2.

Tabla 3-3 Especificaciones del equipo de trabajo

Característica	Descripción
Procesador	Intel(R) Core (TM) i5-2400 CPU @ 3.10GHz 3.30 GHz
RAM instalada	24,0 GB
Tipo de sistema	Sistema operativo de 64 bits, procesador x64
S.O.	Windows 10
Versión	20H2
Compilación	19042.630

La Tabla 3-4 muestra las características técnicas de la máquina virtual para el entorno en PNetLab en la que se implementan los escenarios planteados.

Tabla 3-4 Características técnicas de la máquina virtual PNetLab

Característica	Descripción
Memoria RAM	12 GB
Procesadores	4
Disco duro	100 GB
S.O.	Windows 10
Adaptador de red 0	Bridge
Adaptador de red 1	Bridge

Los escenarios implementan imágenes de routers Cisco IOL (IOS on Linux) de capa 3, de nombre i86bi_LinuxL3-AdvEnterpriseK9-M2_157_3_May_2018.bin, con las siguientes características técnicas en su versión:

```
Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M),
Version 15.7(3)M2, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 28-Mar-18 11:18 by prod_rel_team

Linux Unix (Intel-x86) processor with 863257K bytes of memory.
Processor board ID 67270657
4 Ethernet interfaces
1024K bytes of NVRAM.
```

La Figura 3-5 muestra la topología de red para L2VPN implementada en PNetLab de acuerdo con los comandos descritos en el Anexo B.

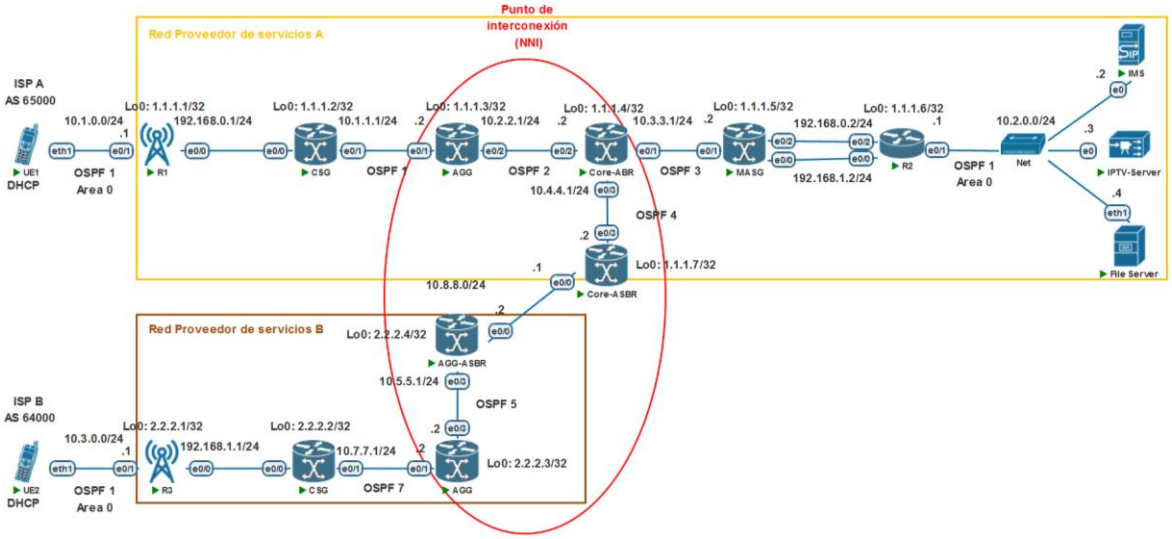


Figura 3-5 Topología de red para L2VPN

La Figura 3-6 muestra la topología de red para L3VPN implementada en PNetLab de acuerdo con los comandos descritos en el Anexo C.

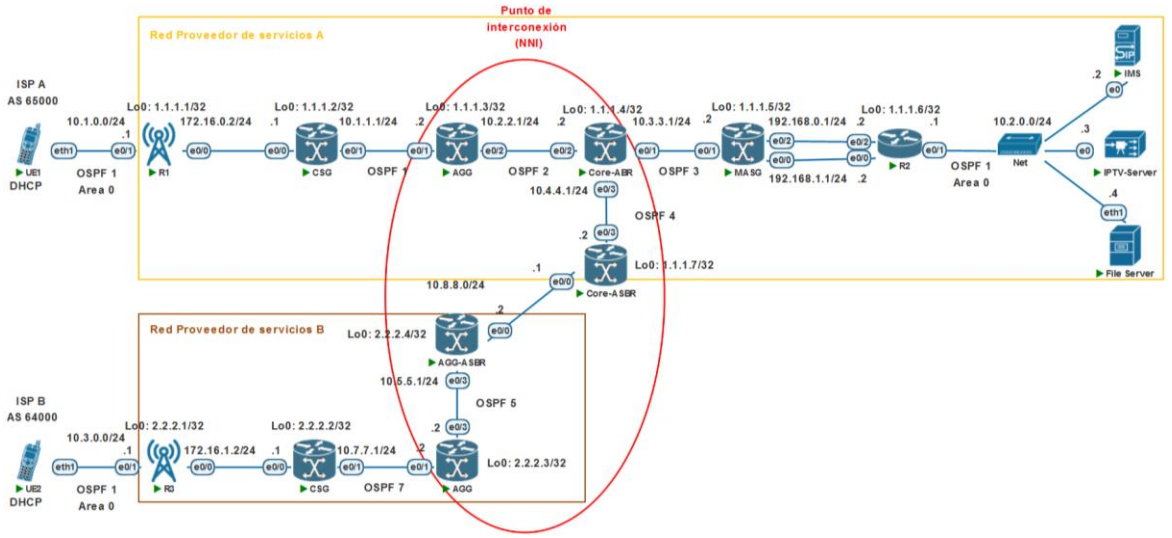


Figura 3-6 Topología de red para L3VPN

El core IMS se encuentra virtualizado en una imagen QEMU como un servidor dentro de PNetLab con las siguientes características técnicas descritas en la Tabla 3-5.

Tabla 3-5 Características técnicas del core IMS en QEMU

Característica	Descripción
Memoria RAM	4096 MB

Característica	Descripción
Procesadores	4
Disco duro	20 GB
S.O.	Ubuntu Server 20.04
Adaptador de red	Ethernet
Consola primaria	Telnet
Consola secundaria	VNC

La implementación del core IMS en Kamailio y el HSS de Fokus utilizan la siguiente distribución de sockets IP, descrita en la Tabla 3-6.

Tabla 3-6 Distribución de sockets IP del core IMS en Kamailio

Elemento	Socket
P-CSCF	10.2.0.3:5060
I-CSCF	10.2.0.3:4060
S-CSCF	10.2.0.3:6060
HSS	10.2.0.3:8080

La Figura 3-7 describe el core IMS en Kamailio y el HSS emulado, en QEMU para todos los escenarios planteados de acuerdo con los comandos descritos en el Anexo D.

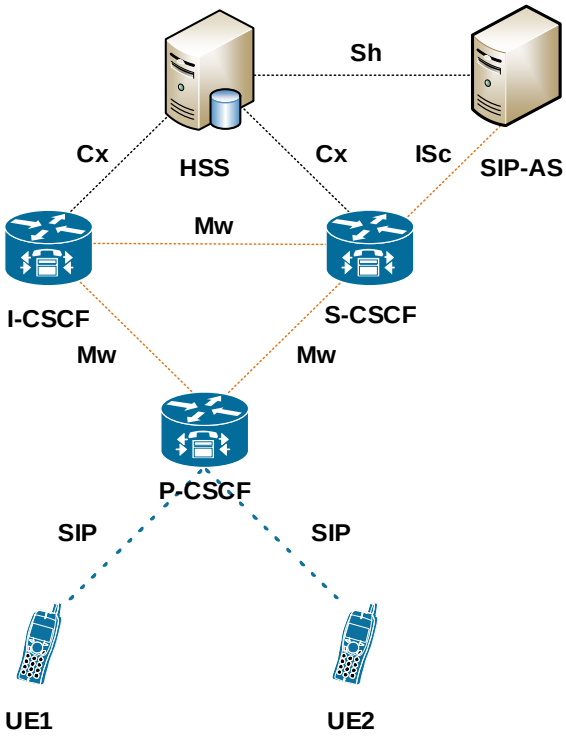


Figura 3-7 Core IMS en Kamailio emulado en QEMU

La Tabla 3-7 describe los usuarios creados en el HSS para los UE correspondientes.

Tabla 3-7 Usuarios creados en el HSS para los UE correspondientes

Nombre	Identidad pública	Identidad privada	Contraseña	SIP URI	TEL URI	UE
Alice	sip:alice@ims.isp1.test	alice@ims.isp1.test	alice	alice	+1000	UE1
Bob	sip:bob@ims.isp1.test	bob@ims.isp1.test	bob	bob	+1001	UE2
Eve	sip:eve@ims.isp1.test	eve@ims.isp1.test	eve	eve	+1002	UE1

La Figura 3-8 muestra la configuración realizada en el HSS de Fokus para el usuario Alice, de acuerdo con los parámetros descritos en la Tabla 3-7. Los parámetros SIP URI y TEL URI, hacen parte de la configuración de ENUM en el DNS del core IMS.

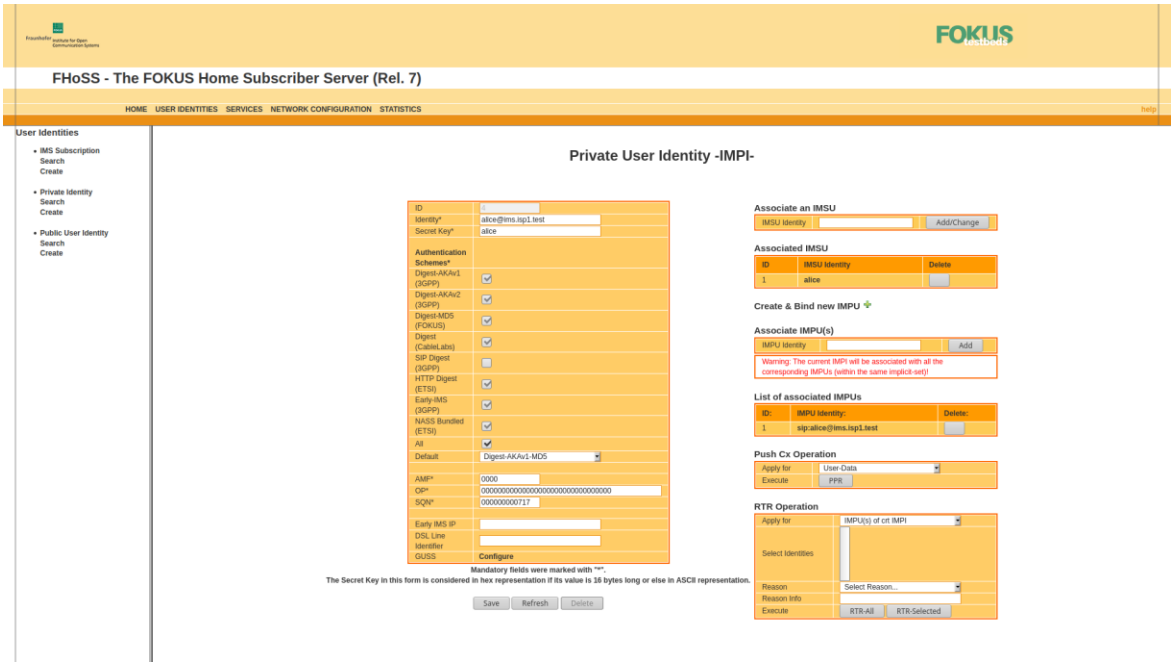


Figura 3-8 Configuración de usuarios en el HSS de Fokus

La Figura 3-9 muestra la configuración de los UE realizada en Zoiper de acuerdo con los parámetros descritos en la Tabla 3-7.

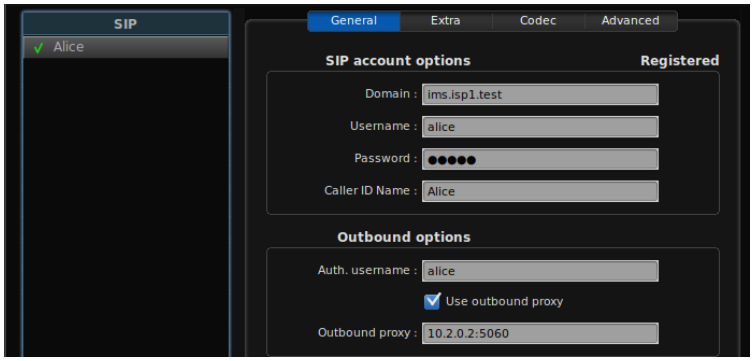


Figura 3-9 Configuración de UE en Zoiper

En la Figura 3-10, se observa que para el servicio de IPTV, se crea un canal de streaming en vivo en Wowza Streaming Engine con la dirección rtsp://10.2.0.3:1935/live/001.stream, con un throughput de red de entrada de 748.820 Kbps y de 812.540 Kbps.

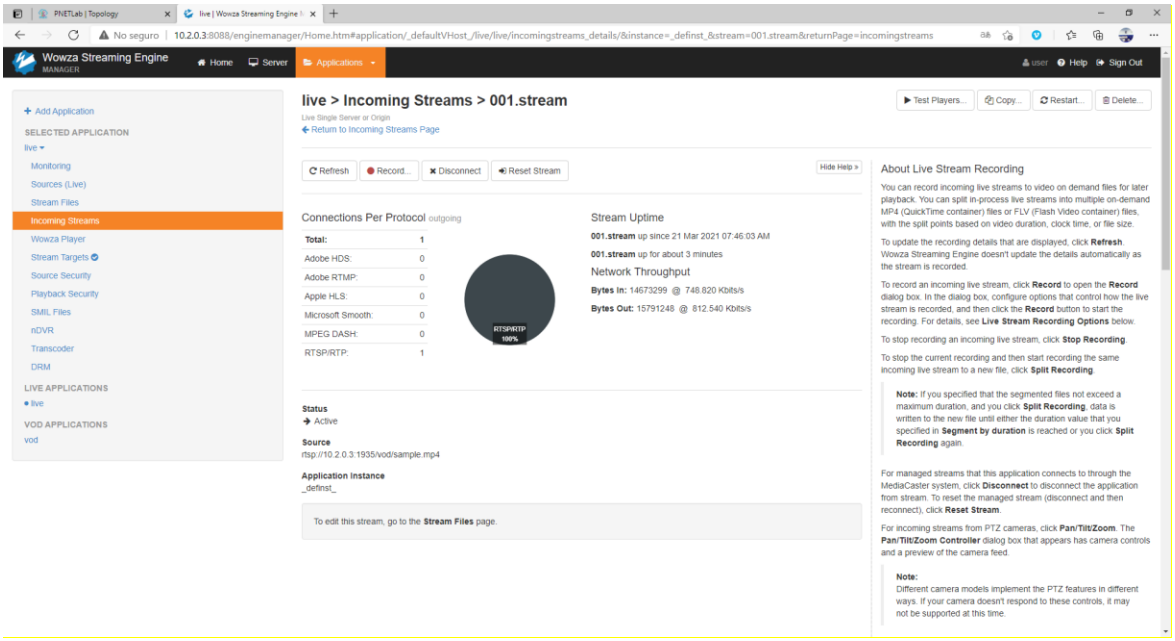


Figura 3-10 Canal de streaming en IPTV creado en Wowza Streaming Server

En la Figura 3-11 se observan las características de los códecs de audio y video del canal de streaming IPTV, así como la resolución y tasa de cuadros por segundo en Wowza Streaming Engine.

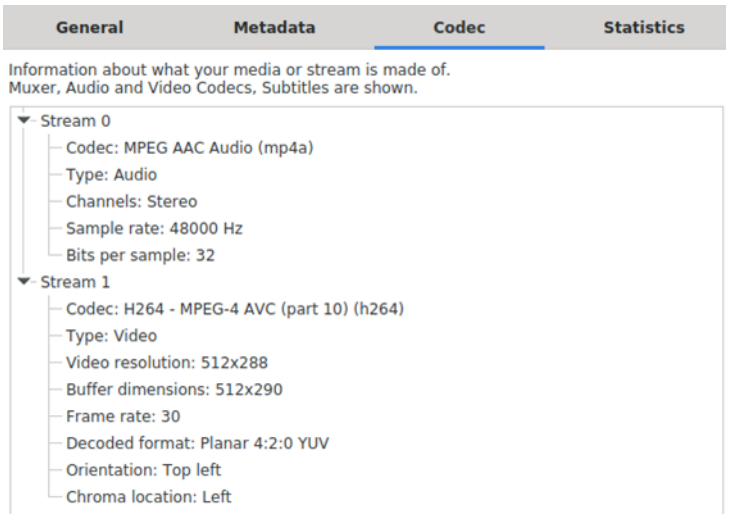


Figura 3-11 Detalles de los códecs de audio y video utilizados por el canal de streaming IPTV en Wowza Streaming Engine

3.6 Metodología de evaluación de parámetros de QoS para la conectividad intra-AS e inter-AS seamless MPLS L2VPN y L3VPN

Para la realización de las pruebas de evaluación de parámetros de QoS de extremo a extremo, correspondientes al retardo, el jitter, la pérdida de paquetes y el ancho de banda de la conectividad de los enlaces intra-AS e inter-AS seamless MPLS L2VPN y L3VPN, se propone el uso de las siguientes herramientas en el entorno Linux Ubuntu para los UE y los servidores de voz, datos y video [115].

- El retardo se evaluará en función del tiempo de ida y vuelta (Round Trip Time, RTT) mediante el comando ping, y los saltos de red con la herramienta traceroute.
- El ancho de banda se evaluará con la herramienta iperf3, con pruebas mediante el protocolo TCP. Esta prueba se validará con una prueba de descarga de un archivo de 1GB mediante el comando scp, donde se espera contrastar el valor de la tasa de transferencia (ancho de banda) de iperf3 con el de la descarga. El archivo se crea en el servidor de archivos mediante el comando:

```
fallocate -l 1G large.test
```

- El jitter y la pérdida de paquetes se evaluarán con la herramienta iPerf3, con pruebas mediante el protocolo UDP.

- Las pruebas en iPerf 3 se ejecutarán durante 60 segundos. La Tabla 3-8 muestra los parámetros configurados tanto en el lado del cliente (para el UE correspondiente), como en el lado del servidor, tomando como referencia los parámetros descritos en [116].

Tabla 3-8 Comandos para pruebas de medición en iPerf3

Elemento	Comandos UDP	Comandos TCP
Servidor	iperf3 -s -p 5101	iperf3 -s -p 5101
Cliente	iperf3 -c 10.2.0.4 -u -t 60 -b Límite de ancho de banda en Mbps -p 5101 -i 1	iperf3 -c 10.2.0.4 -t 60 -b 0 -p 5101 -i 1

- Para las pruebas del servicio de voz se utilizará la herramienta Wireshark para visualizar la señalización SIP en el registro y el establecimiento de la llamada entre los usuarios, y para la visualización de los valores de jitter de los canales de envío y retorno en la llamada. Por otro lado, se utilizará la herramienta Homer SIP Capture para visualizar los valores de la pérdida de paquetes, el jitter total de la llamada y el MOS (Mean Opinion Score) que pertenece a la QoE.
- En cuanto al video, se utilizará la herramienta VLC para evaluar el audio y el video reproducido en los UE según las métricas medidas en los puntos anteriores.

Siguiendo el diseño planteado en la Figura 3-4, se procede a implementar las topologías para las L2VPN en la Figura 3-5 y L3VPN en la Figura 3-6 en los siguientes escenarios:

- Conectividad intra-AS e inter-AS seamless MPLS L2VPN sin QoS.
- Conectividad intra-AS e inter-AS seamless MPLS L3VPN sin QoS.
- Conectividad intra-AS e inter-AS seamless MPLS L2VPN con QoS.
- Conectividad intra-AS e inter-AS seamless MPLS L3VPN con QoS.

3.7 Evaluación de la conectividad intra-AS e inter-AS seamless MPLS L2VPN sin QoS

Con el objetivo de evaluar la conectividad intra-AS e inter-AS seamless MPLS L2VPN sin QoS en la topología de red planteada en la Figura 3-5 Topología de red para L2VPN, se proceden a realizar pruebas de conectividad mediante la herramienta ping con el fin de establecer los tiempos de retardo de ida y vuelta, pruebas de saltos de red mediante la herramienta traceroute y medición de los parámetros de QoS con las herramientas iPerf3 y Wireshark de acuerdo con las características de los tipos de tráfico en la sección 2.8.

3.7.1 Conectividad L2VPN intra-AS sin QoS

Para evaluar la conectividad intra-AS seamless MPLS L2VPN, se ejecuta el comando ping en el UE1 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=62 time=2.96 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=62 time=4.64 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=62 time=3.50 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=62 time=3.87 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=62 time=3.02 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=62 time=4.25 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=62 time=3.39 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=62 time=3.86 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=62 time=4.06 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=62 time=4.08 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 2.955/3.762/4.642/0.513 ms
root@vm:/home/user#
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9017ms, con un RTT promedio de 3.762ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE1 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.1.0.1)  1.114 ms  1.041 ms  0.973 ms
 2  192.168.0.2 (192.168.0.2)  3.904 ms  5.298 ms  5.589 ms
 3  10.2.0.4 (10.2.0.4)  5.151 ms  5.491 ms  6.475 ms
```

Con la respuesta anterior se observan tres saltos de red desde el origen en la red del UE1, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-9 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-9 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE1)	0.00-60.00	165	23.1
Servidor de archivos	0.00-60.01	165	23.1

Los resultados muestran que el enlace intra-AS seamless MPLS L2VPN sin QoS tiene un ancho de banda de 23.1Mbps que equivalen a 2.88MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user/Descargas# scp
root@10.2.0.4:/home/admin/Downloads/large.test /home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   3.5MB/s   04:54
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 3.5MB/s o 28Mbps en un tiempo de 04:54min. Para efectos de cálculo se tomará la tasa de 3.5MB/s para encontrar los valores de jitter y pérdida de paquetes en iPerf3. La Tabla 3-10 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 3.5MB/s, equivalente a 28Mbps en iPerf3.

Tabla 3-10 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	200	28.0	0.000	0/145027 (0%)
Servidor de archivos	0.00-60.01	193	27.0	0.442	4930/145024 (3.4%)

Las pruebas realizadas muestran que para un ancho de banda de 3.5MBps o 28Mbps, se tiene un jitter de 0.442ms y unas pérdidas de paquetes del 3.4%.

La Figura 3-12 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad intra-AS seamless MPLS L2VPN sin QoS, donde se puede observar un tiempo de registro de 0.308327312s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

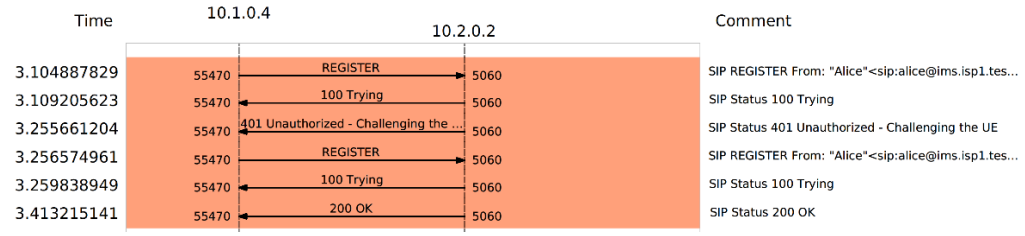


Figura 3-12 Registro SIP UE con conectividad intra-AS seamless MPLS L2VPN sin QoS

La Figura 3-13, muestra los detalles de la llamada entre usuarios SIP, de Alice a Eve, con conectividad intra-AS seamless MPLS L2VPN sin QoS, con un total de 35 paquetes generados y una duración de 33s.

Start Time	Stop Time	Initial Speaker	From	To	Protocolo	Duration	Paquetes	State	Comments
0.000000	33.750058	10.1.0.4	"Alice"<sip:alice@ims.isp1.test;transport=UDP>	<sip:eve@ims.isp1.test;transport=UDP>	SIP	00:00:33	35	COMPLETED	INVITE 200

Figura 3-13 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS

La Figura 3-14 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad intra-AS seamless MPLS L2VPN sin QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Eve y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Eve, de 3.253593s. La llamada tiene una duración efectiva de 30.477445s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Eve, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Eve, lo que da una duración total de la llamada de 30.496465s que se valida por la Figura 3-13.

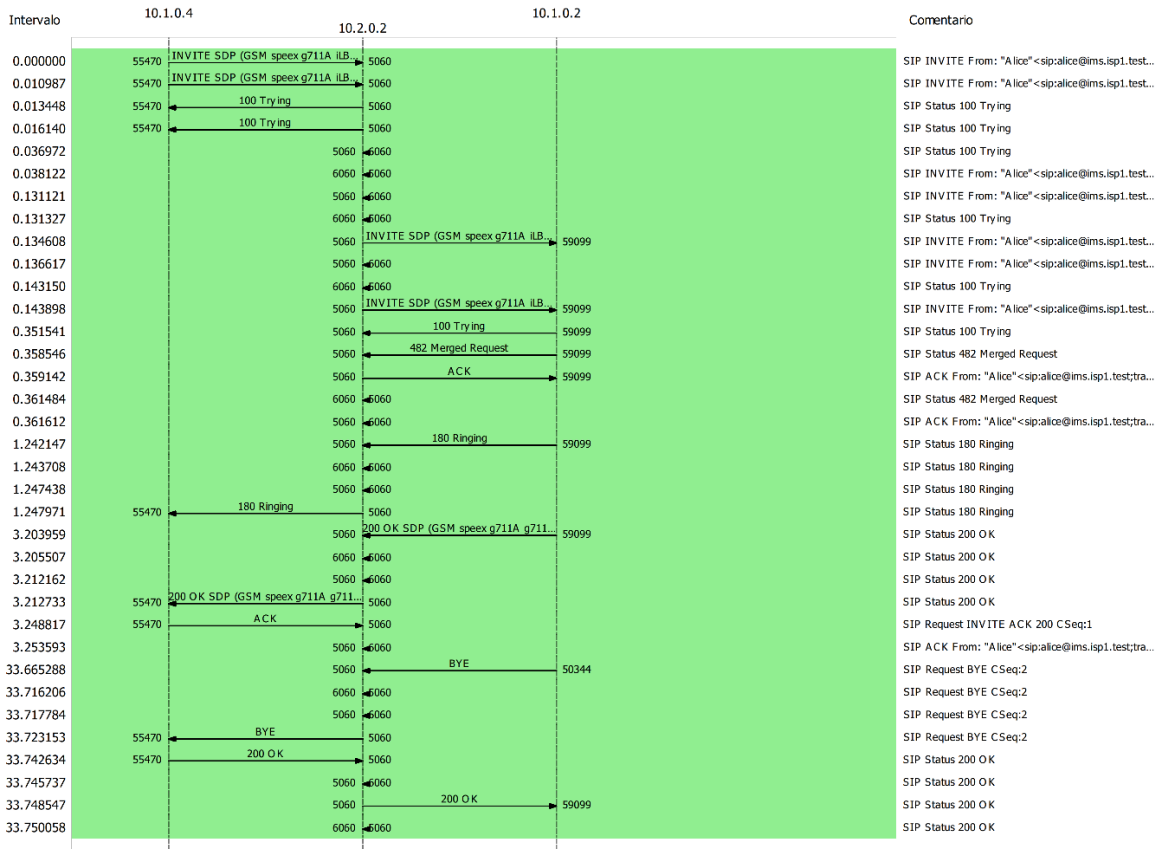


Figura 3-14 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS

La Figura 3-15 muestra la evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 848.88 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 74.58ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.26 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-15 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN sin QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-16 se realiza una conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine.

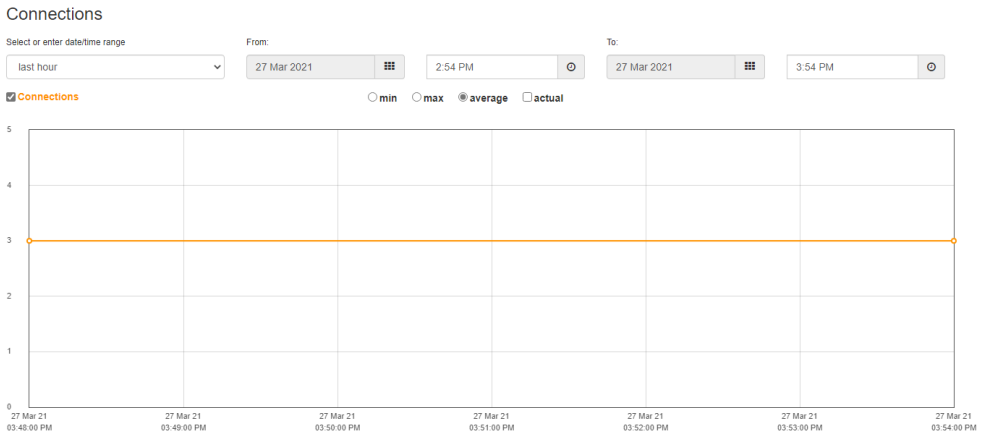


Figura 3-16 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine

En la Figura 3-17 se observa un promedio de ancho de banda utilizado de 4.090Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

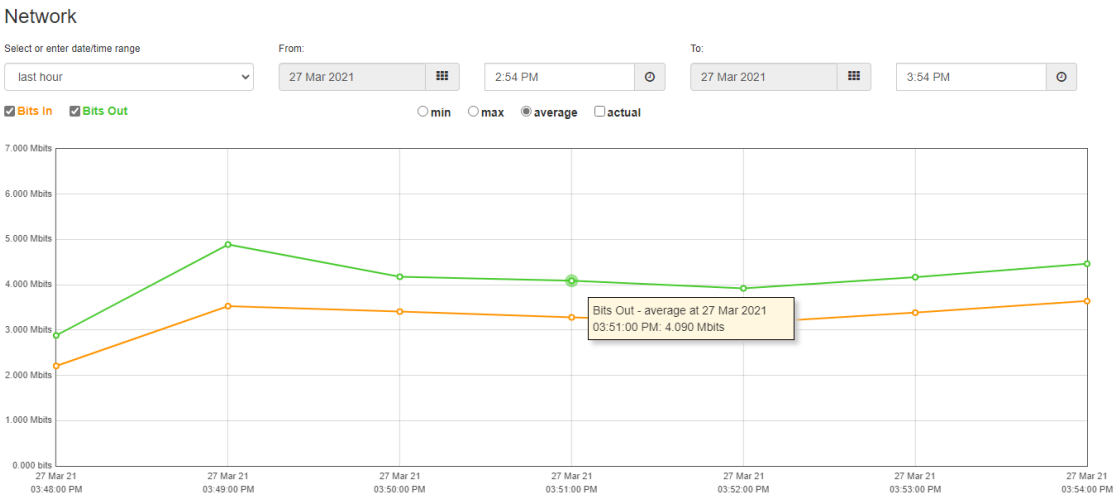


Figura 3-17 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine

En la Figura 3-18, se observa que en el video reproducido en el UE se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen y sonido entrecortado.

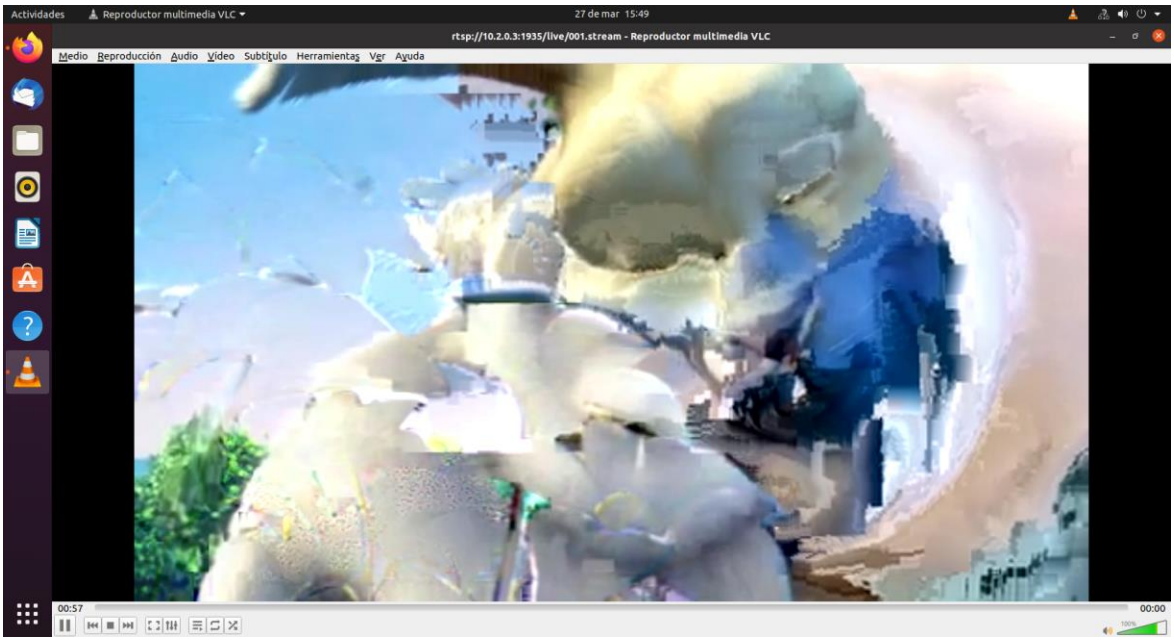


Figura 3-18 Pérdidas de cuadros del video, congelamiento de imagen y sonido entrecortado del servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine

3.7.2 Conectividad L2VPN inter-AS sin QoS

Para evaluar la conectividad inter-AS seamless MPLS L2VPN, se ejecuta el comando ping en el UE2 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=62 time=4.00 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=62 time=5.77 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=62 time=5.14 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=62 time=5.64 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=62 time=5.75 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=62 time=5.99 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=62 time=6.63 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=62 time=5.86 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=62 time=5.59 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=62 time=5.64 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 4.003/5.600/6.632/0.639 ms
root@vm:/home/user#
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9018ms, con un RTT promedio de 5.600ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE2 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.3.0.1)  2.035 ms  0.850 ms  2.776 ms
 2  192.168.1.2 (192.168.1.2)  8.479 ms  8.078 ms  8.366 ms
 3  10.2.0.4 (10.2.0.4)  6.572 ms  6.626 ms  6.912 ms
```

Con la respuesta anterior se observan tres saltos de red desde el origen en la red del UE2, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-11 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-11 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE2)	0.00-60.00	145	20.3
Servidor de archivos	0.00-60.00	145	20.3

Los resultados muestran que el enlace inter-AS seamless MPLS L2VPN sin QoS tiene un ancho de banda de 20.3Mbps que equivalen a 2.53MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user# scp root@10.2.0.4:/home/admin/Downloads/large.test
/home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   2.5MB/s   06:43
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 2.5MB/s o 20Mbps en un tiempo de 06:43min. Para comparar con el escenario de conectividad L2VPN intra-AS sin QoS, se tomará la tasa de 3.5MB/s o 28Mbps para encontrar los valores de jitter y pérdida de paquetes en iPerf3. La Tabla 3-12 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 3.5MB/s, equivalente a 28Mbps en iPerf3.

