

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA
**UNIVERSIDAD
CATÓLICA**
DEL PERÚ

PROPUESTA DE MIGRACIÓN DE LA RED NGN DE UNA OPERADORA IMPLEMENTADA EN IP HACIA MPLS

Tesis para optar el Título de Ingeniero de las Telecomunicaciones, que presenta el
bachiller:

Giancarlo García Girón

ASESOR: Ing. Diego Quintana Cruz

Lima, Noviembre de 2009

RESUMEN

La presente Tesis consiste en brindar una propuesta técnica para la migración del core de la red NGN de una operadora implementada en IP hacia IP/MPLS. Durante el desarrollo de este proyecto se presenta el marco teórico de las redes NGN y se realiza la comparación entre las tecnologías IP y MPLS con el objetivo de observar las ventajas que presenta MPLS al brindar QoS.

Luego, se presenta la Propuesta de migración en la cual se presenta el escenario inicial así como los aspectos técnicos, plan de trabajo y el escenario final de la migración.

Por último, se detallan las conclusiones obtenidas al final de este proyecto, recomendaciones y trabajos futuros.



DEDICATORIA



A mis padres,
A mis hermanas,
A mis abuelos,
A Yovi,
Y a mis amigos.

AGRADECIMIENTOS

En primer lugar, quiero agradecer a Dios por haberme permitido culminar esta Tesis y, además, por las experiencias y oportunidades ganadas a lo largo de este camino.

A mis padres y hermanas quienes me ayudaron a salir adelante y mantenerme en pie gracias a sus consejos y apoyo. Gracias por la mejor educación que haya podido recibir.

A Yovi, por su apoyo y compañía durante todas las amanecidas necesarias para poder realizar este proyecto además de su ayuda para la toma de decisiones. Gracias por estar a mi lado.

A mi tío Tony, por su apoyo en mis estudios.

Al ingeniero Igor Luna-Victoria, por su ayuda con la herramienta utilizada para la simulación y por sus consejos para la presentación de la Tesis.

Al ingeniero Diego Quintana, por aceptar ser mi asesor y por su ayuda con las correcciones y planteamientos de la Tesis.

A mis amigos y familia que sin querer olvido y colaboraron en el desarrollo de este proyecto.

Por último, quisiera agradecer a la Pontificia Universidad Católica del Perú que me permitió obtener los conocimientos necesarios para poder aplicarlos en el mundo profesional.

ÍNDICE

RESUMEN	II
DEDICATORIA	V
AGRADECIMIENTOS	VI
ÍNDICE	VII
LISTA DE FIGURAS	XI
LISTA DE TABLAS	XIII
GLOSARIO	XIV
1. FUNDAMENTO DE LA TESIS	1
1.1. INTRODUCCIÓN	1
1.2. DEFINICIÓN DEL PROBLEMA Y JUSTIFICACIÓN	1
1.3. OBJETIVOS	2
1.4. ESTRUCTURA DE LA TESIS	2
2. MARCO TEÓRICO	3
2.1. ESTUDIO DE LAS REDES NGN.....	3
2.1.1. Definición de NGN	3
2.1.2. Características de NGN	3
2.1.3. Arquitectura NGN.....	4
2.1.3.1. Diferentes capas	4
2.1.3.2. Definiciones	6
2.1.3.3. Arquitectura Funcional NGN de la ITU-T	7
2.1.4. Principios generales de la arquitectura funcional NGN	9
2.1.5. Tendencias en los modelos de red	10
2.1.6. Evolución de las redes hacia NGN.....	11
2.2. ESTUDIO DE LOS COMPONENTES DE LA ARQUITECTURA NGN.....	12
2.2.1. Media Gateway.....	12
2.2.1.1. Trunking Gateway	12
2.2.1.2. Access Gateway	13
2.2.1.3. Residential Gateway	13
2.2.2. Signaling Gateway	13
2.2.3. Universal Media Gateway	13
2.2.4. Media Gateway Controller.....	13
2.2.5. Servidor de aplicaciones.....	14
2.2.6. Interconexión con la PSTN	14
2.2.6.1. Emulación de la PSTN	14
2.2.6.2. Simulación de la PSTN	14
3. ANÁLISIS PREVIO A MIGRACIÓN	16
3.1. ESTUDIO DE LOS PROTOCOLOS Y NORMAS DE SEÑALIZACIÓN EMPLEADOS 16	16
3.1.1. SIP.....	16
3.1.1.1. Funcionamiento.....	16
3.1.1.2. Componentes.....	16
3.1.1.3. Mensajes.....	16
3.1.2. SIP-T	18
3.1.3. SIP-I.....	19
3.1.4. H.323.....	19
3.1.4.1. Componentes.....	19
3.1.4.2. Tipos de señalización.....	19
3.1.4.3. Procedimiento de una llamada	20
3.1.5. R2.....	22
3.1.5.1. Funcionamiento.....	22
3.1.5.2. Proceso de llamada.....	22

3.1.6.	SS7.....	24
3.1.6.1.	Definición.....	24
3.1.6.2.	Arquitectura de red SS7.....	24
3.1.6.3.	Pila de protocolos SS7.....	25
3.1.6.4.	Proceso de llamada.....	27
3.1.7.	SIGTRAN.....	28
3.1.7.1.	Definición.....	28
3.1.7.2.	Arquitectura.....	28
3.1.8.	MGCP.....	31
3.1.9.	H.248.....	32
3.1.10.	ISDN.....	32
3.1.10.1.	Canales.....	32
3.1.10.2.	Servicios.....	32
3.1.10.3.	Arquitectura de capas.....	33
3.2.	PARÁMETROS DE QoS.....	34
3.2.1.	Definición de QoS.....	34
3.2.2.	Parámetros de QoS.....	34
3.2.2.1.	Retardo.....	34
3.2.2.2.	Retardo medio.....	34
3.2.2.3.	Tasa de errores.....	35
3.2.2.4.	Tasa de pérdida de paquetes.....	35
3.2.2.5.	Jitter.....	35
3.2.2.6.	Tasa de paquetes espurios.....	35
3.2.2.7.	Porcentaje de indisponibilidad del servicio.....	35
3.2.3.	Clases de Servicio.....	35
3.2.3.1.	Clase 0: Aplicaciones en tiempo real muy interactivas.....	35
3.2.3.2.	Clase 1: Aplicaciones en tiempo real.....	36
3.2.3.3.	Clase 2: Transacciones de datos muy interactivas.....	36
3.2.3.4.	Clase 3: Transacciones de datos.....	36
3.2.3.5.	Clase 4: Exclusivo para aplicaciones de bajas pérdidas.....	36
3.2.3.6.	Clase 5: Aplicaciones tradicionales en redes IP.....	36
3.2.3.7.	Clase 6: Emulación de circuitos TDM con alta interacción.....	36
3.2.3.8.	Clase 7: Emulación de circuitos TDM.....	37
3.2.4.	QoS en NGN.....	37
3.3.	TIPOS DE TRÁFICO.....	38
3.3.1.	Multimedia.....	38
3.3.2.	Señalización.....	38
3.3.3.	Enrutamiento.....	38
3.3.4.	Operación y Mantenimiento.....	38
3.3.5.	Billing.....	38
3.4.	ARQUITECTURAS DE QoS EN IP.....	38
3.4.1.	IP Best Effort.....	38
3.4.2.	IntServ.....	39
3.4.2.1.	Funcionamiento.....	39
3.4.2.2.	Ventajas.....	39
3.4.2.3.	Desventajas.....	40
3.4.3.	DiffServ.....	40
3.4.3.1.	Funcionamiento.....	40
3.4.3.2.	Ventajas.....	41
3.4.3.3.	Desventajas.....	41
3.4.4.	MPLS.....	41
3.4.4.1.	Modos.....	41
3.4.4.2.	Conceptos Previos.....	42
3.4.4.3.	Funcionamiento.....	42
3.4.4.4.	MPLS LDP.....	44

3.4.4.5.	MPLS RSVP-TE	45
3.4.4.6.	Ventajas	45
3.4.4.7.	Desventajas	45
3.4.5.	Comparación IP y MPLS	46
3.4.5.1.	Comparación de cabeceras IP y MPLS	46
3.4.5.2.	Cuadro comparativo entre IP y MPLS	46
4.	PRUEBAS DE DESEMPEÑO	47
4.1.	PRINCIPIOS SIMULACIÓN	47
4.2.	SIMULACIÓN	47
4.2.1.	Detalles Previos	47
4.2.2.	Simulación IP <i>Best Effort</i>	50
4.2.3.	Simulación MPLS RSVP-TE	54
4.3.	RESULTADOS	58
5.	PROPUESTA DE MIGRACIÓN	60
5.1.	ESCENARIO INICIAL DE MIGRACIÓN	60
5.1.1.	Demanda actual de enlaces y tráfico	62
5.2.	PROPUESTA FINAL	63
5.2.1.	Aspectos Técnicos	63
5.2.1.1.	Verificación de routers	63
5.2.1.2.	Distribución de etiquetas	63
5.2.1.3.	Protocolo de enrutamiento	63
5.2.1.4.	Routers especiales	64
5.2.1.5.	Distribución de routers en el territorio peruano	64
5.2.1.6.	Justificación de ubicación de nodos y subnodos de la red	64
5.2.1.7.	Enlaces	65
5.2.1.8.	Conexiones con otros equipos NGN	65
5.2.1.9.	Direccionamiento IP	65
5.2.1.10.	Clasificación de tipos de servicios	66
5.2.1.11.	Gestión de equipos	66
5.2.2.	Escenario final	66
5.2.2.1.	Distribución de routers	67
5.2.2.2.	Direccionamiento IP	71
5.2.2.3.	Protocolo de enrutamiento	73
5.2.2.4.	Configuración de etiquetas	75
5.2.3.	Plan de trabajo	75
5.2.3.1.	Etapas de migración	75
5.2.3.2.	Desarrollo de las etapas	77
5.2.4.	Propuesta Económica	77
5.2.4.1.	Costo de <i>upgrades</i>	78
5.2.4.2.	Costo de personal	78
5.2.4.3.	Costo total	79
5.3.	JUSTIFICACIÓN DE LA PROPUESTA	79
5.4.	SERVICIOS A BRINDARSE	79
5.4.1.	Telefonía Local y LDN	80
5.4.2.	Telefonía LDI	80
5.4.3.	IP Centrex	80
5.4.4.	Primario IP	80
5.4.5.	Acceso Internet Residencial	80
5.4.6.	Acceso Internet Empresarial	81
5.4.7.	Servicio de red privada de datos	81
6.	CONCLUSIONES	82
7.	RECOMENDACIONES Y TRABAJOS FUTUROS	83
7.1.	RECOMENDACIONES	83

7.2. TRABAJOS FUTUROS	83
BIBLIOGRAFÍA.....	84
ANEXOS.....	88



LISTA DE FIGURAS

FIGURA 2-1: ARQUITECTURA NGN.....	5
FIGURA 2-2: ARQUITECTURA FUNCIONAL NGN.....	7
FIGURA 2-3: MODELO VERTICAL.....	10
FIGURA 2-4: MODELO HORIZONTAL.....	10
FIGURA 2-5: REDES CLÁSICAS.....	11
FIGURA 2-6: ELEMENTOS DE LA NGN.....	15
FIGURA 3-1: LLAMADA SIP.....	18
FIGURA 3-2: LLAMADA H.323.....	21
FIGURA 3-3: MULTITRAMA R2.....	22
FIGURA 3-4: LLAMADA R2.....	23
FIGURA 3-5: TIPOS DE ENLACE SS7.....	25
FIGURA 3-6: MODELO DE REFERENCIA OSI Y PILA DE PROTOCOLOS SS7.....	26
FIGURA 3-7: LLAMADA SS7.....	28
FIGURA 3-8: ARQUITECTURA SIGTRAN.....	29
FIGURA 3-9: PROTOCOLO M2PA.....	30
FIGURA 3-10: PROTOCOLO M2UA.....	30
FIGURA 3-11: PROTOCOLO M3UA.....	31
FIGURA 3-12: PROTOCOLO SUA.....	31
FIGURA 3-13: CABECERA MPLS.....	42
FIGURA 3-14: FUNCIONAMIENTO MPLS.....	44
FIGURA 4-1: TOPOLOGÍA DE RED A SIMULAR.....	48
FIGURA 4-2: TOPOLOGÍA DE SIMULACIÓN FINAL.....	50
FIGURA 4-3: RED DE SIMULACIÓN IP BEST EFFORT.....	51
FIGURA 4-4: INTERCAMBIO MENSAJES OSPF.....	51
FIGURA 4-5: FTP RETARDO.....	52
FIGURA 4-6: HTTP RETARDO.....	52
FIGURA 4-7: SIP RETARDO.....	53
FIGURA 4-8: VIDEOSTREAMING RETARDO.....	53
FIGURA 4-9: RTP RETARDO.....	54
FIGURA 4-10: RED DE SIMULACIÓN MPLS RSVP-TE.....	55
FIGURA 4-11: INTERCAMBIO DE MENSAJES OSPF.....	55
FIGURA 4-12: FTP RETARDO.....	56
FIGURA 4-13: HTTP RETARDO.....	56
FIGURA 4-14: SIP RETARDO.....	57
FIGURA 4-15: VIDEOSTREAMING RETARDO.....	57
FIGURA 4-16: RTP RETARDO.....	58
FIGURA 5-1: CORE IP INICIAL.....	60
FIGURA 5-2: ESCENARIO INICIAL DE MIGRACIÓN.....	61
FIGURA 5-3: DISTRIBUCIÓN DE ROUTERS.....	69
FIGURA 5-4: CORE MPLS FINAL.....	70
FIGURA 5-5: CORE NGN FINAL.....	71
FIGURA 5-6: DIRECCIONAMIENTO IP.....	73
FIGURA 5-7: ÁREAS OSPF.....	74

FIGURA 5-8: ETAPAS DE MIGRACIÓN76
FIGURA 5-9: TIEMPOS ESTIMADOS77



LISTA DE TABLAS

TABLA 3-1: PROTOCOLOS EN NGN.....	34
TABLA 3-2: CLASES DE CALIDAD DE SERVICIO.....	37
TABLA 3-3: CUADRO COMPARATIVO IP Y MPLS.....	46
TABLA 4-1: TRÁFICO A SIMULAR.....	48
TABLA 4-2: PROTOCOLOS IMPLEMENTADOS.....	49
TABLA 4-3: PARÁMETROS DE SIMULACIÓN.....	49
TABLA 4-4: RESULTADOS IP BEST EFFORT.....	54
TABLA 4-5: RESULTADOS MPLS.....	58
TABLA 5-1: ENLACES Y TRÁFICO SECTOR RESIDENCIAL.....	62
TABLA 5-2: ENLACES Y TRÁFICO SECTOR EMPRESARIAL.....	62
TABLA 5-3: DIRECCIONES IP.....	65
TABLA 5-4: NOMBRAMIENTO DE ROUTERS.....	67
TABLA 5-5: DIRECCIONAMIENTO IP.....	72
TABLA 5-6: ÁREAS OSPF.....	74
TABLA 5-7: FEC.....	75
TABLA 5-8: DEFINICIÓN DE ETAPAS DE MIGRACIÓN.....	76
TABLA 5-9: COSTO DE UPGRADES.....	78
TABLA 5-10: COSTO DE PERSONAL.....	78
TABLA 5-11: COSTO TOTAL.....	79

GLOSARIO

ACM	<i>Address Complete Message</i>
ADSL	<i>Asymmetric Digital Subscriber Line</i>
ATA	<i>Analog Telephone Adapter</i>
ATM	<i>Asynchronous Transfer Mode</i>
BA	<i>Behavior Aggregate</i>
BE	<i>Best Effort</i>
BICC	<i>Bearer Independent Call Control protocol</i>
BSC	<i>Base Station Controller</i>
CAS	<i>Channel Associated Signaling</i>
CDR	<i>Call Detail Record</i>
CIC	<i>Circuit Identification Number</i>
CLC	<i>Close Logical Channel</i>
DBW	<i>Dedicated Bandwidth</i>
DCF	<i>Disengage Confirm</i>
DoS	<i>Denial of service</i>
DPC	<i>Destination Point Code</i>
DRQ	<i>Disengage Request</i>
DS	<i>Differentiated Services</i>
DSCP	<i>Differentiated Service Code Point</i>
ESC	<i>End Session Command</i>
FEC	<i>Forwarding Equivalence Class</i>
FIFO	<i>First In First Out</i>
FTP	<i>File Transfer Protocol</i>
GTT	<i>Global Title Translation</i>
HTTP	<i>HyperText Transfer Protocol</i>
IAM	<i>Initial Address Message</i>
IETF	<i>Internet Engineering Task Force</i>
IP	<i>Internet Protocol</i>
IPDV	<i>IP Packet Delay Variation</i>
IPER	<i>IP Packet Error Ratio</i>
IPLR	<i>IP Packet Loss Ratio</i>
IPTD	<i>IP Packet Transfer Delay</i>
ISDN	<i>Integrated Services Digital Network</i>
ISUP	<i>ISDN User Part</i>
ITU	<i>International Telecommunication Union</i>