Tabla 3-12 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	200	28.0	0.000	0/145026 (0%)
Servidor de archivos	0.00-60.00	161	22.5	0.543	28625/145023 (20%)

Las pruebas realizadas muestran que para un ancho de banda de 3.5MBps o 28Mbps, se tiene un jitter de 0.780ms y unas pérdidas de paquetes del 20%.

La Figura 3-19 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad inter-AS seamless MPLS L2VPN sin QoS, donde se puede observar un tiempo de registro de 0.785073386s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

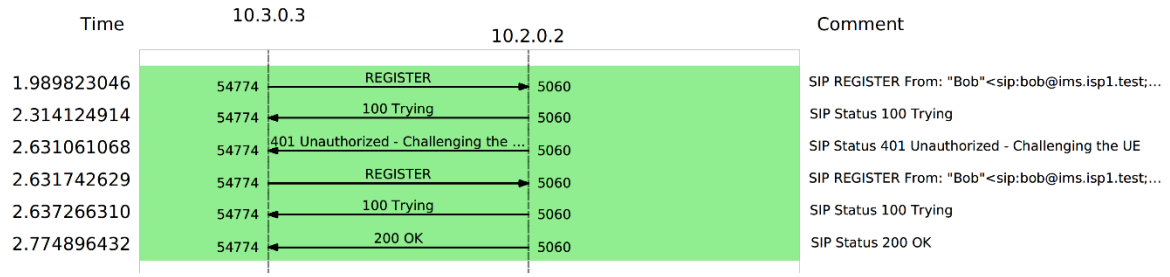
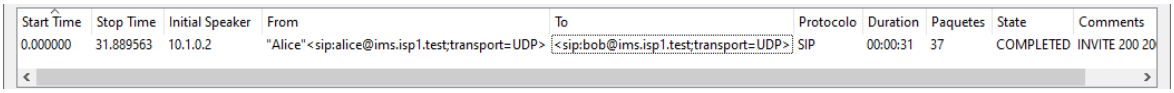


Figura 3-19 Registro SIP UE con conectividad inter-AS seamless MPLS L2VPN sin QoS

La Figura 3-20, muestra los detalles de la llamada entre usuarios SIP, de Alice a Bob, con conectividad inter-AS seamless MPLS L2VPN sin QoS, con un total de 37 paquetes generados y una duración de 31s.



Start Time	Stop Time	Initial Speaker	From	To	Protocolo	Duration	Paquetes	State	Comments
0.000000	31.889563	10.1.0.2	"Alice"<sip:alice@ims.isp1.test;transport=UDP>	<sip:bob@ims.isp1.test;transport=UDP>	SIP	00:00:31	37	COMPLETED	INVITE 200 20

Figura 3-20 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS

La Figura 3-21 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad inter-AS seamless MPLS L2VPN sin QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Bob y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 1.807883s. La llamada tiene una duración efectiva de 30.059732s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 31.867615s que se valida por la Figura 3-20.

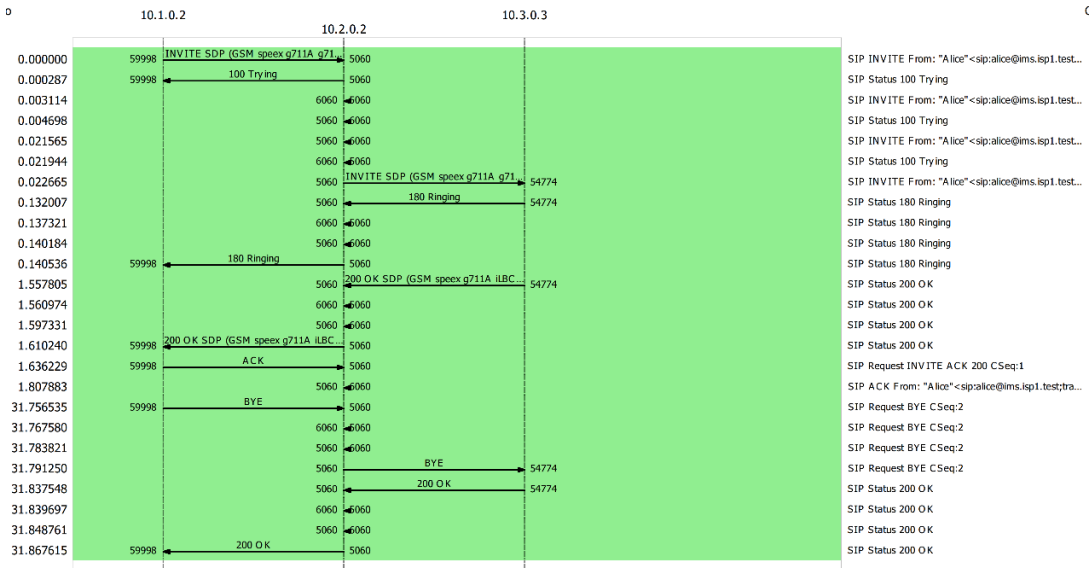


Figura 3-21 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS

La Figura 3-22 muestra la evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 877.9 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 70.6ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.27 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-22 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN sin QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-23 se realiza una conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine.

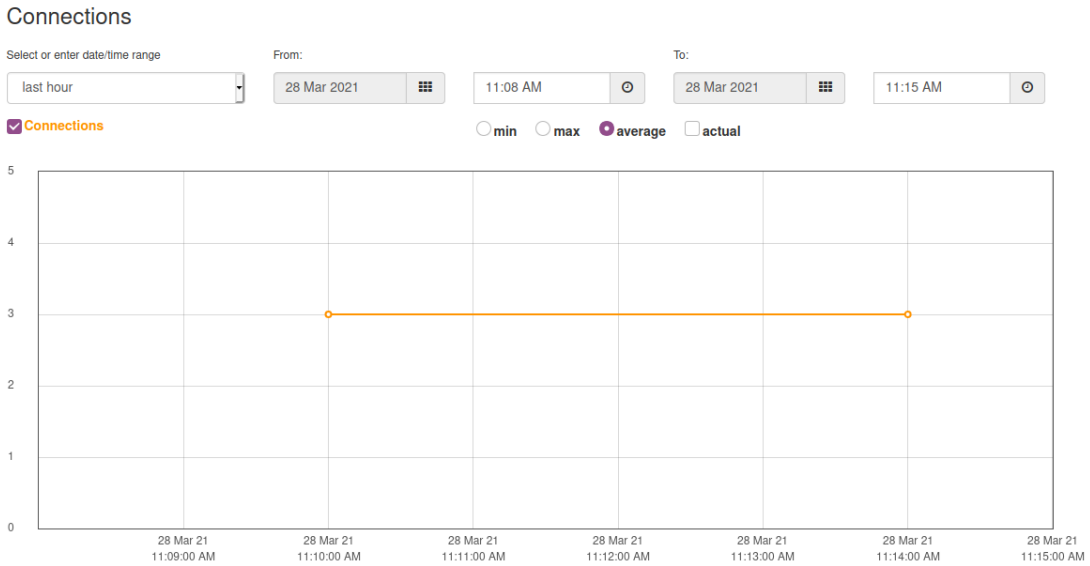


Figura 3-23 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

En la Figura 3-24 se observa un promedio de ancho de banda utilizado de 3.970Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

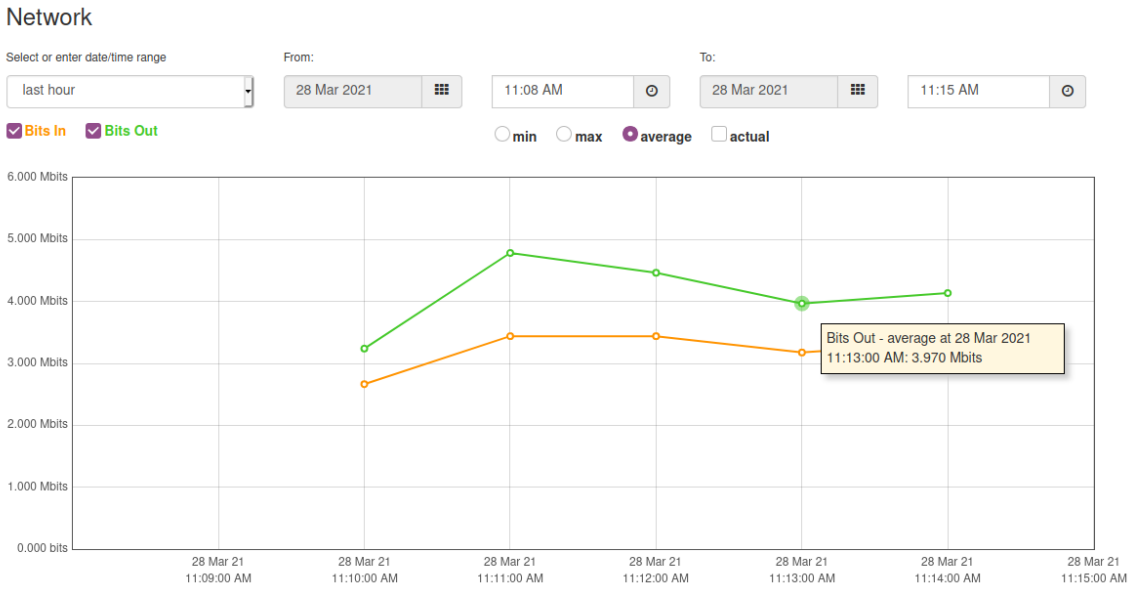


Figura 3-24 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine

En la Figura 3-25, se observa que en el video reproducido en el UE se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen y cortes en el sonido.

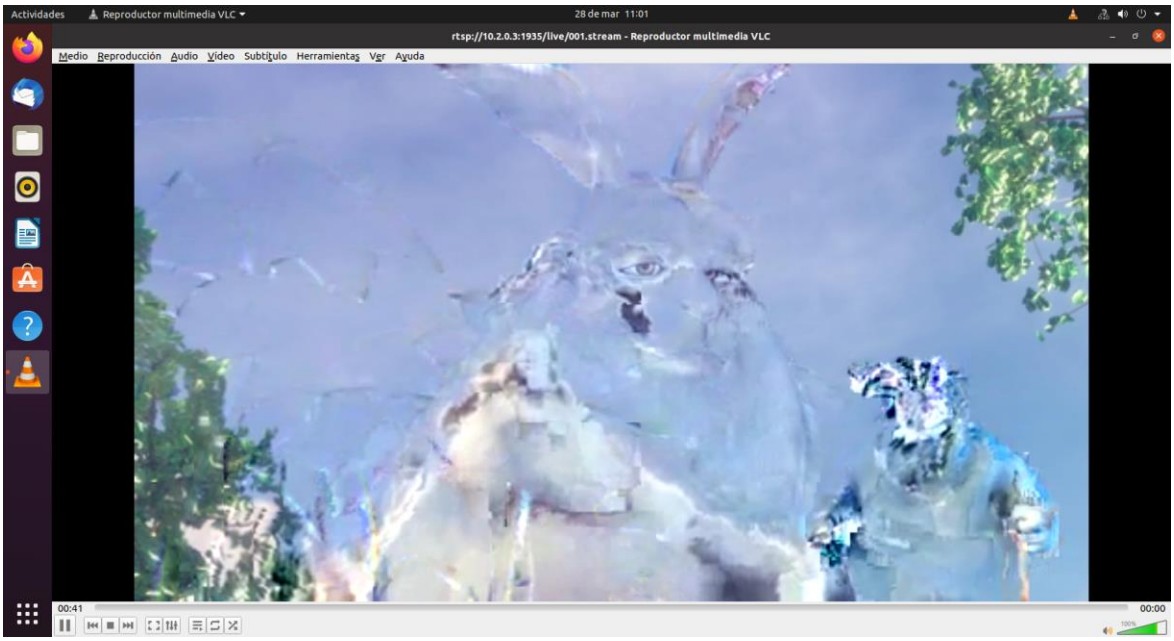


Figura 3-25 Pérdidas de cuadros, congelamiento en las imágenes y cortes en el sonido del servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN sin QoS en Wowza Streaming Engine

3.7.3 Análisis comparativo de los escenarios L2VPN intra-AS e inter-AS sin QoS

Los resultados obtenidos en las pruebas de conectividad mediante la herramienta ping, muestran que el escenario intra-AS presenta un mayor retardo de ida y vuelta (3.762ms) con respecto al escenario inter-AS (5.600ms).

Con las pruebas de saltos de red mediante la herramienta traceroute, se encuentra que el escenario intra-AS presenta la misma cantidad de saltos de red con respecto al escenario inter-AS (tres saltos).

Respecto al jitter, en las pruebas realizadas en iPerf3, se encuentra que en el escenario intra-AS se tiene un valor de 0.442ms y en el escenario inter-AS un valor de 0.780ms.

En relación con la pérdida de paquetes, se observa que en el escenario intra-AS, con una tasa de transferencia de 28Mbps desde el cliente, se obtuvo unas pérdidas del 3.4% y en

el escenario inter-AS se obtuvo unas pérdidas del 20%. Dado que la prueba de descarga en el escenario inter-AS mostro una tasa de transferencia de 20Mbps, para la línea base del diseño de las políticas de QoS se establece con un ancho de banda de 20 Mbps en CIR y de 28 Mbps en PIR en los escenarios de conectividad intra-AS e inter-AS seamless MPLS L2VPN.

Con respecto al servicio de voz, se observa que en conectividad intra-AS se tiene tiempo de registro en SIP de 0.308327312s, mientras que en la conectividad inter-AS L2VPN es de 0.785073386s. En el escenario intra-AS, el jitter promedio fue de 74.58ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.26 en el MOS y en el escenario inter-AS, el jitter promedio fue de 70.6ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.27 en el MOS.

Para el servicio de video en streaming en IPTV, se observa que tanto para la conectividad intra-AS como inter-AS se tienen problemas de pérdida de imágenes y congelamiento en el video, siendo mayor el problema en la conectividad inter-AS al presentar cortes en el sonido para ambos casos. Se observa una utilización de ancho de banda de 4.090Mbps en promedio para la conectividad intra-AS y de 3.970Mbps para la conectividad inter-AS utilizando el códec de video MPEG-4.

3.8 Evaluación de la conectividad intra-AS e inter-AS seamless MPLS L3VPN sin QoS

Con el objetivo de evaluar la conectividad intra-AS e inter-AS seamless MPLS L2VPN sin QoS en la topología de red planteada en la Figura 3-5 Topología de red para L2VPN, se proceden a realizar pruebas de conectividad mediante la herramienta ping con el fin de establecer los tiempos de retardo de ida y vuelta, pruebas de saltos de red mediante la herramienta traceroute y medición de los parámetros de QoS con las herramientas iPerf3 y Wireshark de acuerdo con las características de los tipos de tráfico en la sección 2.8.

3.8.1 Conectividad L3VPN intra-AS sin QoS

Para evaluar la conectividad intra-AS seamless MPLS L3VPN, se ejecuta el comando ping en el UE1 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=58 time=3.73 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=58 time=4.29 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=58 time=5.27 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=58 time=4.58 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=58 time=3.85 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=58 time=5.31 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=58 time=5.12 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=58 time=4.99 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=58 time=5.12 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=58 time=4.41 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 3.727/4.665/5.309/0.551 ms
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9017ms, con un RTT promedio de 4.665ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE1 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.1.0.1)  2.097 ms  18.154 ms  18.913 ms
 2  172.16.0.1 (172.16.0.1)  20.327 ms  20.962 ms  30.078 ms
 3  10.1.1.2 (10.1.1.2)  37.787 ms  37.841 ms  37.784 ms
 4  10.2.2.2 (10.2.2.2)  37.815 ms  37.929 ms  37.946 ms
 5  192.168.0.1 (192.168.0.1)  37.599 ms  37.620 ms  37.666 ms
 6  192.168.0.2 (192.168.0.2)  37.698 ms  19.023 ms  19.020 ms
 7  10.2.0.4 (10.2.0.4)  18.977 ms  32.906 ms  34.906 ms
```

Con la respuesta anterior se observan siete saltos de red desde el origen en la red del UE1, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-13 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-13 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE1)	0.00-60.00	181	25.3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Servidor de archivos	0.00-60.01	181	25.3

Los resultados muestran que el enlace intra-AS seamless MPLS L3VPN sin QoS tiene un ancho de banda de 25.3Mbps que equivalen a 3.16MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user/Descargas# scp
root@10.2.0.4:/home/admin/Downloads/large.test /home/user/Descargas/
root@10.2.0.4's password:
large.test
100% 1024MB   3.9MB/s   04:20
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 3.9MB/s o 31.2Mbps en un tiempo de 04:20min. Para efectos de cálculo se tomará una tasa de 4MB/s para encontrar los valores de jitter y pérdida de paquetes en iPerf3. La Tabla 3-14 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 4MB/s, equivalente a 32Mbps en iPerf3.

Tabla 3-14 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	229	32.0	0.000	0/165744 (0%)
Servidor de archivos	0.00-60.00	225	31.4	0.361	2883/165744 (1.7%)

Las pruebas realizadas muestran que para un ancho de banda de 4MBps o 32Mbps, se tiene un jitter de 0.361ms y unas pérdidas de paquetes del 1.7%.

La Figura 3-26 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad intra-AS seamless MPLS L3VPN sin QoS, donde se puede observar un

tiempo de registro de 0.572164246s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

Figura 3-26 Registro SIP UE con conectividad intra-AS seamless MPLS L3VPN sin QoS

La Figura 3-27, muestra los detalles de la llamada entre usuarios SIP, de Alice a Eve, con conectividad intra-AS seamless MPLS L3VPN sin QoS, con un total de 26 paquetes generados y una duración de 33s.

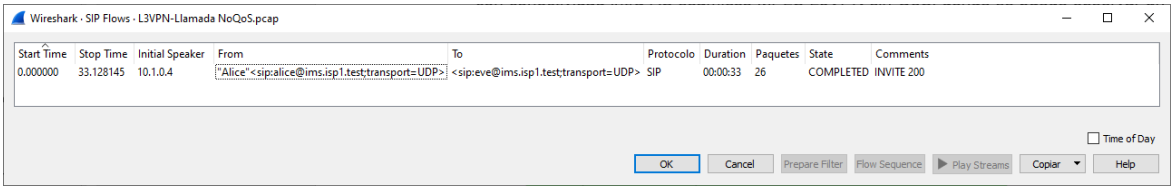


Figura 3-27 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS

La Figura 3-28 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad intra-AS seamless MPLS L3VPN sin QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Eve y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Eve, de 2.650700s. La llamada tiene una duración efectiva de 30.477445s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Eve, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Eve, lo que da una duración total de la llamada de 33.128145s que se valida por la Figura 3-27.

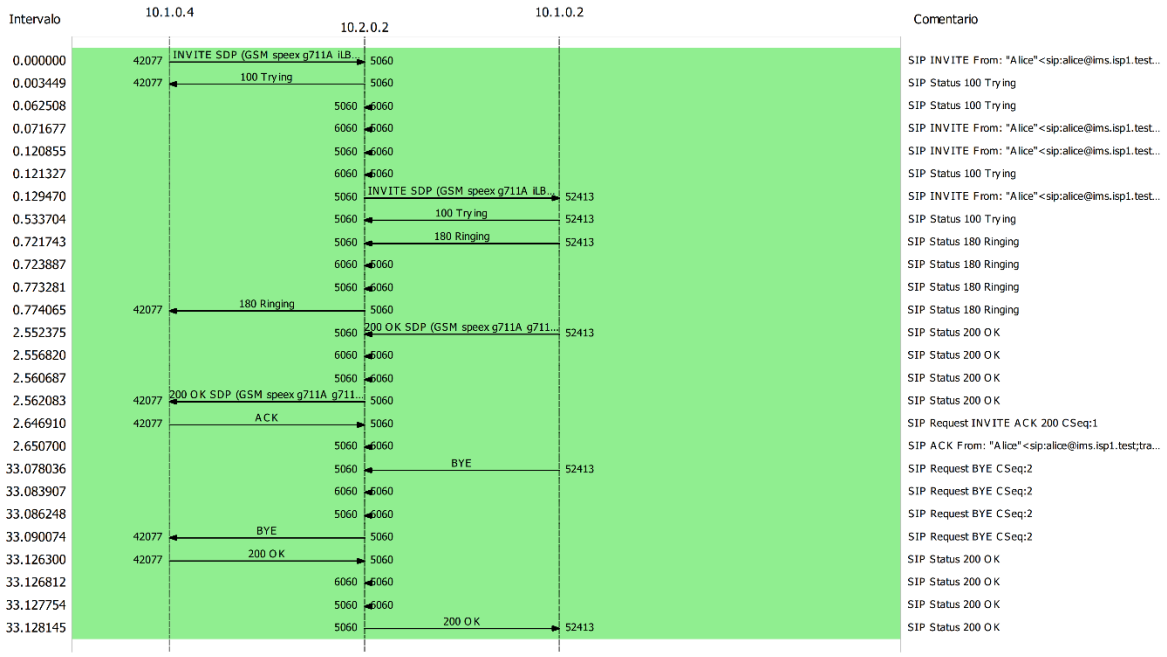


Figura 3-28 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS

La Figura 3-29 muestra la evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 854.67 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 67.95ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.28 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-29 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN sin QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-30 se realiza una conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine.

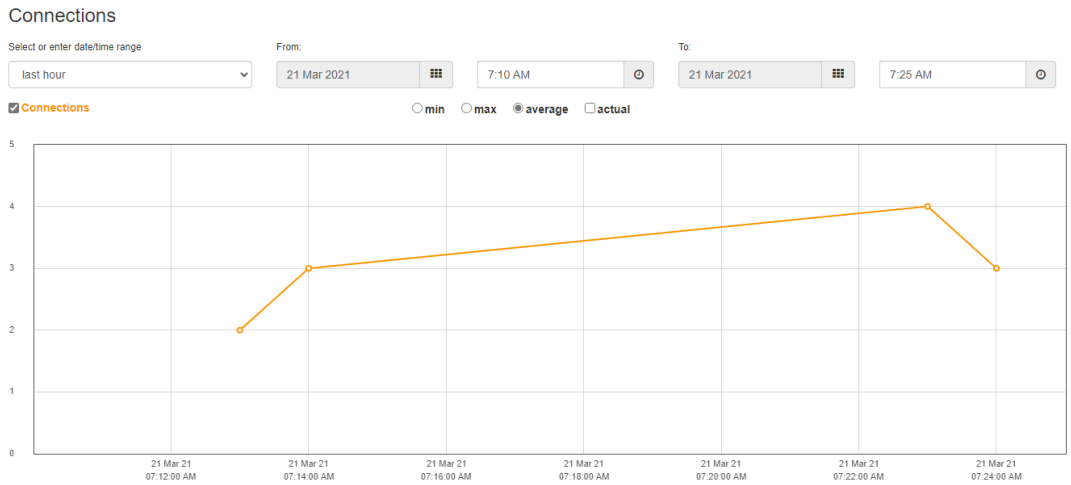


Figura 3-30 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

En la Figura 3-31 se observa un promedio de ancho de banda utilizado de 4.250 Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

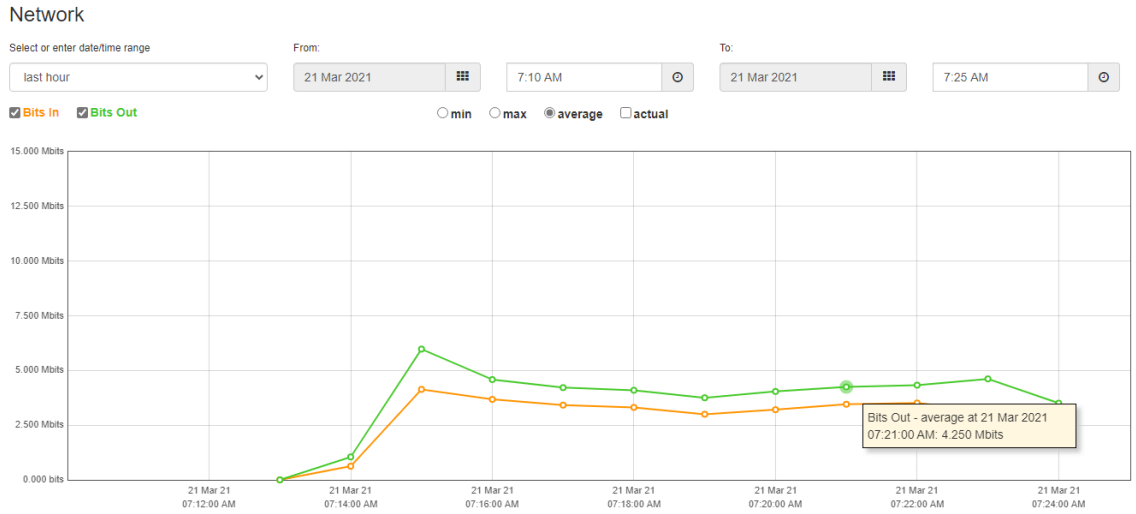


Figura 3-31 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

En la Figura 3-32, se observa que en el video reproducido en el UE se presentan problemas de pérdidas de cuadros del video y congelamiento de imagen, el sonido fluye sin cortes.

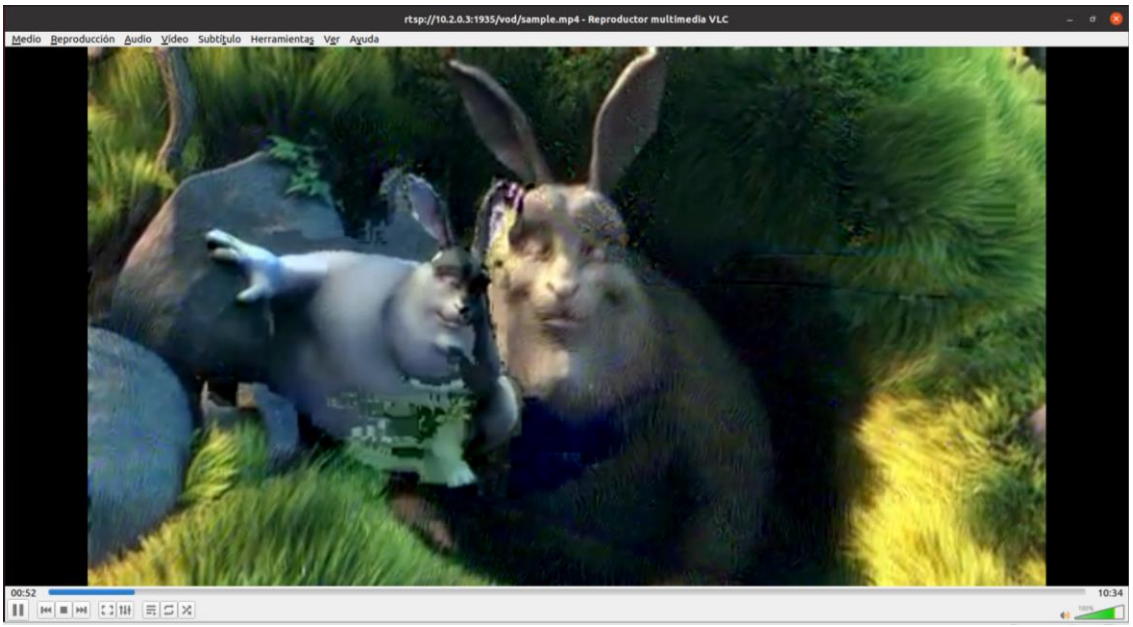


Figura 3-32 Pérdidas de cuadros y congelamiento en las imágenes del servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

3.8.2 Conectividad L3VPN inter-AS sin QoS

Para evaluar la conectividad inter-AS seamless MPLS L3VPN, se ejecuta el comando ping en el UE2 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=56 time=3.72 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=56 time=3.30 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=56 time=2.98 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=56 time=4.43 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=56 time=5.57 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=56 time=2.95 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=56 time=3.40 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=56 time=3.06 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=56 time=4.37 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=56 time=10.6 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.950/4.442/10.632/2.208 ms
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9014ms, con un RTT promedio de 4.442ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE2 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.3.0.1)  5.720 ms  5.627 ms  6.148 ms
 2  172.16.1.1 (172.16.1.1)  6.893 ms  8.820 ms *
 3  10.7.7.2 (10.7.7.2)  103.801 ms  119.568 ms  122.054 ms
 4  10.5.5.1 (10.5.5.1)  41.617 ms  41.893 ms  41.775 ms
 5  10.8.8.1 (10.8.8.1)  68.303 ms  71.045 ms  153.257 ms
 6  10.4.4.1 (10.4.4.1)  152.296 ms  155.829 ms  157.964 ms
 7  192.168.1.1 (192.168.1.1)  153.671 ms  153.312 ms  153.204 ms
 8  192.168.1.2 (192.168.1.2)  142.289 ms  124.248 ms  125.431 ms
 9  10.2.0.4 (10.2.0.4)  125.343 ms  98.798 ms  96.004 ms
root@vm:/home/user#
```

Con la respuesta anterior se observan nueve saltos de red desde el origen en la red del UE1, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-15 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-15 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE2)	0.00-60.00	139	19.5
Servidor de archivos	0.00-60.02	139	19.4

Los resultados muestran que el enlace intra-AS seamless MPLS L3VPN sin QoS tiene un ancho de banda de 19.5Mbps que equivalen a 2.43MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user/Descargas# scp
root@10.2.0.4:/home/admin/Downloads/large.test /home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   2.1MB/s
08:00
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 2.1MB/s o 16.8Mbps en un tiempo de 08:00min. Para comparar con el escenario intra-AS L3VPN sin QoS se tomará una tasa de 4MB/s para encontrar los valores de jitter y pérdida de paquetes en iPerf3. La Tabla 3-16 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 4MB/s, equivalente a 32Mbps en iPerf3.

Tabla 3-16 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN sin QoS en el tráfico UDP, limitando el ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	229	32.0	0.000	0/165744 (0%)
Servidor de archivos	0.00-60.01	201	28.1	0.443	20318/165744 (12%)

Las pruebas realizadas muestran que para un ancho de banda de 4MBps o 32Mbps, se tiene un jitter de 0.443ms y unas pérdidas de paquetes del 12%.

La Figura 3-33 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad inter-AS seamless MPLS L3VPN sin QoS, donde se puede observar un tiempo de registro de 0.35600303s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

Figura 3-33 Registro SIP UE con conectividad inter-AS seamless MPLS L3VPN sin QoS

La Figura 3-34, muestra los detalles de la llamada entre usuarios SIP, de Alice a Bob, con conectividad inter-AS seamless MPLS L3VPN sin QoS, con un total de 25 paquetes generados y una duración de 33s.

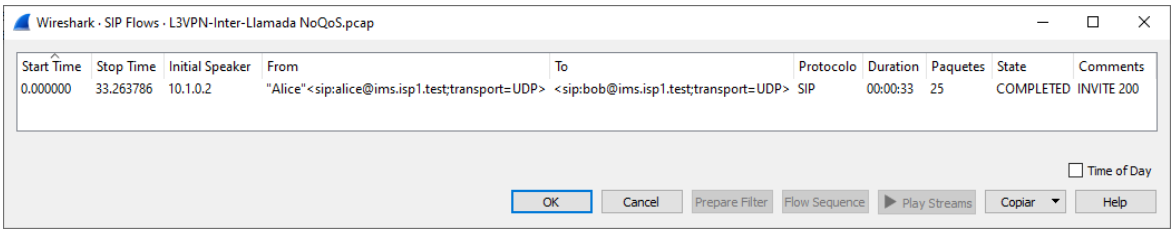


Figura 3-34 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS

La Figura 3-35 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad inter-AS seamless MPLS L3VPN sin QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Bob y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 2.725521s. La llamada tiene una duración efectiva de 30.477445s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 33.263786s que se valida por la Figura 3-34.

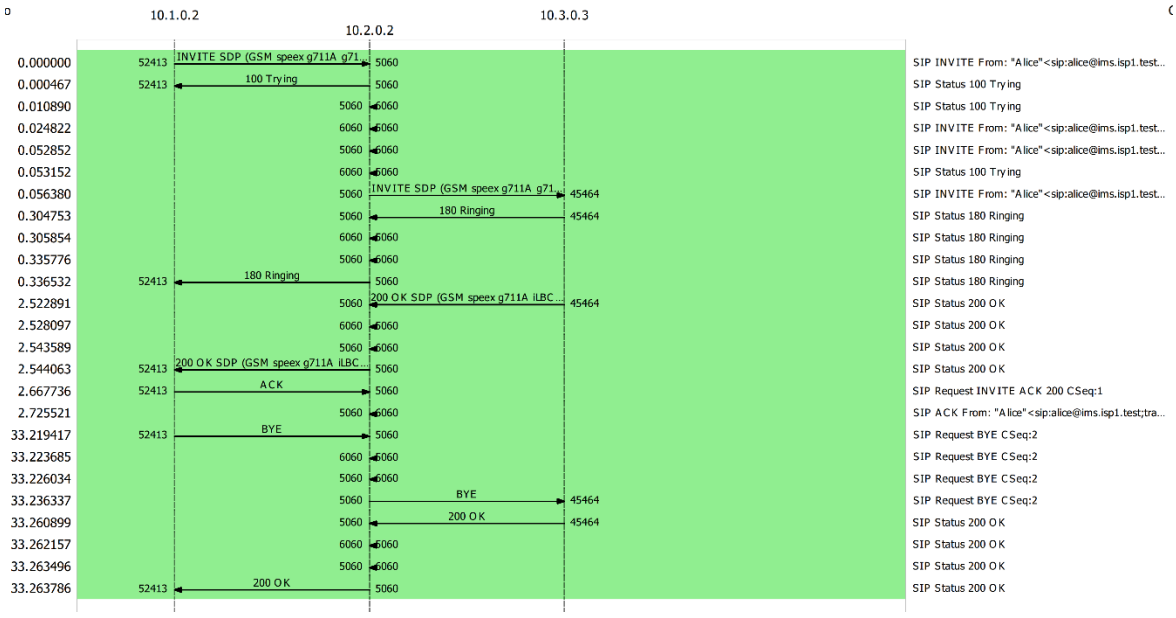


Figura 3-35 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS

La Figura 3-36 muestra la evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 893.14 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 97.98ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.16 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

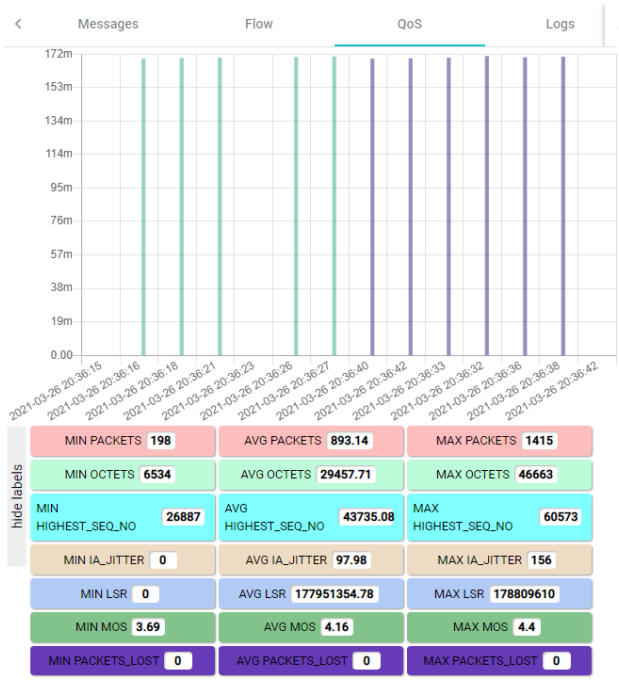


Figura 3-36 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN sin QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-37 se realiza una conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine.

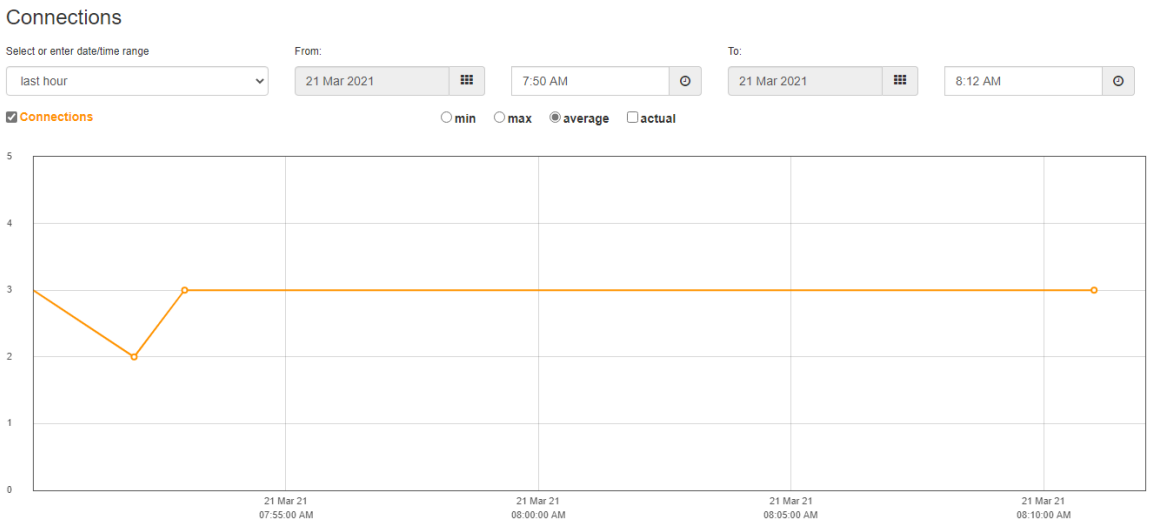


Figura 3-37 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

En la Figura 3-38 se observa un promedio de ancho de banda utilizado de 4.070 Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

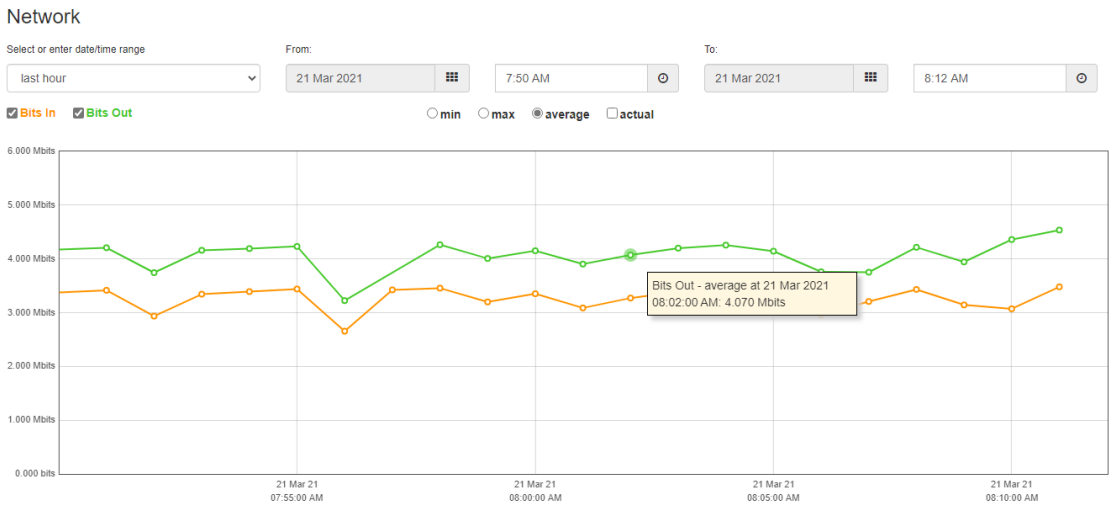


Figura 3-38 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

En la Figura 3-39, se observa que en el video reproducido en el UE se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen y cortes en el sonido.

Figura 3-39 Pérdidas de cuadros, congelamiento en las imágenes y cortes en el sonido del servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN sin QoS en Wowza Streaming Engine

3.8.3 Análisis comparativo de los escenarios L3VPN intra-AS e inter-AS sin QoS

Los resultados obtenidos en las pruebas de conectividad mediante la herramienta ping, muestran que el escenario intra-AS presenta un mayor retardo de ida y vuelta (4.665 ms) con respecto al escenario inter-AS (4.442ms).

Con las pruebas de saltos de red mediante la herramienta traceroute, se encuentra que el escenario intra-AS presenta menos saltos de red (siete saltos) con respecto al escenario inter-AS (nueve saltos).

Respecto al jitter, en las pruebas realizadas en iPerf3, se encuentra que en el escenario intra-AS se tiene un valor de 0.361ms y en el escenario inter-AS un valor de 0.443ms.

En relación con la pérdida de paquetes, se observa que en el escenario intra-AS, con una tasa de transferencia de 32.0Mbps desde el cliente, se obtuvo unas pérdidas del 1.7% y en el escenario inter-AS se obtuvo unas pérdidas del 12%. Dado que la prueba de descarga en el escenario inter-AS mostro una tasa de transferencia de 16.8Mbps, para la línea base del diseño de las políticas de QoS se establece con un ancho de banda de 17 Mbps en CIR y de 32 Mbps en PIR en los escenarios de conectividad intra-AS e inter-AS seamless MPLS L3VPN.

Con respecto al servicio de voz, se observa que en conectividad intra-AS se tiene tiempo de registro en SIP de 0.572164246s, mientras que en la conectividad inter-AS L3VPN es de 0.35600303s. En el escenario intra-AS, el jitter promedio fue de 67.95ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.28 en el MOS y en el escenario inter-AS, el jitter promedio fue de 97.98ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.16 en el MOS.

Para el servicio de video en streaming en IPTV, se observa que tanto para la conectividad intra-AS como inter-AS se tienen problemas de pérdida de imágenes y congelamiento en el video, siendo mayor el problema en la conectividad inter-AS al presentar cortes en el sonido para ambos casos. Se observa una utilización de ancho de banda de 4.250Mbps

en promedio para la conectividad intra-AS y de 4.070 Mbps para la conectividad inter-AS utilizando el códec de video MPEG-4.

3.9 Diseño e implementación de políticas de QoS

Con base en el tráfico identificado en la Tabla 3-1, se plantean las siguientes políticas de QoS para los escenarios de L2VPN y L3VPN con conectividad intra-AS e inter-AS seamless MPLS de acuerdo con los puntos tratados en la sección 2.10.

La Figura 3-40 muestra el sitio de aplicación de las políticas de QoS en el diseño de red planteado, en donde se busca clasificar el tráfico generado por los UE en el punto de ingreso a la red correspondiente a los nodos de acceso R1 y R3 en el tráfico ascendente, y en R2 para el tráfico descendente, aportado por los servidores. De la misma forma en R1, R2 y R3 se debe organizar el tráfico marcado para establecer el ancho de banda asignado en la cola establecida según su clasificación. Por último, el tráfico se acondiciona para adecuarse al CIR identificado en las pruebas de conectividad L2VPN y L3VPN para ser enviado a la red del SP estableciendo las prioridades correspondientes para el acceso a los servidores en un canal simétrico.

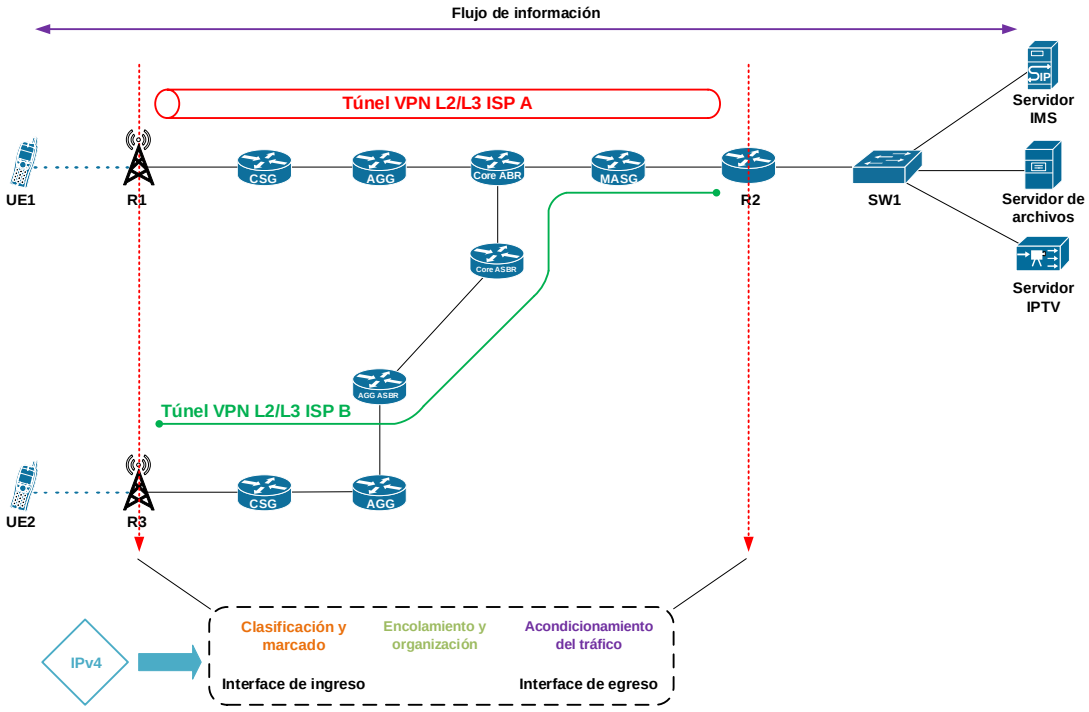


Figura 3-40 Sitio de aplicación de políticas de QoS

3.9.1 Clasificación y marcado del tráfico

De acuerdo con el tráfico identificado en la Tabla 3-1 se establece el mapeo de clases en R1, R2 y R3 descrito a continuación mediante la identificación de aplicaciones a través de NBAR como alternativa a las ACL:

```
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
 match protocol rtsp
```

El marcado de las clases se realiza de la siguiente manera:

```
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
```

```
class CMAP_SIGNALING_SIP
 set dscp cs5
class CMAP_VOICE_RTP
 set dscp ef
class CMAP_VOICE_CONTROL
 set dscp ef
class CMAP_MATCH_BROADCAST_VIDEO
 set dscp cs3
class CMAP_MATCH_OAM
 set dscp cs2
class class-default
 set dscp default
```

El tráfico de enrutamiento (OSPF y BGP) es marcado de forma automática por el IOS de Cisco como CS6. De manera similar en el caso de necesitar el descubrimiento de vecinos en IPv6, el tráfico es marcado de manera automática como CS7 [107].

Por último, se aplican las reglas de clasificación y marcado del tráfico en las interfaces de entrada de R1, R2 y R3 de la siguiente manera:

```
interface e0/1
 service-policy input PMAP_INGRESS_EDGE_MARK
```

Para verificar el tráfico marcado en R1 o en R3, generado por el UE correspondiente, se ejecuta el siguiente comando:

```
show policy-map interface e0/1
```

3.9.2 Encolamiento y organización del tráfico

Una vez que el tráfico ha sido clasificado y marcado se procede a organizar el tráfico marcado en colas, distribuyendo la utilización del ancho de banda disponible en el enlace del puerto de salida de los router R1, R2 o R3 entre las colas planteadas en la Figura 3-41.

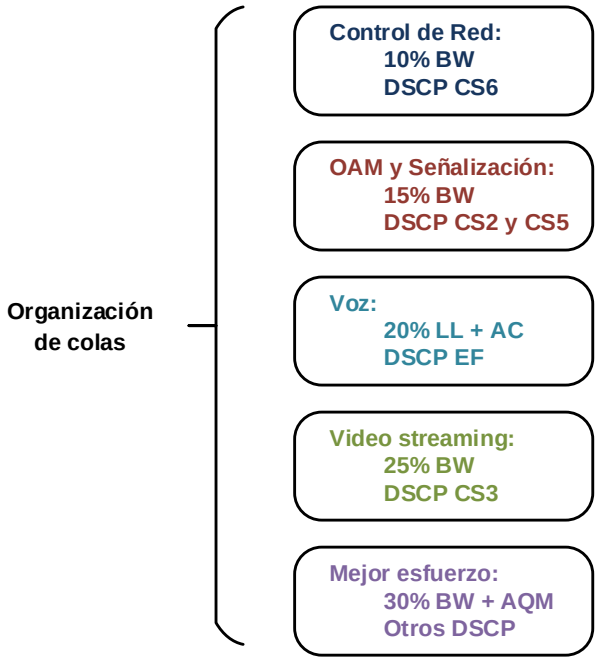


Figura 3-41 Organización del tráfico y distribución del ancho de banda en colas

Se define el uso de cinco colas, entre las que se encuentra el tráfico de control de red (tráfico OSPF y BGP marcados como CS6), operación y mantenimiento (tráfico SSH marcado como CS2 y SIP marcado como CS5), voz (tráfico RTP y RTCP marcados como EF), video streaming (tráfico UDP marcado como CS3) y, por último, todo el resto del tráfico que no entre en esta clasificación será manejado en la cola de tráfico de mejor esfuerzo (tráfico marcado con cualquier valor DSCP).

De acuerdo con lo descrito en [106] referente a la cantidad de colas a declarar, en un entorno de producción es recomendable no manejar más de seis colas, con el objetivo de tener un mejor control en la configuración y administración de los equipos activos en el que se apliquen las políticas de encolamiento.

La asignación de ancho de banda disponible para cada cola se realiza con base en las mejores prácticas descritas en [106] y [107] en entornos de producción, los valores se dan en los porcentajes descritos en la Figura 3-41 para las colas correspondientes, donde la suma aritmética de los anchos de banda asignados para cada cola, debe corresponder al 100%.

La creación de las colas se realiza de la siguiente manera en R1 y R3:

```
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2 cs5
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
```

La distribución de ancho de banda se realiza de la siguiente forma:

```
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
```

3.9.3 Acondicionamiento del tráfico

Para el acondicionamiento del tráfico en R1 y R3, se plantea la utilización de un modelador (shaper), debido a que el trato del tráfico no es tan agresivo como al aplicar una política de vigilancia dado que al exceder el valor del CIR el tráfico no se descarta. Teniendo en cuenta los escenarios de conectividad L2VPN y L3VPN respecto de los valores del PIR de 28Mbps y del CIR, establecido de manera práctica en 20Mbps para L2VPN y de 32Mbps en PIR y 17Mbps en CIR para L3VPN. En la Tabla 3-17 se muestran los resultados de los cálculos correspondientes con las ecuaciones planteadas en la sección 2.10.6 para los valores de Bc y Be.

Tomando como referencia el mínimo valor de Tc soportado por el IOS de Cisco en 4ms. Se toma como referencia un valor de Tc pequeño, dado que mejora el desempeño del tráfico en tiempo real como la voz [107].

Tabla 3-17 Valores calculados para el acondicionamiento del tráfico mediante un modelador

Conectividad	PIR	CIR	Tc	Bc (bits / bytes)	Be (bits / bytes)
L2VPN	28 Mbps	20 Mbps	4 ms	80000 / 10000	32000 / 4000
L3VPN	32 Mbps	17 Mbps	4 ms	68000 / 8500	60000 / 7500

Tomando en cuenta los valores de la Tabla 3-17, se configura el modelador para el caso de la conectividad L2VPN en los routers R1, R2 y R3, integrando las políticas de encolamiento y organización en las interfaces de salida de los routers de la siguiente manera:

```
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 20000000 80000 32000
   service-policy PMAP_EGRESS_QUEUE
```

Para el caso de la conectividad L3VPN se configura el modelador en los routers R1 y R3 de la siguiente manera:

```
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 17000000 68000 60000
   service-policy PMAP_EGRESS_QUEUE
```

Por último, se aplican las reglas acondicionamiento del tráfico del tráfico en las interfaces de salida de los routers R1, R3 y en el router R2 para el caso de la conectividad intra-AS de la siguiente manera:

```
interface e0/0
 service-policy output PMAP_EGRESS_SHAPE
```

Para el router R2 en el caso de la conectividad inter-AS:

```
interface e0/2
 service-policy output PMAP_EGRESS_SHAPE
```

Para verificar el tráfico marcado en los routers R1, R2 y R3, generado por el UE correspondiente, se ejecuta el siguiente comando según sea el caso:

```
show policy-map interface e0/X | include shape|Class|%
```

3.10 Evaluación de políticas de QoS

Teniendo en cuenta las políticas de QoS diseñadas para la conectividad intra-AS e inter-AS seamless MPLS en L2VPN y L3VPN, se procede a evaluar su implementación en la red emulada.

3.10.1 Conectividad L2VPN intra-AS con QoS

Para evaluar la conectividad intra-AS seamless MPLS L3VPN, se ejecuta el comando ping en el UE1 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=62 time=3.71 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=62 time=4.33 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=62 time=5.08 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=62 time=5.37 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=62 time=4.28 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=62 time=2.65 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=62 time=4.63 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=62 time=3.99 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=62 time=4.53 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=62 time=5.92 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9020ms
rtt min/avg/max/mdev = 2.651/4.449/5.924/0.866 ms
root@vm:/home/user#
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9020ms, con un RTT promedio de 4.449ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE1 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.1.0.1)  7.406 ms  7.356 ms  7.457 ms
 2  192.168.0.2 (192.168.0.2)  5.048 ms  5.515 ms  5.996 ms
 3  10.2.0.4 (10.2.0.4)  5.614 ms  5.851 ms  5.807 ms
root@vm:/home/user#
```

Con la respuesta anterior se observan tres saltos de red desde el origen en la red del UE1, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-18 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-18 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE1)	0.00-60.00	136	19.0
Servidor de archivos	0.00-60.00	135	18.9

Los resultados muestran que el enlace intra-AS seamless MPLS L2VPN con QoS tiene un ancho de banda de 18.9Mbps que equivalen a 2.3625MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user# scp root@10.2.0.4:/home/admin/Downloads/large.test
/home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   2.2MB/s   07:45
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 2.2MB/s o 17.6Mbps en un tiempo de 07:45min.

Para validar el diseño de las políticas de QoS en conectividad L2VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del CIR, correspondiente a 20Mbps. La Tabla 3-19 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 2.5MB/s, equivalente a 20Mbps en iPerf3.

Tabla 3-19 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	143	20.0	0.000	0/103591 (0%)

Servidor de archivos	0.00-60.23	138	19.2	1.051	3733/103588 (3.6%)

Las pruebas realizadas muestran que para un ancho de banda de 2.5MBps o 20Mbps, se tiene un jitter de 1.051ms y unas pérdidas de paquetes del 3.6%.

Para comparar el diseño de las políticas de QoS en conectividad L2VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del PIR, correspondiente a 28Mbps. La Tabla 3-20 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 3.5MB/s, equivalente a 28Mbps en iPerf3.

Tabla 3-20 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	200	28.0	0.000	0/145028 (0%)
Servidor de archivos	0.00-60.21	136	18.9	1.561	46741/145026 (32%)

Las pruebas realizadas muestran que para un ancho de banda de 3.5MBps o 28Mbps, se tiene un jitter de 1.561ms y unas pérdidas de paquetes del 32%. Al comparar esta prueba con la Tabla 3-19 se observa que cuando el tráfico excede el valor del CIR, la política de modelado actúa, manteniendo el bitrate y descartando de forma aleatoria aquellos paquetes que saturen el nivel de tráfico que no puede ser manejado en la cola.

La Figura 3-42 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad intra-AS seamless MPLS L2VPN con QoS, donde se puede observar un tiempo de registro de 0.114853681s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

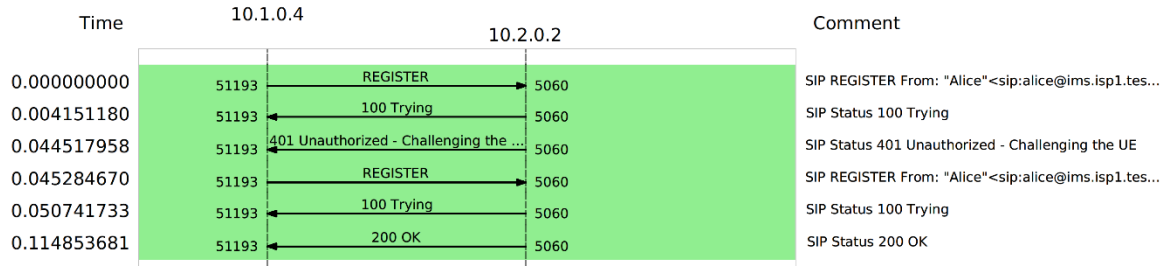


Figura 3-42 Registro SIP UE con conectividad intra-AS seamless MPLS L2VPN con QoS

La Figura 3-43, muestra los detalles de la llamada entre usuarios SIP, de Alice a Eve, con conectividad intra-AS seamless MPLS L2VPN con QoS, con un total de 26 paquetes generados y una duración de 32s.

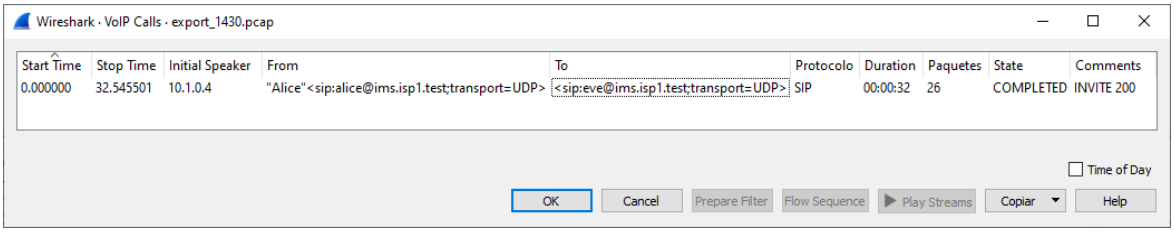


Figura 3-43 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS

La Figura 3-44 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad intra-AS seamless MPLS L2VPN con QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Eve y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 2.861150s. La llamada tiene una duración efectiva de 29.684351s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 32.545501s que se valida por la Figura 3-43.

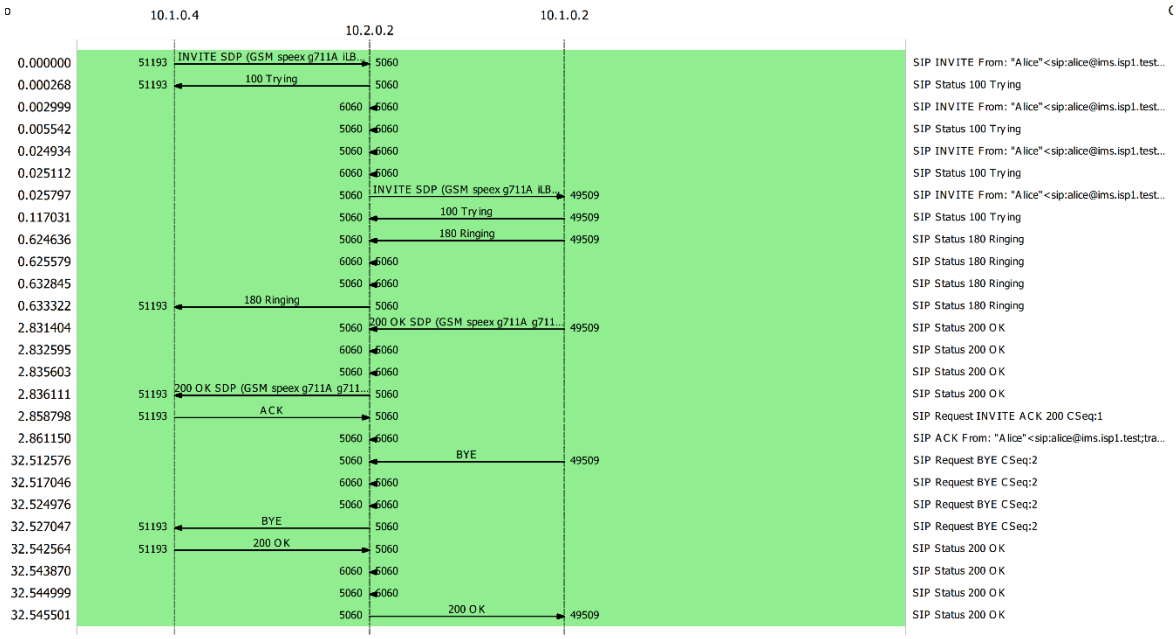


Figura 3-44 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN con QoS

La Figura 3-45 muestra la evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN con QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 875.55 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 69.95ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.24 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-45 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L2VPN con QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-46 se realiza una conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine.

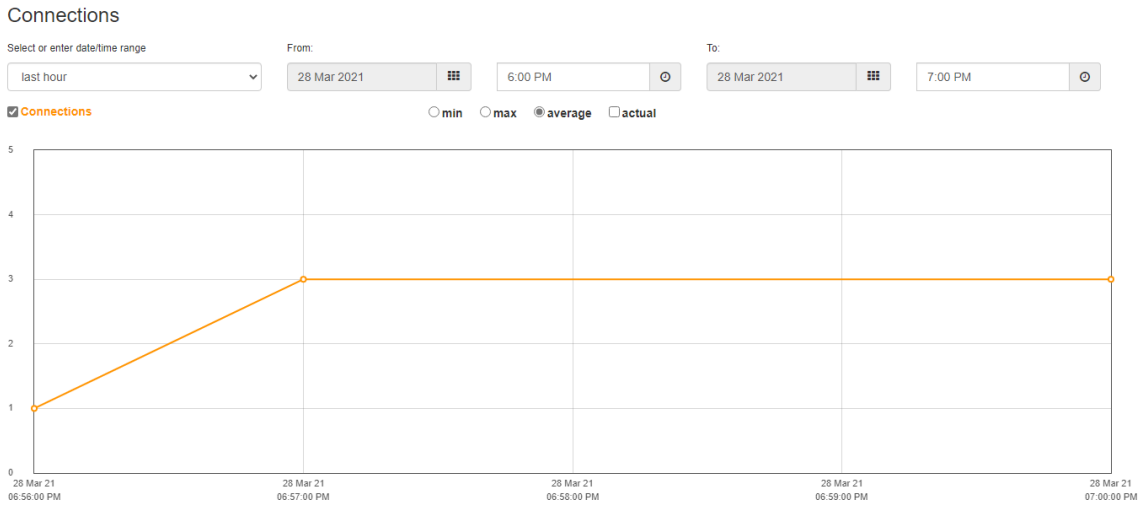


Figura 3-46 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

En la Figura 3-47 se observa un promedio de ancho de banda utilizado de 3.710Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

Figura 3-47 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

En la Figura 3-48, se observa que en el video reproducido en el UE no se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen, sin embargo, se presentan cortes en el sonido de manera esporádica.

Figura 3-48 Reproducción de video en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

3.10.2 Conectividad L2VPN inter-AS con QoS

Para evaluar la conectividad inter-AS seamless MPLS L2VPN, se ejecuta el comando ping en el UE2 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
root@vm:/home/user# ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=62 time=3.24 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=62 time=5.79 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=62 time=4.62 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=62 time=5.48 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=62 time=5.01 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=62 time=5.33 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=62 time=2.93 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=62 time=3.55 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=62 time=4.92 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=62 time=6.33 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 2.929/4.718/6.325/1.076 ms
root@vm:/home/user#
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9018ms, con un RTT promedio de 4.718ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE2 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
root@vm:/home/user# traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.3.0.1)  0.870 ms  0.851 ms  0.922 ms
 2  192.168.1.2 (192.168.1.2)  7.113 ms  7.109 ms  7.754 ms
 3  10.2.0.4 (10.2.0.4)  7.725 ms  9.411 ms  9.307 ms
root@vm:/home/user#
```

Con la respuesta anterior se observan tres saltos de red desde el origen en la red del UE2, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-21 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-21 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE2)	0.00-60.00	131	18.4
Servidor de archivos	0.00-60.01	131	18.3

Los resultados muestran que el enlace inter-AS seamless MPLS L2VPN con QoS tiene un ancho de banda de 18.3Mbps que equivalen a 2.2875MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user# scp root@10.2.0.4:/home/admin/Downloads/large.test
/home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   2.2MB/s   07:46
root@vm:/home/user#
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 2.2MB/s o 17.6Mbps en un tiempo de 07:46min.

Para validar el diseño de las políticas de QoS en conectividad L2VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del CIR, correspondiente a 20Mbps. La Tabla 3-22 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 2.5MB/s, equivalente a 20Mbps en iPerf3.

Tabla 3-22 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	143	20.0	0.000	0/103591 (0%)
Servidor de archivos	0.00-60.21	135	18.8	1.112	5798/103590 (5.6%)

Las pruebas realizadas muestran que para un ancho de banda de 2.5MBps o 20Mbps, se tiene un jitter de 1.112ms y unas pérdidas de paquetes del 5.6%.

Para comparar el diseño de las políticas de QoS en conectividad L2VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho

de banda al valor del PIR, correspondiente a 28Mbps. La Tabla 3-23 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 3.5MB/s, equivalente a 28Mbps en iPerf3.

Tabla 3-23 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L2VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	200	28.0	0.000	0/145027 (0%)
Servidor de archivos	0.00-60.21	138	19.3	0.881	44849/144907 (31%)

Las pruebas realizadas muestran que para un ancho de banda de 3.5MBps o 28Mbps, se tiene un jitter de 0.881ms y unas pérdidas de paquetes del 31%. Al comparar esta prueba con la Tabla 3-22 se observa que cuando el tráfico excede el valor del CIR, la política de modelado actúa, manteniendo el bitrate y descartando de forma aleatoria aquellos paquetes que saturen el nivel de tráfico que no puede ser manejado en la cola.

La Figura 3-49 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad inter-AS seamless MPLS L2VPN con QoS, donde se puede observar un tiempo de registro de 0.733073349s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

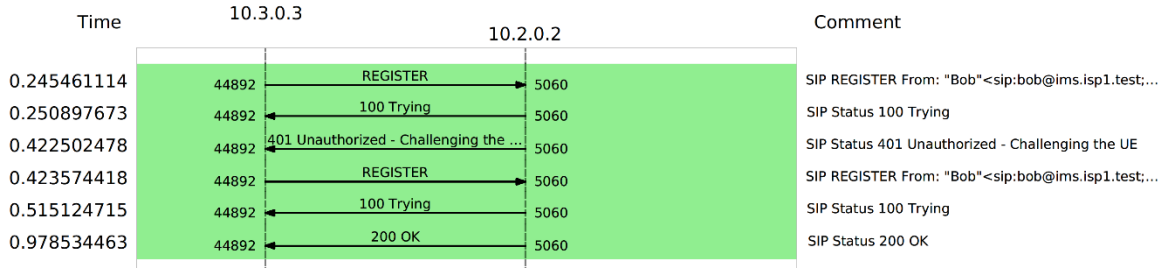


Figura 3-49 Registro SIP UE con conectividad inter-AS seamless MPLS L2VPN con QoS

La Figura 3-50, muestra los detalles de la llamada entre usuarios SIP, de Alice a Bob, con conectividad inter-AS seamless MPLS L2VPN con QoS, con un total de 25 paquetes generados y una duración de 31s.