ITU-T	<i>International Telecommunication Union - Telecommunication Standardization Sector</i>
IUA	<i>ISDN User Adaptation</i>
Kbps	<i>Kilobit per second</i>
LAN	<i>Local Area Network</i>
LACNIC	<i>Latin American and Caribbean Internet Addresses Registry</i>
LDN	<i>Larga Distancia Nacional</i>
LDI	<i>Larga Distancia Internacional</i>
LDP	<i>Label Distribution Protocol</i>
LSP	<i>Label Switched Path</i>
LSR	<i>Label Switching Router</i>
LAP-D Link	<i>Access Protocol – D Channel</i>
MCU	<i>Multipoint Control Unit</i>
MEGACO	<i>Media Gateway Control Protocol</i>
MG	<i>Media Gateway</i>
MGC	<i>Media Gateway Controller</i>
MMUSIC	<i>Multimedia Session Control</i>
MPLS	<i>Multiprotocol Label Switching</i>
MTP	<i>Message Transfer Part</i>
NGN	<i>Next Generation Networks</i>
OPC	<i>Origination Point Code</i>
PABX	<i>Private Automatic Branch Exchange</i>
PHB	<i>Per-Hop Behavior</i>
POTS	<i>Plain Old Telephone Service</i>
PSTN	<i>Public Switched Telephone Network</i>
QoS	<i>Quality of Service</i>
RAS	<i>Registration, Admission and Status</i>
REL	<i>Release</i>
RFC	<i>Request for Comments</i>
RLC	<i>Release Complete</i>
RSVP	<i>Resource Reservation Protocol</i>
RTCP	<i>RTP Control Protocol</i>
RTP	<i>Real-time Transport Protocol</i>
SBW	<i>Statistical Bandwidth</i>
SCCP	<i>Signaling Connection Control Part</i>
SCP	<i>Service Control Point</i>
SCTP	<i>Stream Control Transmission Protocol</i>

SIGTRAN	<i>Signaling Transport</i>
SIP	<i>Session Initiation Protocol</i>
SDP	<i>Session Description Protocol</i>
SG	<i>Signaling Gateway</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SSH	<i>Secure Shell</i>
SSP	<i>Service Switching Point</i>
SS7	<i>Signaling System 7</i>
STM	<i>Synchronous Transport Module</i>
STP	<i>Signal Transfer Point</i>
TACACS	<i>Terminal Access Controller Access Control System</i>
TCAP	<i>Transaction Capabilities Applications Part</i>
TDM	<i>Time Division Multiplexing</i>
TELNET	<i>Telecommunication Network</i>
TS	<i>Time Slot</i>
TUP	<i>Telephone User Part</i>
VCi	<i>Virtual Channel Identifier</i>
VPI	<i>Virtual Path Identifier</i>
VoIP	<i>Voice over IP</i>
WAN	<i>Wide Area Network</i>
WiFi	<i>Wireless Fidelity</i>
WiMax	<i>Worldwide Interoperability for Microwave Access</i>
xDSL	<i>x Digital Subscriber Line</i>

CAPÍTULO 1

FUNDAMENTO DE LA TESIS

1.1. INTRODUCCIÓN

Debido a la alta exigencia en la calidad de servicio, las redes públicas de telefonía tienden a migrar a las Redes de Próxima Generación (NGN) con las cuales podrán soportar todos los servicios de voz y datos a través de una sola red basada en conmutación de paquetes. Todo esto, con la finalidad de brindar mayor confiabilidad en los enlaces así como también facilidad en la gestión y mantenimiento y obtener, como consecuencia, una reducción en los costos.

El objetivo de la presente Tesis consiste en dar una propuesta técnica para la migración de la red, en el nivel de transporte, del protocolo IP a IP/MPLS con el fin de proporcionar la calidad de servicio que las aplicaciones de hoy en día requieren para poder funcionar con toda su capacidad debido a la complejidad que estas presentan.

La metodología que se utiliza en esta propuesta consiste en la presentación del marco teórico necesario para poder entender la arquitectura NGN así como los equipos y protocolos utilizados en estas redes y de esta manera tener pleno conocimiento de cómo afectará la migración que se propone a la red ya existente.

A continuación se presenta la actual red NGN basada en IP la cual se propone migrar y, a la vez, se realiza un estudio de las diferentes formas existentes para obtener calidad de servicio y una comparación entre estas. Luego se realizan las pruebas correspondientes para reconocer las ventajas del protocolo que se utilizará para la migración, MPLS, frente al protocolo ya utilizado, IP, en cuestiones de calidad.

Por último, se realiza la propuesta técnica para la migración y los métodos para llevarla a cabo así como también los posibles resultados luego de este proceso.

1.2. DEFINICIÓN DEL PROBLEMA Y JUSTIFICACIÓN

Actualmente, las redes de los proveedores de telefonía pública utilizan la conmutación de circuitos con la cual se establece una ruta fija entre el transmisor y el receptor para ofrecer sus servicios. Este tipo de conmutación, si bien proporciona calidad de servicio no brinda la confiabilidad en el enlace por valerse de una sola ruta. Como opción a este tipo de comunicación, se tiene la conmutación de paquetes con la cual se obtiene una mayor confiabilidad debido a la existencia de una ruta que puede variar según el estado de la red permitiendo así, evitar congestiones o problemas que se pudieran dar dentro de esta.

Por otro lado, los actuales proveedores necesitan de redes diferentes para poder ofrecer sus diversos servicios como voz, datos, video, etc. lo cual hace que el costo de mantenimiento y operación aumente. En cambio, las Redes de Próxima Generación se basan en la conmutación de paquetes permitiendo proporcionar servicios de voz y otros como datos y

video por una misma red a costos razonables debido a la unificación de estas redes y la gestión centralizada que permite.

A través de la red NGN de una operadora, cuyo nivel de transporte se basa en IP, se pueden transportar los servicios mencionados anteriormente; sin embargo, este protocolo ya no cumple con las exigencias de calidad de servicio para los usuarios debido al aumento en la complejidad de las aplicaciones ya existentes y que irán apareciendo en el futuro.

El desarrollo de la presente Tesis asegurará la provisión de calidad de servicio a través de la migración de la red IP a la red MPLS con la finalidad de establecer un nivel óptimo en los servicios de voz, datos y video para satisfacer la cada vez más elevada exigencia de calidad por parte de los usuarios.

1.3. OBJETIVOS

La descripción mostrada anteriormente permite plantear los siguientes objetivos para el desarrollo de la tesis:

- Estudio de las redes NGN, su arquitectura y protocolos de señalización así como la comparación de los diferentes mecanismos que permitan brindar QoS.
- Brindar una propuesta técnica para la migración de IP a IP/MPLS en la red NGN de una operadora en el escenario peruano con el fin de determinar el papel fundamental que cumple MPLS dentro de esta arquitectura para proporcionar calidad de servicio.

1.4. ESTRUCTURA DE LA TESIS

La Tesis contiene en total 6 capítulos, incluido el capítulo de Fundamentos de la Tesis. Cada capítulo se detalla a continuación:

- El capítulo 1 especifica los fundamentos de la tesis y los objetivos.
- En el capítulo 2, se realiza el estudio de las redes NGN tanto en su arquitectura así como los elementos que las conforman.
- En el capítulo 3, se realiza el análisis previo mediante el estudio de los diferentes protocolos y normas de señalización utilizados en las redes NGN, los parámetros de QoS a utilizar y se definen las arquitecturas que proporcionan QoS.
- En el capítulo 4, se detallan las pruebas de desempeño a realizar para la comparación entre IP y MPLS con el objetivo de determinar la arquitectura que ofrece QoS en el nivel *core*.
- El capítulo 5 detalla el escenario inicial de migración y la propuesta final para la migración de IP a IP/MPLS en la red NGN.
- Por último, en los capítulos 6 y 7, se mencionan las conclusiones finales, recomendaciones y trabajos futuros.

CAPÍTULO 2

MARCO TEÓRICO

2.1. ESTUDIO DE LAS REDES NGN

2.1.1. Definición de NGN

Por sus siglas en inglés, NGN, *Next Generation Networks*, hace referencia a las Redes de Próxima Generación las cuales marcarán la evolución de las actuales redes tanto a nivel de *core* o *backbone* y acceso así como los servicios que se podrán brindar a través de estas. Debido al incremento de tráfico a través de las redes actuales por la aparición de nuevos servicios, se hace necesaria la optimización de estas. Como consecuencia, se produce la convergencia hacia este nuevo modelo de red.

Actualmente, no se ha podido llegar a un acuerdo para la definición de NGN debido a que ninguno de los conceptos que se tienen abarcan todos los escenarios posibles según el entorno y situación en que se den. Sin embargo, según las diferentes definiciones dadas por diversos organismos, encontrados en [TEL2005], se puede notar que todas coinciden en que NGN es una red convergente multiservicios constituida por diferentes niveles, los cuales se basan en una serie de normas para permitir la integración de todos los servicios bajo una misma red mediante la separación de las funciones de transferencia de información y el control de esta transferencia.

La presente tesis se basa en la definición dada por la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) según la referencia bibliográfica [ITU2004] donde se menciona que NGN es una “red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la calidad de servicio, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios”.

2.1.2. Características de NGN

Debido a la necesidad de convergencia y optimización de las actuales redes como consecuencia del aumento del tráfico digital, se deben tener en cuenta las siguientes características para que una red NGN pueda ser llamada así. Estas características han sido tomadas de las referencias bibliográficas [ITU2004] y [ITU2005A].

- Transferencia de información basada en paquetes.
- Separación entre las funciones de control, transporte y servicio.

- Capacidades de banda ancha con garantías de calidad de servicio de extremo a extremo de forma transparente para el usuario.
- Utilización de interfaces y protocolos abiertos con el fin de obtener la interoperabilidad entre productos de diferentes fabricantes y además con otras redes ya existentes.
- Movilidad generalizada, es decir, dará a los usuarios la habilidad para comunicarse y acceder, mediante sus terminales, a los servicios independientemente de su ubicación o el entorno tecnológico en el que se encuentren.
- Convergencia de servicios entre redes fijas y móviles.
- Soportará conexiones con redes acceso de diferentes tecnologías y capacidades.
- Disociación entre la provisión del servicio y el transporte de este, es decir, el desacoplamiento del acceso y el transporte.
- Soporte de servicios y aplicaciones de diferente naturaleza: en tiempo real/no tiempo real, *streaming* y servicios multimedia.
- Acceso sin restricciones de los usuarios a diferentes proveedores de servicios.
- Variedad de esquemas de identificación la cual puede ser resuelta con el direccionamiento IP.
- Cumplimiento de todos los requisitos de regulación (comunicaciones, emergencia, seguridad, privacidad, interceptación legal, etc.).
- Características unificadas para el mismo servicio, como es percibida por el usuario.

2.1.3. Arquitectura NGN

Debido a que las redes actuales presentan complejidad al momento de acceder a los servicios que estas brindan, las Redes de Próxima Generación deberán presentar una arquitectura que permita la integración perfecta de servicios de telecomunicaciones, tanto nuevos como tradicionales [REA2008] permitiendo así que estos últimos sean preservados. Para este fin, estos tipos de redes deberán poseer interfaces y protocolos abiertos permitiendo la interoperabilidad de productos de distintos proveedores y el soporte de múltiples tecnologías de acceso.

2.1.3.1. Diferentes capas

De una manera más simplificada, se puede dividir la arquitectura de este tipo de redes a nivel de entidades funcionales, obteniendo cuatro diferentes capas [ZAM2005] y [GON2006].

a) Capa de Acceso y Transporte

El nivel de Acceso comprende las diferentes tecnologías utilizadas para alcanzar al usuario, llamadas también tecnologías de última milla las cuales comprenden las

tecnologías de cobre, como Cable, xDSL, etc.; y las inalámbricas, como WiFi, WiMax, etc.

El nivel de Transporte es el que proporciona el enrutamiento y/o conmutación del tráfico. Se puede basar en diferentes tecnologías como Frame Relay, ATM, IP o MPLS con el fin de garantizar la calidad de servicio.

b) Capa de Medios

En esta capa, se encuentran pasarelas cuya función es adaptar el tráfico (voz u otros) a la red de transporte. Estas pasarelas de medios se interconectan ya sea con los dispositivos de usuario final, con redes de acceso o con la Red Telefónica Pública Conmutada (PSTN).

c) Capa de Control

Como su nombre indica, esta capa se encarga del control de las diferentes funciones de la red facilitando el aprovisionamiento, supervisión y mantenimiento. Es además, esencial para reducir costos ya que la gestión de la red está centralizada en esta capa.

d) Capa de Servicios

Esta capa es la que está constituida por los diferentes equipos y servidores que brindan los servicios y aplicaciones disponibles a la red. Estos servicios se ofrecerán sin importar la ubicación del usuario por lo que deberán ser independientes de la tecnología de acceso que se utilice.

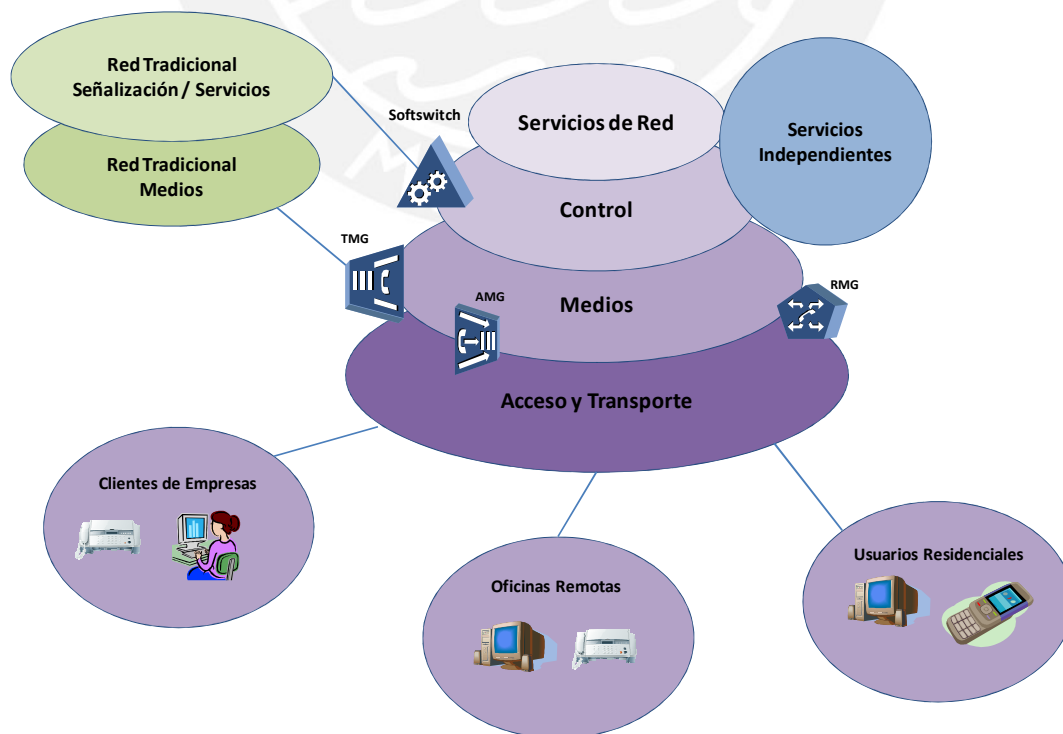


FIGURA 2-1: ARQUITECTURA NGN

2.1.3.2. Definiciones

- Plano: Categoría que identifica a una colección de objetos que ejecutan funciones similares o complementarias.
- Estrato: Categoría que identifica a un nivel independiente cuyos miembros realizan, en conjunto, una misma función o funciones complementarias.

De acuerdo a la Recomendación Y.2001 de la ITU-T [ITU2004], las funciones de la NGN se dividen en dos estratos independientes llamados Estrato de Servicios y Estrato de Transporte. Esta independencia se logra debido a que cada uno de estos estratos está constituido por sus respectivos planos de usuario, control y gestión donde cada plano tiene diferentes funciones.

Según [ITU2005A] se tienen las siguientes definiciones:

a) Estrato de Transporte

Parte de la NGN que provee las funciones para el control y gestión de los recursos de transporte y la transferencia de datos entre entidades terminales.

b) Estrato de Servicios

Parte de la NGN que provee las funciones que permiten la transferencia de datos entre los usuarios y servicios así como las funciones para el control y gestión de los recursos de los servicios de la red.

c) Plano de Transporte

Provee transferencia, ya sea unidireccional o bidireccional, de información de usuario de un lugar a otro.

d) Plano de Usuario

Clasificación para los objetos que permiten la transferencia de información final para el usuario.

e) Plano de Control

Conjunto de funciones que controlan la operación de las entidades en el estrato que se esté analizando. Además, incluye las funciones requeridas para el soporte de este control.

f) Plano de Gestión

Conjunto de funciones para la gestión de las entidades del estrato bajo análisis así como las funciones necesarias para el soporte de esta gestión.

2.1.3.3. Arquitectura Funcional NGN de la ITU-T

La arquitectura funcional descompone la NGN en una serie de entidades, cada una de las cuales proveen una única función como se puede observar en la Figura 1-2.

Cada estrato realiza diferentes funciones [ITU2005B]:

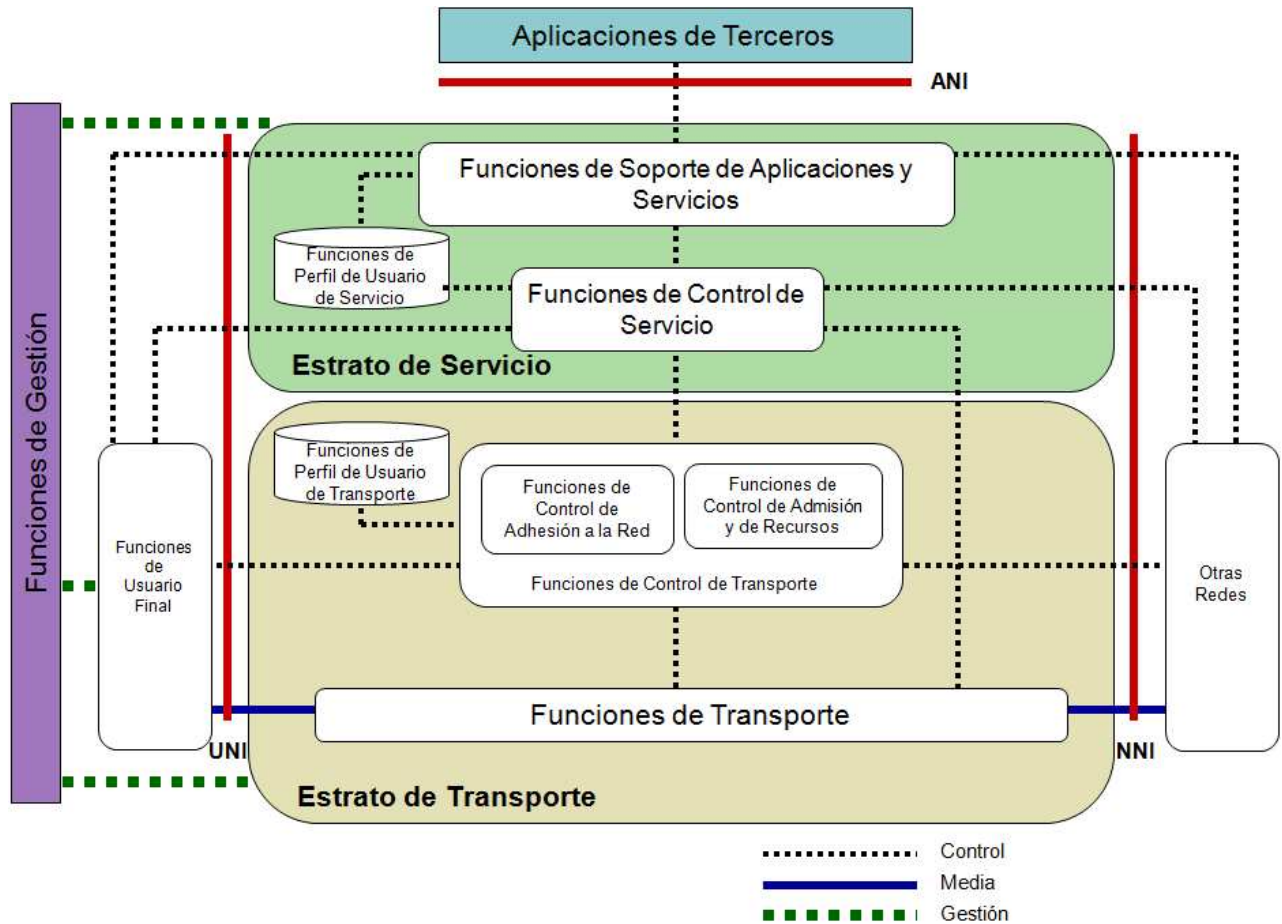


FIGURA 2-2: ARQUITECTURA FUNCIONAL NGN

a) Funciones del estrato de Transporte

Incluye las funciones de Transporte y Control de este estrato.

- **Funciones de Transporte**

Proveen la conectividad para todos los componentes y funciones físicamente separadas en la NGN. Además proveen soporte para la transferencia de información así como la transferencia de información de control y gestión.

- **Funciones de Acceso**

Permiten que los usuarios finales tengan acceso a la red core así como el manejo de políticas de QoS tratando directamente con el tráfico de usuario.

Para estas funciones, se tienen diferentes tecnologías como xDSL, cable, inalámbricas y ópticas.

- Funciones de Borde

Se utilizan para procesamiento de tráfico de diferentes redes de acceso los cuales se dirigen hacia la red *core* de transporte. Estas funciones dan soporte a QoS y el control de tráfico.

También son usadas entre redes *core* de transporte.

- Funciones de Núcleo de Transporte

Estas funciones son las responsables de asegurar el transporte de información a través de la red *core*. Proveen además, manejo de políticas de QoS y de seguridad.

- Funciones de Gateway

Proveen la capacidad para interconectarse con otras redes ya sea con redes existentes (PSTN/ISDN, Internet, etc.) o con otras NGN. Estas funciones pueden ser controladas con las Funciones de Control del estrato de Servicio o con las Funciones de Control del estrato de Transporte.

- Funciones de manejo de media

Permiten el procesamiento de información para la provisión del servicio como generación de señales de tono, eliminación de eco, etc.

▪ **Funciones de Control de Transporte**

- Funciones de Control de Adhesión a la Red

Incluye las funciones de iniciación y registro de usuario a nivel de Acceso para acceder a los servicios de la NGN. Proveen identificación y autenticación así como el manejo de direcciones y sesiones.

Proveen también provisión dinámica de direcciones IP, autenticación al nivel IP y autorización de la red de acceso basado en el perfil de usuario.

- Funciones de Control de Admisión y de Recursos

Regula la negociación y asignación de recursos entre las Funciones de Control del estrato de Servicio y las Funciones de Transporte. Además, controla y gestiona las políticas de QoS.

Estas dos funciones interactúan durante el acceso del usuario a la red comprobando el nivel de servicio acordado con el proveedor de los servicios de la NGN.

- **Funciones de Perfil de Usuario de Transporte**

Hacen referencia a una base de datos la cual contiene perfiles de usuario. Estos incluyen información para cada usuario además de información de control en el estrato de Transporte.

- b) Funciones del estrato de Servicio**

- **Funciones de Control de Servicio**

Incluye funciones de control de sesiones, registro, autenticación y autorización en el nivel de servicio.

- **Funciones de Soporte de Aplicaciones**

Provee funciones de registro, autenticación y autorización en el nivel de Aplicación.

- **Funciones de Perfil de Usuario de Servicio**

Representa la información de usuario y otra información de control mediante perfiles de usuario en el estrato de Servicio en una base de datos.

- c) Funciones de Usuario final**

Permite el soporte de diferentes equipos de usuario final ya sean antiguos o de última generación, así como fijos o móviles.

- d) Funciones de Gestión**

Son funciones que permiten la gestión de la red NGN con la finalidad de proveer sus servicios con la calidad, seguridad y confiabilidad esperada. Estas funciones pueden ser aplicadas en el estrato de Transporte o de Servicio.

Incluyen la gestión de fallas, configuraciones, seguridad, desempeño y facturación.

2.1.4. Principios generales de la arquitectura funcional NGN

De la arquitectura funcional propuesta por la ITU-T, se pueden resaltar las siguientes características y principios según [MAR2002] y [ITU2005B]:

- Enfoque más orientado a datos, es decir, el transporte se basa en paquetes.
- Interfaces abiertas en cada nivel de red.
- Dimensionado flexible del ancho de banda.
- Migraciones de software más eficientes en los nodos que la controlan, reduciendo los costos operativos.
- Soporte de múltiples tecnologías de acceso.
- Control distribuido.

- Provisión de servicios independiente debido a que esta provisión está separada de la operación de la red.
- Soporte de servicios de redes convergentes facilitando el uso de servicios multimedia.
- Mayor seguridad y protección

2.1.5. Tendencias en los modelos de red

Durante los últimos años, las redes se han basado en un modelo vertical, en el cual se tenían redes separadas para cada servicio que ofrecía un proveedor de Telecomunicaciones.

Presenta las siguientes características:

- Presenta una dependencia entre las redes y los servicios, donde cada servicio está ligado a una tecnología de acceso específica.
- Cuando se tienen muchos servicios, se complica la integración en el acceso.

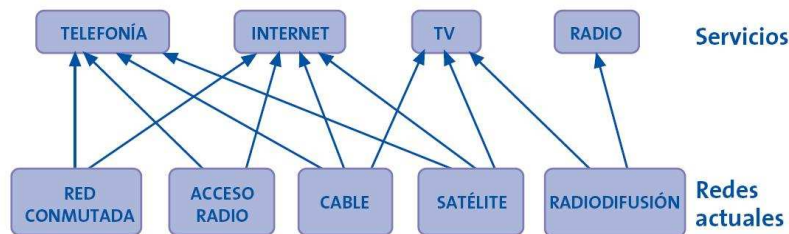


FIGURA 2-3: MODELO VERTICAL

Fuente: “Integración de infraestructuras Mediante NGN” [TEL2005A]

Mientras la necesidad de calidad de servicio así como la variedad de servicios por parte de los usuarios aumenta, estas redes se vuelven más ineficientes en cuestión de costo, mantenimiento y operación lo que ha ocasionado la aparición del modelo horizontal en el que se logra la independencia entre red y servicio por medio de una infraestructura común.

Este modelo presenta las siguientes características:

- Provee una interfaz común para acceso y servicio la cual provee la calidad, seguridad y confiabilidad requerida por los servicios.
- Simplifica la introducción de nuevos dispositivos y servicios.

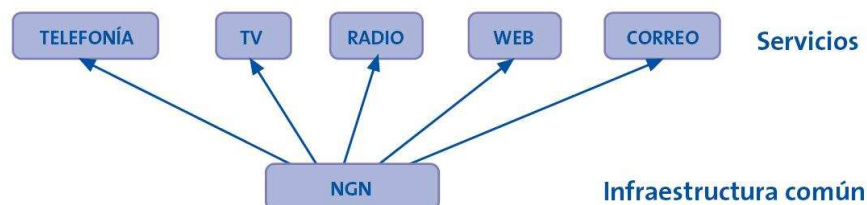


FIGURA 2-4: MODELO HORIZONTAL

Fuente: “Integración de infraestructuras Mediante NGN” [TEL2005A]

2.1.6. Evolución de las redes hacia NGN

A continuación se describe el proceso de evolución hacia las Redes de Próxima Generación (NGN) tomando como punto de partida las redes clásicas así como los factores que llevaron a dicha evolución [TEL2005A].

Para tener un mejor entendimiento de este proceso de evolución, primero es necesario describir las características de las redes que han predominado hasta la actualidad, llamadas también redes clásicas.

- El ancho de banda es escaso y, en consecuencia, caro.
- Presentan un modelo vertical, es decir, los servicios se encuentran ligados a la infraestructura de red.
- Los equipos de red son complejos, costosos así como de difícil y costosa explotación.
- La calidad de servicio se alcanza mediante la asignación y reserva de recursos.
- Los servicios masivos de distribución de contenidos presentan gran complejidad debido a que estas redes no soportan la tecnología multicast de forma nativa.



FIGURA 2-5: REDES CLÁSICAS

Fuente: "Redes NGN" [VIL2008]

Con el paso de los años, las necesidades de los usuarios fueron cambiando y pasaron a ser más exigentes y, de la misma forma, el cambio del mercado de las telecomunicaciones originó diversos factores que motivaron la evolución de estas redes clásicas:

- Tendencia hacia la apertura, es decir, desregulación y liberación, impulsando la libre competencia y generando como consecuencia la aparición de nuevos servicios ofrecidos por los operadores.
- Incapacidad de las redes clásicas para el soporte de nuevos servicios.

- Desarrollo de Internet desencadenando, con el paso de los años, el crecimiento del tráfico lo que ha originado la congestión de la red.
- Necesidad de reducir costos.
- Necesidad de compartir infraestructuras de red.
- Necesidad de simplificar y unificar la gestión, operación y mantenimiento tanto de la red como de los servicios.
- Debido a estos factores, el proceso de evolución de estas redes clásicas tendrá una tendencia hacia el modelo NGN, es decir pasará de un modelo vertical a un modelo horizontal. Para que esto sea posible, la evolución partirá desde el *core* de la red y se irá extendiendo hacia el nivel de acceso de tal forma que las tecnologías existentes en este nivel, puedan seguir siendo utilizadas.

2.2. ESTUDIO DE LOS COMPONENTES DE LA ARQUITECTURA NGN

2.2.1. Media Gateway

Es el equipo que actúa como interfaz entre el *core* de la red NGN con otra que transporta diferentes tipos de datos permitiendo la intercomunicación de estos convirtiendo los datos de un tipo al otro. De esta forma, se logra el acceso de los usuarios a los servicios brindados por estas redes.

El Media Gateway (MG) tiene diferentes características [NOR2007], entre ellas:

- Acepta todo tipo de tráfico como voz, datos y video.
- Permite el uso de diferentes interfaces como STM-1, hacia la red de transporte; E1, hacia la PSTN; Ethernet, FastEthernet o GigabitEthernet, hacia la red de conmutación de paquetes; entre otras.
- Compresión y paquetización de la voz utilizando diferentes codecs como ITU-T G.711, G.729, etc.
- Cancelación de eco.
- Utilización de mecanismos de tratamiento para brindar Calidad de Servicio.

Existen diferentes MG según el tipo de red con la que se conectan, entre estos [GON2006], [ITU2005B], [STA2005] y [TEL2007]:

2.2.1.1. Trunking Gateway

Provee la interconexión entre la red basada en paquetes de la NGN y las líneas troncales provenientes de la red TDM de la PSTN mediante la conversión de flujos TDM de 64 Kbps en paquetes de datos y viceversa. Soporta funciones de paquetización, control de eco, etc.

2.2.1.2. Access Gateway

Permite la conexión de los usuarios con diferentes tecnologías de acceso a la red *core* IP sirviendo como interfaz entre estos. Entre los usuarios, se tienen:

- Usuarios de líneas analógicas.
- Usuarios de servicios ISDN.
- Usuarios de PABX.
- Usuarios con acceso xDSL.

2.2.1.3. Residential Gateway

Es un dispositivo que permite la conexión entre la red del operador y las aplicaciones en el local del usuario; es decir, entre la LAN y la WAN. Este dispositivo es utilizado por los usuarios de redes analógicas, ADSL, acceso por cable, WiMax, etc. permitiendo que estos puedan conectar directamente al Gateway sus equipos como teléfonos, computadoras, TV, etc.

La diferencia con el Access Gateway es que el Residential Gateway se encuentra ubicado en el local del usuario permitiendo que este tenga acceso a los servicios de la NGN por un sólo equipo.

2.2.2. Signaling Gateway

Es el elemento de la red que funciona como interfaz entre la red de conmutación de paquetes de la NGN y la PSTN realizando la conversión de señalización entre estas dos redes, usualmente, de SS7 a IP y viceversa.

2.2.3. Universal Media Gateway

Es equivalente a un Trunking Gateway pero que además posee funciones de Signaling Gateway y Access Media Gateway pudiendo conectar diferentes dispositivos como centrales de la PSTN, PABX, BSC y otras redes a la NGN. Realiza la conversión de protocolo por uno que pueda ser entendido por el Softswitch.

2.2.4. Media Gateway Controller

También llamado Softswitch, es el elemento del *core* de la NGN que implementa el *switching* mediante software con el objetivo de administrar el control de las llamadas y las funciones de señalización. Sus principales funciones son [NOR2007]:

- Control de las llamadas.
- Control de los Media Gateways.
- Control del Signaling Gateway permitiendo la interoperabilidad entre los protocolos de señalización.