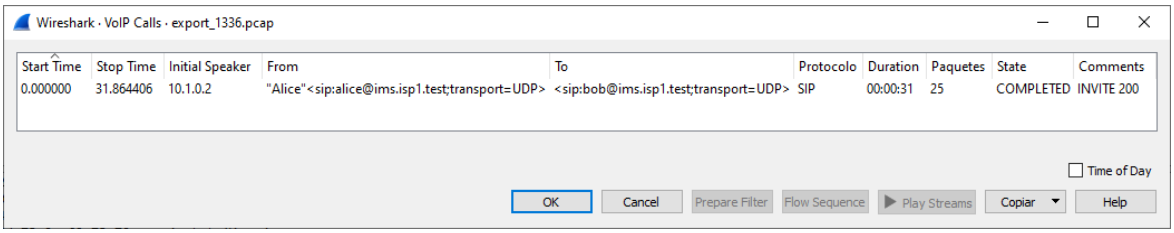


Figura 3-50 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS

La Figura 3-51 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad inter-AS seamless MPLS L2VPN con QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Bob y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 2.164121s. La llamada tiene una duración efectiva de 29.700285s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 31.864406s que se valida por la Figura 3-27.

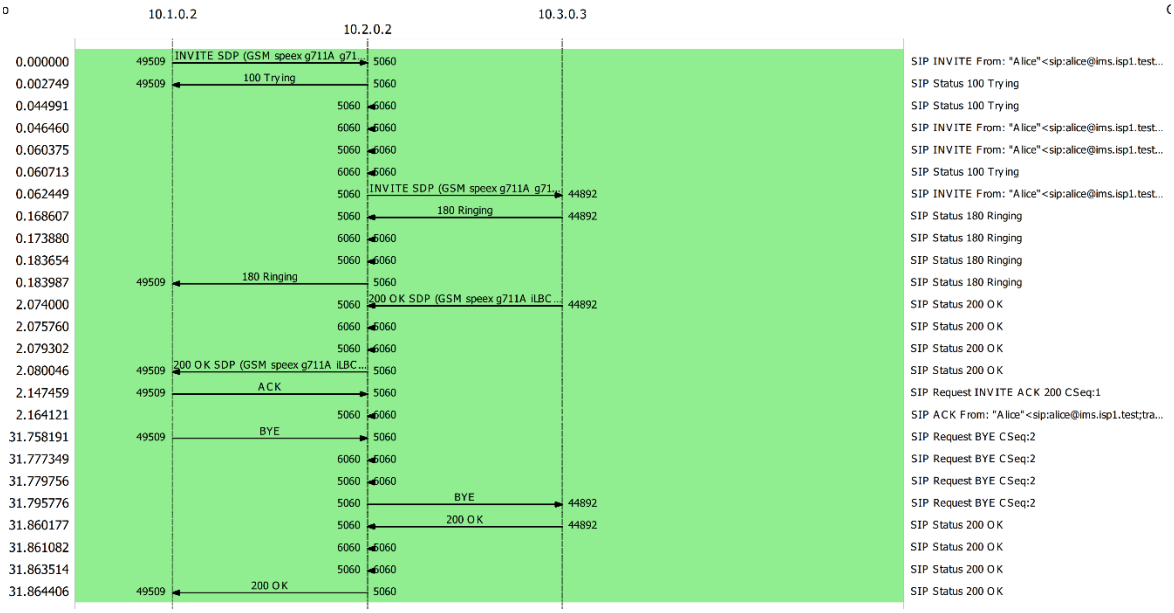


Figura 3-51 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS

La Figura 3-52 muestra la evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 909.43 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 108.63ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.16 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-52 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L2VPN con QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-53 se realiza una conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine.

Figura 3-53 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

En la Figura 3-54 se observa un promedio de ancho de banda utilizado de 3.880Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

Figura 3-54 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

En la Figura 3-55, se observa que en el video reproducido en el UE no se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen, sin embargo, se presentan cortes en el sonido de manera esporádica.

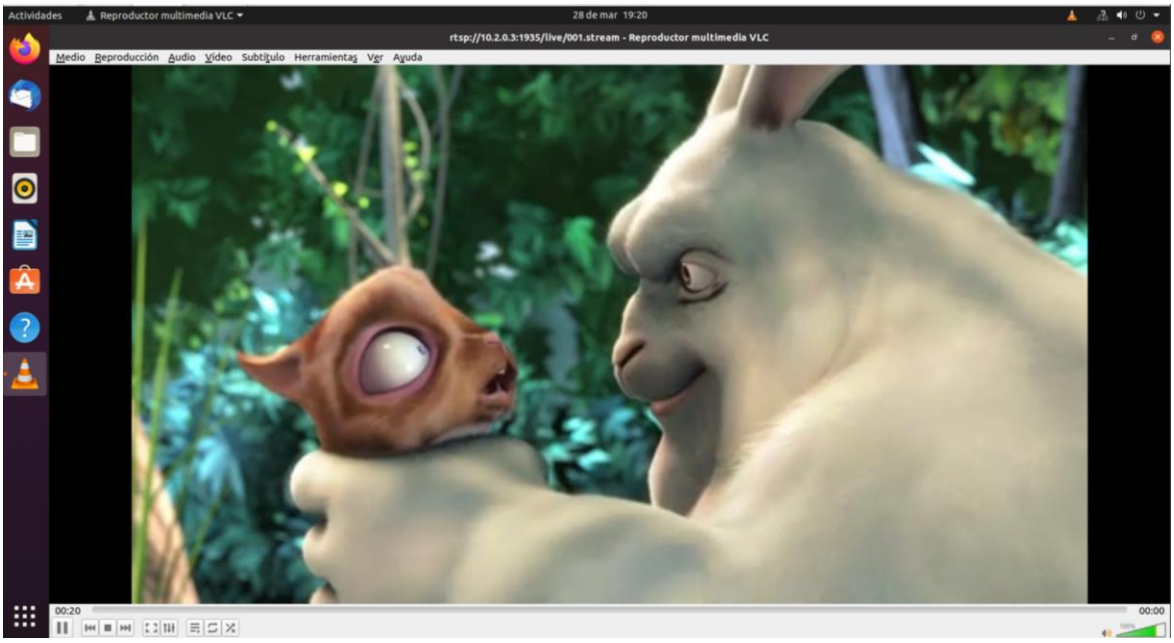


Figura 3-55 Reproducción de video en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L2VPN con QoS en Wowza Streaming Engine

3.10.3 Análisis comparativo de los escenarios L2VPN intra-AS e inter-AS con QoS

Los resultados obtenidos en las pruebas de conectividad mediante la herramienta ping, muestran que el escenario intra-AS presenta un menor retardo de ida y vuelta (4.449ms) con respecto al escenario inter-AS (4.718ms).

Con las pruebas de saltos de red mediante la herramienta traceroute, se encuentra que el escenario intra-AS presenta la misma cantidad de saltos de red con respecto al escenario inter-AS (tres saltos).

Respecto al jitter y las pérdidas de paquetes, en las pruebas realizadas en iPerf3 limitando el ancho de banda al valor del CIR de 20 Mbps, se encuentra que en el escenario intra-AS se tiene un valor de 1.051ms y unas pérdidas de paquetes del 3.6% y para el escenario inter-AS se tiene un jitter de 1.112ms y unas pérdidas de paquetes del 5.6%. Al limitar el ancho de banda al valor del PIR de 28Mbps, se encuentra que en el escenario intra-AS se tiene un jitter de 1.561ms y unas pérdidas de paquetes del 32% y en el escenario inter-AS se tiene un jitter de 0.881ms y unas pérdidas de paquetes del 31%.

Respecto del servicio de voz, se observa que en conectividad intra-AS se tiene tiempo de registro en SIP de 0.114853681s, mientras que en la conectividad inter-AS L2VPN es de 0.733073349s. En el escenario intra-AS, el jitter promedio fue de 69.95ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.24 en el MOS y en el escenario inter-AS, el jitter promedio fue de 108.63ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.16 en el MOS.

Para el servicio de video en streaming en IPTV, se observa que tanto para la conectividad intra-AS como inter-AS no se tienen problemas de pérdida de imágenes y congelamiento en el video, sin embargo, se presentan cortes en el sonido para ambos casos. Se observa una utilización de ancho de banda de 3.710Mbps en promedio para la conectividad intra-AS y de 3.880Mbps para la conectividad inter-AS utilizando el códec de video MPEG-4.

3.10.4 Conectividad L3VPN intra-AS con QoS

Para evaluar la conectividad intra-AS seamless MPLS L3VPN, se ejecuta el comando ping en el UE1 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
user@vm:~$ ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=58 time=2.94 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=58 time=2.96 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=58 time=2.59 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=58 time=4.95 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=58 time=3.22 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=58 time=2.93 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=58 time=4.12 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=58 time=2.78 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=58 time=2.69 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=58 time=4.88 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 2.594/3.406/4.953/0.855 ms
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9015ms, con un RTT promedio de 3.406ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE1 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
user@vm:~$ traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.1.0.1)  0.999 ms  0.831 ms  3.234 ms
 2  172.16.0.1 (172.16.0.1)  3.095 ms  3.003 ms  2.449 ms
 3  10.1.1.2 (10.1.1.2)  9.185 ms  9.076 ms  8.955 ms
 4  10.2.2.2 (10.2.2.2)  9.564 ms  13.617 ms  15.879 ms
 5  192.168.0.1 (192.168.0.1)  9.574 ms  9.457 ms  9.636 ms
 6  192.168.0.2 (192.168.0.2)  13.020 ms  12.989 ms  12.826 ms
 7  10.2.0.4 (10.2.0.4)  9.863 ms  11.246 ms  11.115 ms
```

Con la respuesta anterior se observan siete saltos de red desde el origen en la red del UE1, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-24 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-24 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE1)	0.00-60.00	114	15.9
Servidor de archivos	0.00-60.02	113	15.9

Los resultados muestran que el enlace intra-AS seamless MPLS L3VPN con QoS tiene un ancho de banda de 15.9Mbps que equivalen a 1.98MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user/Descargas# scp
root@10.2.0.4:/home/admin/Downloads/large.test /home/user/Descargas/
root@10.2.0.4's password:
large.test                                    100% 1024MB   1.9MB/s   08:54
root@vm:/home/user#
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 1.9MB/s o 15.2Mbps en un tiempo de 08:54min.

Para validar el diseño de las políticas de QoS en conectividad L3VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del CIR, correspondiente a 17Mbps. La Tabla 3-25 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless

MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 2.125MB/s, equivalente a 17Mbps en iPerf3.

Tabla 3-25 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	122	17.0	0.000	0/88052 (0%)
Servidor de archivos	0.00-60.03	117	16.3	1.019	3438/88052 (3.9%)

Las pruebas realizadas muestran que para un ancho de banda de 2.125MB/s o 17Mbps, se tiene un jitter de 1.019ms y unas pérdidas de paquetes del 3.9%.

Para comparar el diseño de las políticas de QoS en conectividad L3VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del PIR, correspondiente a 32Mbps. La Tabla 3-26 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 4MB/s, equivalente a 32Mbps en iPerf3.

Tabla 3-26 Resultados promedio de la evaluación de la conectividad intra-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE1)	0.00-60.00	229	32.0	0.000	0/165745 (0%)
Servidor de archivos	0.00-60.08	118	16.4	0.883	80599/165744 (49%)

Las pruebas realizadas muestran que para un ancho de banda de 4MBps o 32Mbps, se tiene un jitter de 0.883ms y unas pérdidas de paquetes del 49%. Al comparar esta prueba con la Tabla 3-25 se observa que cuando el tráfico excede el valor del CIR, la política de modelado actúa, manteniendo el bitrate y descartando de forma aleatoria aquellos paquetes que saturen el nivel de tráfico que no puede ser manejado en la cola.

La Figura 3-56 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad intra-AS seamless MPLS L3VPN con QoS, donde se puede observar un

tiempo de registro de 0.999093408s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

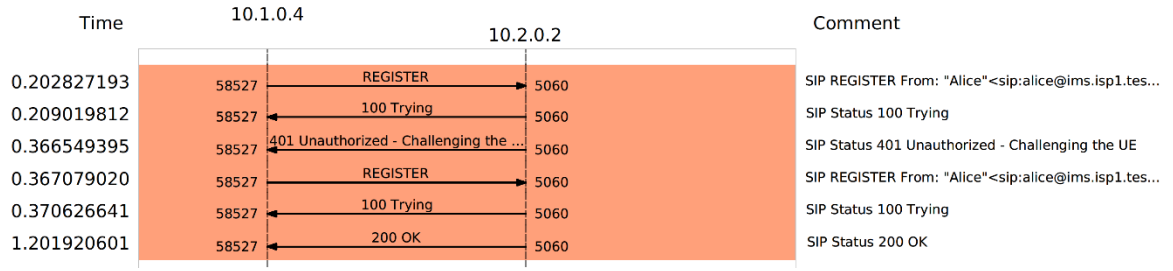


Figura 3-56 Registro SIP UE con conectividad intra-AS seamless MPLS L3VPN con QoS

La Figura 3-57, muestra los detalles de la llamada entre usuarios SIP, de Alice a Eve, con conectividad intra-AS seamless MPLS L3VPN con QoS, con un total de 26 paquetes generados y una duración de 32s.

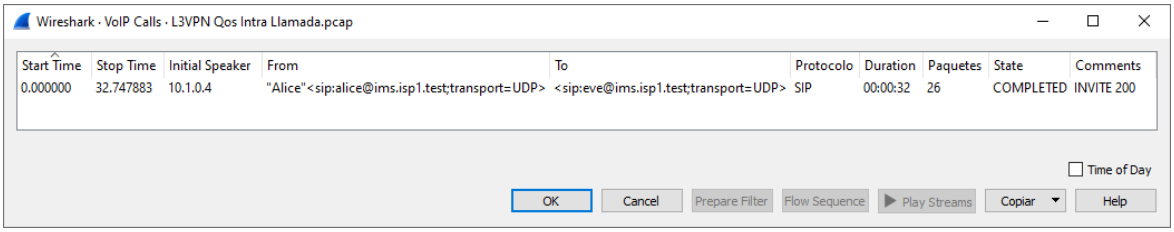


Figura 3-57 Detalles de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS

La Figura 3-58 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad intra-AS seamless MPLS L3VPN con QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Eve y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 3.265097s. La llamada tiene una duración efectiva de 29.482786s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 32.747883s que se valida por la Figura 3-57.

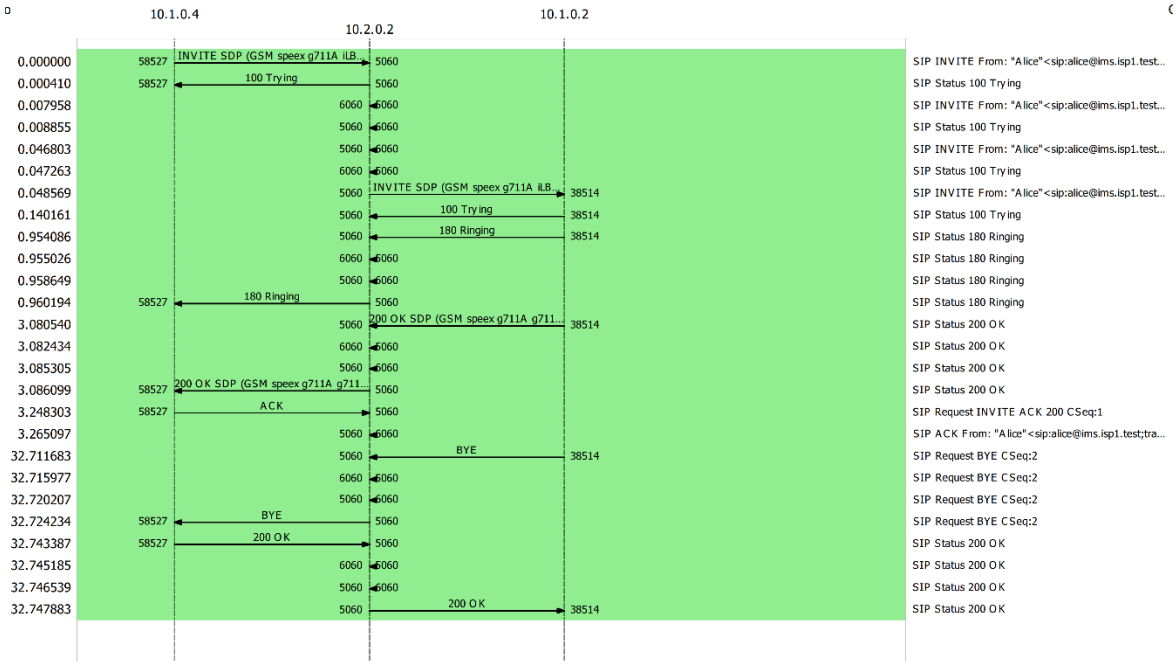


Figura 3-58 Llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS

La Figura 3-59 muestra la evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS en HOMER SIP. Esta se realiza sobre los paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 825.54 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 57.67ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.29 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-59 Evaluación de la llamada entre usuarios SIP con conectividad intra-AS seamless MPLS L3VPN con QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-60 se realiza una conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine.

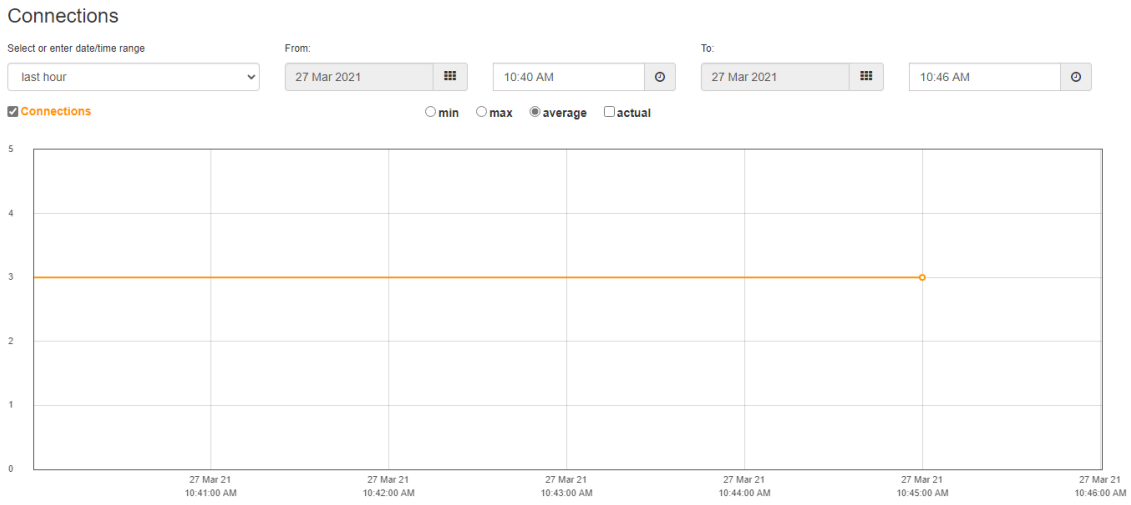


Figura 3-60 Conexión al servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

En la Figura 3-61 se observa un promedio de ancho de banda utilizado de 3.960Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

Figura 3-61 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

En la Figura 3-62, se observa que en el video reproducido en el UE no se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen, sin embargo, se presentan cortes en el sonido de manera esporádica.

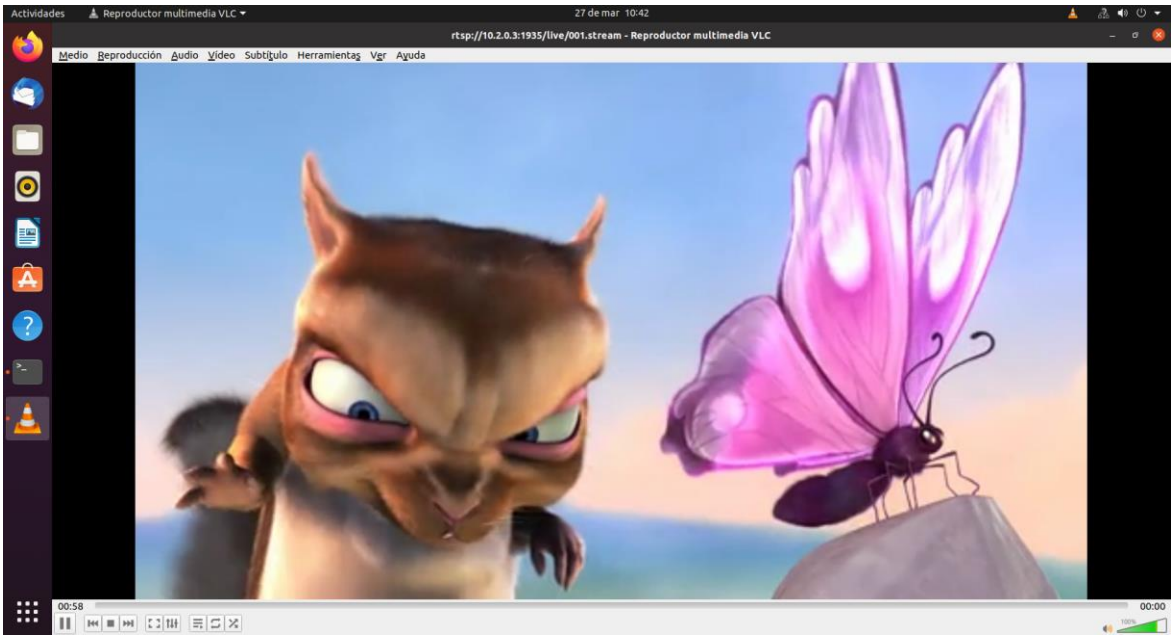


Figura 3-62 Reproducción de video en el servicio de streaming en IPTV con conectividad intra-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

3.10.5 Conectividad L3VPN inter-AS con QoS

Para evaluar la conectividad inter-AS seamless MPLS L3VPN, se ejecuta el comando ping en el UE2 con la dirección IP del servidor de archivos obteniendo los siguientes resultados:

```
user@vm:~$ ping 10.2.0.4 -c 10
PING 10.2.0.4 (10.2.0.4) 56(84) bytes of data.
64 bytes from 10.2.0.4: icmp_seq=1 ttl=56 time=5.42 ms
64 bytes from 10.2.0.4: icmp_seq=2 ttl=56 time=7.43 ms
64 bytes from 10.2.0.4: icmp_seq=3 ttl=56 time=15.3 ms
64 bytes from 10.2.0.4: icmp_seq=4 ttl=56 time=9.63 ms
64 bytes from 10.2.0.4: icmp_seq=5 ttl=56 time=6.82 ms
64 bytes from 10.2.0.4: icmp_seq=6 ttl=56 time=65.1 ms
64 bytes from 10.2.0.4: icmp_seq=7 ttl=56 time=11.8 ms
64 bytes from 10.2.0.4: icmp_seq=8 ttl=56 time=65.3 ms
64 bytes from 10.2.0.4: icmp_seq=9 ttl=56 time=38.8 ms
64 bytes from 10.2.0.4: icmp_seq=10 ttl=56 time=5.07 ms

--- 10.2.0.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 5.066/23.067/65.336/23.055 ms
```

Se observa que fueron transmitidos y recibidos 10 paquetes, con una pérdida del 0% en un tiempo de 9018ms, con un RTT promedio de 23.067ms. De igual manera, se evalúan los saltos de red con el comando traceroute en el UE2 con la dirección IP del servidor de archivos, obteniendo los siguientes resultados:

```
user@vm:~$ traceroute 10.2.0.4
traceroute to 10.2.0.4 (10.2.0.4), 30 hops max, 60 byte packets
 1  _gateway (10.3.0.1)  2.433 ms  2.465 ms  2.377 ms
 2  172.16.1.1 (172.16.1.1)  7.718 ms  7.656 ms  7.529 ms
 3  10.7.7.2 (10.7.7.2)  29.341 ms  29.282 ms  29.183 ms
 4  10.5.5.1 (10.5.5.1)  29.019 ms  31.048 ms  30.977 ms
 5  10.8.8.1 (10.8.8.1)  30.920 ms  30.860 ms  30.802 ms
 6  10.4.4.1 (10.4.4.1)  30.743 ms  52.036 ms  51.791 ms
 7  192.168.1.1 (192.168.1.1)  31.850 ms  31.919 ms  42.562 ms
 8  192.168.1.2 (192.168.1.2)  42.471 ms  40.583 ms  76.706 ms
 9  10.2.0.4 (10.2.0.4)  76.684 ms  76.623 ms  74.971 ms
```

Con la respuesta anterior se observan siete saltos de red desde el origen en la red del UE2, hasta la red del servidor de archivos, con sus respectivas latencias de ida y vuelta (mínima, media y máxima) para cada salto.

La Tabla 3-27 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3.

Tabla 3-27 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico TCP, sin límite de ancho de banda en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)
Cliente (UE2)	0.00-60.00	116	16.2
Servidor de archivos	0.00-60.02	115	16.1

Los resultados muestran que el enlace inter-AS seamless MPLS L3VPN con QoS tiene un ancho de banda de 16.1Mbps que equivalen a 2.01MBps, el cual se valida mediante una prueba de descarga de acuerdo con el punto 3.6 con el siguiente resultado:

```
root@vm:/home/user/Descargas# scp
root@10.2.0.4:/home/admin/Downloads/large.test /home/user/Descargas/
large.test                                    100% 1024MB   1.9MB/s   08:55
root@vm:/home/user#
```

Los resultados muestran que para descargar un archivo de 1GB, se tiene una tasa de transferencia de 1.9MB/s o 15.2Mbps en un tiempo de 08:55min.

Para validar el diseño de las políticas de QoS en conectividad L3VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho de banda al valor del CIR, correspondiente a 17Mbps. La Tabla 3-28 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 2.125MB/s, equivalente a 17Mbps en iPerf3.

Tabla 3-28 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del CIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	122	17.0	0.000	0/88052 (0%)
Servidor de archivos	0.00-60.02	116	16.2	1.072	4278/88052 (4.9%)

Las pruebas realizadas muestran que para un ancho de banda de 2.125MB/s o 17Mbps, se tiene un jitter de 1.072ms y unas pérdidas de paquetes del 4.9%.

Para comparar el diseño de las políticas de QoS en conectividad L3VPN y encontrar los valores de jitter y pérdida de paquetes, se ejecuta la prueba en iPerf3 limitando el ancho

de banda al valor del PIR, correspondiente a 32Mbps. La Tabla 3-29 muestra los resultados promedio de los parámetros de QoS en la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda a la tasa de transferencia de 4MB/s, equivalente a 32Mbps en iPerf3.

Tabla 3-29 Resultados promedio de la evaluación de la conectividad inter-AS seamless MPLS L3VPN con QoS en el tráfico UDP, limitando el ancho de banda al valor del PIR en iPerf3

Elemento	Intervalo (seg)	Transferencia (MBytes)	Bitrate (Mbits/seg)	Jitter (ms)	Datagramas Perdidos/Total
Cliente (UE2)	0.00-60.00	229	32.0	0.000	0/165745 (0%)
Servidor de archivos	0.00-60.00	117	16.4	1.039	80884/165745 (49%)

Las pruebas realizadas muestran que para un ancho de banda de 4MBps o 32Mbps, se tiene un jitter de 1.039ms y unas pérdidas de paquetes del 49%. Al comparar esta prueba con la Tabla 3-28 se observa que cuando el tráfico excede el valor del CIR, la política de modelado actúa, manteniendo el bitrate y descartando de forma aleatoria aquellos paquetes que saturen el nivel de tráfico que no puede ser manejado en la cola.

La Figura 3-63 muestra el proceso de registro de un usuario SIP en IMS en el escenario con conectividad inter-AS seamless MPLS L3VPN con QoS, donde se puede observar un tiempo de registro de 0.502628504s entre la respuesta 200 OK y el método REGISTER enviado al P-CSCF del core IMS.

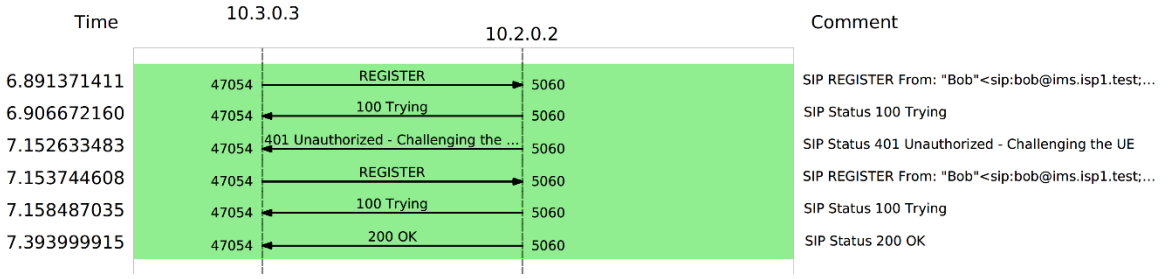


Figura 3-63 Registro SIP UE con conectividad inter-AS seamless MPLS L3VPN con QoS

La Figura 3-64, muestra los detalles de la llamada entre usuarios SIP, de Alice a Bob, con conectividad inter-AS seamless MPLS L3VPN con QoS, con un total de 26 paquetes generados y una duración de 31s.

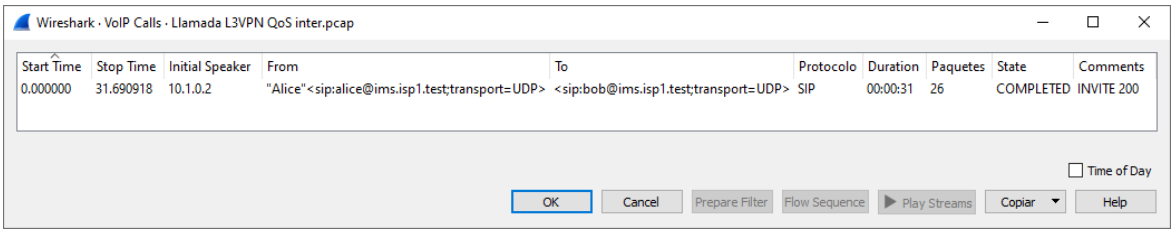


Figura 3-64 Detalles de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS

La Figura 3-65 muestra el flujo de señalización SIP para una llamada entre usuarios con conectividad inter-AS seamless MPLS L3VPN con QoS. Se observa un tiempo de establecimiento de llamada, entre el método INVITE SDP originado por el usuario Alice hacia el usuario Bob y la confirmación de la negociación de los códecs de voz mediante SDP en la respuesta ACK al código 200 OK enviada por el usuario Alice hacia el usuario Bob, de 1.855711s. La llamada tiene una duración efectiva de 29.835207s, estimada entre el primer mensaje RTP, enviado desde el usuario Alice hacia Bob, hasta la confirmación de la terminación de la llamada con el método BYE y respuesta 200 OK enviado por el usuario Alice hacia el usuario Bob, lo que da una duración total de la llamada de 31.690918s que se valida por la Figura 3-27.

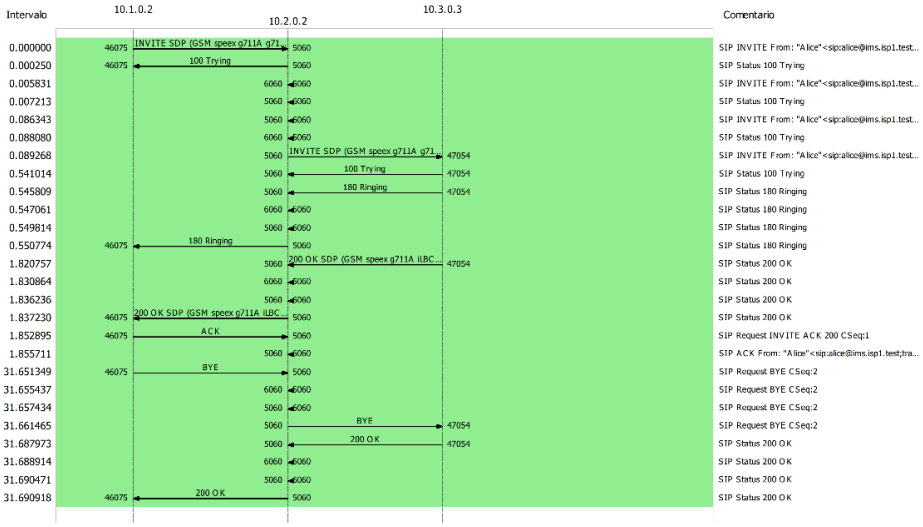


Figura 3-65 Llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS

La Figura 3-66 muestra la evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS en HOMER SIP. Esta se realiza sobre los

paquetes RTP que transportan la conversación y que fueron transmitidos en la llamada. Al respecto se observa que en relación con los parámetros de QoS, en la llamada se generó un promedio de 880.92 paquetes RTP en el tiempo que duró la llamada. El jitter promedio fue de 94.1ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.18 en el MOS, parámetro que está definido por la QoE y que es subjetivo.

Figura 3-66 Evaluación de la llamada entre usuarios SIP con conectividad inter-AS seamless MPLS L3VPN con QoS en HOMER SIP

Para el servicio de IPTV, se observa en la Figura 3-67 se realiza una conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine.

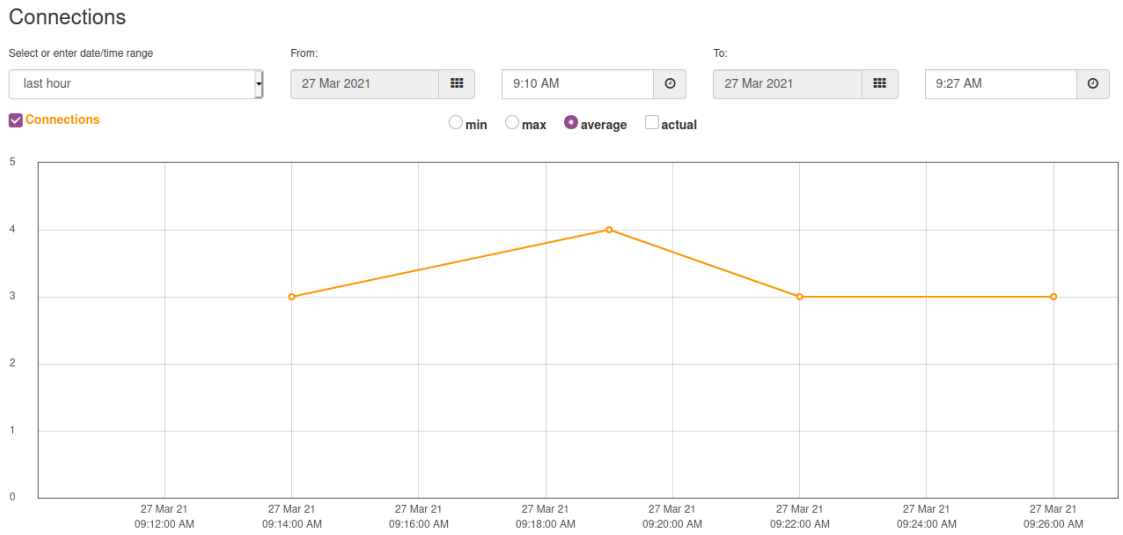


Figura 3-67 Conexión al servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

En la Figura 3-68 se observa un promedio de ancho de banda utilizado de 3.880Mbits/seg por el canal de streaming rtsp://10.2.0.3:1935/live/001.stream en el UE.

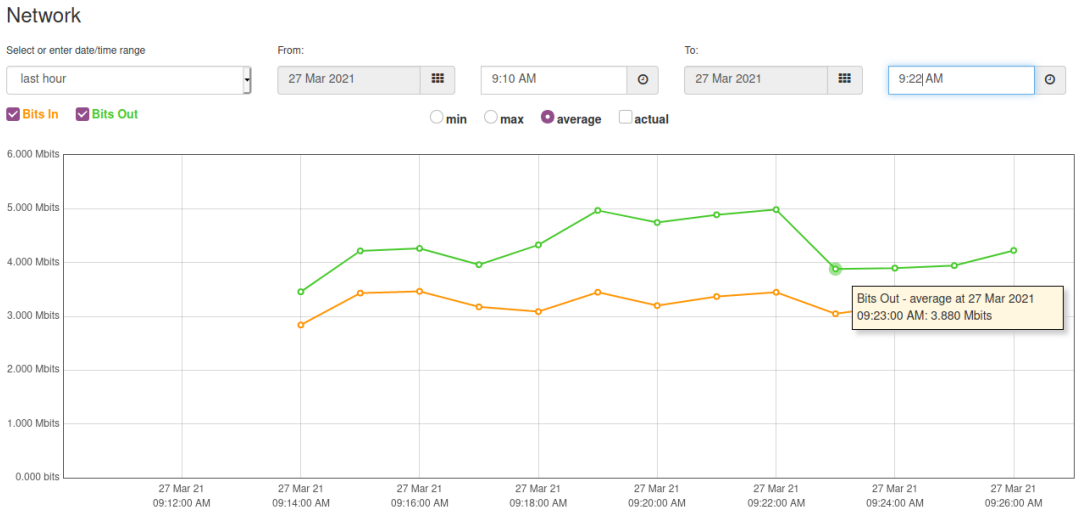


Figura 3-68 Ancho de banda utilizado en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

En la Figura 3-69, se observa que en el video reproducido en el UE no se presentan problemas de pérdidas de cuadros del video, congelamiento de imagen, sin embargo, se presentan cortes en el sonido de manera esporádica.

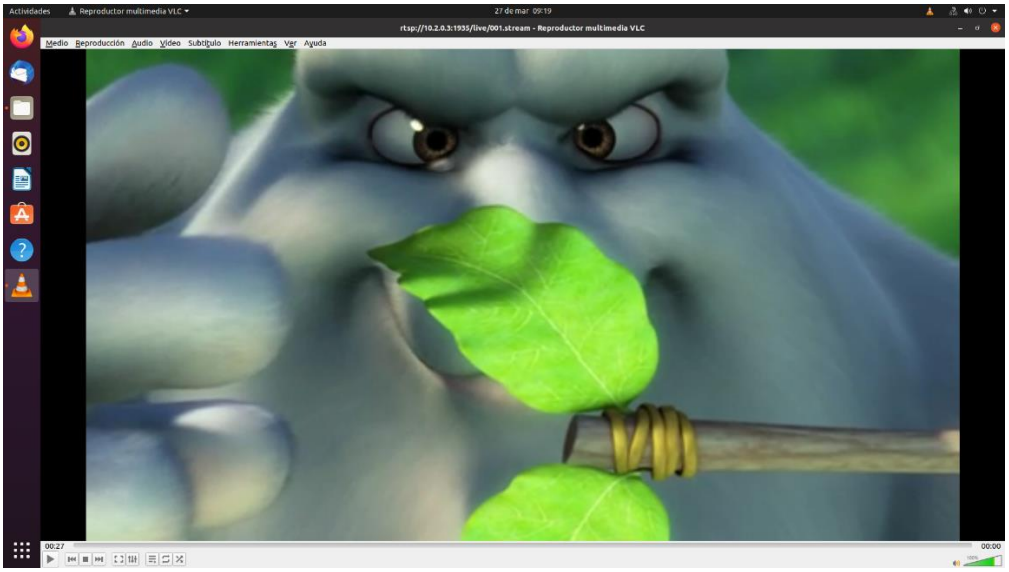


Figura 3-69 Reproducción de video en el servicio de streaming en IPTV con conectividad inter-AS seamless MPLS L3VPN con QoS en Wowza Streaming Engine

3.10.6 Análisis comparativo de los escenarios L3VPN intra-AS e inter-AS con QoS

La Tabla 3-30 muestra un resumen de los valores obtenidos de RTT en prueba ping y Saltos de red en prueba traceroute para L2VPN y L3VPN sin y con QoS.

Tabla 3-30 Resumen de valores obtenidos de RTT en prueba ping y Saltos de red en prueba traceroute para L2VPN y L3VPN sin y con QoS

Descriptor		RTT (ms)		Saltos de red	
		Sin QoS	Con QoS	Sin QoS	Con QoS
L2VPN	Intra-AS	3.762	4.449	3	
	Inter-AS	5.600	4.718		
L3VPN	Intra-AS	4.665	3.406	7	
	Inter-AS	4.442	23.067	9	

Los resultados obtenidos en las pruebas de conectividad mediante la herramienta ping, muestran que el escenario intra-AS presenta un menor retardo de ida y vuelta (3.406ms) con respecto al escenario inter-AS (23.067ms).

Con las pruebas de saltos de red mediante la herramienta traceroute, se encuentra que el escenario intra-AS presenta menos saltos de red (siete saltos) con respecto al escenario inter-AS (nueve saltos).

Con respecto al jitter y las pérdidas de paquetes, en las pruebas realizadas en iPerf3 limitando el ancho de banda al valor del CIR de 17 Mbps, se encuentra que en el escenario intra-AS se tiene un jitter de 1.019ms y unas pérdidas de paquetes del 3.9% y para el escenario inter-AS se tiene un jitter de 1.072ms y unas pérdidas de paquetes del 4.9%. Al limitar el ancho de banda al valor del PIR de 32Mbps, se encuentra que en el escenario intra-AS se tiene un jitter de 0.883ms y unas pérdidas de paquetes del 49% y en el escenario inter-AS se tiene un jitter de 1.039ms y unas pérdidas de paquetes del 49%.

Con respecto al servicio de voz, se observa que en conectividad intra-AS se tiene tiempo de registro en SIP de 0.999093408s, mientras que en la conectividad inter-AS L2VPN es de 0.502628504s. En el escenario intra-AS, el jitter promedio fue de 57.67ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.29 en el MOS y en el escenario inter-AS, el jitter promedio fue de 94.1ms, no hubo pérdida de paquetes y la llamada obtuvo un puntaje promedio de 4.18 en el MOS.

Para el servicio de video en streaming en IPTV, se observa que tanto para la conectividad intra-AS como inter-AS no se tienen problemas de pérdida de imágenes y congelamiento en el video, sin embargo, se presentan cortes en el sonido para ambos casos. Se observa una utilización de ancho de banda de 3.960Mbps en promedio para la conectividad intra-AS y de 3.880Mbps para la conectividad inter-AS utilizando el códec de video MPEG-4.

4. Definición de los lineamientos técnicos para la provisión de QoS extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios de voz, datos y video

En este capítulo se definen los lineamientos técnicos para la provisión de QoS extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS) para los servicios de voz, datos y video, donde se identifican los actores del negocio y las relaciones que se establecen para la suscripción y prestación de servicios, los aspectos que definen la QoS en interconexión en NGN, el entorno regulatorio definido por la UIT a nivel internacional, por la CRC a nivel nacional, y las metodologías para el aseguramiento de la QoS y la QoE, en donde se abordan los sistemas de medición, el modelo de red para mediciones de la QoS y las metodologías de evaluación de la calidad.

4.1 Actores del negocio y relaciones

En el sector de las telecomunicaciones, los actores involucrados en interconexión y las relaciones que existen entre ellos, para la suscripción y prestación de servicios, se describen en la Figura 4-1 de acuerdo con lo observado en [26].

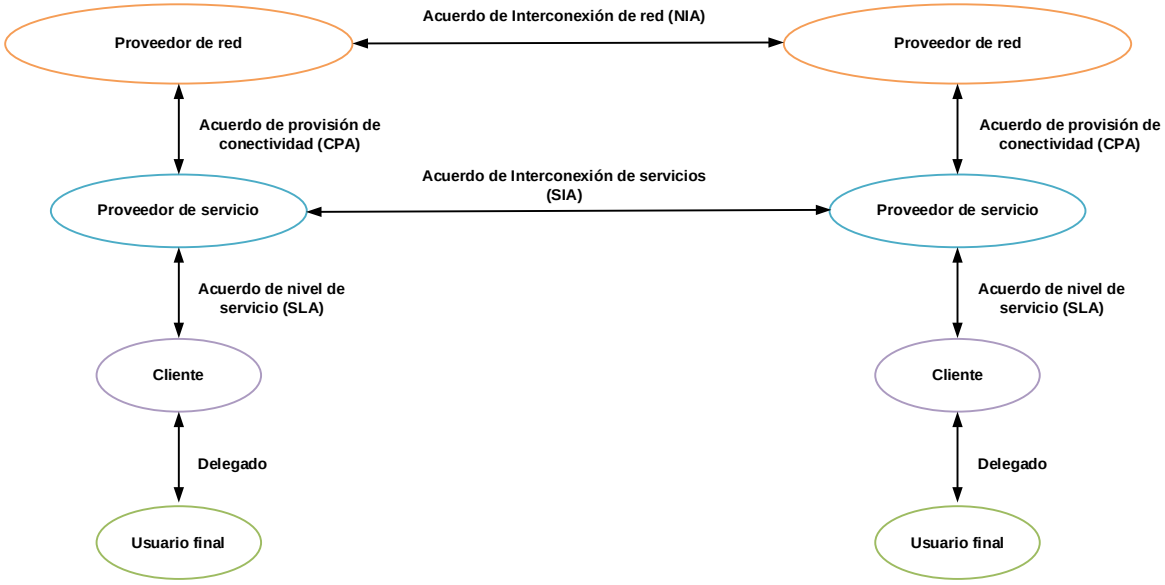


Figura 4-1 Actores del negocio y relaciones [26]

4.1.1 Actores del negocio

Se definen los actores de la siguiente manera [26]:

- **Proveedor de red:** es la entidad responsable de mantener y administrar el conjunto de recursos y capacidades para la entrega de servicios de conectividad en capa 2 y en capa 3 del modelo OSI. Los proveedores de servicios utilizan las capacidades subyacentes de los proveedores de red para la entrega de servicios de valor agregado.
- **Proveedor de servicio:** es la entidad que administra un conjunto de equipos y recursos específicos de los servicios, tales como la facturación, la autenticación, los perfiles de los clientes en bases de datos, donde se interactúa con la entrega de los servicios de valor agregado, entre otros, poniendo a disposición de los clientes el portafolio de servicios. Este portafolio es un paquete de capacidades que resultan del proceso de ingeniería de un conjunto de recursos y equipos.

- **Cliente:** el cliente denota la entidad del negocio que suscribe una oferta de servicios entregada por un proveedor de servicios. Un servicio ofrece diversas características funcionales de acuerdo con las necesidades del cliente.
- **Usuario final:** es la entidad que invoca y consume un servicio, debido al SLA negociado por el cliente. Generalmente el usuario final y el cliente son entidades que pueden llegar a ser la misma indistintamente, sin embargo en [26] se aclara que el cliente es la entidad que suscribe una oferta de servicios, la cual es manejada y ofertada por el proveedor de servicios. El usuario final se refiere a aquellas personas que utilizan el servicio y que son delegadas por el cliente, quien es el responsable legal en relación con la utilización del servicio de acuerdo con los SLA suscritos con el proveedor de servicio.

4.1.2 Relaciones entre los actores del negocio

Se definen las relaciones entre los actores del negocio de la siguiente manera [26]:

- **Acuerdo de nivel de servicio (SLA):** Como se ha mencionado un SLA es un contrato acordado entre un cliente y un proveedor de servicio. Este acuerda el derecho de consumo de un servicio, en el que se definen las cláusulas administrativas y técnicas detalladas en un contrato, definiendo el alcance de los servicios entregados y las garantías asociadas.
- **Acuerdo de provisión de conectividad (CPA):** Para poder entregar sus servicios, el proveedor de servicios debe confiar en las capacidades subyacentes que son gestionadas por el proveedor de red. Esas capacidades son utilizadas debido a la suscripción de un acuerdo dedicado, llamado acuerdo de provisión de conectividad, donde la conectividad se refiere a la capacidad de alcanzar y transferir recursos resultado de la interconexión de los diferentes nodos que conforman la red para asegurar la prestación de un servicio. En el CPA se define el alcance de los servicios de conectividad y garantías asociadas, incluyendo la QoS y la disponibilidad.
- **Acuerdo de interconexión de red (NIA):** Los proveedores de red, con el objetivo de extender el alcance de los servicios de conectividad más allá de sus propios dominios administrativos, generan acuerdos de interconexión de red con otros

proveedores de redes que pueden actuar en diferentes segmentos, tales como la red de acceso o la red de núcleo, los cuales proveen el tránsito provisional de servicios. En estos acuerdos se deben especificar aspectos técnicos, económicos y administrativos relacionados con la interconexión.

- **Acuerdo de interconexión de servicios (SIA):** Los acuerdos de interconexión de servicios son negociados entre dos proveedores de servicio. Estos acuerdos toman lugar para extender el alcance de un servicio y extender la entrega de este, más allá del dominio administrativo del proveedor de servicios. Un SIA debe describir el alcance de la interconexión, la QoS, la disponibilidad, y cláusulas administrativas y técnicas.

4.2 Aspectos de la QoS en interconexión en NGN

Dentro de los aspectos que definen la QoS en interconexión en NGN se encuentran desafíos técnicos, comerciales y regulatorios (ver Figura 4-2) de acuerdo con [50].

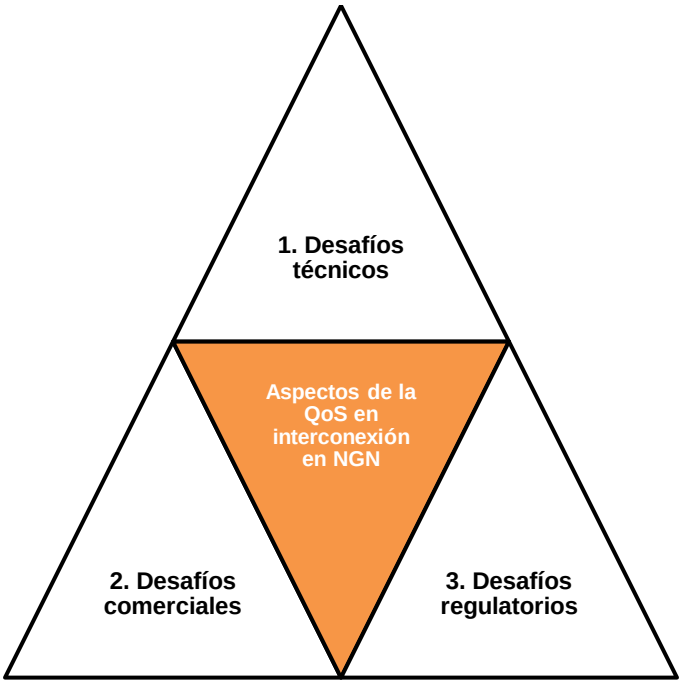


Figura 4-2 Aspectos de la QoS en interconexión en NGN [63]

4.2.1 Desafíos técnicos

Se observan los siguientes desafíos desde la perspectiva técnica de la QoS tradicional de acuerdo con [117]:

- Desafío de integración: Falta de consideración sobre cómo hacer uso de varios esquemas de control de tráfico.
- Desafío de la complejidad: Falta de compensación explícita entre el beneficio de varios esquemas de control de tráfico y su complejidad.
- Desafío de interoperabilidad: Falta de arreglo comercial de QoS entre operadores.
- Desafío contable: No existe una contabilidad separada de las diferentes clases de ancho de banda. Hoy en día, solo se contabiliza el ancho de banda total utilizado en la interfaz de usuario. Si la facturación del usuario se basa en el uso, entonces dicho ancho de banda se utilizará para fines de facturación.
- Desafío de diferenciación: Falta de diferenciación perceptible por el usuario final entre mejor esfuerzo y las múltiples clases de servicios.

4.2.2 Desafíos comerciales

Se observan los siguientes desafíos comerciales de acuerdo con [117]:

- Existe un dilema con respecto a quién debe obtener QoS, los clientes que lo necesitan o los clientes que están dispuestos a pagar por ello.
- Vender QoS después de vender conectividad de red implica dos ventas.
- La competencia dificulta la venta de QoS además de la conectividad de red, porque los competidores pueden atacar la calidad del servicio básico.
- A los proveedores de servicio les gustaría cobrar QoS a empresas como los proveedores de contenido de Internet (ICP). Sin embargo, la controversia sobre la neutralidad de la red puede evitar que eso suceda. Incluso sin neutralidad en la red, las tecnologías de multidifusión y P2P plantearán desafíos para ofrecer QoS a las empresas. Cobrar QoS a los consumidores es menos atractivo económicamente y puede requerir un mecanismo de señalización, que no existe hoy en día con el propósito de priorizar el tráfico en la entrada de la red.
- Hay una falta de acuerdo de QoS entre proveedores. Esto impide que los SP cooperen en QoS y dificulta que los SP comercialicen la QoS. Incluso si existen acuerdos de QoS entre proveedores, la coordinación requerida entre los SP sería complicada y costosa.

4.2.3 Desafío regulatorio

Se observan los siguientes desafíos regulatorios de acuerdo con [50] y [117]:

- Régimen de interconexión: El régimen de interconexión debería proporcionar incentivos para invertir en QoS, pero también considerar la complejidad de la implementación regulatoria.
- Parámetros de QoS:
  - No existen estándares que garanticen la QoS de un extremo a otro en las redes establecidas para redes NGN interconectadas.
  - Solo los acuerdos bilaterales (SLA) facilitan la QoS.
  - Deben definirse los parámetros mínimos de calidad: ancho de banda, retardo, jitter, pérdida de paquetes, ...
- Medidas de QoS: Se necesitan procedimientos de medición adecuados para garantizar los parámetros de QoS. Las preguntas clave que deben abordarse son:
  - ¿Se cumplen los compromisos de servicio?
  - ¿Quién proporciona las estadísticas para esto?
  - ¿Se puede divulgar suficiente información?
  - ¿Cuáles son las responsabilidades y la compensación cuando no se cumplen los compromisos?
  - ¿Quién supervisa?

4.3 Entorno regulatorio

El objetivo primordial de la regulación es asegurar que los clientes de un proveedor de servicios obtengan la calidad propia de los servicios que consumen de manera satisfactoria, en función del precio que están pagando por su aprovisionamiento. Se define el alcance de la regulación de la QoS, en las que se contempla [25]:

- Ayudar a los clientes de los proveedores de telecomunicaciones a tomar decisiones informadas.
- Verificar las reclamaciones de los operadores.
- Entender el estado del mercado de telecomunicaciones.
- Mantener o mejorar la QoS en presencia de competidores.
- Mantener o mejorar la QoS en ausencia de competidores.

- Ayudar a los operadores de telecomunicaciones a lograr una competencia justa.
- Ayudar a las redes interconectadas a trabajar en conjunto por el aseguramiento de la QoS extremo a extremo.

Tomando en cuenta los objetivos descritos, la UIT define un conjunto de actividades que se deben adoptar por el ente nacional, adoptándolo a su contexto.

4.3.1 Regulación de la QoS definida por la UIT

En [25] se observan las actividades definidas por la UIT en [31], de acuerdo con la **Figura 4-3**, de manera periódica para la autoridad nacional reguladora (NRA).

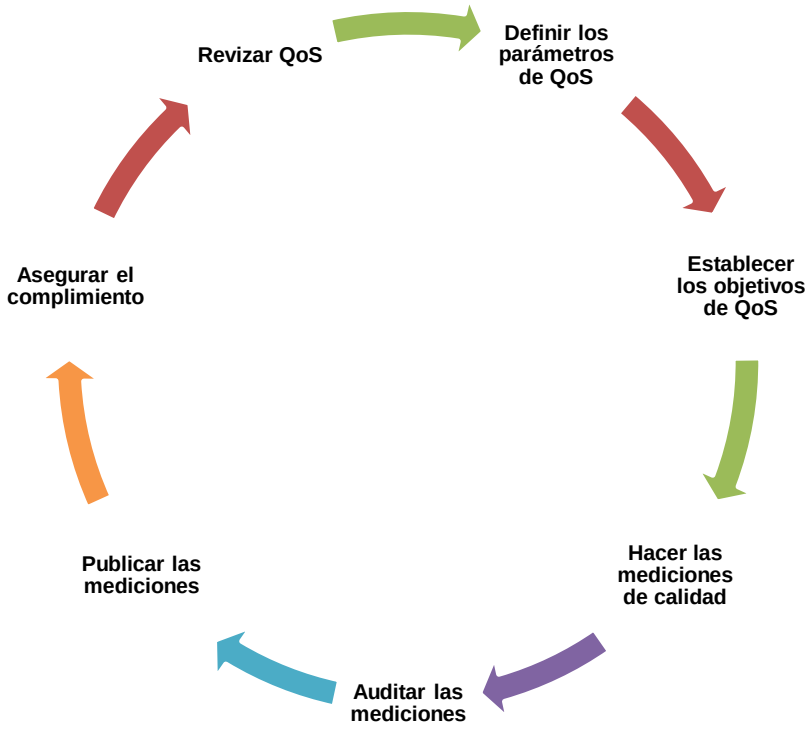


Figura 4-3 Actividades de regulación de la QoS definidas por la UIT [25]

A continuación, se definen las actividades:

- **Definir los parámetros de QoS:** Los parámetros de QoS que son sujeto de monitoreo y/o aplicación son definidas por la NRA previa consulta con los operadores de dicho país.

- **Establecer los objetivos de QoS:** Los valores objetivo para los parámetros definidos de QoS también son establecidos por la NRA, basados en la consulta a los operadores y a la información obtenida del monitoreo de los datos de mediciones recolectadas y consultas de los estándares y mejores prácticas a nivel nacional, regional y global.
- **Hacer las mediciones de calidad:** Las mediciones pueden ser hechas por el operador de telecomunicaciones, la NRA, agencias de medición externas o usuarios finales.
- **Auditar las mediciones:** La verificación de las mediciones puede ser realizada por los empleados de los operadores de telecomunicaciones, dentro de un proceso de auto certificación, o pueden ser auditadas por una agencia de auditoría de QoS externa, o revisadas por la NRA.
- **Publicar las mediciones:** Por lo general los resultados de las mediciones de la QoS deben ser publicados por la NRA para ofrecer una comparación de los niveles de QoS provistos por los diferentes operadores de telecomunicaciones.
- **Asegurar el cumplimiento:** Se pueden encontrar diferentes metodologías definidas por la NRA, con diferentes medidas establecidas para asegurar el cumplimiento del aseguramiento de la QoS a través de multas, sanciones o penalizaciones.

4.3.2 Documentos de la CRC relacionados con los indicadores de calidad

La Tabla 4-1 muestra los documentos definidos por la CRC en Colombia relacionados con los indicadores de calidad, en los que se resalta la resolución 3067 de 2011 y las resoluciones 4000 de 2012 y 4007 de 2012, y la resolución 3101 de 2011 por la cual se expide el régimen de acceso, uso e interconexión de redes de telecomunicaciones, entre otras relacionadas, vigentes para la fecha de elaboración de la presente investigación, las cuales establecen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones a cumplir por parte de los operadores de telecomunicaciones.

Tabla 4-1 Documentos de la CRC relacionados con los indicadores de calidad e interconexión [118]

Año	Documento	Restrictor
2007	Resolución 1740 de 2007 Comisión de Regulación de Telecomunicaciones	Define los indicadores de calidad para los servicios de telecomunicaciones, aplicable a todas las redes y los servicios de telecomunicaciones del Estado, salvo los servicios de Televisión consagrados en la Ley 182 de 1995 y sus modificaciones, y los servicios de Radiodifusión Sonora, Auxiliares de Ayuda y Especiales de que trata el Decreto-ley 1900 de 1990. El régimen de calidad establecido, deberán cumplirlo los operadores de servicios públicos y redes de telecomunicaciones en su relación con los usuarios de los servicios. Señala las obligaciones generales de los operadores, las obligaciones de calidad para el servicio de valor agregado de acceso a internet, las obligaciones de calidad para servicios de TMC, PCS y Trunking, las obligaciones de calidad para servicios de TPBC, y dicta disposiciones sobre el control y vigilancia y el plazo de implementación de las medidas adoptadas en la presente resolución.
2009	Resolución 2091 de 2009 Comisión de Regulación de Telecomunicaciones	Modifica el Anexo 2 de la Resolución CRT 2030 de 2008, que define los indicadores de calidad para los servicios de telecomunicaciones, aplicable a todas las redes y los servicios de telecomunicaciones del Estado, salvo los servicios de Televisión consagrados en la Ley 182 de 1995 y sus modificaciones, y los servicios de Radiodifusión Sonora, Auxiliares de Ayuda y Especiales de que trata el Decreto-ley 1900 de 1990.
2010	Resolución 2352 de 2010 Comisión de Regulación de Comunicaciones	Modifica las resoluciones CRT 1740 DE 2007 y 1940 de 2008.
2010	Resolución 2353 de 2010 Comisión de Regulación de Comunicaciones	Establece la metodología para la medición del nivel de satisfacción del usuario de los servicios TPBCL y TPBCLE. De igual forma, recoge el procedimiento para el cálculo del factor de calidad.
2011	Resolución 3067 de 2011 Comisión de Regulación de Comunicaciones	Define los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones. El régimen de calidad definido en esta resolución aplica a todas las redes y los servicios de telecomunicaciones del Estado, independientemente del tipo de habilitación que ostenta el proveedor, exceptuando los Servicios de Televisión consagrados en la Ley 182 de 1995 y sus modificaciones, Servicios Auxiliares de Ayuda y Especiales y los Servicios de Radiodifusión Sonora de que trata la Ley 1341 de 2009.
2011	Resolución 3101 de 2011 Comisión de Regulación de Comunicaciones	Por medio de la cual se expide el régimen de acceso, uso e interconexión de redes de telecomunicaciones, y se dictan otras disposiciones. Establece reglas para los proveedores de redes y servicios de telecomunicaciones y a aquellos proveedores que hacen uso de dichas redes, exceptuando las redes de telecomunicaciones que no se utilicen para suministrar servicios al público. Entre otros: trae algunas definiciones, principios y obligaciones (Cap. I); regula el régimen de interconexiones (Cap. II) y de acceso (Cap. III); además establece los parámetros para las instalaciones esenciales para acceso y/o interconexión (Cap. IV),

Año	Documento	Restrictor
		así como para la oferta básica de interconexión y solicitudes de acceso e interconexión (Cap. V); establece obligaciones derivadas del acceso y/o interconexión (Cap. VI); y las obligaciones de información de los proveedores de redes y servicios de telecomunicaciones (Cap. VII).
2011	Resolución 3503 de 2011 Comisión de Regulación de Comunicaciones	Definen las condiciones de calidad para el servicio de acceso a Internet, se modifican las Resoluciones CRC 3067 y 3496 de 2011 y se dictan otras disposiciones.
2012	Resolución 4000 de 2012 Comisión de Regulación de Comunicaciones	Modifica las Resoluciones CRC 3067 y 3496 de 2011, dispone sobre las comunicaciones de voz a través de redes móviles y la obligación de reportar los indicadores de calidad para las comunicaciones de voz a través de redes móviles, en municipios con una población superior a cien mil (100.000) habitantes y en capitales con una población superior a quinientos mil (500.000) habitantes, deberá cumplirse por parte de los proveedores de redes y servicios a partir del 1° de enero de 2013, por lo que los reportes correspondientes al periodo comprendido entre los meses de septiembre y diciembre del año 2012 serán realizados tal y como se efectuó en el periodo comprendido entre los meses de enero y agosto de 2012.
2012	Resolución 4007 de 2012 Comisión de Regulación de Comunicaciones	Hace una Fe de Erratas a la Resolución número CRC 4000 de 2012.
2016	Resolución 5050 de 2012 Comisión de Regulación de Comunicaciones	Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones.
2020	Resolución 1272 de 2020 Ministerio de Tecnologías de la Información y las Comunicaciones	Realiza definiciones de acceso universal, servicio universal y elimina la definición de interconexión e interoperabilidad, del glosario de definiciones de la Resolución 202 de 2010.

4.4 Metodologías para el aseguramiento de la QoS y la QoE

El principal objetivo de las mediciones de calidad es proveer información a los clientes, potenciales clientes y proveedores de servicio. Las mediciones de calidad pueden ser usadas para la generación de reportes a los clientes sobre la entrega de servicios, o para atraer a nuevos clientes enfocándose en la calidad. Los proveedores de servicio y terceras partes deben utilizar las mediciones de calidad para el diseño y la oferta de servicios, para la resolución de problemas, para propósitos de marketing, así como para la planeación de la capacidad y desarrollo de servicios futuros de acuerdo con [25].

4.4.1 Sistemas de medición de QoS/QoE

Los sistemas de medición proveen una entrada de datos para el dimensionamiento de la red y para la mejora en la capacidad y la optimización de esta. Con el objetivo de que las mediciones sean comparables, las mediciones deben ser repetibles independientemente si son efectuadas por la misma entidad u otra. Además, las mediciones del sistema deben ser aplicables para diferentes tipos de tráfico, diferentes tecnologías de capa de enlace y diferentes tipos de redes IP. Para asegurar la QoS el sistema tiene que ser confiable y las mediciones comparables con los objetivos de los SLA. Los sistemas de medición deben tomar en cuenta los siguientes requerimientos [25]:

- **Precisión:** Los resultados de las mediciones deben ser confiables, reproducibles y consistentes en el tiempo para los indicadores de QoS y QoE.
- **Comparabilidad:** Los indicadores claves de desempeño (KPI), definidos por la NRA, deben poder compararse independientemente del proveedor de servicio, o del mismo servicio provisto por proveedores de diferentes regiones.
- **Confiabilidad:** Los componentes del sistema de medición deben ser confiables a lo largo del tiempo, basado en procedimientos acordados y deben estar protegidos contra ataques de seguridad, que pueden poner en peligro la integridad de los resultados.
- **Apertura:** se refiere a la disponibilidad de los detalles de una medición, el sistema de medición de calidad debe estar basado en especificaciones, estándares, recomendaciones y mejores prácticas.
- **Pruebas futuras:** los sistemas de medición deben ser flexibles, extensibles y escalables en relación con la introducción de nuevos escenarios de pruebas. En este sentido el sistema debe ser costo-efectivo.

Los sistemas de medición pueden emplear dos métodos de medida [25]:

- **Método de medición pasivo:** Este tipo de medición está basado en la observación de los paquetes de datos de los usuarios en un enlace de red, de manera no intrusiva, recolectando la información estadística de los parámetros de calidad mediante un monitoreo o sniffing.

- **Método de medición activo:** En este caso se despliegan estaciones de prueba con agentes basados en software o dispositivos de hardware en los elementos de red del operador. Las fuentes de tráfico y los sumideros de los paquetes se pueden separar en dispositivos de medición o nodos de red que pueden ser habilitados para las tareas de medición, transportando los datos del tráfico y realizando tareas de medición de la QoS de forma simultánea.

La Tabla 4-2 muestra el intervalo de confianza y tamaños de las muestras para las mediciones desde el punto de vista estadístico, que deben tener en cuenta los operadores con el ánimo de obtener resultados confiables y comparables [25].

Tabla 4-2 Intervalo de confianza y tamaños de las muestras para las mediciones [25]

Característica	Valor			
Nivel de confianza	95%			
Grado de variabilidad	0.5			
Nivel de precisión	±3%	±5%	±7%	±10%
Número requerido de muestras	1067	384	196	96

4.4.2 Modelo de red para mediciones de la QoS

En la Figura 4-4 se ilustra el modelo de red para mediciones de la QoS, donde se plantea la realización de mediciones entre los mismos dispositivos finales para cada tipo de tráfico de cliente. Estos dispositivos finales son los terminales del cliente (TE – Terminal endpoint), router de borde del cliente (CE – Customer Edge), o router de borde del proveedor (PE – Provider Edge). La red IP se encuentra dividida en segmentos, en los que se incluye la red de acceso, la red de núcleo (segmentos de ingreso y egreso) y redes de tránsito. El punto de interconexión (POI) de la red de acceso y la red regional es referida como punto de demarcación (POP). Los proveedores ofrecen servicios entre diferentes puntos finales que incluyen los siguientes casos [25]:

- **Servicios de borde a borde:** En este caso los puntos de demarcación son los routers de borde del proveedor (PEs).
- **Servicios de sitio a sitio:** En este caso los servicios se extienden al punto de borde del cliente (CEs).
- **Servicios de terminal a terminal:** En este caso los servicios se extienden a los terminales de los clientes (TEs).

Teniendo en cuenta los tipos de servicios ofrecidos por los proveedores, se define el posicionamiento de las mediciones, donde cada segmento es monitoreado de forma independiente según el caso [25].

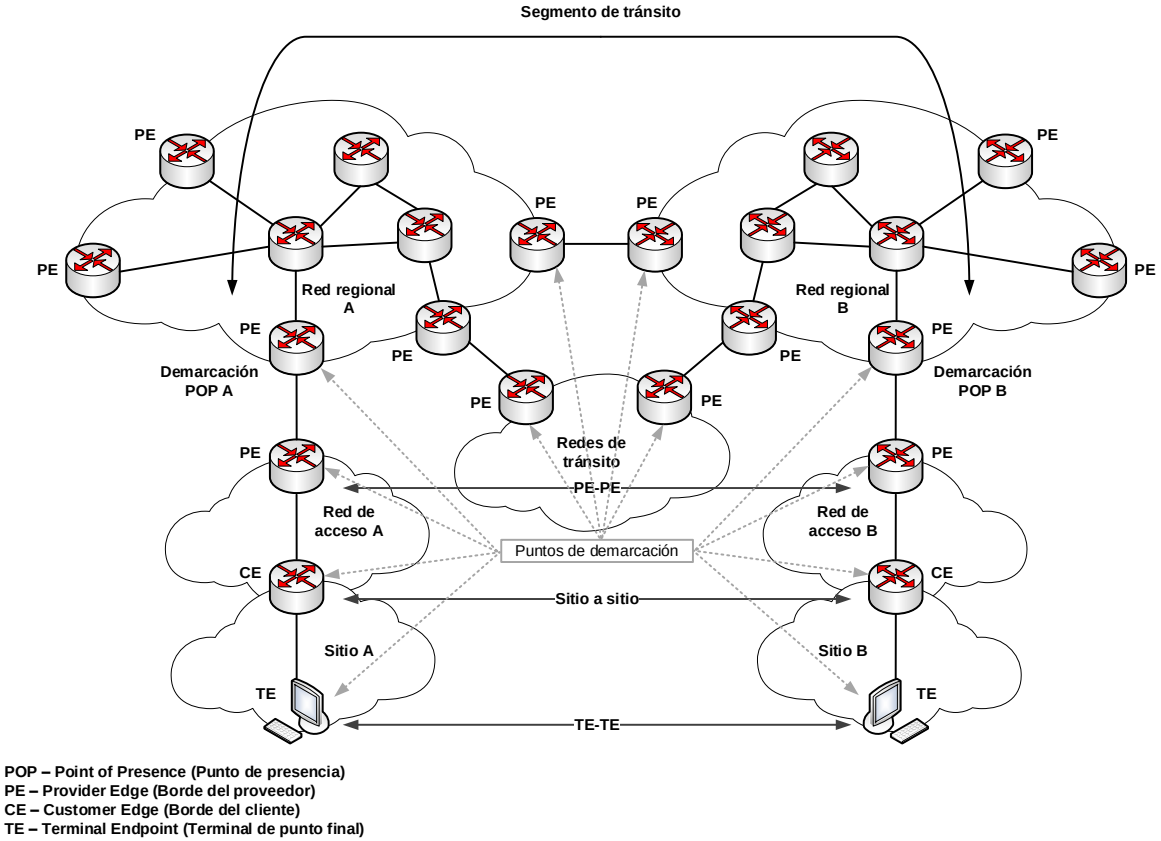


Figura 4-4 Modelo de red para mediciones de QoS [25]

4.4.3 Metodologías de evaluación de la calidad

Se tienen dos metodologías de evaluación de la calidad de acuerdo con [25]:

- **Método de evaluación subjetivo:** En este caso los servicios consumidos de audio o de video, son evaluados en términos subjetivos bajo diferentes condiciones de prueba, en los que se requieren habitaciones a prueba de sonido o dispositivos profesionales audiovisuales. Como se observó anteriormente en la sección 1.4.3, el parámetro MOS es el más utilizado como métrica de evaluación de la QoE, de acuerdo con el promedio subjetivo de las opiniones percibidas en cuestionarios aplicados a los clientes con relación a los servicios entregados.

- **Método de evaluación objetivo:** En este método se encuentran todos los parámetros de QoS abordados en esta investigación, sin embargo, también se pueden encontrar modelos que evalúan la QoE basados en estimaciones estadísticas, tales como, modos de prueba intrusiva, modos de prueba no intrusiva y modos de planeación o diseño de sistemas de telecomunicaciones.

Con base en los métodos de evaluación definidos, en la Figura 4-5 se muestran los análisis de las percepciones del cliente y el proveedor de servicio en relación con el desempeño de los servicios y la red, con el objetivo de tomar las acciones correctivas o proactivas necesarias para mejorar la calidad de acuerdo con el diseño y optimización de la red.

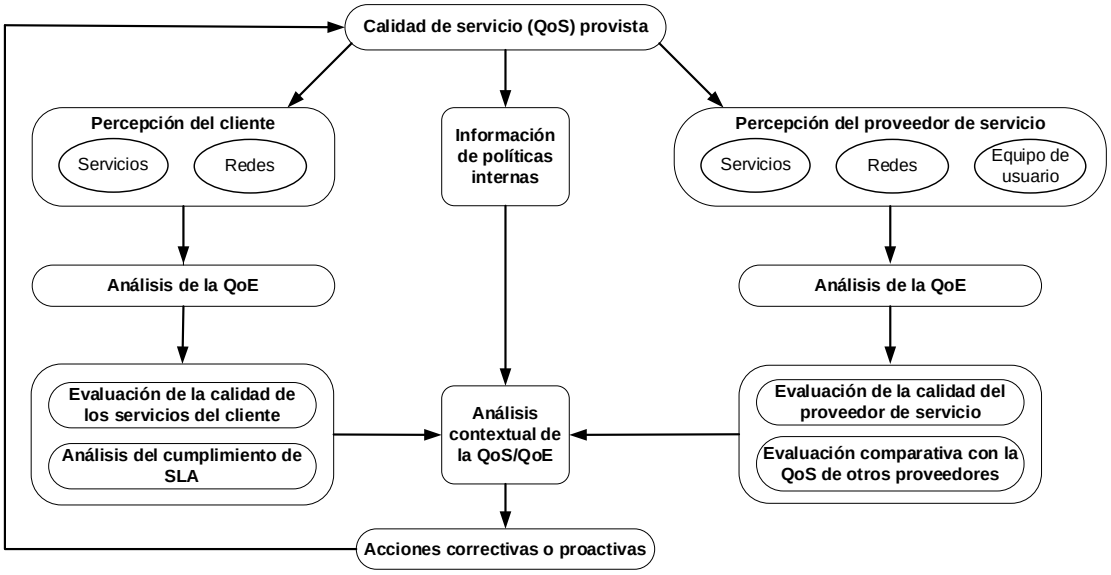


Figura 4-5 Percepciones del cliente y el proveedor de servicio [25]

4.5 Proceso para la provisión de QoS extremo a extremo

De acuerdo con [119], la QoS es una tarea de ingeniería que permite que múltiples tecnologías de red trabajen juntas de una manera consistente para ofrecer un comportamiento de red predecible, donde para tener un esquema de servicio de QoS de extremo a extremo en la red, todos los elementos de la red deben estar armonizados para preservar la configuración de QoS a medida que atraviesan la red en la pila de protocolos y a través de los elementos de la red independientemente del tipo de nodo, esto incluye el siguiente paso a paso descrito en la Figura 4-6, donde estas funciones se ejecutan en el

borde de los dominios de la red (nodos de entrada/salida) y pocas de ellas en los nodos de tránsito (clasificación y encolamiento/transmisión). Esto permite acelerar el procesamiento en la red:

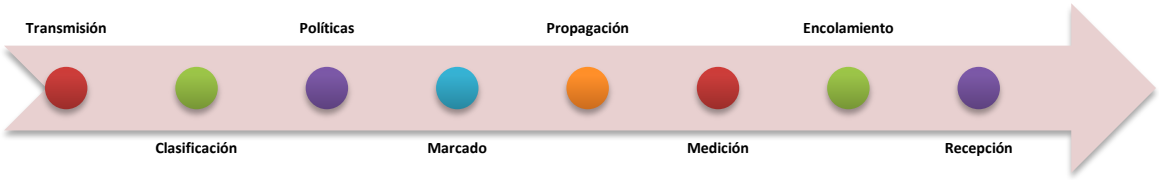


Figura 4-6 Proceso para la provisión de QoS extremo a extremo [119]

- **Clasificación:** Todos los paquetes de la red deben ser clasificados según la aplicación (voz, datos, video, etc.)
- **Políticas:** El ancho de banda se aplicará en el puerto de entrada. es decir, asignación de bloques de recursos del planificador de enlace ascendente.
- **Marcado:** Asegura que los paquetes tengan la configuración de QoS adecuada.
- **Propagación:** El marcado de QoS debe ser coherente a medida que atraviesan diferentes dominios de red (redes inalámbricas, IP, Ethernet o MPLS) y a medida que avanzan en la pila de protocolos (IP → Ethernet → MPLS → Ethernet). El objetivo es garantizar que la configuración de QoS en la capa de transporte sea coherente con la capa de aplicación del modelo OSI.
- **Medición:** El ancho de banda se aplicará en el puerto de salida, donde por ejemplo se asigna un bloque de recursos en el programador de enlace descendente.
- **Encolamiento:** Todos los paquetes se acumulan temporalmente en una cola hasta que se transmiten por cable o aire. Cada interfaz tiene múltiples colas para almacenar las tramas a transmitir con diferentes prioridades. En la red inalámbrica, los programadores de enlace descendente y ascendente admiten diferentes disciplinas de programación 3GPP. Para Ethernet y redes de transporte, los

enrutadores y conmutadores admiten múltiples técnicas de programación IETF/RFC, es decir, RFC7141.

- **Transmisión/Recepción:** Es la acción de serializar los datos en las interfaces físicas, por lo tanto, este paso agrega retraso en el proceso y depende en gran medida de la velocidad de la interfaz, es decir, 10 Gbps o 1 Gbps.

4.6 Lineamiento técnico

Para la provisión de QoS extremo a extremo en interconexión bajo IP Multimedia Subsystem en los servicios de voz, datos y video, se definen el siguiente lineamiento acor de a la Figura 4-7:

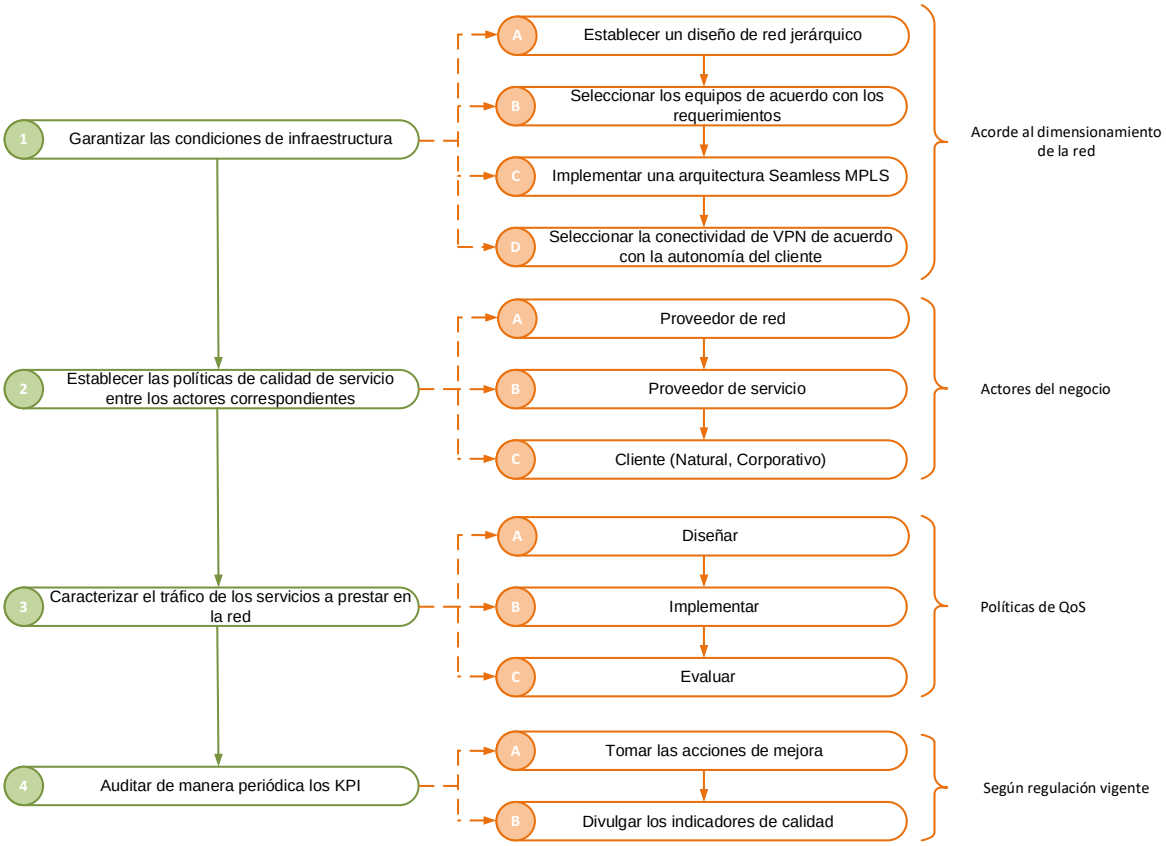


Figura 4-7 Lineamiento técnico

1. Garantizar las condiciones necesarias para la operatividad de la red, entre las cuales se encuentran los elementos de alimentación eléctrica, refrigeración, temperatura, sistemas mecánicos, elementos arquitecturales, entre otros relacionados, de acuerdo con las condiciones de infraestructura en la cual son

instalados los equipos activos de la red, como por ejemplo los centros de datos (datacenter), según las normas y estándares internacionales, como por ejemplo la norma TIA-942, en la que se establecen las recomendaciones y directrices para garantizar la disponibilidad de los servicios a prestar.

a. Establecer un diseño de red jerárquico (de dos capas, núcleo colapsado, en los que mantiene la capa de acceso y se funcionan los niveles de distribución y núcleo, o tres capas, acceso, distribución y núcleo) de acuerdo con el dimensionamiento del tráfico de la red y las funciones de los equipos de transporte, para que su diseño, configuración, mantenimiento, escalabilidad y gestión sean eficientes en relación con las necesidades de flexibilidad, robustez, tolerancia a fallas, seguridad, disponibilidad y calidad de servicio.
b. Seleccionar los equipos de la red de transporte (routers o switches) de acuerdo con los requerimientos en la capacidad en los recursos de hardware y software (identificados mediante el dimensionamiento del tráfico de la red), la capacidad para manejar multiservicios de forma integrada, funcionalidades avanzadas en la gestión y automatización de la red para brindar eficiencia en operación y mantenimiento (O&M), alta escalabilidad y modularidad en el transcurso del tiempo, donde se contemple el soporte de protocolos de transporte, gestión y monitoreo mediante tecnologías entre las que se encuentran el direccionamiento IP en las interfaces lógicas o físicas de los routers (IPv4/IPv6), protocolos de enrutamiento IGP (OSPF/IS-IS), protocolo de enrutamiento EGP (iBGP, eBGP, MP-BGP), protocolo para el manejo de etiquetas y distribución dinámica (MPLS, VPN, IP QoS, Ingeniería de tráfico - TE), así como la capacidad para optimizar el uso de ancho de banda, aunque existan distintas tecnologías de transporte y la capacidad para aplicar mecanismos de Calidad de Servicio (QoS) tales como la asignación de prioridades de servicio (voz, video por demanda (VoD), datos, etc.), mecanismos de reducción de latencia, mecanismos para asegurar el ancho de banda mínimo para determinados servicios y mecanismos para evitar la pérdida significativa de paquetes.
c. Implementar una arquitectura Seamless MPLS con los objetivos de simplificar la operación de los nodos de acceso, segmentar la red al introducir las capas de acceso, agregación y núcleo en IP RAN, aislar las subredes en secciones

específicas para reducir la carga de consumo de recursos de hardware en los equipos de la red IP MPLS, reducir la complejidad de los escenarios en donde la configuración de la arquitectura tradicional de MPLS hace difícil la gestión de la red, por lo que se simplifican los procesos de O&M, permitir la creación de servicios VPN de capas 2 y 3 de forma mucho más flexible, lo que reduce los costos de O&M y aplicar técnicas de QoS en MPLS.

d. Seleccionar la conectividad de VPN de capas 2 o 3 de acuerdo con la autonomía del cliente en las necesidades de gestión de las políticas de enrutamiento e información sobre la topología de la red y servicios convergentes a prestar.

2. Establecer las políticas de calidad de servicio entre los actores correspondientes
   a. Establecer las políticas de calidad de servicio en los acuerdos de acceso uso, e interconexión (NIA) junto con los operadores requeridos, para garantizar la conectividad de los usuarios conforme a la regulación vigente.
   b. Establecer las políticas de calidad de servicio en los CPA entre los operadores junto con los proveedores de servicio requeridos, para proveer los servicios de conectividad y garantías asociadas conforme a la regulación vigente.
   c. Establecer las políticas de calidad de servicio en los SIA entre los proveedores de servicio, con el objetivo de describir el alcance de la interconexión, la disponibilidad, y las cláusulas administrativas y técnicas conforme a la regulación vigente.
   d. Establecer los SLA de acuerdo con las necesidades del cliente, para definir las cláusulas técnicas que se deben garantizar en la prestación de los servicios según la regulación vigente.
3. Caracterizar el tráfico de los servicios a prestar en la red, en función de su elasticidad, protocolos de transporte, necesidades de ancho de banda, retardo, jitter y pérdida de paquetes, aplicando el RFC 4594 y su correspondencia con el fabricante de los equipos de la red de transporte.
   a. Diseñar las políticas de QoS siguiendo la metodología de clasificación y marcado del tráfico, encolamiento y organización y acondicionamiento del tráfico, de acuerdo con las características identificadas en los servicios a prestar.
   b. Implementar las políticas de QoS en los puntos de ingreso y egreso a la red del proveedor de servicio.

c. Evaluar las políticas de QoS diseñadas, mediante la definición de una metodología de pruebas para cada tipo de tráfico, que establezca las herramientas y elementos o sistemas de monitoreo de las métricas de ancho de banda, retardo, jitter y pérdidas de paquetes en los puntos de monitoreo de la red identificados por el operador, tomando un número de muestras que garantice la confiabilidad de las mediciones.

4. Auditar de manera periódica los KPI que permitan identificar los puntos de mejora en la prestación de los servicios, de acuerdo con el sistema de gestión de calidad del proveedor de servicios según la regulación vigente.
   a. Tomar las acciones de mejora que corresponda en función del análisis de los resultados y hallazgos obtenidos en las auditorias.
   b. Divulgar los indicadores de calidad con el objetivo de generar confianza en los clientes y posicionar la imagen corporativa del proveedor de servicio.

5. Conclusiones, recomendaciones y contribuciones

5.1 Conclusiones

El presente trabajo de investigación generó un lineamiento técnico para la provisión de Calidad de Servicio (QoS) extremo a extremo en interconexión bajo IP Multimedia Subsystem (IMS), en la cual se realizó una revisión de los requerimientos técnicos para la implementación de la QoS en redes convergentes en los servicios de voz, datos y video, mediante la implementación de un entorno emulado que permitiera evaluar y validar, desde un enfoque sistémico, los resultados experimentales del diseño de políticas de calidad en redes interconectadas, donde, al integrar múltiples tecnologías subyacentes, se resalta la importancia de los estándares, las normas, los procedimientos, las metodologías, las recomendaciones, los lineamientos y las buenas prácticas que se encuentran en organismos internacionales como la UIT o el 3GPP, entre otros y la industria, con base en la regulación vigente, que le permita a los operadores o proveedores de servicio estructurar sus procedimientos y acciones para la mejora continua del desempeño de las redes en función del portafolio que ofrecen a sus clientes, teniendo en cuenta que no existe un único procedimiento de implementación que defina cómo se puede proveer la QoS en redes interconectadas.

La revisión de los antecedentes y fundamentos teóricos permite establecer que se debe proporcionar QoS consistente de extremo a extremo en un servicio IP, de tal manera que se cumplan los requisitos de QoS solicitados por el cliente, cumpliendo con la regulación vigente, cuando en el despliegue de una infraestructura de servicio se involucren dos o más operadores, siendo redes autónomas, cuyos dominios administrativos se gestionan de acuerdo con sus propias políticas. Aunque los operadores deben acordar los requisitos de QoS para un servicio particular entre un conjunto de servicios IP, los operadores no configuran sus redes de la misma manera. Por otro lado, los operadores y proveedores de

servicios tienen sus propias topologías internas y mecanismos de QoS que dependen de sus dispositivos y otros requisitos de gestión que no son técnicos.

Se observa en la Figura 1-2 que el IMS se ha convertido en el estándar de facto en el despliegue de redes LTE y redes 5G a nivel de control conforme a la arquitectura NGN, por sus interfaces abiertas para el despliegue de servicios convergentes, donde se deben caracterizar los servicios de acuerdo con el tipo de tecnología a implementar, para garantizar que las políticas de QoS aplicadas en la red correspondan con los valores de las métricas de retardo, jitter, pérdida de paquetes y ancho de banda requeridos en el transporte de extremo a extremo, establecidos en la diferenciación del tráfico de los identificadores QCI o 5QI, de acuerdo con el tipo de acceso a la red (4G o 5G), cumpliendo con las características técnicas enunciadas en la sección 2. Las políticas de QoS bajo IMS dependen de una red subyacente donde la robustez de la infraestructura física, las características técnicas de los equipos de grado carrier, la calidad de los enlaces físicos entre los equipos activos de la red, y la optimización de la configuración de los protocolos del modelo OSI involucrados en el despliegue de servicios, son la base de la entrega de servicios de valor agregado en el portafolio de un proveedor, por lo que es necesario que el operador disponga de personal calificado en el diseño, implementación, mantenimiento y optimización de las redes de telecomunicaciones, dada la complejidad de las tecnologías relacionadas y su integración en el proceso de interconexión.

La caracterización de los servicios de voz, datos y video, permite identificar en la Figura 2-29, la Tabla 2-9 y la Tabla 2-10, que cada servicio tiene unos requerimientos específicos para el diseño de políticas de QoS, donde se debe tener en cuenta que en el usuario, los terminales o dispositivos finales, deben configurarse con el soporte de protocolos, códecs y aplicaciones adecuadas para el consumo de dichos servicios, y desde el proveedor de servicio se debe tener en cuenta la transcodificación en caso de que se necesite la negociación de códecs para la voz o el video, en caso de que los usuarios no soporten dicha funcionalidad.

Mediante la evaluación del impacto técnico de la negociación de los parámetros de QoS interdominio en el tráfico de servicios de voz, datos y video, en un entorno IMS emulado, se establece que la infraestructura de red impacta el transporte del tráfico de servicios por

lo que los umbrales de congestión deben definirse entre el 75% y el 90% de la utilización de la cola de acuerdo con [119] para el diseño de las políticas de QoS. El proveedor de servicios debe adecuar la utilización de los recursos de hardware conforme a la cantidad de tráfico que transporta en diferentes horarios de operación de la red, incluyendo el crecimiento esperado de esta, conforme a su negocio, siendo necesario realizar tareas de optimización en la configuración de la red de forma periódica. Sin embargo, los recursos de hardware de los dispositivos finales de los usuarios también guardan relación con la calidad en que son recibidos, en especial en lo referente al servicio de video, dado que, si los terminales de usuario no tienen la capacidad suficiente de procesamiento para manejar contenidos de altas resoluciones, se observarán caídas en el video y cortes en el audio por el bitrate con el que el proveedor está entregando el servicio conforme a las pruebas realizadas en los numerales 3.10.3 y 3.10.6 de la presente investigación, que no son necesariamente generados por problemas de infraestructura del operador o la conectividad que el usuario tiene en la red del proveedor. Por otro lado, si los clientes no tienen contratado suficiente ancho de banda (estableciendo los parámetros de CIR y PIR en el SLA) para manejar una alta demanda de servicios, estos tendrán una mala experiencia, puesto que su red se verá saturada por el nivel de tráfico que generan y/o consume de acuerdo con los resultados observados en las tablas Tabla 3-10, Tabla 3-12, Tabla 3-14 y Tabla 3-16, las figuras Figura 3-15, Figura 3-22, Figura 3-29, Figura 3-36, y, en consecuencia, la congestión y la pérdida de paquetes los afectará de manera negativa.

Al evaluar las condiciones de red para obtener los datos de las métricas de QoS, de acuerdo con la Tabla 4-2, es necesario contar con una cantidad de usuarios suficientes para generar estrés en la red de acuerdo con el dimensionamiento de la red que realice el operador de telecomunicaciones en función del tráfico cursado, y de igual forma, se deben realizar un número de pruebas significativas en el tiempo de ejecución establecido en un (1) minuto, de acuerdo con la recomendación UIT-T Y.1541, que garantice la repetibilidad y un nivel estadístico de confiabilidad significativo, según lo observado en [25], para poder hacer la comparación de métricas de QoS entre proveedores, a pesar de las limitaciones de los recursos de hardware observadas en las pruebas realizadas en el entorno emulado. Este proceso requiere de una metodología y un proceso estricto de evaluación, puesto que estos resultados deben reportarse al ente regulador, siendo de interés para todos aquellos actores interesados, lo que genera un impacto en la imagen corporativa del proveedor, donde si los usuarios obtienen una mala experiencia, la consecuencia que tiene el

proveedor (de red o servicio) será que sus usuarios cambien entre los competidores del mercado, y, por otro lado, las afectaciones derivadas de las sanciones correspondientes que establezca el ente regulador.

Esta investigación demuestra mediante la Figura 4-2, la Figura 4-3 y Tabla 4-1 que existen desafíos técnicos, comerciales y regulatorios para los operadores en la provisión de políticas de calidad, que se reflejan de forma directa en la experiencia que tienen los usuarios al momento de consumir los servicios que contratan. La diferenciación y priorización del tráfico toma relevancia para usuarios corporativos que necesiten este tratamiento del tráfico, dada la naturaleza de la misión de sus negocios, en comparación a usuarios naturales que pueden manejar su tráfico mediante la técnica de mejor esfuerzo, reflejándose así en los aspectos económicos que conlleva la implementación de la QoS en la red, sin desechar que se deben cumplir con los mínimos establecidos en la regulación vigente por parte de los proveedores de red o servicio, que garanticen los derechos de los clientes de los operadores. Desde el punto de vista de los proveedores de servicio, que se conocen en el ámbito de las telecomunicaciones como proveedores "*Over-the-Top*" (OTT), tales como Spotify y Netflix, se genera una oportunidad de negocio para establecer alianzas comerciales con los operadores de red, para que estos garanticen la QoS mediante sus infraestructuras, a los servicios y contenidos que ofrecen a sus clientes, para que así se genere un valor agregado de cara a los consumidores de estos contenidos.

5.2 Recomendaciones

En próximas investigaciones se pueden abordar las temáticas de redes definidas por software (SDN), funciones de red virtualizadas (NFV) y radio definido por software (SDR), como medios para el acceso y control de la red a nivel de transporte y señalización. Durante la realización de esta investigación se observaron diferentes plataformas que pueden integrarse al modelo de red presentado, tales como los proyectos Open5GS (open5gs.org) para la red 5G y el proyecto Open Air Interface (openairinterface.org) para redes 4G y 5G.

Dada la heterogeneidad en las características de los servicios de voz, datos y video, y de métodos para proveer calidad de servicio en la red y calidad de la experiencia, en trabajos

futuros se pueden realizar optimizaciones o desarrollos a nivel de los algoritmos involucrados, incluyendo técnicas de automatización o inteligencia artificial tanto para la evaluación y monitoreo del tráfico, como para el aprovisionamiento en la red.

Se recomienda realizar una implementación en un ambiente real con los equipos de acceso, transporte y control involucrados, para evaluar el impacto de diferentes niveles de carga en los servicios elásticos e inelásticos, en función del tráfico generado y consumido para determinar herramientas para el dimensionamiento, diseño y optimización de las redes NGN.

Es importante profundizar en los aspectos económicos, comerciales y regulatorios, relacionados con los indicadores de desempeño (KPI) en interconexión en la diferenciación de los servicios convergentes.

5.3 Contribuciones

A continuación, se presenta el listado de productos académicos obtenidos durante el desarrollo de la presente investigación:

1. Artículo publicado (Vargas & Cadena, 2017)

Vargas Rodríguez, M. A., & Cadena, E. (2017). Review of Quality of Service (QoS) mechanisms over IP Multimedia Subsystem (IMS). *Ingeniería y Desarrollo*, *35*(1), 262–281. http://rcientificas.uninorte.edu.co/index.php/ingenieria/article/view/7933/8952

2. Ponencia (Vargas Rodríguez, 2012a)

Vargas Rodríguez, M. A. (2012a). Calidad de Servicio (QoS) en IP Multimedia Subsystem (IMS). *V Conferencia Científica de Telecomunicaciones, Tecnologías de La Información y Las Telecomunicaciones*. https://citic.org.ec/

3. Consultoría técnica (Vargas Rodríguez, 2012b)

Vargas Rodríguez, M. A. (2012b). *Redes de Próxima Generación (NGN) y su interconexión en el Laboratorio de Conocimiento en Redes Avanzadas - ANKLA del Centro de Investigación de las Telecomunicaciones - CINTEL*. https://cintel.co/

A. Valores recomendados de PHB y DSCP

Tipo de trafico	RFC 4594 DSCP	Cisco DSCP	PHB	Latencia (ms)	Jitter (ms)	Pérdida de paquetes	Elasticidad	AQM/WRED	Control de admisión	Notas
Control de red	CS6	CS6	Reserva BW	No importa	No importa	Mínima	Inelástico	No	No	Protocolos de enrutamiento y otro tráfico que mantiene unida a la red
Señalización	CS5	CS3	Reserva BW	No importa	No importa	Mínima	Inelástico	No	No	Señalización interactiva de voz / video (configuración de llamadas, reenvío, etc.)
OAM	CS2	CS2	Reserva BW	No importa	No importa	Mínima	Inelástico	No	No	Operaciones de red: SNMP, SSH, RADIUS, TACACS, Netflow
Voz	EF	EF	Baja-latencia/prioridad	< 150	< 30	< 1%	Inelástico	No	Si	Muy sensible a la latencia, la fluctuación y la pérdida
Transmisión de video	CS3	CS5	LL/prioridad (posible)	No importa	No importa	< 0.1%	Inelástico	No	Si	Normalmente tiene almacenamiento en búfer a nivel de aplicación. Incluye transmisiones de video en vivo, IPTV, CCTV
Interactivo en tiempo real	CS4	CS4	LL/prioridad (posible)	< 200	< 50	< 0.1%	Inelástico	No	Si	Telepresencia; SLA similar a VOIP

Tipo de trafico	RFC 4594 DSCP	Cisco DSCP	PHB	Latencia (ms)	Jitter (ms)	Pérdida de paquetes	Elasticidad	AQM/WRED	Control de admisión	Notas
										con un poco más de latencia, pero menos pérdida
Conferencia multimedia	AF4x	AF4x	AF + reserva BW	< 200	No importa	< 1%	Elástico	Si	Si	Medios de software bidireccionales, como Webex
Transmisión multimedia	AF3x	AF3x	AF + reserva BW	< 400	No importa	< 1%	Elástico	Si	Posible	Video a pedido, Youtube / videos de capacitación, visualización de video unidireccional
Datos de transacción (LL)	AF2x	AF2x	AF + reserva BW	No importa	No importa	No importa	Elástico	Si	No	Aplicaciones interactivas de primer plano; los usuarios esperan una respuesta (ERP, CRM)
Datos masivos (HT)	AF1x	AF1x	AF + reserva BW	No importa	No importa	No importa	Elástico	Si	No	Aplicaciones de fondo no interactivas; sincronización de base de datos, trabajos de copia de seguridad
Mejor esfuerzo	CS0 / DF	CS0 / DF	DF + reserva BW (posible)	No importa	No importa	No importa	Elástico	Posible	No	La mayoría de las aplicaciones encajan aquí, cualquier cosa no clasificada (también DNS, DHCP)
Scavenger	CS1	CS1	Mínimo BW	No importa	No importa	No importa	Elástico	No	No	De baja prioridad explícita, videojuegos, tráfico de igual a igual

B. Anexo: Configuración de la red de transporte L2VPN

A continuación, se presentan los archivos de configuración para cada router, de acuerdo con los requerimientos presentados en una L2VPN y con la topología de la Figura 3-5 sin aplicar políticas de QoS.

1. Configuración del ISP A

- **Router R1**