- Control de conexión.
- Permite el acceso a los servidores de aplicaciones para proveer los diferentes servicios de la NGN.
- Asignación de recursos.
- Autenticación y tarificación.

2.2.5. Servidor de aplicaciones

Es el elemento encargado de la ejecución de los servicios como el servidor de llamadas, el servidor de mensajes, etc. Aparece como resultado de la separación del control del servicio y de las llamadas. Entre otros servidores, también se tienen los de registro de llamadas (CDR), tarificación, autenticación y autorización.

2.2.6. Interconexión con la PSTN

Entre las diferentes formas de interconectar la PSTN con la NGN se tienen [ITU2005B]:

2.2.6.1. Emulación de la PSTN

Provee los servicios de la red clásica de telefonía mediante el uso de mecanismos de adaptación, como Trunking Media Gateway y Access Media Gateway, hacia la red de conmutación de paquetes. Este tipo de interconexión soporta el uso de los dispositivos terminales clásicos.

2.2.6.2. Simulación de la PSTN

Se basa en los servicios brindados por la red de telefonía clásica para brindar servicios similares. Esto se alcanza mediante el uso de sesiones sobre interfaces e infraestructura basadas en conmutación de paquetes y la utilización de Teléfonos IP o terminales de adaptación, ATAs, conectados a teléfonos clásicos.

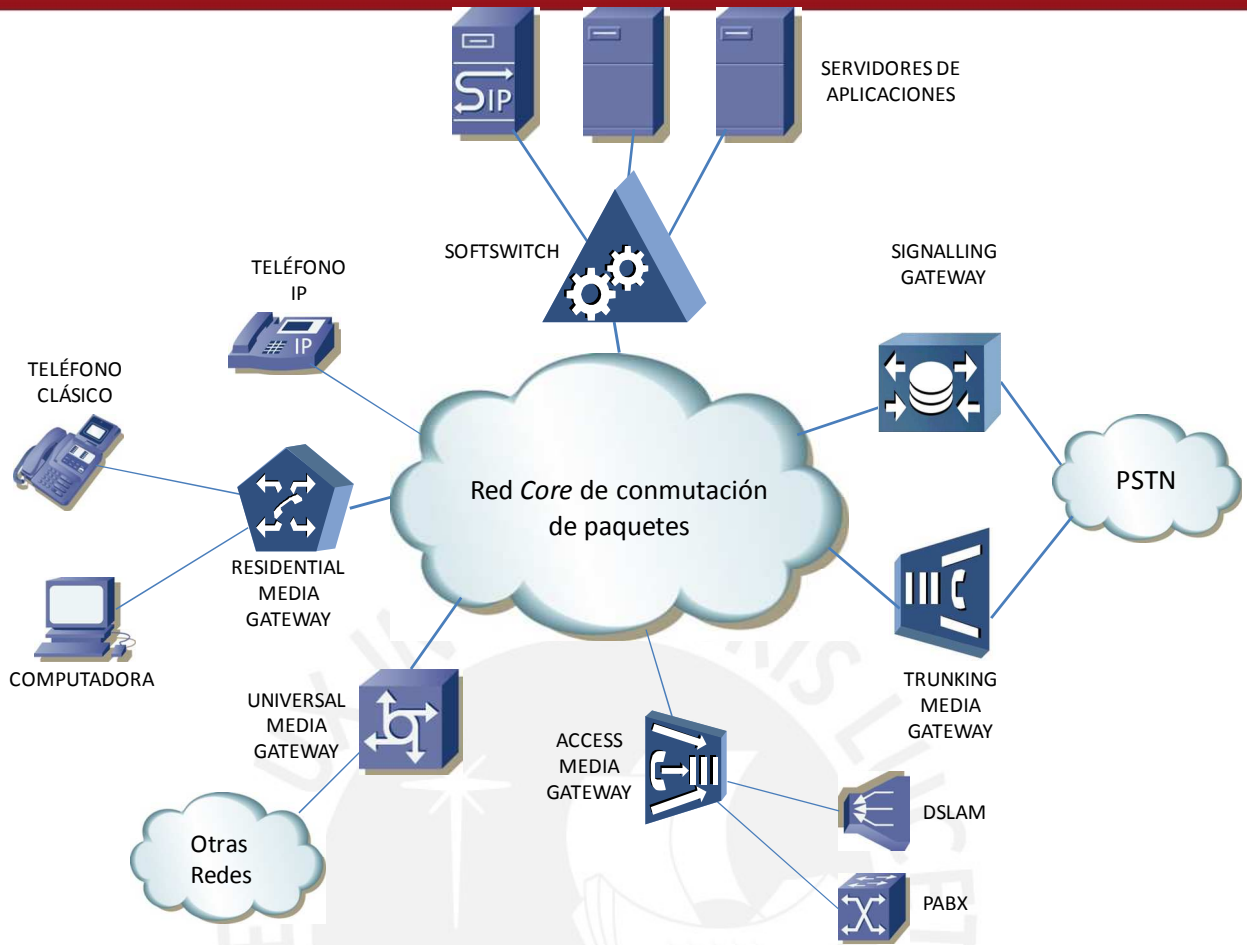


FIGURA 2-6: ELEMENTOS DE LA NGN

CAPÍTULO 3

ANÁLISIS PREVIO A MIGRACIÓN

3.1. ESTUDIO DE LOS PROTOCOLOS Y NORMAS DE SEÑALIZACIÓN EMPLEADOS

3.1.1. SIP

SIP es un protocolo de señalización perteneciente al nivel de aplicación que permite el establecimiento de comunicaciones multimedia sobre redes IP mediante la iniciación, modificación y finalización de sesiones. Fue desarrollado por el grupo MMUSIC del IETF e inicialmente publicado en la RFC2543 y posteriormente modificado en la RFC3261.

3.1.1.1. Funcionamiento

Este protocolo abierto se fundamenta en una arquitectura simple textual de respuesta a pedidos similar al protocolo HTTP [OEA2006] y en una arquitectura cliente – servidor en la cual el cliente inicia las llamadas y el servidor responde a estas. Funciona en colaboración con otros protocolos como SDP, para la comunicación de parámetros como puertos IP y *codecs* empleados, y RTP, para el transporte de los contenidos de voz y video.

3.1.1.2. Componentes

Los componentes de SIP son [ROD2005] y [QUI2007]:

a) User Agent (UA):

Consisten en dos partes distintas las cuales están presentes en todos los agentes de usuario:

- User Agent Client (UAC): genera peticiones SIP y recibe respuestas a esas peticiones.
- User Agent Server (UAS): genera respuestas a las peticiones SIP.

b) Servidores SIP:

- Proxy Server: es una entidad intermedia que retransmite solicitudes y decide a qué otro servidor debe remitir.
- Registrar Server: recibe peticiones de registro y hace la correspondencia entre direcciones IP y SIP con el fin de brindar un servicio de localización.
- Redirect Server: retransmite las peticiones recibidas hacia el próximo servidor.

3.1.1.3. Mensajes

Se definen dos tipos de mensajes [RFC3261]:

a) Peticiones:

Existen seis métodos básicos que describen las peticiones de los clientes:

- Invite: permite invitar a un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
- ACK: confirma el establecimiento de una sesión.
- Option: solicita información de un servidor.
- Bye: indica la terminación de una sesión
- Cancel: cancela una petición pendiente.
- Register: registra al Agente Usuario.

b) Respuestas:

Existen seis respuestas a las peticiones de los clientes las cuales se diferencian por el primer dígito de su código:

- 1xx: Mensajes provisionales.
- 2xx: Respuestas de éxito.
- 3xx: Respuestas de redirección.
- 4xx: Respuestas de falla de método.
- 5xx: Respuestas de fallas de servidor.
- 6xx: Respuestas de fallas globales.

A continuación se muestra el proceso para una llamada utilizando el protocolo SIP.

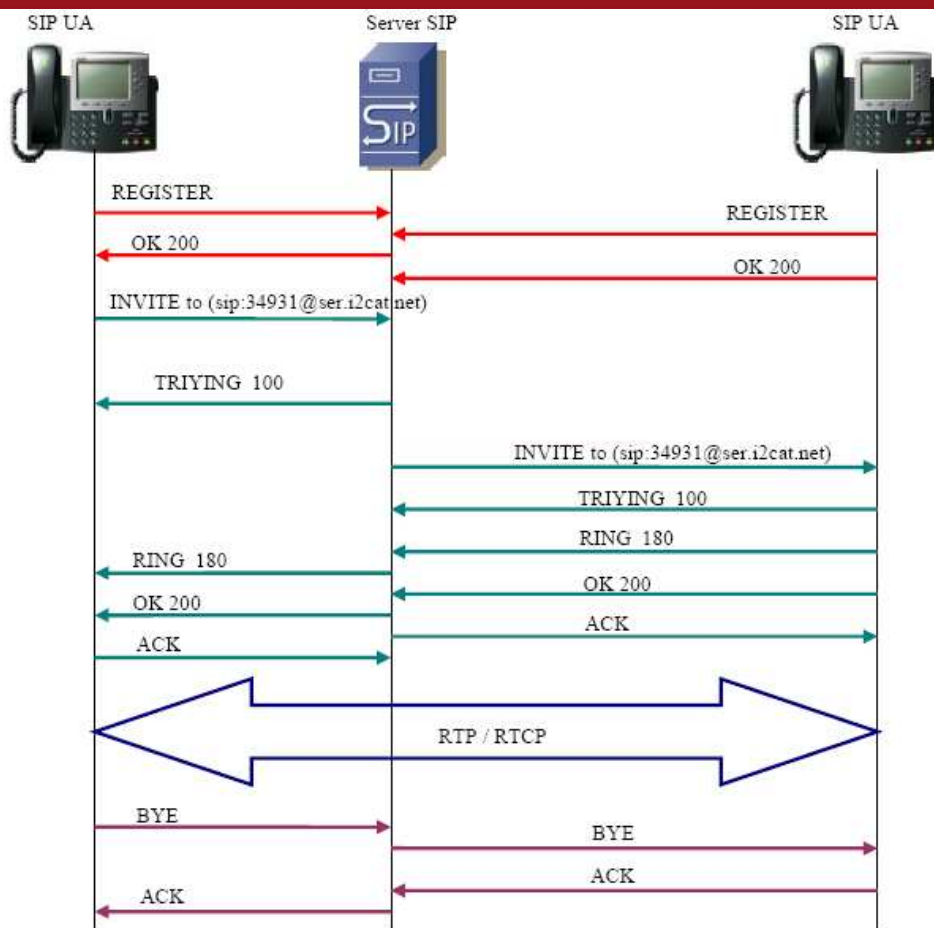


FIGURA 3-1: LLAMADA SIP

Fuente: “Diseño e implementación de un Punto Neutro para VoIP” [ROD2005]

3.1.2. SIP-T

SIP-T es un mecanismo que utiliza el protocolo SIP para facilitar la interconexión de la PSTN con redes SIP el cual fue desarrollado por el IETF en la RFC3372 [OEA2006] y [RFC3372]. Este mecanismo surge debido a que es necesario que la información del protocolo SS7 esté disponible durante las sesiones SIP.

La integración entre la señalización convencional y los mensajes SIP se logra mediante la encapsulación y traducción respectivamente. En los *gateways* SIP-ISUP, se encapsulan los mensajes ISUP en el protocolo SIP con el fin de mantener la información necesaria para los diferentes servicios. Sin embargo, algunos servidores SIP, como los Proxy Servers, no son capaces de entender mensajes ISUP por lo que se traducen estos mensajes por sus correspondientes dentro de la cabecera SIP.

3.1.3. SIP-I

SIP-I es un mecanismo desarrollado por la ITU-T mediante la recomendación Q1912.5 donde se define el interfuncionamiento de los mensajes ISUP y BICC con los mensajes SIP y SDP. Especifica los parámetros entre las redes PSTN y SIP así como los servicios suplementarios que no son soportados por SIP-T. Por otro lado, es ampliamente aceptado por proveedores, operadores y organizaciones.

3.1.4. H.323

H.323 es una recomendación de la ITU-T que define sistemas de comunicación multimedia (audio, video y datos) basados en paquetes. Engloba varios protocolos y estándares que norman todos los procedimientos que permiten lograr una transmisión multimedia. Uno de esos procedimientos es la señalización de llamadas [VAN2005] y [QUI2007].

3.1.4.1. Componentes

El sistema H.323 está compuesto de Terminales, *Gateways*, *Gatekeepers* y Unidades de Control Multipunto (MCU) [ROD2005].

a) Terminal

Es un dispositivo de usuario final que facilita las comunicaciones bidireccionales en tiempo real con otro terminal, *Gateway* o MCU. Debe contener una unidad de control del sistema, un sistema de transmisión de media, un *codec* de audio y una interfaz de red.

b) Gateways

Es un dispositivo que proporciona comunicaciones entre terminales H.323 y terminales de otros tipos de redes realizando la traducción entre ambos para su integración.

c) Gatekeepers

Es un dispositivo que realiza las funciones de conversión de dirección, control de admisiones, control de ancho de banda, gestión de zona y control de señalización.

d) MCU

Es la Unidad de Control Multipunto, encargado de dar soporte para la realización de conferencias entre tres o más terminales y *gateways*. Negocia y supervisa las capacidades de transmisión entre estos para garantizar un nivel adecuado de comunicación.

3.1.4.2. Tipos de señalización

H.323 propone dos tipos de señalización [QUI2007]:

a) Señalización de control de llamada

Se realiza mediante el protocolo H.225.0, el cual define el establecimiento o finalización de llamadas entre terminales a través del *gatekeeper* si existiese – proceso RAS. En caso no exista *gatekeeper*, define la señalización de llamada entre los dos terminales directamente – recomendación Q.931.

b) Señalización de control de canal

Se realiza mediante el protocolo H.245 con el cual se establecen los canales lógicos a través de los cuales se transmite la media definiendo las capacidades de intercambio como tasa máxima de bits y *codecs*.

3.1.4.3. Procedimiento de una llamada

Se caracteriza por las siguientes fases de señalización [ROD2005]:

a) Establecimiento de la comunicación

Luego del registro y solicitud de admisión al *Gatekeeper* mediante el uso de mensajes RAS, el usuario que desea establecer la comunicación envía un mensaje SETUP. El usuario llamado contesta con un mensaje *CallProceeding* y, después su respectiva solicitud de admisión al *Gatekeeper*, se envía el mensaje *Alerting* indicando el inicio de la comunicación. Este último mensaje es similar al *Ring Back Tone*. Cuando el usuario descuelga el teléfono, se envía un mensaje de *Connect*.

b) Señalización de Control

En esta fase se abre una negociación mediante el protocolo H.245 (control de canal). El intercambio de los mensajes petición y respuesta entre los dos terminales establecen quién será maestro y quién esclavo, las capacidades de los participantes y *codecs* de audio y video. Además, se abre el canal de comunicación (direcciones IP y puertos).

c) Comunicación

Los terminales inician la comunicación mediante el protocolo RTP/RTCP.

d) Finalización de la llamada

Cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante los mensajes *Close Logical Channel* (CLC) y *End Session Command* (ESC). Después, ambos terminales deben informar al *Gatekeeper* sobre el fin de la comunicación mediante el uso de mensajes RAS DRQ (*Disengage Request*) y DCF (*Disengage Confirm*).

En la siguiente figura 3-2, se muestran las fases descritas anteriormente.

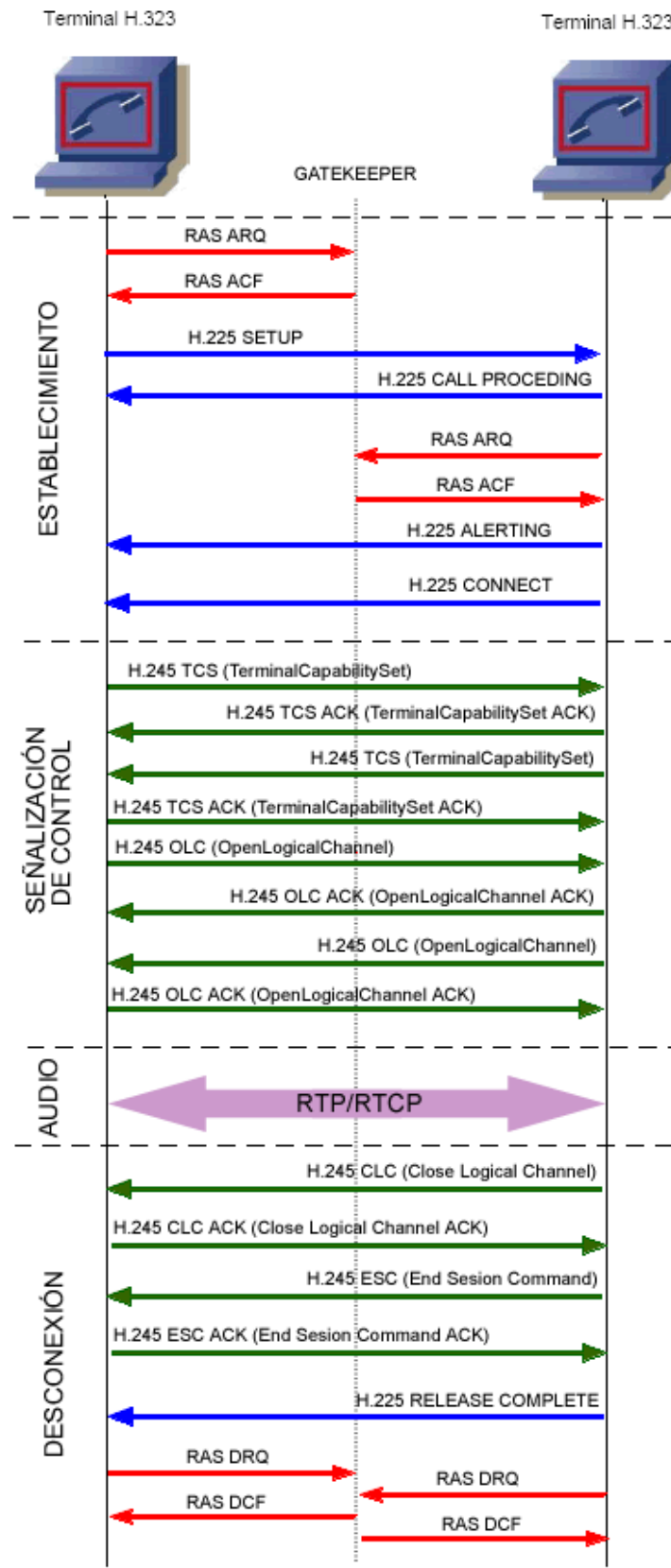


FIGURA 3-2: LLAMADA H.323

Fuente: "Ejemplo de llamada H.323" [VOI2009]

3.1.5. R2

R2 es protocolo de señalización CAS (Channel Associated Signaling) comúnmente utilizado en troncales E1 cuyas especificaciones se definen en las recomendaciones Q.400 hasta Q.490 de la ITU-T [CIS2006].

3.1.5.1. Funcionamiento

a) Trama

Este protocolo emplea una trama digital de 2.048 Kbps divididos en 32 *time slots* (TS0 hasta TS31) DE 64 Kbps cada uno. El TS0 es utilizado para sincronismo y el TS16 para señalización. En este último, se hace uso de un grupo de cuatro bits denominados ABCD. Los 30 *time slots* restantes son usados como canales de voz.

b) Multitrama

Para lograr la señalización por canal asociado, se construye una multitrama con 16 tramas (0 – 15). El TS16 de la trama 0 es usado para el sincronismo de toda la multitrama; mientras que los TS16 de las tramas restantes, son empleados para la señalización de dos canales de voz cada uno mediante el uso de dos grupos de bits ABCD por cada TS16. Por este motivo, cada canal refresca su señalización cada 16 tramas, es decir, cada 2 ms.

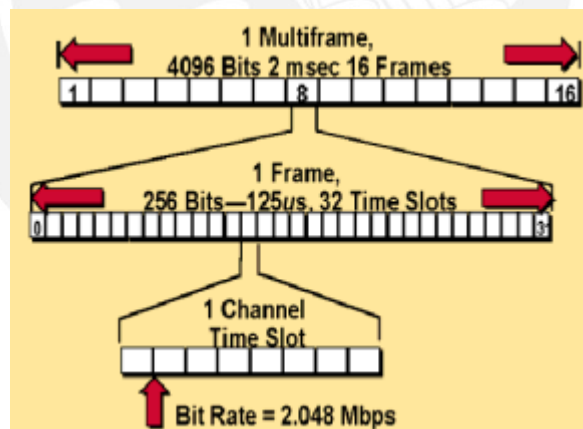


FIGURA 3-3: MULTITRAMA R2

Fuente: "E1 R2 Signaling Theory" [CIS2006]

3.1.5.2. Proceso de llamada

El establecimiento de la llamada se hace mediante la toma del canal de voz con los bits ABCD de señalización del canal respectivo. Para esto, se modifican estos bits con el fin de intercambiar mensajes *Seizure* y *Seizure Acknowledge*. Por otro lado, para el envío del número discado, se intercambian tonos multifrecuencia a través del canal de voz en cuestión.

A continuación se muestra el proceso de llamada con el protocolo R2.

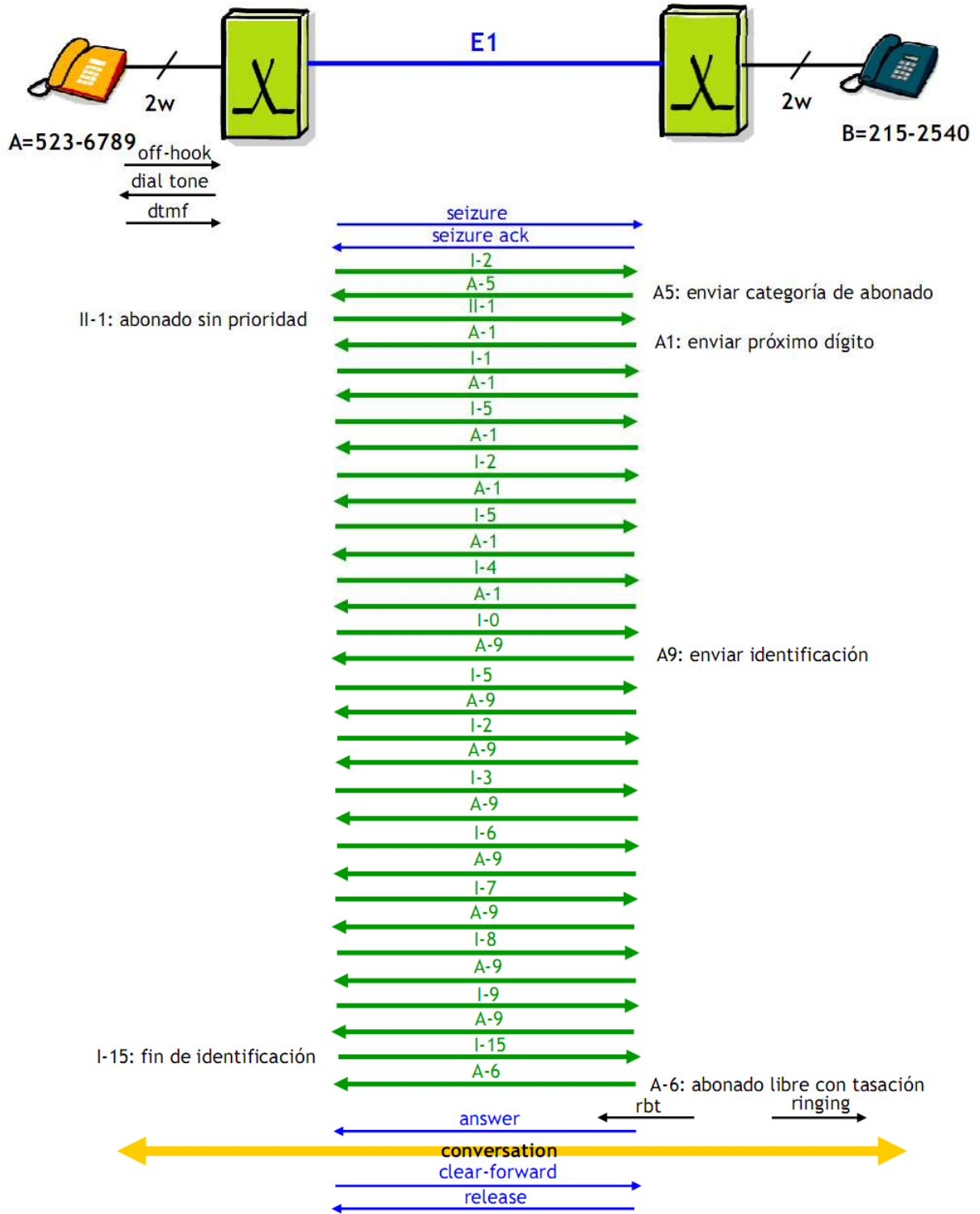


FIGURA 3-4: LLAMADA R2

Fuente: "Señalización" [VEL2008]

3.1.6. SS7

3.1.6.1. Definición

SS7 es un protocolo de señalización estandarizado por la ITU-T que define los procedimientos para el intercambio de información entre los elementos de red, ya sea fija o celular, para los diferentes servicios como [PER2003]:

- Establecimiento y finalización de llamadas
- Portabilidad numérica
- Red Inteligente
- Roaming y mensajería celular

3.1.6.2. Arquitectura de red SS7

SS7 puede emplear diferentes tipos de nodos y enlaces.

a) Tipos de nodos

Se tienen tres diferentes elementos de señalización [DRY2004].

- **Service Switching Point (SSP)**

Es una central de conmutación de voz que posee funcionalidades SS7 con el fin de originar y terminar mensajes señalización pero no transferirlos. Mediante estos mensajes, puede realizar la conexión de una llamada así como consultas a la base de datos de la red.

- **Signal Transfer Point (STP)**

Es el encargado de la transferencia de los mensajes SS7 entre nodos según la información contenida en los mensajes de señalización actuando como un ruteador. Este elemento no genera mensajes SS7.

- **Service Control Point (SCP)**

Actúa como interface entre la base de datos y la red SS7 el cual es consultado por el SSP a través del STP. El SCP es utilizado para la provisión de diferentes servicios como HLR y VLR en telefonía celular, *Global Title Translation*, Portabilidad Numérica, entre otros.

Estos nodos son identificados con direcciones numéricas llamadas Códigos de Punto (*Point Codes*) únicos por cada elemento. Entre estos identificadores se tienen OPC (Código de Punto del nodo origen) y DPC (Código de Punto del nodo destino) los cuales se especifican en el intercambio de mensajes SS7.

b) Tipos de enlaces

La señalización se realiza fuera de banda mediante el intercambio de mensajes a través de canales bidireccionales de 64 Kbps llamados enlaces de señalización. Según los elementos que estos interconecten, se tienen los siguientes tipos de enlaces [PER2003]:

- Enlace A: enlace de acceso (*access*) que conecta un STP con un elemento final de señalización (SCP o SSP). Sólo transmite mensajes originados desde o enviados hacia este último.
- Enlace B: enlace puente (*bridge*) que conecta un STP con otro STP de otra red.
- Enlace C: enlace cruzado (*cross*) que conecta dos STP que realizan la misma función.
- Enlace D: enlace diagonal (*diagonal*) que conecta un STP primario a un secundario.
- Enlace E: enlace extendido (*extended*) que conecta un SSP con un STP alternativo el cual se utiliza en caso de falla en el enlace A.
- Enlace F: enlace totalmente asociado (*fully associated*) que conecta dos elementos finales de señalización. Estos enlaces no son utilizados en redes donde se utilizan STP.

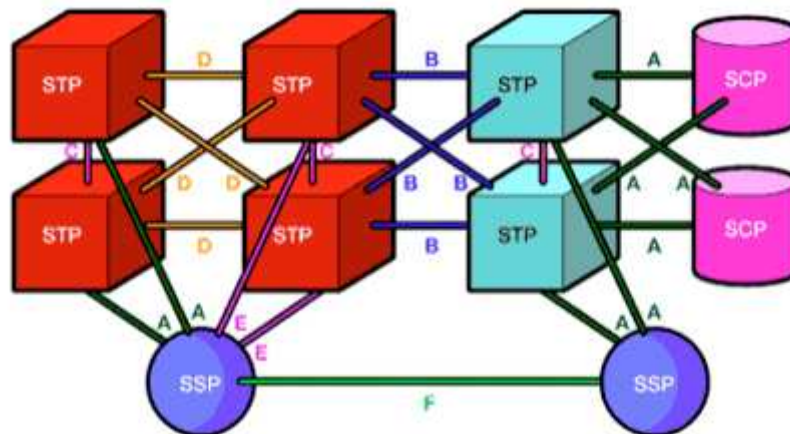


FIGURA 3-5: TIPOS DE ENLACE SS7

Fuente: "Tutorial on Signaling System 7 (SS7)" [PER2003]

3.1.6.3. Pila de protocolos SS7

El protocolo SS7 está dividido en niveles los cuales se pueden observar en la figura 4-6 [PER2003] y [DRY2004].

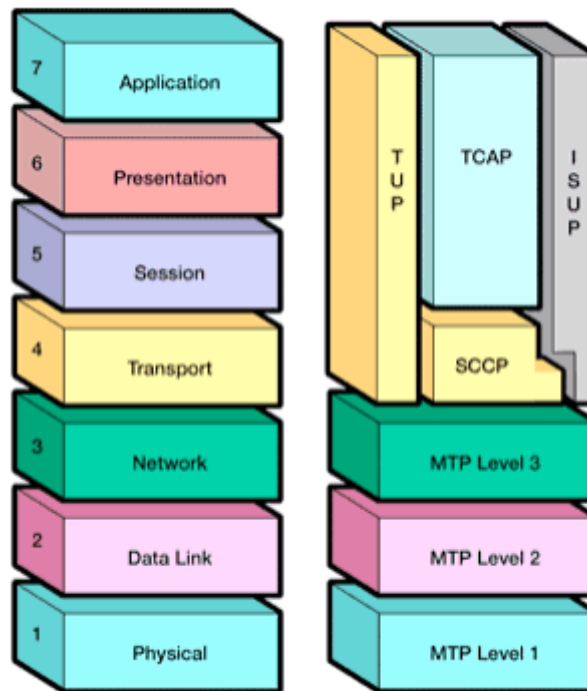


FIGURA 3-6: MODELO DE REFERENCIA OSI Y PILA DE PROTOCOLOS SS7

Fuente: "Tutorial on Signaling System 7 (SS7)" [PER2003]

a) Message Transfer Part (MTP)

Se divide en tres niveles diferentes los cuales tiene la función de transportar la información de un elemento de señalización a otro.

- **MTP1**

Equivalente a la capa Física OSI el cual define las características físicas, eléctricas y funcionales del enlace de señalización. Incluye interfaces E1, DS-1, V.35, DS-0, etc.

- **MTP2**

Equivalente a la capa de Enlace OSI. Este nivel asegura la transferencia confiable de mensajes mediante la implementación de control de flujo y monitoreo y corrección de errores.

- **MTP3**

Equivalente a la capa de Red OSI. Provee el enrutamiento de los mensajes SS7 entre los diferentes nodos de la red según la información del OPC y DPC.

También es el encargado del re-enrutamiento de tráfico en caso de fallas o congestión.

b) ISDN User Part (ISUP)

Define el protocolo usado para el establecimiento, gestión y liberación de canales de voz correspondientes a llamadas telefónicas, ya sean ISDN o no, entre diferentes centrales. Llamadas originadas y terminadas en una misma central, no utilizan este protocolo.

c) Telephone User Part (TUP)

Utilizado para el establecimiento y finalización de llamadas. Debido a que sólo soporta circuitos analógicos, actualmente, ha sido reemplazado por ISUP.

d) Signaling Connection Control Part (SCCP)

Protocolo empleado para el soporte de señalización de consultas a un SCP. Es utilizado como nivel de transporte para servicios TCAP.

e) Transaction Capabilities Applications Part (TCAP)

Transporta consultas y respuestas entre un SSP y un SCP permitiendo la comunicación entre diferentes aplicaciones como GTT (*Global Title Translation*), Portabilidad Numérica, entre otros.

3.1.6.4. Proceso de llamada

Para el establecimiento y finalización de llamadas se utilizan diferentes mensajes del protocolo ISUP explicado anteriormente.

Cuando se desea establecer una llamada, el SSP transmite un mensaje IAM hacia el SSP destino para la reserva de un circuito o canal de voz. Este mensaje contiene información como OPC, DPC, CIC (Código Identificador de Circuito) y número llamante y llamado. Luego, el SSP destino responde con un mensaje ACM indicando que se ha realizado la reserva del canal. Después de enviado el ACM, se envía el *Ring Back Tone*. Cuando el número destino contesta el teléfono, un mensaje ANM es enviado indicando que la llamada está activa.

Cuando el que origina la llamada cuelga el teléfono, se envía un mensaje REL hacia el SSP destino para liberar el canal de voz entre las dos centrales. El SSP destino responde con un mensaje RLC.