```
!
hostname R1
!
ip dhcp excluded-address 10.1.0.1
!
ip dhcp pool UE
 network 10.1.0.0 255.255.255.0
 default-router 10.1.0.1
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
```

```
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
 class CMAP_SIGNALING_SIP
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 20000000 80000 32000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
```

```
 no shutdown
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
router ospf 1
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
end
```

- **Router CSG:**

```
!
hostname CSG
!
ip multicast-routing
!
mpls label range 100 199
!
pseudowire-class CSG
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
!
interface Loopback0
 no shutdown
 ip address 1.1.1.2 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Ethernet0/0
 no shutdown
 no ip address
 duplex auto
 xconnect 1.1.1.5 1 encapsulation l2tpv3 manual pw-class CSG
  l2tp id 1 2
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.1111.1111
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
router ospf 1
 network 10.1.1.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
```

```
 neighbor 1.1.1.3 remote-as 65000
 neighbor 1.1.1.3 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 1.1.1.2 mask 255.255.255.255
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
end
```

- **Router AGG:**

```
!
hostname AGG
!
ip multicast-routing
!
mpls label range 200 299
!
interface Loopback0
 no shutdown
 ip address 1.1.1.3 255.255.255.255
 ip pim sparse-mode
 ip ospf 2 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.2222.2222
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
interface Ethernet0/2
 no shutdown
 mac-address 0000.2222.2222
 ip address 10.2.2.1 255.255.255.0
 ip pim sparse-mode
```

```
 duplex auto
 mpls ip
!
router ospf 2
 network 10.2.2.0 0.0.0.255 area 0
!
router ospf 1
 redistribute ospf 2 subnets match internal route-map ospf2-into-ospf1
 network 10.1.1.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.2 remote-as 65000
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.2 send-label
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
  neighbor 1.1.1.4 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 send-community extended
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 send-community extended
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
 exit-address-family
!
ip pim ssm range 1
!
ip prefix-list prefix-list-ospf2-into-ospf1 seq 5 permit 1.1.1.3/32
!
```

```
route-map ospf2-into-ospf1 permit 10
 match ip address prefix-list prefix-list-ospf2-into-ospf1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
end
```

- **Router Core-ABR**

```
!
hostname Core-ABR
!
ip multicast-routing
!
mpls label range 300 399
!
interface Loopback0
 no shutdown
 ip address 1.1.1.4 255.255.255.255
 ip pim sparse-mode
 ip ospf 4 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.3.3.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 3 area 0
 duplex auto
 mpls ip
!
interface Ethernet0/2
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 2 area 0
 duplex auto
 mpls ip
!
interface Ethernet0/3
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.4.4.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 4 area 0
 duplex auto
 mpls ip
!
router ospf 4
 redistribute ospf 3 subnets
!
router ospf 3
 redistribute ospf 4 subnets
!
```

```
router ospf 2
 redistribute ospf 4 subnets
 redistribute ospf 3 subnets
!
router bgp 65000
 bgp router-id 1.1.1.4
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.3 remote-as 65000
 neighbor 1.1.1.3 update-source Loopback0
 neighbor 1.1.1.5 remote-as 65000
 neighbor 1.1.1.5 update-source Loopback0
 neighbor 2.2.2.3 remote-as 64000
 neighbor 2.2.2.3 ebgp-multihop 255
 neighbor 2.2.2.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 route-reflector-client
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.3 send-label
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 1.1.1.5 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
  neighbor 1.1.1.3 route-reflector-client
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community extended
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community both
  neighbor 2.2.2.3 next-hop-unchanged
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
  neighbor 1.1.1.3 route-reflector-client
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community extended
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community both
  neighbor 2.2.2.3 next-hop-unchanged
 exit-address-family
!
ip pim ssm range 1
```

```
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
end
```

- **Router Core-ASBR**

```
!
hostname Core-ASBR
!
interface Loopback0
 no shutdown
 ip address 1.1.1.7 255.255.255.255
 ip ospf 4 area 0
!
interface Ethernet0/0
 no shutdown
 ip address 10.8.8.1 255.255.255.0
 duplex auto
 mpls bgp forwarding
!
interface Ethernet0/3
 no shutdown
 ip address 10.4.4.2 255.255.255.0
 ip ospf 4 area 0
 duplex auto
 mpls ip
!
router ospf 4
 redistribute bgp 65000 subnets route-map REDISTRIBUTE_IN_IGP
!
router bgp 65000
 bgp log-neighbor-changes
 network 1.1.1.4 mask 255.255.255.255
 network 1.1.1.5 mask 255.255.255.255
 neighbor 10.8.8.2 remote-as 64000
 neighbor 10.8.8.2 send-label
!
ip prefix-list FOREIGN_PREFIXES seq 5 permit 2.2.2.3/32
ip prefix-list FOREIGN_PREFIXES seq 10 permit 2.2.2.2/32
ipv6 ioam timestamp
!
route-map REDISTRIBUTE_IN_IGP permit 10
 match ip address prefix-list FOREIGN_PREFIXES
!
end
```

- **Router MASG**

```
!
hostname MASG
!
ip multicast-routing
!
```

```
mpls label range 400 499
!
pseudowire-class MASG
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
!
interface Loopback0
 no shutdown
 ip address 1.1.1.5 255.255.255.255
 ip pim sparse-mode
 ip ospf 3 area 0
!
interface Ethernet0/0
 no shutdown
 no ip address
 duplex auto
 xconnect 1.1.1.2 1 encapsulation l2tpv3 manual pw-class MASG
  l2tp id 2 1
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.4444.4444
 ip address 10.3.3.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
interface Ethernet0/2
 no shutdown
 no ip address
 duplex auto
 xconnect 2.2.2.2 1 encapsulation l2tpv3 manual pw-class MASG
  l2tp id 4 3
!
router ospf 3
 network 10.3.3.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.5
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 1.1.1.5 mask 255.255.255.255
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
```

```
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
end
```

- **Router R2**

```
!
hostname R2
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
```

```
 class CMAP_SIGNALING_SIP
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 20000000 80000 32000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 1.1.1.6 255.255.255.255
 ip pim sparse-mode
!
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
 no shutdown
 ip address 10.2.0.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
interface Ethernet0/2
 no shutdown
```

```
 ip address 192.168.1.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
router ospf 1
!
end
```

2. Configuración del ISP B

- **Router R3:**

```
!
hostname R3
!
ip dhcp excluded-address 10.3.0.1
!
ip dhcp pool UE
 network 10.3.0.0 255.255.255.0
 default-router 10.3.0.1
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
 class CMAP_SIGNALING_SIP
```

```
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 20000000 80000 32000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 2.2.2.1 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Ethernet0/0
 no shutdown
 ip address 192.168.1.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
 no shutdown
 ip address 10.3.0.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
router ospf 1
!
```

```
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
end
```

- **Router CSG:**

```
!
hostname CSG
!
ip multicast-routing
!
mpls label range 800 899
!
pseudowire-class CSG
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
!
interface Loopback0
 no shutdown
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
 ip ospf 7 area 0
!
interface Ethernet0/0
 no shutdown
 no ip address
 duplex auto
 xconnect 1.1.1.5 1 encapsulation l2tpv3 manual pw-class CSG
  l2tp id 3 4
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.8888.8888
 ip address 10.7.7.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
router ospf 7
 network 10.7.7.0 0.0.0.255 area 0
!
router bgp 64000
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2.2.2.3 remote-as 64000
 neighbor 2.2.2.3 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 2.2.2.2 mask 255.255.255.255
  neighbor 2.2.2.3 activate
```

```
  neighbor 2.2.2.3 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
!
ip pim ssm range 2
!
access-list 2 permit 239.233.0.0 0.0.255.255
!
end
```

- **Router AGG:**

```
!
hostname AGG
!
ip multicast-routing
!
mpls label range 700 799
!
interface Loopback0
 no shutdown
 ip address 2.2.2.3 255.255.255.255
 ip pim sparse-mode
 ip ospf 5 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.7777.7777
 ip address 10.7.7.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 7 area 0
 duplex auto
 mpls ip
!
interface Ethernet0/3
 no shutdown
 mac-address 0000.7777.7777
 ip address 10.5.5.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 5 area 0
 duplex auto
 mpls ip
```

```
!
router ospf 7
 redistribute ospf 5 subnets
!
router ospf 5
 redistribute ospf 7 subnets
!
router bgp 64000
 bgp router-id 2.2.2.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 ebgp-multihop 255
 neighbor 1.1.1.4 update-source Loopback0
 neighbor 2.2.2.2 remote-as 64000
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
  neighbor 2.2.2.2 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community both
  neighbor 1.1.1.4 next-hop-unchanged
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
end
```

- **Router AGG-ASBR:**

```
!
hostname AGG-ASBR
!
interface Loopback0
 no shutdown
 ip address 2.2.2.4 255.255.255.255
```

```
 ip ospf 5 area 0
!
interface Ethernet0/0
 no shutdown
 ip address 10.8.8.2 255.255.255.0
 duplex auto
mpls bgp forwarding
!
interface Ethernet0/3
 no shutdown
 ip address 10.5.5.1 255.255.255.0
 ip ospf 5 area 0
 duplex auto
 mpls ip
!
router ospf 5
 redistribute bgp 64000 subnets route-map REDISTRIBUTE_IN_IGP
!
router bgp 64000
 bgp log-neighbor-changes
 network 2.2.2.2 mask 255.255.255.255
 network 2.2.2.3 mask 255.255.255.255
 neighbor 10.8.8.1 remote-as 65000
 neighbor 10.8.8.1 send-label
!
ip prefix-list FOREIGN_PREFIXES seq 5 permit 1.1.1.5/32
ip prefix-list FOREIGN_PREFIXES seq 10 permit 1.1.1.4/32
!
route-map REDISTRIBUTE_IN_IGP permit 10
 match ip address prefix-list FOREIGN_PREFIXES
!
end
```

C. Anexo: Configuración de la red de transporte L3VPN

A continuación, se presentan los archivos de configuración para cada router, de acuerdo con los requerimientos presentados en una L3VPN y con la topología de la Figura 3-6 sin aplicar políticas de QoS.

1. Configuración del ISP A

- **Router R1**

```
!
hostname R1
!
ip dhcp excluded-address 10.1.0.1
!
ip dhcp pool UE
 network 10.1.0.0 255.255.255.0
 default-router 10.1.0.1
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
```

```
 match protocol rtp-audio
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
 class CMAP_SIGNALING_SIP
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 17000000 68000 60000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface Ethernet0/0
 no shutdown
 ip address 172.16.0.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
```

```
 no shutdown
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
router bgp 65100
 bgp log-neighbor-changes
 redistribute connected
 neighbor 172.16.0.1 remote-as 65000
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
end
```

- **Router CSG**

```
!
hostname CSG
!
vrf definition 100:A
 rd 1.1.1.2:100
 !
 address-family ipv4
  mdt auto-discovery pim
  mdt default 239.232.0.1
  route-target export 65000:100
  route-target import 65000:100
 exit-address-family
!
ip multicast-routing
ip multicast-routing vrf 100:A
!
mpls label range 100 199
!
interface Loopback0
 no shutdown
 ip address 1.1.1.2 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Ethernet0/0
 no shutdown
 vrf forwarding 100:A
 ip address 172.16.0.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.1111.1111
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
```

```
 mpls ip
!
interface Ethernet0/2
 no shutdown
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
 duplex auto
!
router ospf 1
 network 10.1.1.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.3 remote-as 65000
 neighbor 1.1.1.3 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 1.1.1.2 mask 255.255.255.255
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf 100:A
  neighbor 172.16.0.2 remote-as 65100
  neighbor 172.16.0.2 activate
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
end
```

- **Router AGG**

```
!
```

```
hostname AGG
!
ip multicast-routing
!
mpls label range 200 299
!
interface Loopback0
 no shutdown
 ip address 1.1.1.3 255.255.255.255
 ip pim sparse-mode
 ip ospf 2 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.2222.2222
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
interface Ethernet0/2
 no shutdown
 mac-address 0000.2222.2222
 ip address 10.2.2.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
router ospf 2
 network 10.2.2.0 0.0.0.255 area 0
!
router ospf 1
 redistribute ospf 2 subnets match internal route-map ospf2-into-ospf1
 network 10.1.1.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.2 remote-as 65000
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.2 send-label
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
  neighbor 1.1.1.4 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
```

```
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 send-community extended
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 send-community extended
  neighbor 1.1.1.2 route-reflector-client
  neighbor 1.1.1.2 next-hop-self all
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 1.1.1.4 route-reflector-client
  neighbor 1.1.1.4 next-hop-self all
 exit-address-family
!
ip pim ssm range 1
!
ip prefix-list prefix-list-ospf2-into-ospf1 seq 5 permit 1.1.1.3/32
ipv6 ioam timestamp
!
route-map ospf2-into-ospf1 permit 10
 match ip address prefix-list prefix-list-ospf2-into-ospf1
!
access-list 1 permit 239.232.0.0 0.0.255.255
!
end
```

- **Router Core-ABR**

```
!
hostname Core-ABR
!
ip multicast-routing
!
mpls label range 300 399
!
interface Loopback0
 no shutdown
 ip address 1.1.1.4 255.255.255.255
 ip pim sparse-mode
 ip ospf 4 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.3.3.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 3 area 0
 duplex auto
 mpls ip
```

```
!
interface Ethernet0/2
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 2 area 0
 duplex auto
 mpls ip
!
interface Ethernet0/3
 no shutdown
 mac-address 0000.3333.3333
 ip address 10.4.4.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 4 area 0
 duplex auto
 mpls ip
!
router ospf 4
 redistribute ospf 3 subnets
!
router ospf 3
 redistribute ospf 4 subnets
!
router ospf 2
 redistribute ospf 4 subnets
 redistribute ospf 3 subnets
!
router bgp 65000
 bgp router-id 1.1.1.4
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.3 remote-as 65000
 neighbor 1.1.1.3 update-source Loopback0
 neighbor 1.1.1.5 remote-as 65000
 neighbor 1.1.1.5 update-source Loopback0
 neighbor 2.2.2.3 remote-as 64000
 neighbor 2.2.2.3 ebgp-multihop 255
 neighbor 2.2.2.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 route-reflector-client
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.3 send-label
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 1.1.1.5 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
  neighbor 1.1.1.3 route-reflector-client
```

```
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community extended
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.3 activate
  neighbor 1.1.1.3 send-community extended
  neighbor 1.1.1.3 route-reflector-client
  neighbor 1.1.1.3 next-hop-self all
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community extended
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community both
  neighbor 2.2.2.3 next-hop-unchanged
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community extended
  neighbor 1.1.1.5 route-reflector-client
  neighbor 1.1.1.5 next-hop-self all
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
end
```

- **Router Core-ASBR**

```
!
hostname Core-ASBR
!
ip multicast-routing
!
interface Loopback0
 no shutdown
 ip address 1.1.1.7 255.255.255.255
 ip pim sparse-mode
 ip ospf 4 area 0
!
interface Ethernet0/0
 no shutdown
 ip address 10.8.8.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
```

```
 mpls bgp forwarding
 mpls ip
!
interface Ethernet0/3
 no shutdown
 ip address 10.4.4.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 4 area 0
 duplex auto
 mpls ip
!
router ospf 4
 redistribute bgp 65000 subnets route-map REDISTRIBUTE_IN_IGP
!
router bgp 65000
 bgp log-neighbor-changes
 network 1.1.1.4 mask 255.255.255.255
 network 1.1.1.5 mask 255.255.255.255
 neighbor 10.8.8.2 remote-as 64000
 neighbor 10.8.8.2 send-label
!
ip pim ssm range 2
!
ip prefix-list FOREIGN_PREFIXES seq 5 permit 2.2.2.3/32
ip prefix-list FOREIGN_PREFIXES seq 10 permit 2.2.2.2/32
ipv6 ioam timestamp
!
route-map REDISTRIBUTE_IN_IGP permit 10
 match ip address prefix-list FOREIGN_PREFIXES
!
access-list 2 permit 239.233.0.0 0.0.255.255
!
end
```

- **Router MASG**

```
!
hostname MASG
!
vrf definition 100:A
 rd 1.1.1.5:100
 !
 address-family ipv4
  mdt auto-discovery pim
  mdt default 239.232.0.1
  route-target export 65000:100
  route-target import 65000:100
 exit-address-family
!
vrf definition 101:B
 rd 1.1.1.5:101
 !
 address-family ipv4
  mdt auto-discovery pim
  mdt default 239.233.0.1
```

```
  route-target export 65000:101
  route-target import 64000:101
 exit-address-family
!
ip multicast-routing
ip multicast-routing vrf 100:A
ip multicast-routing vrf 101:B
!
mpls label range 400 499
!
interface Loopback0
 no shutdown
 ip address 1.1.1.5 255.255.255.255
 ip pim sparse-mode
 ip ospf 3 area 0
!
interface Ethernet0/0
 no shutdown
 vrf forwarding 100:A
 ip address 192.168.0.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.4444.4444
 ip address 10.3.3.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
interface Ethernet0/2
 no shutdown
 vrf forwarding 101:B
 ip address 192.168.1.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
!
router ospf 3
 network 10.3.3.0 0.0.0.255 area 0
!
router bgp 65000
 bgp router-id 1.1.1.5
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 1.1.1.5 mask 255.255.255.255
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-label
 exit-address-family
 !
```

```
 address-family ipv4 mvpn
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf 100:A
  neighbor 192.168.0.2 remote-as 65200
  neighbor 192.168.0.2 activate
 exit-address-family
 !
 address-family ipv4 vrf 101:B
  neighbor 192.168.1.2 remote-as 65200
  neighbor 192.168.1.2 activate
 exit-address-family
!
ip pim ssm range 1
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
end
```

- **Router R2**

```
!
hostname R2
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
  description MATCH BROADCAST VIDEO
```

```
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
 class CMAP_SIGNALING_SIP
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 17000000 68000 60000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 1.1.1.6 255.255.255.255
 ip pim sparse-mode
!
interface Ethernet0/0
 no shutdown
 ip address 192.168.0.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
```

```
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
 no shutdown
 ip address 10.2.0.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
interface Ethernet0/2
 no shutdown
 ip address 192.168.1.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
router bgp 65200
 bgp log-neighbor-changes
 redistribute connected
 neighbor 192.168.0.1 remote-as 65000
 neighbor 192.168.1.1 remote-as 65000
!
end
```

2. Configuración del ISP B

- **Router R3**

```
!
hostname R3
!
ip dhcp excluded-address 10.3.0.1
!
ip dhcp pool UE
 network 10.3.0.0 255.255.255.0
 default-router 10.3.0.1
!
ip multicast-routing
!
class-map match-all CMAP_SIGNALING_SIP
  description MATCH SIGNALING_SIP
 match protocol sip
class-map match-all CMAP_QUEUE_OAM_SIGNALING
  description NETOPS AND VOICE SIGNALING TRAFFIC
 match dscp cs2  cs5
class-map match-all CMAP_VOICE_CONTROL
  description MATCH VOICE CONTROL
 match protocol rtcp
class-map match-all CMAP_MATCH_OAM
  description MATCH NETOPS/OAM TRAFFIC
 match protocol ssh
class-map match-all CMAP_QUEUE_VOICE
  description VOICE BEARER TRAFFIC
 match dscp ef
class-map match-all CMAP_MATCH_BROADCAST_VIDEO
```

```
  description MATCH BROADCAST VIDEO
 match protocol rtsp
class-map match-all CMAP_VOICE_RTP
  description MATCH VOICE_RTP
 match protocol rtp-audio
class-map match-all CMAP_QUEUE_BROADCAST_VIDEO
  description ONE-WAY, INELASTIC VIDEO TRAFFIC
 match dscp cs3
class-map match-any CMAP_QUEUE_NETCONTROL
  description NETWORK CONTROL (ROUTING, ETC)
 match dscp cs6
!
policy-map PMAP_INGRESS_EDGE_MARK
 description CLASSIFY AND MARK TRAFFIC FROM UEs
 class CMAP_SIGNALING_SIP
  set dscp cs5
 class CMAP_VOICE_RTP
  set dscp ef
 class CMAP_VOICE_CONTROL
  set dscp ef
 class CMAP_MATCH_BROADCAST_VIDEO
  set dscp cs3
 class CMAP_MATCH_OAM
  set dscp cs2
 class class-default
  set dscp default
policy-map PMAP_EGRESS_QUEUE
 description EGRESS QUEUING POLICY
 class CMAP_QUEUE_VOICE
  priority percent 20
 class CMAP_QUEUE_BROADCAST_VIDEO
  bandwidth percent 25
 class CMAP_QUEUE_NETCONTROL
  bandwidth percent 10
 class CMAP_QUEUE_OAM_SIGNALING
  bandwidth percent 15
 class class-default
  bandwidth percent 30
  random-detect dscp-based
  random-detect dscp 0 20 40 10
  random-detect dscp 8 10 20 8
policy-map PMAP_EGRESS_SHAPE
 description HIERARCHICAL SHAPER
 class class-default
  shape average 17000000 68000 60000
   service-policy PMAP_EGRESS_QUEUE
!
interface Loopback0
 no shutdown
 ip address 2.2.2.1 255.255.255.255
 ip pim sparse-mode
!
interface Ethernet0/0
 no shutdown
 ip address 172.16.1.2 255.255.255.0
 ip pim sparse-mode
```

```
 duplex auto
 service-policy output PMAP_EGRESS_SHAPE
!
interface Ethernet0/1
 no shutdown
 ip address 10.3.0.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 service-policy input PMAP_INGRESS_EDGE_MARK
!
router bgp 64100
 bgp log-neighbor-changes
 redistribute connected
 neighbor 172.16.1.1 remote-as 64000
!
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
end
```

- **Router CSG**

```
!
hostname CSG
!
vrf definition 101:B
 rd 2.2.2.2:101
 !
 address-family ipv4
  mdt auto-discovery pim
  mdt default 239.233.0.1
  route-target export 64000:101
  route-target import 65000:101
 exit-address-family
!
ip multicast-routing
ip multicast-routing vrf 101:B
!
mpls label range 800 899
!
interface Loopback0
 no shutdown
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
 ip ospf 7 area 0
!
interface Ethernet0/0
 no shutdown
 vrf forwarding 101:B
 ip address 172.16.1.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.8888.8888
```

```
 ip address 10.7.7.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls ip
!
router ospf 7
 network 10.7.7.0 0.0.0.255 area 0
!
router bgp 64000
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2.2.2.3 remote-as 64000
 neighbor 2.2.2.3 update-source Loopback0
 !
 address-family ipv4
  bgp additional-paths select backup
  bgp additional-paths install
  network 2.2.2.2 mask 255.255.255.255
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf 101:B
  neighbor 172.16.1.2 remote-as 64100
  neighbor 172.16.1.2 activate
 exit-address-family
!
ip pim ssm range 2
!
access-list 2 permit 239.233.0.0 0.0.255.255
!
end
```

- **Router AGG**

```
!
hostname AGG
!
ip multicast-routing
!
```

```
mpls label range 700 799
!
interface Loopback0
 no shutdown
 ip address 2.2.2.3 255.255.255.255
 ip pim sparse-mode
 ip ospf 5 area 0
!
interface Ethernet0/1
 no shutdown
 mac-address 0000.7777.7777
 ip address 10.7.7.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 7 area 0
 duplex auto
 mpls ip
!
interface Ethernet0/3
 no shutdown
 mac-address 0000.7777.7777
 ip address 10.5.5.2 255.255.255.0
 ip pim sparse-mode
 ip ospf 5 area 0
 duplex auto
 mpls ip
!
router ospf 5
 redistribute ospf 7 subnets
!
router ospf 7
 redistribute ospf 5 subnets
!
router bgp 64000
 bgp router-id 2.2.2.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.4 remote-as 65000
 neighbor 1.1.1.4 ebgp-multihop 255
 neighbor 1.1.1.4 update-source Loopback0
 neighbor 2.2.2.2 remote-as 64000
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
  neighbor 2.2.2.2 send-label
 exit-address-family
 !
 address-family ipv4 mvpn
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
```

```
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community both
  neighbor 1.1.1.4 next-hop-unchanged
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.4 activate
  neighbor 1.1.1.4 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 2.2.2.2 route-reflector-client
  neighbor 2.2.2.2 next-hop-self all
 exit-address-family
!
ip pim ssm range 2
!
access-list 2 permit 239.233.0.0 0.0.255.255
!
end
```

- **Router AGG-ASBR**

```
!
hostname AGG-ASBR
!
ip multicast-routing
!
interface Loopback0
 no shutdown
 ip address 2.2.2.4 255.255.255.255
 ip pim sparse-mode
 ip ospf 5 area 0
!
interface Ethernet0/0
 no shutdown
 ip address 10.8.8.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 mpls bgp forwarding
 mpls ip
!
interface Ethernet0/3
 no shutdown
 ip address 10.5.5.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 5 area 0
 duplex auto
 mpls ip
!
```

```
router ospf 5
 redistribute bgp 64000 subnets route-map REDISTRIBUTE_IN_IGP
!
router bgp 64000
 bgp log-neighbor-changes
 network 2.2.2.2 mask 255.255.255.255
 network 2.2.2.3 mask 255.255.255.255
 neighbor 10.8.8.1 remote-as 65000
 neighbor 10.8.8.1 send-label
!
ip pim ssm range 2
!
ip prefix-list FOREIGN_PREFIXES seq 5 permit 1.1.1.5/32
ip prefix-list FOREIGN_PREFIXES seq 10 permit 1.1.1.4/32
ipv6 ioam timestamp
!
route-map REDISTRIBUTE_IN_IGP permit 10
 match ip address prefix-list FOREIGN_PREFIXES
!
access-list 2 permit 239.233.0.0 0.0.255.255
!
end
```

D. Anexo: Configuración del servidor SIP Kamailio IMS

Para la preparación de los escenarios de prueba se utiliza Kamailio IMS

1. Contar con el sistema operativo Ubuntu 18.04.4 LTS

2. Instalar las siguientes dependencias

```
$ apt update && apt upgrade -y && apt install -y mysql-server tcpdump
screen ntp ntpdate git-core dkms gcc flex bison libmysqlclient-dev make\
libssl-dev libcurl4-openssl-dev libxml2-dev libpcre3-dev bash-completion
g++ autoconf rtpproxy libmnl-dev libsctp-dev ipsec-tools libradcli-dev\
libradcli4\
```

3. Clonar el repositorio de Kamailio y validar la versión 5.2 del repositorio

```
$ mkdir -p /usr/local/src/
$ cd /usr/local/src/
$ git clone https://github.com/herlesupreeth/kamailio
$ cd kamailio
$ git checkout -b 5.2 origin/5.2
```

4. Generar archivos de configuración de compilación

```
$ cd /usr/local/src/kamailio
$ make cfg
```

5. Habilitar el módulo MySQL y todos los módulos IMS necesarios

Edite el archivo ***modules.lst*** presente en ***/usr/local/src/kamailio/src***. El contenido del archivo ***modules.lst*** debe ser el siguiente:

```
# this file is autogenerated by make modules-cfg

# the list of sub-directories with modules
modules_dirs:=modules

# the list of module groups to compile
cfg_group_include=
```

```
# the list of extra modules to compile
include_modules= cdp cdp_avp db_mysql dialplan ims_auth ims_charging
ims_dialog ims_diameter_server ims_icscf ims_ipsec_pcscf ims_isc ims_ocs
ims_qos ims_registrar_pcscf ims_registrar_scscf ims_usrloc_pcscf
ims_usrloc_scscf outbound presence presence_conference
presence_dialoginfo presence_mwi presence_profile presence_reginfo
presence_xml pua pua_bla pua_dialoginfo pua_reginfo pua_rpc pua_usrloc
pua_xmpp sctp tls utils xcap_client xcap_server xmlops xmlrpc

# the list of static modules
static_modules=

# the list of modules to skip from compile list
skip_modules=

# the list of modules to exclude from compile list
exclude_modules= acc_json acc_radius app_java app_lua app_lua_sr
app_mono app_perl app_python app_python3 app_ruby auth_ephemeral
auth_identity auth_radius cnxcc cplc crypto db2_ldap db_berkeley
db_cassandra db_mongodb db_oracle db_perlvdb db_postgres db_redis
db_sqlite db_unixodbc dnssec erlang evapi geoip geoip2 gzcompress h350
http_async_client http_client jansson janssonrpcc json jsonrpcc kafka
kazoo lcr ldap log_systemd lost memcached misc_radius ndb_cassandra
ndb_mongodb ndb_redis nsq osp peering phonenum pua_json rabbitmq regex
rls rtp_media_server snmpstats systemdops topos_redis uuid websocket
xhttp_pi xmpp $(skip_modules)

modules_all= $(filter-out modules/CVS,$(wildcard modules/*))
modules_noinc= $(filter-out $(addprefix modules/, $(exclude_modules)
$(static_modules)), $(modules_all))
modules= $(filter-out $(modules_noinc), $(addprefix modules/,
$(include_modules) )) $(modules_noinc)
modules_configured:=1
```

6. Compilar e instalar Kamailio

```
$ cd /usr/local/src/kamailio
$ export RADCLI=1
$ make Q=0 all | tee make_all.txt
$ make install | tee make_install.txt
$ ldconfig
```

7. Los binarios y los scripts ejecutables se instalan en: ***/usr/local/sbin***

```
kamailio - Kamailio SIP server
kamdbctl - script to create and manage the Databases
kamctl - script to manage and control Kamailio SIP server
kamcmd - CLI - command line tool to interface with Kamailio SIP server
```

Para poder utilizar los archivos binarios desde la línea de comandos, asegúrese de que ***/usr/local/sbin*** esté configurado en la variable de entorno ***PATH***. Puede verificar eso con

echo $PATH. Si no es así y está utilizando ***bash***, abra ***/root/.bash_profile*** y al final agregue:

```
PATH=$PATH:/usr/local/sbin
export PATH
```

Los módulos de Kamailio se instalan en: ***/usr/local/lib64/kamailio/modules***
La documentación y los archivos Léame se instalan en: ***/usr/local/share/doc/kamailio***
Los archivos de configuración se instalan en: ***/usr/local/etc/kamailio***
En caso de que configure la variable ***PREFIX*** en el comando ***make cfg***, reemplace /***usr/local*** en todas las rutas anteriores con el valor de ***PREFIX*** para ubicar los archivos instalados.

8. Edite el archivo ***/etc/default/rtpproxy*** de la siguiente manera:

```
# Defaults for rtpproxy

# The control socket.
#CONTROL_SOCK="unix:/var/run/rtpproxy/rtpproxy.sock"
# To listen on an UDP socket, uncomment this line:
#CONTROL_SOCK=udp:127.0.0.1:22222
CONTROL_SOCK=udp:127.0.0.1:7722

# Additional options that are passed to the daemon.
EXTRA_OPTS="-l <PUBLIC_IP> -d DBUG:LOG_LOCAL0"
```

En la opción ***-l <PUBLIC_IP>***, ingrese la dirección IP del proxy RTP y ejecute el siguiente comando:

```
$ systemctl restart rtpproxy
```

9. Cree una nueva base de datos ***mysql*** para las entidades del core IMS pcscf, icscf y scscf, complete bases de datos y otorgue permisos a los usuarios respectivos identificados por una contraseña según se indica a continuación:

```
$ mysql
mysql> CREATE DATABASE `pcscf`;
mysql> CREATE DATABASE `scscf`;
mysql> CREATE DATABASE `icscf`;
mysql> exit
```

En todos los pasos cuando se le solicite la contraseña de usuario ***root*** de ***mysql***, déjela en blanco, es decir, presione la tecla ***Enter***:

```
$ cd /usr/local/src/kamailio/utils/kamctl/mysql
$ mysql -u root -p pcscf < standard-create.sql
```

```
$ mysql -u root -p pcscf < presence-create.sql
$ mysql -u root -p pcscf < ims_usrloc_pcscf-create.sql
$ mysql -u root -p pcscf < ims_dialog-create.sql

$ mysql -u root -p scscf < standard-create.sql
$ mysql -u root -p scscf < presence-create.sql
$ mysql -u root -p scscf < ims_usrloc_scscf-create.sql
$ mysql -u root -p scscf < ims_dialog-create.sql
$ mysql -u root -p scscf < ims_charging_create.sql

$ cd /usr/local/src/kamailio/misc/examples/ims/icscf
$ mysql -u root -p icscf < icscf.sql
```

Ejecute los comandos línea por línea y presione la tecla Enter:

```
$mysql
mysql> grant delete,insert,select,update on pcscf.* to pcscf@localhost
identified by 'heslo';
mysql> grant delete,insert,select,update on scscf.* to scscf@localhost
identified by 'heslo';
mysql> grant delete,insert,select,update on icscf.* to icscf@localhost
identified by 'heslo';
mysql> grant delete,insert,select,update on icscf.* to
provisioning@localhost identified by 'provi';
mysql> GRANT ALL PRIVILEGES ON pcscf.* TO 'pcscf'@'%' identified by
'heslo';
mysql> GRANT ALL PRIVILEGES ON scscf.* TO 'scscf'@'%' identified by
'heslo';
mysql> GRANT ALL PRIVILEGES ON icscf.* TO 'icscf'@'%' identified by
'heslo';
mysql> GRANT ALL PRIVILEGES ON icscf.* TO 'provisioning'@'%' identified
by 'provi';
mysql> FLUSH PRIVILEGES;
mysql> exit
```

Luego ejecute los siguientes comandos:

```
$ mysql
mysql> use icscf;
mysql> INSERT INTO `nds_trusted_domains` VALUES (1,'ims.<DOMINIO-IMS>');
mysql> INSERT INTO `s_cscf` VALUES (1,'First and only S-
CSCF','sip:scscf.ims.<DOMINIO-IMS>:6060');
mysql> INSERT INTO `s_cscf_capabilities` VALUES (1,1,0),(2,1,1);
```

Se debe tener en cuenta que en el parámetro ***<DOMINIO-IMS>*** se debe configurar el dominio del core IMS correspondiente al ISP.

10. Copie los archivos de configuración de las entidades pcscf, icscf y scscf en la carpeta ***/etc*** y edítelos en consecuencia:

```
$ cd ~ && git clone https://github.com/herlesupreeth/Kamailio_IMS_Config
$ cd Kamailio_IMS_Config
$ cp -r kamailio_icscf /etc
$ cp -r kamailio_pcscf /etc
$ cp -r kamailio_scscf /etc
```

Una vez realizado este proceso, edite las direcciones IP para cada una de las entidades con el comando

```
$ sed -i 's/10.4.128.21/192.168.1.69/g' /etc/kamailio_icscf/*
$ sed -i 's/10.4.128.21/192.168.1.69/g' /etc/kamailio_pcscf/*
$ sed -i 's/10.4.128.21/192.168.1.69/g' /etc/kamailio_scscf/*
```

El parámetro ***<IP>*** debe corresponder con la dirección IP de la VM.

Edite los dominios para cada una de las entidades con el comando

```
$ sed -i 's/mnc001.mcc001.3gppnetwork.org/<DOMINIO-IMS>/g'
/etc/kamailio_icscf/*
$ sed -i 's/mnc001.mcc001.3gppnetwork.org/<DOMINIO-IMS>/g'
/etc/kamailio_pcscf/*
$ sed -i 's/mnc001.mcc001.3gppnetwork.org/<DOMINIO-IMS>/g'
/etc/kamailio_icscf/*
```

El parámetro ***<DOMINIO-IMS>*** debe corresponder con el dominio especificado para el ISP correspondiente.

11. Instalación del DNS para la resolución de nombres de los componentes IMS

```
$ apt install -y bind9
```

Cree la zona DNS para el dominio IMS correspondiente según se muestra:

```
$ORIGIN ims.<DOMINIO-IMS>.
$TTL 1W
@                       1D IN SOA       localhost. root.localhost. (
                                        2006101001      ; serial
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns
ns                      1D IN A         <IP>

ims.<DOMINIO-IMS>.       1D IN A         <IP>
ims.<DOMINIO-IMS>.       1D IN NAPTR 10 50 "s" "SIP+D2U"      ""
_sip._udp
ims.<DOMINIO-IMS>.       1D IN NAPTR 20 50 "s" "SIP+D2T"      ""
_sip._tcp
```