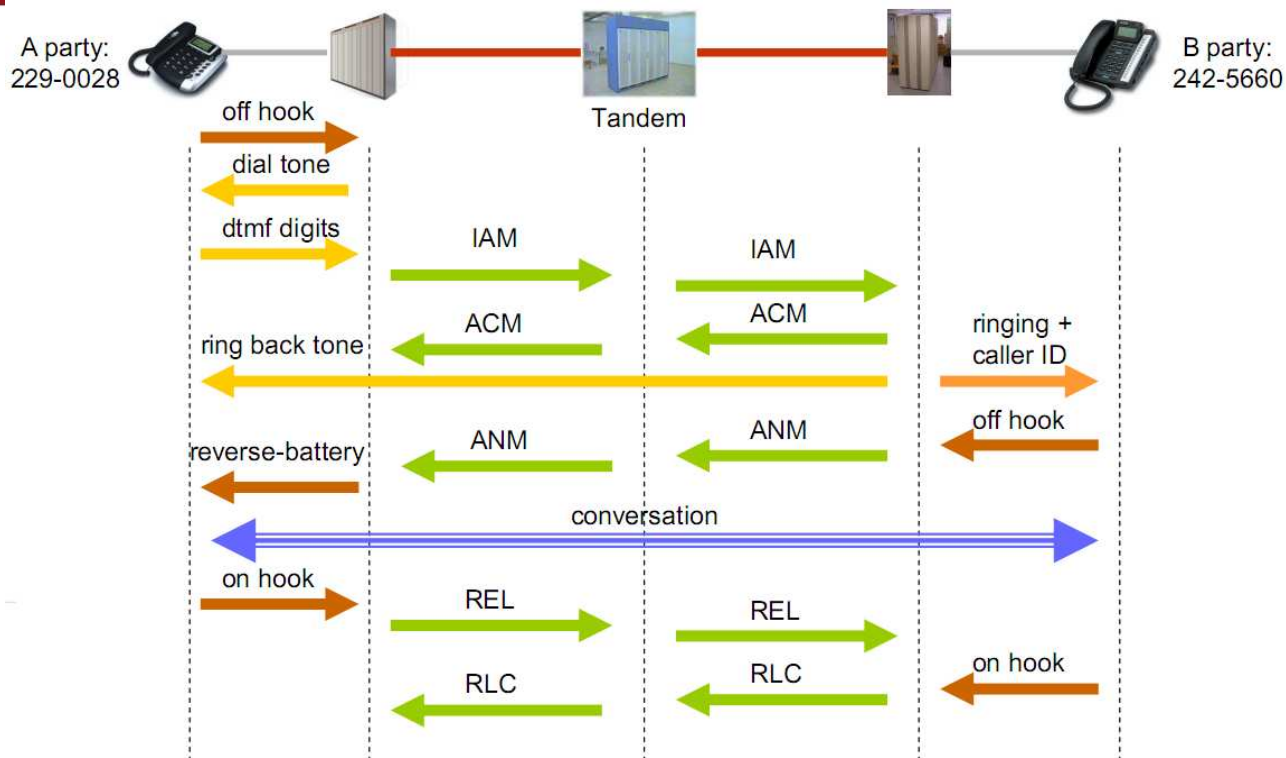


FIGURA 3-7: LLAMADA SS7

Fuente: "Señalización" [VEL2008]

3.1.7. SIGTRAN

3.1.7.1. Definición

SIGTRAN (*Signaling Transport*) es un estándar desarrollado por el grupo de trabajo SIGTRAN de la IETF usado para transportar mensajes de señalización SS7 sobre redes IP.

Este estándar es usualmente empleado por los MG los cuales convierten los mensajes de señalización SS7 en SIGTRAN para su transmisión a través de la red de paquetes.

3.1.7.2. Arquitectura

SIGTRAN define un nuevo protocolo de transporte llamado SCTP y varias capas de adaptación. En la figura 4-8 se pueden observar estos nuevos protocolos que se ubican en las tres capas inferiores [IMM2005] reemplazando a los niveles MTP1 y MTP2 de SS7.

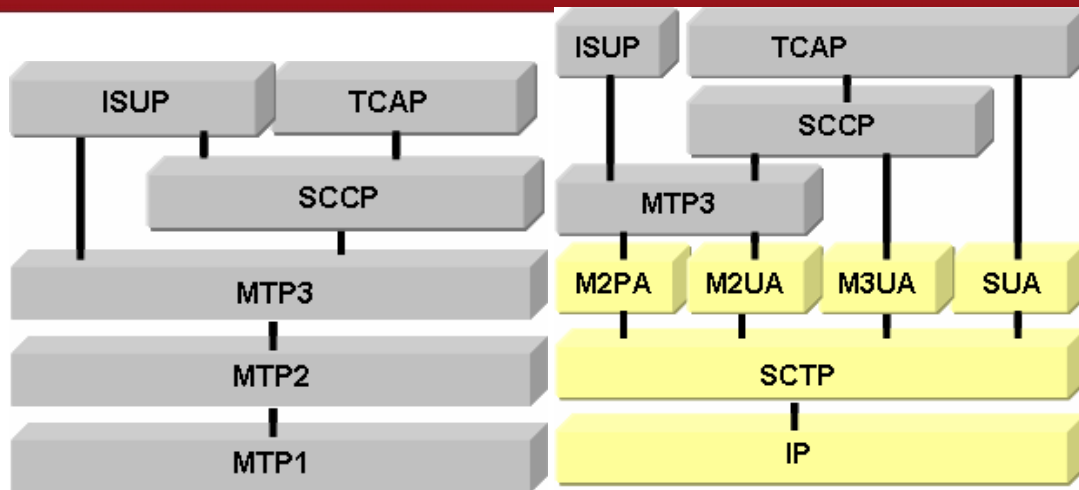


FIGURA 3-8: ARQUITECTURA SIGTRAN

Fuente: "SIGTRAN: Signaling over IP – a step closer to an all-IP network" [IMM2005]

a) SCTP

El *Stream Control Transmission Protocol* es usado como protocolo de transporte para enviar los mensajes SS7 sobre la red IP. Este protocolo es empleado debido a que tiene diferentes características con respecto a TCP o UDP los cuales presentan las desventajas de retardo en la transmisión y falta de confiabilidad respectivamente.

A continuación se presentan las características de SCTP [DAR2008]:

- Define *timers* más pequeños respecto a TCP.
- Provee transporte confiable de datos detectando errores y la corrección de estos.
- Es adaptativo permitiéndole responder ante congestiones de la red.
- Soporta *multi-homing* donde cada elemento de red posee múltiples direcciones IP permitiendo la transmisión continua de datos incluso si una de ellas falla.
- Utiliza un inicio de conexión mediante un *handshake* de cuatro pasos en el cual emplea *cookies* para prevenir ataques de DoS.
- Soporta *bundling* donde cada mensaje SCTP contiene múltiples partes de datos los cuales pueden transportar mensajes de señalización.
- Soporta fragmentación.
- Es un protocolo orientado a mensajes compuestos por una cabecera común.
- Es posible enviar paquetes SCTP en orden o fuera de orden.
- Soporta *multi-streaming* en la cual el dato es dividido en múltiples tramas con diferentes secuencias de entrega. De esta forma se evita el problema de bloqueo presente en TCP.

b) Capas de adaptación

SIGTRAN presenta cuatro capas diferentes de adaptación [IMM2005].

▪ **M2PA**

MTP2 *User Peer-to-peer Adaptation*, es un protocolo de adaptación entre MTP3 y SCTP permitiendo el transporte de mensajes SS7 MTP sobre IP. Con este protocolo, es posible mantener la topología original de la red SS7.

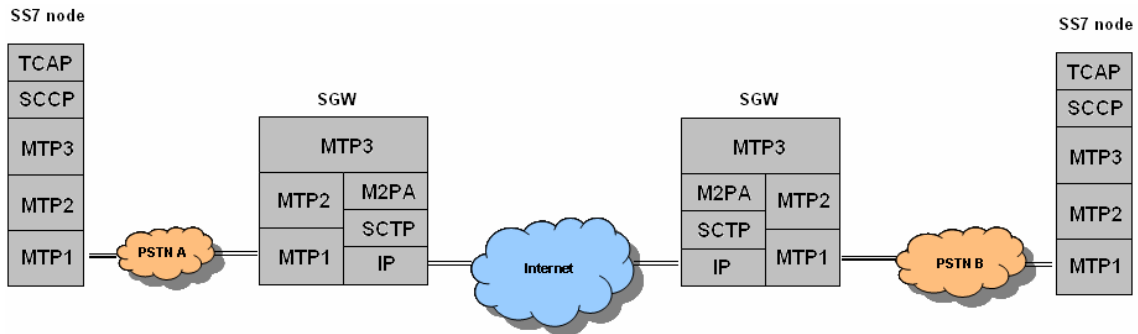


FIGURA 3-9: PROTOCOLO M2PA

Fuente: “SIGTRAN: Signaling over IP – a step closer to an all-IP network” [IMM2005]

▪ **M2UA**

MTP2 *User Adaptation*, permite el intercambio de información de señalización entre el nivel MTP3 de un MGC y el nivel MTP2 de un SG. De esta forma, el nivel MTP3 del MGC es el usuario del nivel MTP2 en el SG, incluso, siendo estos remotos.

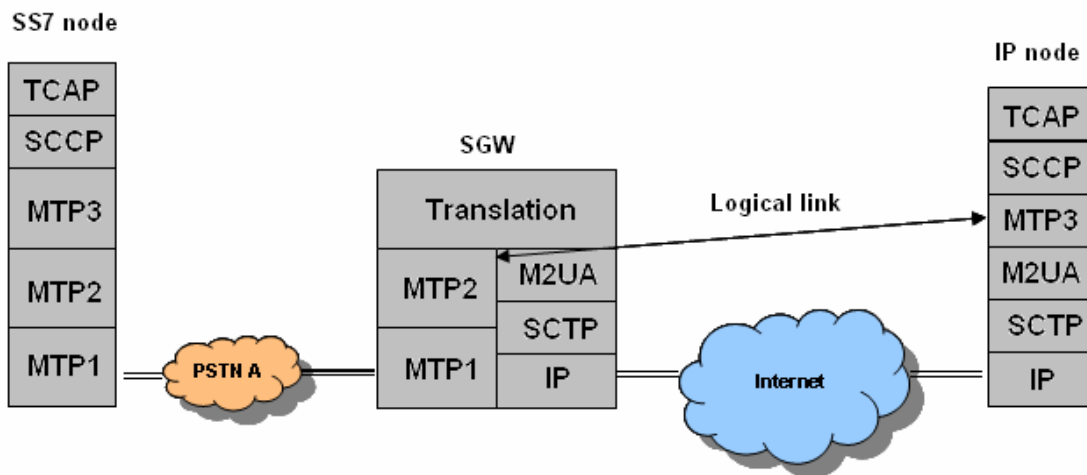


FIGURA 3-10: PROTOCOLO M2UA

Fuente: “SIGTRAN: Signaling over IP – a step closer to an all-IP network” [IMM2005]

▪ **M3UA**

MTP3 *User Adaptation*, provee conexión remota entre el nivel MTP3 en el SG y las aplicaciones (ISUP o SCCP) en el MGC.

Esta capa remueve todas las capas MTP del protocolo SS7 permitiendo que se haga un uso más eficiente de la red IP.

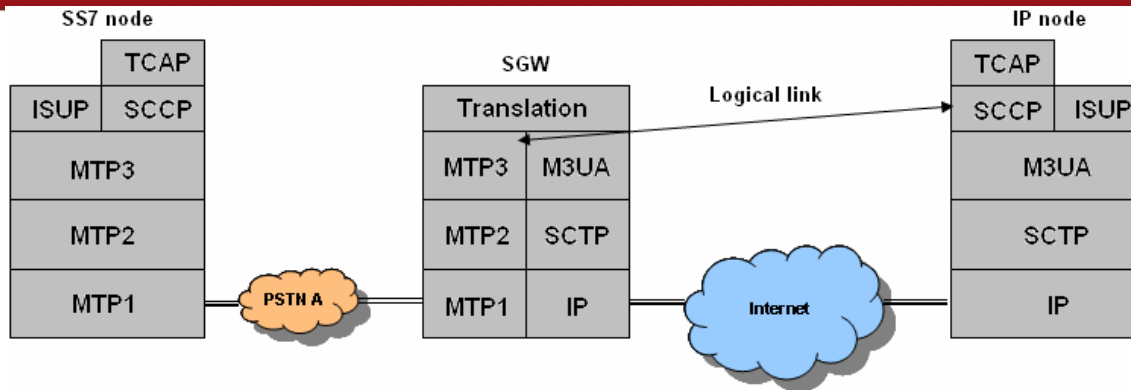


FIGURA 3-11: PROTOCOLO M3UA

Fuente: “SIGTRAN: Signaling over IP – a step closer to an all-IP network” [IMM2005]

- **SUA**

SCCP *User Adaptation*, permite el intercambio de información de usuario del protocolo SCCP, como TCAP, entre el SG y el MGC.

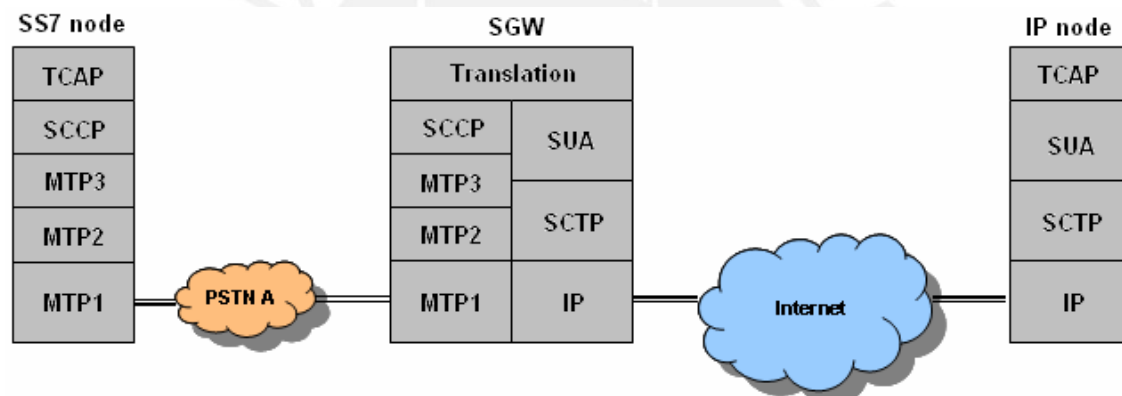


FIGURA 3-12: PROTOCOLO SUA

Fuente: “SIGTRAN: Signaling over IP – a step closer to an all-IP network” [IMM2005]

- **IUA**

Además de las capas de adaptación mencionadas anteriormente, las cuales se utilizan para adaptar el protocolo SS7 a IP, se tiene la capa de adaptación IUA (ISDN *User Adaptation*) que define el método para transportar los mensajes ISDN sobre IP utilizando el protocolo SCTP. IUA es usada entre el SG y el MGC donde el SG recibe señalización ISDN.

3.1.8. MGCP

Es un protocolo de control desarrollado por la IETF que utiliza mensajes en formato de texto para establecer, controlar y terminar sesiones de comunicación multimedia mediante una

arquitectura maestro – esclavo donde el MGC (maestro) controla los MG (esclavos) mediante la ejecución de comandos enviados hacia estos últimos.

Fue diseñado con el objetivo de hacer los dispositivos finales más sencillos ya que emplea un modelo centralizado donde las llamadas deben hacerse a través de un dispositivo controlador.

3.1.9. H.248

H.248, o también llamado MEGACO, es el resultado de esfuerzos conjuntos entre la ITU (ITU-T Recomendación H.248) y el IETF (RFC 2885) que define una arquitectura centralizada para la gestión de sesiones y señalización de aplicaciones multimedia entre múltiples extremos. Este estándar se desarrolló como una extensión del protocolo MGCP haciéndolos iguales desde el punto de vista de arquitectura ya que definen la relación entre el MGC y los MG. La diferencia entre estos dos protocolos radica en que el H.248 soporta diferentes redes, como IP o ATM, y tecnologías de acceso haciéndolo incompatible con el MGCP.

3.1.10. ISDN

ISDN, *Integrated Services Digital Network*, es la evolución de la red telefónica existente que facilita conexiones digitales de extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de datos, integrándolos en un solo acceso. Esta tecnología es más rápida y tiene mejor calidad comparada con las líneas analógicas ya que se pueden alcanzar velocidades de hasta 128 Kbps.

3.1.10.1. Canales

Existen dos tipos de canales ISDN:

a) Canal B

El canal B, *Bearer*, es un canal de 64 Kbps que puede ser usado para transmitir voz o datos. Se pueden utilizar varios canales B para obtener un mayor *bitrate*.

b) Canal D

El canal D, *Delta*, puede ser de 16 Kbps o 64 Kbps y es usado para la señalización entre los elementos de la red.