```
0.0.0.1.ims.<DOMINIO-IMS>. IN NAPTR 5 10 "U" "E2U+sip"
"!^\\+1000$!sip:alice@ims.<DOMINIO-IMS>!".
1.0.0.1.ims.<DOMINIO-IMS>. IN NAPTR 5 10 "U" "E2U+sip"
"!^\\+1001$!sip:bob@ims.<DOMINIO-IMS>!".
0.0.3.0.1.ims.<DOMINIO-IMS>. IN NAPTR 5 10 "U" "E2U+sip"
"!^\\+10300$!sip:10300@10.0.3.32!".
pcscf                   1D IN A         <IP>
_sip.pcscf              1D SRV 0 0 5060 pcscf
_sip._udp.pcscf         1D SRV 0 0 5060 pcscf
_sip._tcp.pcscf         1D SRV 0 0 5060 pcscf

icscf                   1D IN A         <IP>
_sip                    1D SRV 0 0 4060 icscf
_sip._udp               1D SRV 0 0 4060 icscf
_sip._tcp               1D SRV 0 0 4060 icscf

scscf                   1D IN A         <IP>
_sip.scscf              1D SRV 0 0 6060 scscf
_sip._udp.scscf         1D SRV 0 0 6060 scscf
_sip._tcp.scscf         1D SRV 0 0 6060 scscf

hss                     1D IN A         <IP>
```

Se debe tener en cuenta que en el parámetro <DOMINIO-IMS> se debe configurar el dominio del core IMS correspondiente al ISP. De igual manera, el parámetro ***<IP>*** debe corresponder con la dirección IP de la VM.

Edite el archivo ***/etc/bind/named.conf.local*** como se muestra a continuación:

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "ims.<DOMINIO-IMS>" {
        type master;
        file "/etc/bind/ims.<DOMINIO-IMS>";
};
```

Reinicie el servicio de DNS:

```
$ systemctl restart bind9
```

Edite el archivo ***/etc/netplan/50-cloud-init.yaml*** de la siguiente manera:

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
```

```
# To disable cloud-init's network configuration capabilities, write a
file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the
following:
# network: {config: disabled}
network:
  version: 2
  renderer: networkd
  ethernets:
    ens33:
      dhcp4: no
      addresses: [<IP>]
      gateway4: <IP>
      nameservers:
        search: [ims.<DOMINIO-IMS>]
        addresses: [<IP>]
```

Para que los cambios en ***/etc/resolv.conf*** sean persistentes durante el reinicio ejecute:

```
$ netplan apply
$ ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
$ systemctl restart systemd-resolved.service
```

12. Instalación de RTPEngine

Verifique e instale las dependencias y cree paquetes .deb:

```
$ export DEB_BUILD_PROFILES="pkg.ngcp-rtpengine.nobcg729"
$ apt install dpkg-dev
$ git clone https://github.com/sipwise/rtpengine
$ cd rtpengine && git checkout mr7.4.1
$ dpkg-checkbuilddeps
```

El comando anterior verifica las dependencias y le brinda una lista de las dependencias que faltan en el sistema. La siguiente lista es el resultado de este comando:

```
$ apt install debhelper default-libmysqlclient-dev gperf iptables-dev
libavcodec-dev libavfilter-dev libavformat-dev libavutil-dev libbencode-
perl libcrypt-openssl-rsa-perl libcrypt-rijndael-perl libdigest-crc-perl
libdigest-hmac-perl libevent-dev libhiredis-dev libio-multiplex-perl
libio-socket-inet6-perl libiptc-dev libjson-glib-dev libnet-interface-
perl libpcap0.8-dev libsocket6-perl libspandsp-dev libswresample-dev
libsystemd-dev libxmlrpc-core-c3-dev markdown dkms module-assistant
keyutils libnfsidmap2 libtirpc1 nfs-common rpcbind
```

Después de instalar las dependencias, ejecute el siguiente comando nuevamente y verifique que no falten dependencias:

```
$ dpkg-checkbuilddeps
```

Si se cumplen todas las dependencias, los siguientes comandos deberían regresarlo a shell

```
$ dpkg-buildpackage -uc -us
$ cd ..
$ dpkg -i *.deb
$ cp /etc/rtpengine/rtpengine.sample.conf /etc/rtpengine/rtpengine.conf
```

Edite el archivo /etc/rtpengine/rtpengine.conf con la dirección IP de la VM:

```
$ interface = <IP>
```

Edite ***/etc/default/ngcp-rtpengine-daemon*** y ***/etc/default/ngcp-rtpengine-recording-daemon*** de la siguiente manera en los archivos respectivos:

```
RUN_RTPENGINE=yes
```

```
RUN_RTPENGINE_RECORDING=yes
```

Ejecute los siguientes comandos:

```
$ cp /etc/rtpengine/rtpengine-recording.sample.conf
/etc/rtpengine/rtpengine-recording.conf
$ mkdir /var/spool/rtpengine
$ systemctl restart ngcp-rtpengine-daemon.service ngcp-rtpengine-
recording-daemon.service ngcp-rtpengine-recording-nfs-mount.service
$ systemctl enable ngcp-rtpengine-daemon.service ngcp-rtpengine-
recording-daemon.service ngcp-rtpengine-recording-nfs-mount.service

$ systemctl stop rtpproxy
$ systemctl disable rtpproxy
$ systemctl mask rtpproxy
```

13. El script ***init.d***

El script ***init.d*** se puede usar para iniciar o detener el servidor Kamailio, copie el archivo init en ***/etc/init.d/kamailio***. Luego cambie los permisos:

```
$ cp /usr/local/src/kamailio/pkg/kamailio/deb/bionic/kamailio.init
/etc/init.d/kamailio
$ chmod 755 /etc/init.d/kamailio
```

14. Ejecución de las entidades I-CSCF, P-CSCF y S-CSCF como procesos ***systemctl*** separados

Copie el archivo ***init*** para cada uno de los procesos que necesita

```
$ cp /etc/init.d/kamailio /etc/init.d/kamailio_icscf
$ cp /etc/init.d/kamailio /etc/init.d/kamailio_pcscf
$ cp /etc/init.d/kamailio /etc/init.d/kamailio_scscf
```

Cambios requeridos en ***/etc/init.d/kamailio_icscf***

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin
NAME="kamailio_icscf"
CFGFILE=/etc/$NAME/kamailio_icscf.cfg
```

Cambios requeridos en ***/etc/init.d/kamailio_pcscf***

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin
NAME="kamailio_pcscf"
CFGFILE=/etc/$NAME/kamailio_pcscf.cfg
```

Cambios requeridos en ***/etc/init.d/kamailio_scscf***

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin
NAME="kamailio_scscf"
CFGFILE=/etc/$NAME/kamailio_scscf.cfg
```

Copie el archivo de configuración por defecto para cada uno de los procesos que necesita

```
cp /usr/local/src/kamailio/pkg/kamailio/deb/bionic/kamailio.default
/etc/default/kamailio
$ cd /etc/default/
$ cp kamailio kamailio_icscf
$ cp kamailio kamailio_pcscf
$ cp kamailio kamailio_scscf
```

Cree el directorio para el archivo pid:

```
$ mkdir -p /var/run/kamailio
```

Para la configuración predeterminada para ejecutar el servidor SIP Kamailio es necesario definir como usuario kamailio y grupo kamailio. Para eso necesita crear el usuario y establecer la propiedad del proceso

```
$ adduser --quiet --system --group --disabled-password \
        --shell /bin/false --gecos "Kamailio" \
        --home /var/run/kamailio kamailio
$ chown kamailio:kamailio /var/run/kamailio
```

Cambios requeridos en ***/etc/default/kamailio_icscf***

```
CFGFILE=/etc/kamailio_icscf/kamailio_icscf.cfg
RUN_KAMAILIO=yes
```

Cambios requeridos en ***/etc/default/kamailio_pcscf***

```
CFGFILE=/etc/kamailio_pcscf/kamailio_pcscf.cfg
RUN_KAMAILIO=yes
```

Cambios requeridos en ***/etc/default/kamailio_scscf***

```
CFGFILE=/etc/kamailio_scscf/kamailio_scscf.cfg
RUN_KAMAILIO=yes
```

Finalmente ejecute,

```
$ systemctl daemon-reload
$ systemctl start kamailio_icscf kamailio_pcscf kamailio_scscf
```

15. Instalación del FoHSS

Requerimientos para la instalación del FoHSS: Instalación de ***Java JDK*** y ***ant***

Descargue Oracle Java 7 JDK desde el siguiente enlace utilizando un navegador:

https://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html

```
$ mkdir -p  /usr/lib/jvm/
$ tar -zxf jdk-7u*-linux-x64.tar.gz -C /usr/lib/jvm/
$ update-alternatives --install /usr/bin/java java
/usr/lib/jvm/jdk1.7.0_*/bin/java 100
$ update-alternatives --install /usr/bin/javac javac
/usr/lib/jvm/jdk1.7.0_*/bin/javac 100
```

Verifique que Java se haya configurado correctamente ejecutando:

```
$ update-alternatives --display java
$ update-alternatives --display javac
$ update-alternatives --config java
$ update-alternatives --config javac
```

Verifique la versión de Java:

```
$ java -version
```

Instale ***ant***

```
$ cd ~
$ wget http://archive.apache.org/dist/ant/binaries/apache-ant-1.9.14-
bin.tar.gz
$ tar xvfvz apache-ant-1.9.14-bin.tar.gz
$ mv apache-ant-1.9.14 /usr/local/
$ sh -c 'echo ANT_HOME=/usr/local/  >> /etc/environment'
$ ln -s /usr/local/apache-ant-1.9.14/bin/ant /usr/bin/ant
```

Verifique la versión de ***ant*** de la siguiente manera:

```
$ ant -version
```

Cree directorios de trabajo para OpenIMSCore:

```
$ mkdir /opt/OpenIMSCore
$ cd /opt/OpenIMSCore
```

Descargue:

```
$ apt -y install subversion
$ svn checkout svn://svn.code.sf.net/p/openimscore/code/FHoSS/trunk
$ mv trunk FHoSS
```

Compile según la versión del ***jdk***:

```
$ cd FHoSS
$ export JAVA_HOME="/usr/lib/jvm/jdk1.7.0_80"
$ export CLASSPATH="/usr/lib/jvm/jdk1.7.0_80/jre/lib/"
$ ant compile deploy | tee ant_compile_deploy.txt
```

Ingrese en la carpeta ***deploy*** para cambiar los nombres de dominio y la dirección IP de la VM en todos los archivos de configuración

```
$ cd /opt/OpenIMSCore/FHoSS/deploy
$ grep -r open-ims.test *
$ find . -type f -print0 | xargs -0 sed -i 's/open-
ims.test/ims.<DOMINIO-IMS>/g'
$ grep -r 127.0.0.1 *
$ find . -type f -print0 | xargs -0 sed -i 's/127.0.0.1/<IP>/g'
```

Verifique con los comandos:

```
$ grep -r ims.<DOMINIO-IMS> *
$ grep -r <IP> *
```

Ingrese al archivo indicado y cambie la línea:

```
$ nano hibernate.properties
hibernate.connection.url=jdbc:mysql://127.0.0.1:3306/hss_db
```

Prepare la base de datos:

```
$ mysql
mysql> drop database hss_db;
mysql> create database hss_db;
mysql> quit
```

Importe la base de datos localizada en ***/opt/OpenIMSCore*** a ***hss_db***

```
$ cd /opt/OpenIMSCore
$ mysql -u root -p hss_db < FHoSS/scripts/hss_db.sql
$ mysql -u root -p hss_db < FHoSS/scripts/userdata.sql
```

Asigne los permisos a la base de datos ***hss_db***:

```
$ mysql
mysql> grant delete,insert,select,update on hss_db.* to hss@'%'
identified by 'hss';
```

Verifique la base de datos en cuanto al dominio y los usuarios creados, con la contraseña hss

```
$ mysql -u hss -p
mysql> show databases;
mysql> use hss_db;
mysql> select * from impu;
```

Prepare el script de inicio del HSS, copie el archivo startup.sh como hss.sh en el directorio root

```
$ cp /opt/OpenIMSCore/FHoSS/deploy/startup.sh /root/hss.sh
```

Y agregue lo siguiente al archivo ***hss.sh*** antes de ***echo Building Classpath***

```
cd /opt/OpenIMSCore/FHoSS/deploy
JAVA_HOME="/usr/lib/jvm/jdk1.7.0_80"
CLASSPATH="/usr/lib/jvm/jdk1.7.0_80/jre/lib/"
```

Inicie el HSS utilizando el archivo hss.sh

```
$ ./hss.sh
```

Ingrese a la interfaz web del HSS con la dirección ***http://<IP>:8080/***

```
user:      hssAdmin
password:  hss
```

Bibliografía

[1] N. Pignataro, P. Cristiani, D. Belotti, and P. R. Bocca, *Aspectos Técnicos de las Nuevas Tecnologías de Telecomunicaciones -"Diplomado en NGN" - Módulo 3*. ANTEL, 2010.

[2] G. Camarillo and M.-A. García-Martín, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, 3rd ed. Wiley, 2008.

[3] D. Blandón, Y. Díaz, F. G. Guerrero, J. C. Cuellar, A. Navarro C., and C. Ochoa A., *Medición de la calidad del servicio en Redes de Próxima Generación en Colombia*, 1st ed. Centro de Investigación de las Telecomunicaciones - CINTEL, 2010.

[4] E. Imene, D. Thierry, S. Michelle, and S. Tabbane, "Interworking Components for the end-to-end QoS into IMS-based architecture mono provider," in *Computers and Communications (ISCC), 2010 IEEE Symposium on*, 2010, pp. 628–633, doi: 10.1109/ISCC.2010.5546652.

[5] J. Liao, Q. Qi, T. Li, Y. Cao, and X. Zhu, "An optimized QoS scheme for IMS-NEMO in heterogeneous networks," *Int. J. Commun. Syst.*, vol. 25, no. 2, pp. 185–204, 2012, doi: 10.1002/dac.

[6] H. A. Lara Paz, María Camila; Coral Sarria, "QoS del servicio de Video Llamada en una red IMS. Virtualizada," Universidad del Cauca, 2017.

[7] T. Mácha, L. Nagy, Z. Martinásek, and V. Novotný, "IMS Mapping of QoS Requirements on the Network Level," *Elektrorevue*, vol. 1, no. 2, pp. 22–27, 2010.

[8] R. Hernández Sampieri, C. Collado Fernández, and M. del P. Baptista Lucio, *Metodología de la investigación*, 6th ed. Mexico, 2000.

[9] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed. California, 2017.

[10] UIT, *Recomendación UIT-T Y.2021 : Subsistema multimedios IP (IMS) para las redes de próxima generación*. 2006, pp. 1–14.

[11] Telefónica, *Las Telecomunicaciones y la Movilidad en la Sociedad de la Información*, 1st ed. Albadalejo, 2005.

[12] P. Podhradský, “New Multimedia Applications based on IMS NGN Architecture,” in *Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on*, 2011, pp. 1–4.

[13] UIT, *Recomendación UIT-T Y.2001 :Visión general de las redes de próxima generación*. 2004, pp. 1–10.

[14] M. Ilyas and S. A. Ahson, *IP Multimedia Subsystem (IMS) Handbook*, 1st ed. CRC Press, 2008.

[15] A. Handa, *System Engineering for IMS Networks*, 1st ed. Newnes, 2008.

[16] R. Copeland, *Converging NGN Wireline and Mobile 3G Networks with IMS: Converging NGN and 3G Mobile*, 1st ed. Auerbach Publications, 2008.

[17] P. Podhradský, R. Kadlic, J. Londák, O. Lábaj, and D. Levický, “Enhanced ICT in Virtual Training and m-learning,” in *ELMAR, 2011 Proceedings*, 2011, no. September, pp. 14–16.

[18] P. Bellavista, A. Corradi, and L. Foschini, “IMS-based presence service with enhanced scalability and guaranteed QoS for interdomain enterprise mobility,” *IEEE Wirel. Commun.*, vol. 16, no. 3, pp. 16–23, 2009, doi: 10.1109/MWC.2009.5109460.

[19] N. Pignataro, P. Cristiani, D. Belotti, and P. R. Bocca, *Aspectos Técnicos de las Nuevas Tecnologías de Telecomunicaciones -“Diplomado en NGN” - Módulo 4*. 2010.

[20] K. Al-Begain, C. Balakrishna, L. A. Galindo, and D. M. Fernandez, *IMS - A Development and Deployment Perspective*, 1st ed. Wiley, 2009.

[21] N. Psimogiannos, A. Sgora, and D. D. Vergados, “An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking,” *Comput. Commun.*, vol. 34, no. 9, pp. 1077–1099, Jun. 2011, doi:

10.1016/j.comcom.2010.02.017.

[22] T. Russell, *The IP Multimedia Subsystem IMS - Session Control and Other Network Operations*, 1st ed. McGraw-Hill Osborne Media, 2007.

[23] 3GPP, *3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2 (Release 14)*, vol. 1. 2016, pp. 0–316.

[24] CRC, “Resolución 5050 de 2016,” *Resolución*, no. 5050, p. 714, 2016.

[25] T. Janevski, *QoS for Fixed and Mobile Ultra-Broadband*, 1st ed. Great Britain: Wiley - IEEE, 2019.

[26] M. Boucadair, I. Borges, and P. M. Neves, *IP Telephony Interconnection Reference: Challenges, Models, and Engineering*. CRC PressINC, 2011.

[27] GSM Association, “SIP - SDP Inter - IMS NNI Profile,” *Off. Doc. IR.95*, pp. 1–161, 2018.

[28] GSM Association, “RCS Interworking Guidelines,” *Off. Doc. IR.90*, 2019.

[29] GSM Association, “IMS Roaming , Interconnection and Interworking Guidelines,” *Off. Doc. IR.65*, pp. 1–61, 2018.

[30] K. I. Lakhtaria, “Enhancing QOS and QOE in IMS enabled next generation networks,” *Int. J. Appl. graph theory Wirel. ad hoc networks Sens. networks*, vol. 2, no. 2, pp. 61–71, 2010, doi: 10.5121/jgraphoc.2010.2206.

[31] UIT-T, *Recomendación UIT-T E.800 Definiciones de términos relativos a la calidad de servicio*. 2008, pp. 1–34.

[32] T. Truong, T. Nguyen, and H. Nguyen, “On Relationship between Quality of Experience and Quality of Service Metrics for IMS-Based IPTV Networks,” in *Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2012 IEEE RIVF International Conference on*, 2012, pp. 1–6, doi: 10.1109/rivf.2012.6169844.

[33] H. Koumaras, N. Zotos, L. Boula, and A. Kourtis, “A QoE-aware IMS Infrastrusture for Multimedia Services,” in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, 2011, pp. 1–7.

[34] A. Cuevas and J. I. Moreno, “Managing QoS-enabled ‘ information transport

’ as any other service in NGN service platforms,” in *Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–6, doi: 10.1109/WCNC.2010.5506495.

[35] UIT- T, “G.1000 Calidad del servicio en las comunicaciones: marco y definiciones.,” *Ser. G Sist. Y MEDIOS Transm. Sist. Y REDES Digit. Calid. Serv. y Transm.*, pp. 58–60, 2001, [Online]. Available: http://www.itu.int/rec/T-REC-G.1000-200111-I/en.

[36] UIT-T, “Quality of service guaranteed mechanisms and performance model for public packet telecommunication data networks,” *Recom. Y.2617*, 2016.

[37] UIT-T, “Information technology – Quality of Service: Framework,” *Recom. X.641*, vol. 641, 1997.

[38] ITU-T, “Internet protocol data communication service – IP packet transfer and availability performance parameters,” *Recom. Y.1540*, 2019.

[39] J. C. Cuéllar Quiñonez, *Caracterización de mecanismos de QoS utilizados en redes NGN*. Lexinton, 2013.

[40] R. Suarez, A. Solarte, Z. María, Q. Cuéllar, and J. Carlos, “Herramienta para el monitoreo de parámetros de Calidad de Servicio en redes NGN Tools for monitoring Quality of Service parameters in Next Generation Networks,” *Rev. S&T*, vol. 11, no. 26, pp. 81–94, 2013, [Online]. Available: http://www.icesi.edu.co/revistas/index.php/sistemas_telematica.

[41] GSM Association, “Guidelines for IPX Provider networks (Previously Inter - Service Provider IP Backbone Guidelines),” *Off. Doc. IR.34*, no. 13, pp. 1–50, 2016, [Online]. Available: http://www.gsma.com/newsroom/all-documents/official-document-ir-34-guidelines-for-ipx-provider-networks-previously-inter-service-provider-ip-backbone-guidelines-2/.

[42] UIT-T, “Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet,” *Recom. Y.1541*, 2006.

[43] X. Marichal Borges, “Curso Profesional de MPLS QoS,” *Telecapp*, 2019. https://www.telecapp.com/ (accessed Apr. 25, 2020).

[44] M. S. Siddiqui and C. S. Hong, “Virtual platform support for QoS management in IMS based multiple provider networks,” *2010 Int. Conf. Netw. Serv. Manag.*, pp. 350–353, Oct. 2010, doi: 10.1109/CNSM.2010.5691231.

[45] B. Yu, D. Yu, J. Jia, and J. Lin, “A Review of the Policy-Based QoS Architecture in IMS,” in *2010 First International Conference on Pervasive Computing, Signal Processing and Applications*, Sep. 2010, pp. 175–178, doi: 10.1109/PCSPA.2010.54.

[46] B. Raouyane, M. Bellafkih, and D. Ranc, “QoS Management in IMS: DiffServ Model,” in *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies*, Sep. 2009, pp. 39–43, doi: 10.1109/NGMAST.2009.21.

[47] J. W. Evans and C. Filsfils, *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice*, 1st ed. Morgan Kaufmann, 2007.

[48] B. Raouyane, M. Bellafkih, M. Errais, and M. Ramdani, “IMS Management based eTOM framework for Multimedia service,” in *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International*, 2010, no. Figure 1, pp. 1–6.

[49] M. Ageal, R. Good, A. Elmangosh, M. Ashibani, N. Ventura, and F. Ben-, “Centralized policy provisioning for inter-domain IMS QOS,” in *EUROCON 2009*, 2009, pp. 1793–1797, doi: 10.1109/EURCON.2009.5167887.

[50] J. Baraković and H. Bajrić, “QoS Aspects in NGN Interconnection,” 2009.

[51] R. Yavatkar, D. Pendarakis, and R. Guerin, “RFC 2753 - A Framework for Policy- Based Admission Control.” 2000.

[52] S. Venkataram and P. Venkataram, “Transaction-based QoS management in a Hybrid Wireless Superstore Environment,” *I.J. Comput. Netw. Inf. Secur.*, vol. 3, no. March, pp. 1–11, 2011.

[53] C. Egger, M. Happenhofer, J. Fabini, and P. Reichl, “BIQINI – A Flow-Based QoS Enforcement Architecture for NGN Services,” in *Testbeds and Research Infrastructures, Development of Networks and Communities*,

2011, pp. 653–667.

[54] ETSI, *ES 282 003 - V3.4.0 - Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*, vol. 0. 2009, pp. 1–181.

[55] A. Bellabas and A. K. Najah, “Convergent IPTV Services over IP Multimedia Subsystem,” in *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, 2011, pp. 1–5.

[56] M. Samie, H. Yeganeh, and M. Shakiba, “A Proposed Model for QoS Provisioning in IMS-Based IPTV Subsystem,” in *2009 Fourth International Conference on Systems and Networks Communications*, Sep. 2009, pp. 113–118, doi: 10.1109/ICSNC.2009.102.

[57] 3GPP, *3GPP TS 23.203 Policy and charging control architecture (Release 14)*, vol. 0. 2015, pp. 0–245.

[58] T. Grgic, N. Boskovic, and M. Matijasevic, “QoS-enabled IPv6 Emulation Environment Based on the Open IMS Core,” in *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*, 2011, pp. 1–5.

[59] O. Magnus, S. Shabnam, R. Stefan, F. Lars, and C. Mulligan, *SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution*, 1st ed. Academic Press, 2009.

[60] 3GPP, *3GPP TS 23.107 Quality of Service (QoS) concept and architecture (Release 13)*, vol. 0. 2015, pp. 0–42.

[61] 3GPP, *3GPP TS 23.207 End-to-end Quality of Service (QoS) concept and architecture (Release 13)*, vol. 0. 2015, pp. 0–39.

[62] T. Grgic and M. Matijasevic, “Online charging in IMS for multimedia services with negotiable QoS requirements based on service agreements,” *Int. J. Intell. Inf. Database Syst.*, vol. 4, no. 6, pp. 656–672, 2010, doi: 10.1504/IJIIDS.2010.036899.

[63] L. Gupta, “QoS in interconnection of next generation networks,” *Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013*, no. July, pp. 91–96, 2013, doi: 10.1109/CICN.2013.29.

[64] L. Bonati, M. Polese, S. D’Oro, S. Basagni, and T. Melodia, “Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead,” *Comput. Networks*, vol. 182, no. December, pp. 1–32, 2020, doi: 10.1016/j.comnet.2020.107516.

[65] VMWare, “Virtualización,” *Virtualización*. https://www.vmware.com/co/solutions/virtualization.html#:~:text=Tipos de virtualización,-Virtualización de servidores&text=La virtualización de servidores permite,eficiencia del entorno de TI (accessed Feb. 28, 2021).

[66] Red Hat, “¿Qué es un hipervisor?,” *Virtualización*. https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor (accessed Feb. 28, 2021).

[67] Microsoft, “Introduction to Hyper-V on Windows 10,” *The home for Microsoft documentation and learning for developers and technology professionals*, 2018. https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ (accessed Mar. 03, 2021).

[68] VMWare, “VMware Workstation 16 Pro,” *VMWare*, 2013. https://www.vmware.com/co/products/workstation-pro/workstation-pro-evaluation.html (accessed Mar. 03, 2021).

[69] Oracle, “VirtualBox,” *VirtualBox*, 2007. https://www.virtualbox.org/ (accessed Mar. 03, 2021).

[70] F. Bellard, “What is QEMU?,” *QEMU*, 2013. https://www.qemu.org/ (accessed Mar. 03, 2021).

[71] Open Virtualization Alliance, “Kernel Virtual Machine,” *KVM*, 2008. https://www.linux-kvm.org/page/Main_Page (accessed Mar. 03, 2021).

[72] Cisco, “What is VIRL (Virtual Internet Routing Lab),” *Learning Network*, 2020. https://learningnetwork.cisco.com/s/article/what-is-virl-virtual-internet-routing-lab-x (accessed Mar. 03, 2021).

[73] Huawei, “eNSP - Enterprise Network Simulation Platform,” *Asistencia de servicio empresarial - Huawei*, 2018. https://support.huawei.com/enterprise/es/nce-data-communication/ensp-pid-9017384 (accessed Mar. 03, 2021).

[74] GNS3 Team, “GNS3,” *GNS3*, 2019. https://www.gns3.com/ (accessed Mar. 03, 2021).

[75] Eve-ng Ltd., “EVE - Emulated Virtual Environment,” *EVE-ng*, 2021. https://www.eve-ng.net/ (accessed Mar. 03, 2021).

[76] PNetLabs, “PNETLab (Packet Network Emulator Tool Lab),” *The PNETLab Store*, 2020. https://pnetlab.com/pages/main (accessed Mar. 03, 2021).

[77] The Kamailio SIP Server Project, “Kamailio,” *Welcome To Kamailio – The Open Source SIP Server*, 2015. https://www.kamailio.org/ (accessed Feb. 28, 2021).

[78] Fraunhofer FOKUS, “Open IMS Core,” *Open IMS Core’s Homepage*, 2008. http://openimscore.sourceforge.net/ (accessed Feb. 28, 2021).

[79] Metaswitch, “Project Clearwater,” *Clearwater IMS*, 2018. https://www.projectclearwater.org/.

[80] VideoLAN Organization, “VLC Media Player,” *Video LAN*, 2021. https://www.videolan.org/vlc/index.es.html.

[81] Wowza Media System, “Wowza Streaming Engine,” *Wowza Streaming Engine Reliable streaming — no matter the device, scale, or network condition.*, 2021. https://www.wowza.com/products/streaming-engine (accessed Feb. 28, 2021).

[82] Google Corp., “¿Por qué usar contenedores?,” *CONTENEDORES EN GOOGLE Una mejor manera de desarrollar e implementar aplicaciones*, 2020. https://cloud.google.com/containers?hl=es-419 (accessed Feb. 28, 2021).

[83] Docker, “What is a Container?,” *Docker*, 2018. https://www.docker.com/resources/what-container (accessed Mar. 03,

2021).

[84] Cloud Native Computing Foundation, “Cloud Native Computing Foundation becomes home to Pod-Native container engine project rkt,” *Cloud Native Computing Foundation*, 2017. https://www.cncf.io/announcements/2017/03/29/cloud-native-computing-foundation-becomes-home-pod-native-container-engine-project-rkt/ (accessed Mar. 03, 2021).

[85] Apache Foundation, “What is Mesos? A distributed systems kernel,” *Apache Mesos*, 2013. http://mesos.apache.org/.

[86] QXIP Team, “HOMER,” *100% Open-Source VoIP & RTC Capture, Troubleshooting & Monitoring*, 2020. https://github.com/sipcapture/homer (accessed Mar. 03, 2021).

[87] M. Vít, “VoIP Monitor,” *VoIP Monitor*, 2021. https://www.voipmonitor.org/ (accessed Mar. 03, 2021).

[88] S. Ltd., “Zoiper,” *Zoiper*, 2020. https://www.zoiper.com/ (accessed Mar. 03, 2021).

[89] Counterpath, “Bria Solo,” *Counterpath*, 2020. https://www.counterpath.com/ (accessed Mar. 03, 2021).

[90] Doubango, “Boghe IMS client,” *boghe*, 2015. https://code.google.com/archive/p/boghe/ (accessed Mar. 03, 2021).

[91] Doubango, “IMSDroid,” *imsdroid*, 2015. https://code.google.com/archive/p/imsdroid/ (accessed Mar. 03, 2021).

[92] T. W. Team, “Wireshark,” *About Wireshark*, 2012. https://www.wireshark.org/ (accessed Mar. 13, 2021).

[93] J. Dugan, S. Elliott, B. A. Mah, J. Poskanzer, and K. Prabhu, “iPerf,” *iPerf - The ultimate speed test tool for TCP, UDP and SCTP*, 2014. https://iperf.fr/ (accessed Mar. 13, 2021).

[94] X. Marichal, “Curso de Redes IP Backhaul,” *Telecapp*, 2020. https://telecapp.com/ (accessed May 19, 2020).

[95] X. Marichal, “Curso Profesional de MPLS QoS,” *Telecapp*, 2020.

https://telecapp.com/ (accessed Apr. 30, 2020).

[96] X. Marichal, “Curso Profesional de IP RAN,” *Telecapp*, 2020. https://telecapp.com/ (accessed Jan. 08, 2021).

[97] X. Marichal, “Curso de Ingeniería de Tráfico en Redes IP/MPLS,” *Telecapp*, 2020. https://telecapp.com/ (accessed May 20, 2020).

[98] B. Edgeworth, R. Rios, J. Gooley, and D. Hucaby, *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide* , no. 31574. 2019.

[99] R. Molenaar, “BGP Route Reflector,” *Network lessons*, 2020. https://networklessons.com/bgp/bgp-route-reflector (accessed Jan. 25, 2012).

[100] Juniper Networks Inc., “Descripción de las operaciones de etiqueta de MPLS en los conmutadores de la serie EX,” *Manual de usuario de MPLS aplicaciones*, 2020. .

[101] K. Barker, “MPLS Fundamentals,” *CBT Nuggets*, 2015. https://www.cbtnuggets.com/ (accessed Jan. 10, 2021).

[102] N. Leymann, B. Decraene, C. Filsfils, M. Konstantynowicz, and D. Steinberg, “Seamless MPLS Architecture,” *IETF*, 2015. https://tools.ietf.org/html/draft-ietf-mpls-seamless-mpls-07 (accessed Jan. 29, 2021).

[103] Juniper Networks, “Building multi-generation scalable networks with end-to-end MPLS,” 2012. [Online]. Available: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000452-en.pdf.

[104] M. S. Siddiqui, R. A. Shaikh, and C. S. Hong, “QoS Control in Service Delivery in IMS,” in *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, 2009, pp. 157–160.

[105] M. Bellafkih, D. Ranc, and R. Mohammed, “INQA : Management project of QoS in an architecture IMS,” in *Multimedia Computing and Systems, 2009. ICMCS ’09. International Conference on*, 2009, pp. 1–6.

[106] N. Russo, “Designing QoS for IP and MPLS Networks,” *Pluralsight*, 2020.

https://www.pluralsight.com/ (accessed Jan. 31, 2021).

[107] N. Russo, “Implementing and Validating QoS Designs,” *Pluralsight*, 2020. https://www.pluralsight.com/ (accessed Jan. 31, 2021).

[108] R. Molenaar, “Introduction to QoS,” *Quality of Service*, 2017. https://networklessons.com/quality-of-service/introduction-qos-quality-service (accessed Feb. 25, 2021).

[109] 3GPP, “3GPP TS 23.203.” 2019, [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810.

[110] 3GPP, “3GPP TS 23.501.” 3GPP Portal, 2020, [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[111] J. C. Cuéllar Quiñonez, *Caracterización de Mecanismos de QoS utilizados en Redes NGN: Simulación e Implementación*. LAP Lambert Acad. Publ., 2011.

[112] Cisco, “Quality of Service (QoS) Management for SGSN,” *Cisco*, 2016. http://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/20/SGSN/b_20_SGSN_Admin/b_20_SGSN_Admin_chapter_011011.pdf.

[113] F. J. Ramos de Santiago, “Análisis e implementación de un sistema real de medida de ancho de banda,” Universidad Autónoma de Madrid, 2010.

[114] University of Zilina, “NGN/IMS,” *Nerwork Information Library*, 2012. https://nil.uniza.sk/category/ngn-ims/.

[115] Calix, “How to use iPerf for bandwidth/throughput tests,” *Calix Community - Knowl. Artic.*, 2017, [Online]. Available: https://community.calix.com/s/article/How-to-use-iPerf-for-bandwidththroughput-tests-1.

[116] Code World, “Herramienta de prueba de rendimiento de red Iperf3,” *www.codetd.com*, 2020. www.codetd.com (accessed Mar. 13, 2021).

[117] X. Xiao, *Technical, Commercial and Regulatory Challenges of QoS*. Elsevier, 2008.

[118] Alcaldía de Bogotá, “Régimen legal de Bogotá,” *Compilación de Normatividad, Doctrina y Jurisprudencia*, 2021. https://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=28465 (accessed Apr. 12, 2021).

[119] I. Telecom Infra Project, “End-to-End Quality of Service Recommendations for Mobile Networks,” 2021. [Online]. Available: https://telecominfraproject.com/naas/.