3.1.10.2. Servicios

Se tienen dos tipos de servicios:

a) **Basic Rate Interface**

Basic Rate Interface (BRI) ofrece conexión mediante dos canales B y un canal D (2B+D). Este tipo de servicio es utilizado mayormente para conexión a Internet o para líneas telefónicas digitales.

b) **Primary Rate Interface**

Primary Rate Interface (PRI) ofrece 23 canales B y un canal D (23B+D) sobre enlaces T1 (Norte América y Japón) o 30 canales B y un canal D (30B+D) sobre enlaces E1. PRI es principalmente usado por organizaciones que desean transmitir alto tráfico como, por ejemplo, la conexión de su central privada telefónica con la PSTN.

3.1.10.3. **Arquitectura de capas**

ISDN consta de varios niveles correspondientes a las tres primeras capas del modelo OSI [CIS2000] transmitidos por el canal D de señalización.

a) **Nivel 1**

Equivalente a la capa física del modelo OSI. Este nivel utiliza tramas de 48 bits de los cuales, 36 corresponden a datos. Los otros 12 bits son utilizados para sincronización de la trama.

b) **Nivel 2**

Este nivel es empleado para el control y corrección de errores de la información transmitida utilizando el protocolo LAP-D especificado en la ITU-T Q.920 y Q.921. Es equivalente a la capa de enlace del modelo OSI.

c) **Nivel 3**

Utiliza las especificaciones ITU-T Q.930 y Q.931 para la señalización ISDN con las cuales se soportan conexiones por conmutación de circuitos, por conmutación de paquetes y usuario-usuario. Además, para el establecimiento y finalización de llamadas, se definen los mensajes Setup, Connect, Release, User Information, Cancel, Status y Disconnect. Este nivel es equivalente a la capa de Red del modelo OSI.

El uso, en la red NGN, de los protocolos descritos anteriormente, se observa en la tabla 3-1.

TABLA 3-1: PROTOCOLOS EN NGN

PROTOCOLOS	USO
SIGTRAN	Entre red TDM y red IP
SS7 / R2	Para establecimiento de llamadas en la PSTN
SIP / H.323	Para establecimiento de llamadas en red IP
SIP-I / SIP-T	Entre red SS7 y red SIP
H.248 / MGCP	Entre MG y MGC

3.2. PARÁMETROS DE QOS

3.2.1. Definición de QoS

La definición de calidad de servicio es dada por la Recomendación E.800 de la ITU-T donde se indica que “la calidad de servicio (QoS) es el efecto global del funcionamiento de un servicio que determina el grado de satisfacción de un usuario de este servicio”. En otras palabras [GAL2008], este término representa cualitativamente, desde el punto de vista del usuario, cuán rápido pueden ser transmitidos los datos, cuánto se tiene que esperar para recibirlos, cuánta información se pierde, etc.

3.2.2. Parámetros de QoS

Según la Recomendación Y.1540 de la ITU-T, “Servicio de comunicación de datos con Protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes de Protocolo Internet”, se definen los parámetros que se utilizan para evaluar la calidad de funcionamiento con respecto de la velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP del servicio de comunicación de datos [ITU2006]. Cabe recalcar que estos parámetros fueron concebidos para conexiones T1 (1.544 Mbps) y E1 (2.048 Mbps). Estos parámetros son los siguientes:

3.2.2.1. Retardo

El Retardo de paquetes IP (IPTD) o latencia, es el retardo que sufre un paquete IP al ser transmitido entre dos nodos. Este retardo se origina debido a la espera de los paquetes en los distintos nodos de la red ya sea por colas o procesamiento en estos.

3.2.2.2. Retardo medio

Es la media aritmética de los diferentes retardos que sufren los paquetes IP al ser transmitidos por la red.

3.2.2.3. Tasa de errores

La tasa de errores en los paquetes IP (IPER) es la relación entre el total de paquetes IP con errores y los paquetes IP transmitidos. Estos errores pueden ser ocasionados por la codificación o decodificación.

3.2.2.4. Tasa de pérdida de paquetes

La tasa de pérdida de paquetes (IPLR) es la relación entre los paquetes IP perdidos y todos los paquetes transmitidos. Estas pérdidas se dan por congestión en las colas de los nodos, expiración del tiempo de vida de los paquetes o por fallas de transmisión de los nodos.

3.2.2.5. Jitter

También llamado Varianza del retardo de paquetes IP (IPDV), es la variación en el retardo de una secuencia de paquetes.

3.2.2.6. Tasa de paquetes espurios

La Tasa de paquetes IP espurios (SPR) es el total de paquetes espurios detectados en el punto de medición de egreso entre la duración del intervalo de tiempo de observación. Estos paquetes se generan por errores físicos.

3.2.2.7. Porcentaje de indisponibilidad del servicio

El porcentaje de indisponibilidad del servicio IP (PIU) indica el porcentaje del tiempo de servicio programado total que se clasifica como indisponible utilizando la función de disponibilidad del servicio. Esta función se basa en un umbral de la característica IPLR.

3.2.3. Clases de Servicio

Según la Recomendación Y.1541 de la ITU-T, “Objetivos de Calidad de funcionamiento para servicios IP”, se propone dividir las transferencias en comunicaciones IP en ocho clases de QoS según las características de calidad en el servicio que requieran las diferentes aplicaciones de tráfico en la red [ITU2006A]. Estas clases serán utilizadas para el establecimiento de acuerdos entre los usuarios finales y el proveedor del servicio. A continuación se presentan las diferentes clases de QoS.

3.2.3.1. Clase 0: Aplicaciones en tiempo real muy interactivas

Se caracterizan por ser altamente sensibles al retardo y al *jitter*. El retardo medio máximo es 100 ms, el *jitter* debe ser menor a 50 ms, tasa de pérdidas inferior a 10^{-3} y la tasa de errores menor a 10^{-4} . Esta clase incluye aplicaciones como VoIP y videoconferencia.

3.2.3.2. Clase 1: Aplicaciones en tiempo real

Se caracterizan por ser sensibles al retardo y al *jitter* pero no requieren de parámetros tan rígidos como la Clase 0. El retardo medio máximo es 400 ms, el *jitter* debe ser menor a 50 ms, tasa de pérdidas inferior a 10^{-3} y la tasa de errores menor a 10^{-4} . Esta clase incluye aplicaciones como VoIP y videoconferencia con una calidad menor percibida en los extremos.

3.2.3.3. Clase 2: Transacciones de datos muy interactivas

Se caracterizan por ser de alta interacción a pesar de no ser aplicaciones en tiempo real. El retardo medio máximo es 100 ms, el *jitter* está sin especificar y la tasa de pérdidas es inferior a 10^{-3} y la tasa de errores menor a 10^{-4} . Esta clase incluye tráfico de señalización.

3.2.3.4. Clase 3: Transacciones de datos

Se caracterizan por ser de alta interacción a pesar de no ser aplicaciones en tiempo real pero con requerimientos menores que la Clase 3. El retardo medio máximo es 400 ms, el *jitter* está sin especificar y la tasa de pérdidas es inferior a 10^{-3} y la tasa de errores menor a 10^{-4} . Esta clase incluye tráfico de señalización menos rígido.

3.2.3.5. Clase 4: Exclusivo para aplicaciones de bajas pérdidas

Se caracterizan por requerir una baja tasa de pérdida de paquetes. El retardo medio máximo es 1 s, el *jitter* está sin especificar y la tasa de pérdidas es inferior a 10^{-3} y la tasa de errores menor a 10^{-4} . Esta clase incluye transferencias de breve duración, datos en gran volumen y *videostreaming*.

3.2.3.6. Clase 5: Aplicaciones tradicionales en redes IP

Esta clase incluye aplicaciones tradicionales de redes IP sin calidad de servicio como SMTP, FTP, HTTP, etc. Tienen un retardo medio, *jitter*, tasa de pérdidas y tasa de errores sin especificar ya que trabajan con el modelo *Best Effort*.

3.2.3.7. Clase 6: Emulación de circuitos TDM con alta interacción

Se caracterizan por emular circuitos TDM con alta interacción cuyas aplicaciones son muy sensibles a la pérdida de paquetes. El retardo medio máximo es 100 ms, el *jitter* debe ser menor a 50 ms, tasa de pérdidas inferior a 10^{-5} y la tasa de errores menor a 10^{-6} . Esta clase incluye aplicaciones como transferencia de televisión de alta calidad sobre IP, transferencias IP de alta capacidad y aplicaciones que se basan en la emulación de circuitos TDM.

3.2.3.8. Clase 7: Emulación de circuitos TDM

Se caracterizan por emular circuitos TDM con aplicaciones de menor calidad. El retardo medio máximo es 400 ms, el *jitter* debe ser menor a 50 ms, tasa de pérdidas inferior a 10^{-5} y la tasa de errores menor a 10^{-6} . Esta clase incluye aplicaciones como transferencia de televisión de alta calidad sobre IP, transferencias IP de alta capacidad y aplicaciones que se basan en la emulación de circuitos TDM pero con menor interacción y sensibilidad respecto a la Clase 6.

En la siguiente tabla se puede observar un resumen de los requerimientos de todas las clases:

TABLA 3-2: CLASES DE CALIDAD DE SERVICIO

Parámetro de rendimiento	Clases de Calidad de Servicio							
	Clase 0	Clase 1	Clase 2	Clase 3	Clase 4	Clase 5	Clase 6	Clase 7
IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U	100 ms	400 ms
IPDV	50 ms	50 ms	U	U	U	U	50 ms	50 ms
IPLR	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	U	10^{-5}	10^{-5}
IPER	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}	U	10^{-6}	10^{-6}

3.2.4. QoS en NGN

Ofrecer calidad de servicio en las redes NGN es una tarea muy complicada debido a las diversas aplicaciones existentes, las cuales tienen diferentes requerimientos de calidad. Estas aplicaciones no sólo requieren que el tráfico llegue a su destino sino que, además, necesitan de un retardo y ancho de banda asegurados, un *jitter* mínimo, así como un límite máximo en la tasa de errores y pérdida de paquetes.

Uno de los objetivos principales de las redes NGN es proporcionar una calidad equivalente a la PSTN brindando servicios tradicionales de voz y otros servicios auxiliares como fax, módem, entre otros. Por otro lado, para el caso del servicio VoIP, se debe tener en cuenta que se tienen tres tipos diferentes de flujos de datos: los paquetes de Voz, Señalización y Operaciones & Mantenimiento. Estos componentes tienen diferentes necesidades de QoS las cuales, si son satisfechas correctamente, brindarán una buena calidad en la experiencia del usuario.

A nivel de *core* de datos, los protocolos de enrutamiento tradicionales como RIP y OSPF no son capaces de brindar el tratamiento adecuado al tráfico y congestión por lo que se hace necesario el uso de arquitecturas capaces de proporcionar la QoS necesaria para las aplicaciones NGN. Entre estas arquitecturas se tienen las arquitecturas DiffServ, IntServ y

MPLS las cuales serán materia de estudio en la presente Tesis con el objetivo de compararlos con la arquitectura IP *Best Effort* utilizada actualmente por lo operadores NGN.

3.3. TIPOS DE TRÁFICO

Dentro de los tipos de tráfico utilizados en las redes NGN se tienen los siguientes:

3.3.1. Multimedia

Incluye la información transmitida por las aplicaciones en tiempo real, como voz o video, y otras aplicaciones de datos. Este tipo de tráfico debe ser tratado correctamente por los diferentes niveles de la red NGN para brindar una buena calidad en el servicio. Para este estudio, las aplicaciones de voz y video serán clasificadas como Clase 1 y las aplicaciones de datos como Clase 5 de la recomendación Y.1541 de la ITU-T.

3.3.2. Señalización

Incluye la información de control utilizada para el establecimiento y finalización de sesiones o reserva de recursos de la red. Sin una QoS adecuada para la señalización, las sesiones podrían no establecerse o, en su defecto, tomar mucho tiempo para hacerlo. Para este estudio, este tipo de tráfico será clasificado como Clase 2.

3.3.3. Enrutamiento

Es el tráfico ocasionado por los protocolos de enrutamiento utilizados por la red para definir las rutas o caminos y así establecer una comunicación IP. De la calidad asignada para el tráfico de enrutamiento dependerá la rapidez de la red para la solución de eventuales problemas en los nodos o enlaces. Para este estudio, este tipo de tráfico será clasificado como Clase 3.

3.3.4. Operación y Mantenimiento

Incluye el tráfico generado por los protocolos utilizados para la gestión, aprovisionamiento y mantenimiento. Para este estudio, este tipo de tráfico será clasificado como Clase 5.

3.3.5. Billing

Es el tráfico que generan las aplicaciones empleadas para la tarificación de los servicios utilizados por los usuarios. Este tipo de tráfico será clasificado como Clase 4.

3.4. ARQUITECTURAS DE QoS EN IP

3.4.1. IP Best Effort

Es el tipo de arquitectura que trabaja bajo el modelo del mejor esfuerzo, es decir, se realiza la transmisión de datos utilizando los recursos disponibles y sin ofrecer ningún tipo de prioridad o QoS. En este escenario, los distintos tipos de tráfico son tratados de la misma

forma en los diferentes nodos de la red empleando colas del tipo FIFO, donde el paquete que llega primero a la cola es el primero en ser atendido. Es por este motivo, que este modelo no es el adecuado para aplicaciones multimedia sensibles al retardo y al *jitter*, como audio o video en tiempo real.

A pesar de no ofrecer ningún trato especial a los paquetes transmitidos, esta arquitectura es la que se tiene actualmente en la *backbone* de Internet, donde la red hace lo mejor posible pero garantizando poco y, así, se espera que se entregue la información transmitida siempre que estén disponibles los recursos suficientes.

La ITU-T se refiere a este modelo como una arquitectura con Capacidad de Transferencia del tipo Mejor Esfuerzo en la cual se reenvían los paquetes utilizando los recursos disponibles.

3.4.2. IntServ

IntServ, o *Integrated Services*, es una arquitectura donde se garantiza la QoS mediante la reserva recursos de red: los *hosts* solicitan una QoS específica a la red para una aplicación o flujo de datos en particular y los routers envían las solicitudes a los demás routers de la red [DIA2008A].

3.4.2.1. Funcionamiento

Para su funcionamiento, se utiliza el campo Etiqueta de Flujo de la cabecera IPv6 con el objetivo de identificar los flujos enviados a través de la red y, así, asignar recursos a los diferentes flujos definidos.

Además, se hace uso del Protocolo de Reserva de Recursos RSVP definido en el RFC2205 de la IETF con el cual se reservarán recursos en cada nodo por donde transitarán los paquetes pertenecientes al mismo flujo. La solicitud de reserva se hace de origen a destino mediante un mensaje Path y los routers intermedios comunican que tienen los recursos necesarios para la transferencia mediante un mensaje Path State. Por otro lado, el destino envía un mensaje de confirmación Resv por la misma trayectoria y los routers confirman la reserva mediante un mensaje ResvConf.

En este modelo de QoS, se tienen dos tipos de servicio según los recursos que se necesiten: *Guaranteed Rate Service*, donde los recursos se comportan como un circuito virtual, o *Controlled Load Service*, donde los recursos solicitados se asignan de manera dinámica [LUN2007].

3.4.2.2. Ventajas

- Se garantizan los recursos requeridos por el tráfico según su tipo de flujo debido a la señalización realizada antes del envío de la información.

- Debido a la actualización de estados de RSVP, realizada cada 30 segundos, es posible detectar cualquier falla en los nodos de la red.

3.4.2.3. Desventajas

- Debido a la excesiva señalización realizada por cada flujo que se desea enviar por la red, esta arquitectura no permite que la red sea escalable.
- Por la actualización de estados de RSVP, realizada cada 30 segundos, se consumen recursos y ancho de banda por cada flujo existente.

Por estas razones, este tipo de arquitectura no es usada en la actualidad por la cantidad de flujos que se deben controlar resultando difícil y costoso de implementar.

La ITU-T se refiere a este modelo como una arquitectura con Capacidad de Transferencia de Ancho de Banda Dedicada DBW donde se soportan las aplicaciones con un requerimiento de retardo riguroso.

3.4.3. DiffServ

DiffServ, o *Differentiated Services*, es una arquitectura que utiliza el mecanismo de clasificación de tráfico con la finalidad de dar prioridades a los servicios diferenciados para la provisión de QoS en redes IP. Este modelo es muy usado actualmente debido a que tiene la capacidad de aceptar requerimientos de diferentes aplicaciones y poder darles un trato un especial según su clasificación.

3.4.3.1. Funcionamiento

Para su funcionamiento, los routers, marcan los paquetes que pertenecen a una determinada clase, según sus características como direcciones y/o puertos de origen o destino, modificando el subcampo DSCP (*Differentiated Service Code Point*) que se encuentra en el campo DS (*Differentiated Services*) de la cabecera IP [LUN2007]. Asimismo, la diferenciación de servicios se realiza con la definición de comportamientos específicos o prioridades, llamada PHB (*Per-Hop Behavior*), para cada clase definida anteriormente. Al tráfico perteneciente a una misma clase se le llama BA (*Behavior Aggregate*).

En este modelo, se define el conjunto de routers que trabajan bajo las mismas políticas de diferenciación de servicios con el nombre de Dominio DiffServ. En este, se tienen los nodos extremos (routers de entrada y salida) y los nodos internos. Los routers en la entrada del dominio DiffServ son los encargados de la aplicación del control de admisión y la modificación del valor del subcampo DSCP.

3.4.3.2. Ventajas

Una de las ventajas más importantes de DiffServ radica en que la clasificación de los paquetes se realiza en los nodos extremos del dominio DiffServ, permitiendo que los nodos internos se dediquen a tareas de enrutamiento y priorización de paquetes según su clase sin desperdiciar recursos en tareas complejas como esta clasificación. Por este motivo, a diferencia de IntServ, no se requiere de un protocolo de reserva de recursos como RSVP logrando ofrecer mayor escalabilidad sin sobrecargar la red.

3.4.3.3. Desventajas

- Esta arquitectura presenta un problema cuando un paquete viaja a través de dos o más dominios DiffServ diferentes ya que estos pueden actuar bajo diferentes políticas de clasificación.
- Además, debido a que no se reservan recursos en la red, no se tiene una garantía de QoS por lo que el tráfico de baja prioridad puede verse afectado si la red se sobrecarga con tráfico de alta prioridad.
- Por otro lado, en este modelo, la reserva de QoS es unidireccional ya que el principal beneficiario será el destino y siendo el origen el que deba pagar por la diferenciación de su tráfico.

La ITU-T se refiere a este modelo como una arquitectura con Capacidad de Transferencia con Ancho de Banda Estadística SBW (*Statistical Bandwidth*) con el objetivo de soportar aplicaciones que no tengan requisitos rigurosos de retardo.

Por otro lado, la IETF, con su RFC 2475, describe esta arquitectura y recomienda clases de tráfico estandarizadas para permitir la interoperabilidad entre diferentes redes.

3.4.4. MPLS

MPLS (*Multiprotocol Label Switching*) es una arquitectura de red que garantiza QoS mediante la conmutación por etiquetas simplificando, considerablemente, la conmutación de paquetes. Este modelo de red surgió del trabajo conjunto de la IETF y fabricantes, como Cisco System, Toshiba, Ipsilon e IBM, para mejorar la compatibilidad entre la capa de Red (IP) y la capa de Enlace (ATM, Frame Relay, PPP) del modelo OSI [LUN2007].

3.4.4.1. Modos

MPLS posee dos modos de funcionamiento:

- Modo Trama MPLS: se añade una etiqueta de 32 bits de cuatro campos entre las cabeceras de capa de Red y Enlace.
- Modo Celda MPLS: se utilizan los campos VPI/VCI de la cabecera ATM como etiqueta.

Entre estos dos modos, el más utilizado es el modo Trama el cual será el que se detallará en los siguientes puntos.

3.4.4.2. Conceptos Previos

Para entender correctamente el funcionamiento de MPLS, es importante tener en cuenta los siguientes conceptos previos [DIA2008B]:

- FEC (*Forwarding Equivalence Class*): conjunto de paquetes con las mismas características por lo que recibirán el mismo tratamiento en el trayecto a su destino. Estas características pueden ser dirección IP origen o destino, dirección IP de la red, campo Identificador de Protocolo, campo Etiqueta de Flujo de la cabecera IPv6, puerto origen o destino, o campo DSCP.
- LSR (*Label Switching Router*): nodo interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos.
- Edge LSR (*Edge Label Switching Router*) o LER (*Label Edge Router*): nodo MPLS de borde que maneja tráfico entrante o saliente a la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida, la extrae y enruta según la capa de Red.
- LSP (*Label Switched Path*): trayecto definido con QoS entre dos puntos extremos dentro de la red MPLS.
- Ingeniería de Tráfico: proceso de control de flujo de tráfico a través de la red, que optimiza el uso de recursos de esta con el objetivo de mejorar su rendimiento.

3.4.4.3. Funcionamiento

Para su funcionamiento, MPLS añade una cabecera de 32 bits entre las cabeceras de los protocolos de la capa de Red y Enlace respectivamente.

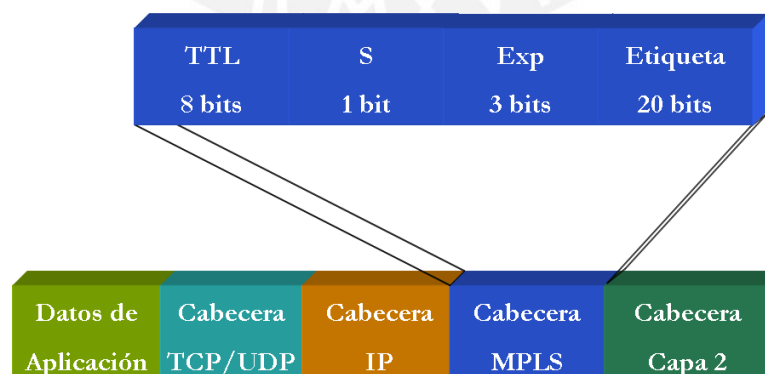


FIGURA 3-13: CABECERA MPLS

Fuente: "Medición y Tráfico en redes MPLS" [LUN2007]

A continuación se describen los campos que la conforman:

- Campo TTL: campo de 8 bits que se utiliza como contador del número de saltos para evitar la creación de bucles. Reemplaza al TTL de la cabecera IP y su valor es disminuido en cada salto.
- Campo S o Stack: campo de 1 bit que indica si se tienen diferentes jerarquías de etiquetas formando una pila de etiquetas.
- Campo Exp o Experimental: campo de 3 bits utilizado para indicar la clase de servicio permitiendo la implementación del modelo DiffServ.
- Campo Etiqueta: campo de 20 bits cuyo valor permite formar un trayecto con Qos.

En general, una red MPLS está formada por un conjunto de nodos, LSRs, capaces de conmutar y enrutar paquetes en base a las etiquetas añadidas a cada uno de estos en el LER de ingreso. Estas etiquetas definen un flujo de paquetes entre dos puntos extremos, llamado FEC. Para cada FEC, se elige un solo trayecto a través de la red, LSP, y se tiene un comportamiento específico en cada nodo que define la QoS requerida.

La transmisión de datos, descrita anteriormente, sigue los siguientes pasos [STA2001]:

- 1° Las etiquetas son definidas por el operador de la red y distribuidas mediante el uso de un protocolo de distribución como LDP o RSVP-TE. Además, se crean las tablas de etiquetas en cada nodo LSR.
- 2° Cuando un paquete ingresa al dominio MPLS, el LER de ingreso lo asocia a un FEC particular añadiéndole la etiqueta correcta y reenvía el paquete al siguiente nodo. Si aún no existe el LSP correspondiente a ese FEC, el LER y los LSRs definen un nuevo LSP para este.
- 3° Debido a que las etiquetas tienen significado local, cada LSR recibe los paquetes etiquetados y les remueve la etiqueta inicial. Luego, le coloca otra etiqueta con el fin de poder reenviar el paquete hacia el siguiente salto del LSP.
- 4° El LER de salida retira la etiqueta y reenvía el paquete hacia su destino final según la cabecera IP.

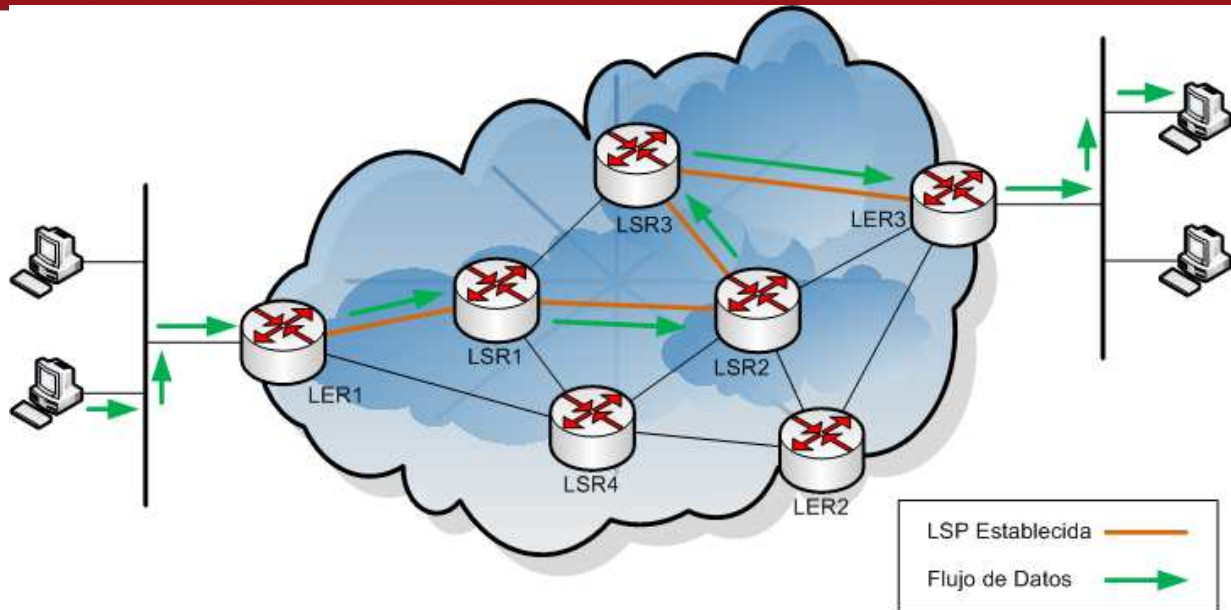


FIGURA 3-14: FUNCIONAMIENTO MPLS

Según la forma cómo se distribuyen las etiquetas, se tienen dos modelos de la arquitectura MPLS:

- MPLS LDP
- MPLS RSVP-TE

3.4.4.4. MPLS LDP

Este modelo utiliza el protocolo LDP (*Label Distribution Protocol*) para la distribución de etiquetas MPLS y establecimiento de LSPs siguiendo el enrutamiento IP existente.

Este protocolo puede operar en dos modos diferentes:

- Modo solicitado: el LER de ingreso envía un requerimiento de etiqueta LDP al siguiente router según su tabla de enrutamiento IP.
- Modo no solicitado: el LER de egreso mapea las etiquetas en el enlace hasta alcanzar los router de ingreso.

Para su funcionamiento, los nodos intercambian cuatro tipos de mensajes:

- *Discovery Messages*: anuncia y mantiene la presencia de un LSP mediante el envío periódico de mensajes HELLO encapsulados en el protocolo UDP.
- *Session Messages*: establecen, mantienen y terminan sesiones LDP usando TCP.
- *Advertisement Messages*: crean, cambian y borran asociaciones de etiquetas a FECs. Se utiliza el protocolo TCP.
- *Notification Messages*: Notifica errores y avisos.

LDP es simple de configurar y evita que se indiquen manualmente los saltos dentro del LSP. LDP se encarga de distribuir las etiquetas y establecer el LSP.

Por otro lado, este protocolo presenta la desventaja de valerse del protocolo OSPF constantemente para la selección de rutas para el siguiente salto en el LSP. En el caso de que un enlace falle, LDP debe esperar a que OSPF converja para poder elegir la ruta adecuada ocasionando una demora en la restitución del LSP.

3.4.4.5. MPLS RSVP-TE

Este modelo hace uso del protocolo RSVP-TE el cual es una extensión del protocolo RSVP, utilizado en la arquitectura IntServ, para la distribución de etiquetas sobre MPLS.

Por otro lado, este protocolo utiliza nuevos objetos como [DIA2007]:

- *Label Request*: para el requerimiento una etiqueta enviado en el mensaje Path.
- *Label*: contienen una etiqueta (mensaje Resv).
- *Explicit_Route*: contiene la lista de direcciones IP de los routers que definen el trayecto LSP (mensaje Path).
- *Record_Router*: contiene direcciones IP de los routers que definen el trayecto LSP (mensaje Path y Resv).

La ventaja de este modelo es que permite la reserva de recursos en cada nodo, la aplicación de Ingeniería de Tráfico y el re-enrutamiento de los trayectos LSP ante casos de caídas de red, congestión o cuellos de botella. Asimismo, este protocolo permite la creación de rutas explícitas con o sin reserva de recursos donde el LER de ingreso es el encargado de especificar los saltos en el LSP.

3.4.4.6. Ventajas

MPLS presenta las siguientes ventajas [GON2008]:

- Soporta QoS y CoS.
- Combina las capacidades de rendimiento y escalabilidad de la conmutación de capa de Enlace de Datos (Capa 2) y la capa de Red (Capa 3) respectivamente.
- Debido a que las etiquetas son de una longitud fija, la conmutación se efectúa a altas velocidades.
- Permite interoperabilidad entre diferentes redes.

3.4.4.7. Desventajas

- Se agrega una capa adicional para su funcionamiento.
- Cada router debe entender MPLS para la conmutación de etiquetas.

3.4.5. Comparación IP y MPLS

3.4.5.1. Comparación de cabeceras IP y MPLS

Como se explicó anteriormente, las cabeceras IP y MPLS tienen gran diferencia en tamaño ya que la primera es de 20 Bytes mientras que la segunda sólo de 4 Bytes. Esto permite que la conmutación de los paquetes en cada uno de los nodos sea más rápida para el caso de MPLS debido a que solo se deben analizar 4 Bytes de información para tomar la decisión de enrutamiento. De esta forma, se reduce tiempo y procesamiento en la transmisión de datos.

3.4.5.2. Cuadro comparativo entre IP y MPLS

En la tabla 3-3, se muestran las diferencias entre las tecnologías IP y MPLS [DIA2007].

TABLA 3-3: CUADRO COMPARATIVO IP Y MPLS

CARACTERÍSTICA	IP	MPLS
Velocidad	Menor: cabecera muy grande (20 Bytes)	Mayor: cabecera pequeña (4 Bytes)
Gestión de QoS	Campo DSCP	Campo EXP
Escalabilidad	Al aplicar QoS, se sobrecarga la red	Menos señalización
Ingeniería de Tráfico	Enrutamiento basado en costos	Enrutamiento basado en el estado actual de la red. Re-enrutamiento inteligente.
Seguridad	Filtros según los campos de cabecera IP	Establecimiento de túneles y redes privadas virtuales
Nuevas redes	Migración de IPv4 a IPv6	Migración de IPv4 a IPv6

CAPÍTULO 4

PRUEBAS DE DESEMPEÑO

4.1. PRINCIPIOS SIMULACIÓN

Como se propone en esta Tesis, el objetivo principal es brindar la propuesta técnica para la migración en el *core* de una red NGN de IP a MPLS. La elección de la arquitectura MPLS se basará en las pruebas de comparación de diferentes arquitecturas para el *core* realizadas en este capítulo. Cabe recalcar que, a pesar de que las pruebas a realizarse serán simuladas, la comparación no pierde valor ya que muchas instituciones y centros de investigación basan sus estudios en diferentes simuladores.

Las arquitecturas tomadas en cuenta para la comparación son:

- IP Best Effort
- MPLS

Para determinar las ventajas y desventajas de estas arquitecturas, se empleará la herramienta de simulación OMNeT++ el cual es un simulador de redes modular de eventos discretos y que se distribuye bajo la Licencia Pública Académica (<http://www.omnetpp.org/>). Actualmente, se ha convertido en una herramienta muy popular en la comunidad científica e instituciones de la industria de las telecomunicaciones ya que permite el diseño y estudio de diferentes arquitecturas y aplicaciones permitiendo gran flexibilidad para las pruebas de diferentes soluciones. Para las pruebas de desempeño a realizarse, se hará uso del paquete INET Framework (<http://inet.omnetpp.org/>). La instalación de esta herramienta se encuentra en el Anexo 1.

Por otro lado, los parámetros tomados en cuenta durante las pruebas de comparación realizadas, serán los propuestos por la ITU-T en sus recomendaciones Y.1540 e Y.1541.

Es necesario mencionar que la medición de estos parámetros se realizarán en el nivel de *core* ya que este es el nivel de estudio dentro de la red NGN inicial.

4.2. SIMULACIÓN

En esta sección, se detallan las pruebas de simulación realizadas con las arquitecturas IP y MPLS aplicadas en el *core* de la NGN propuesta en el capítulo anterior.

4.2.1. Detalles Previos

La topología de red del *core* a simular, presentada a continuación, está formada por 52 routers como se puede observar en la figura 4-1.

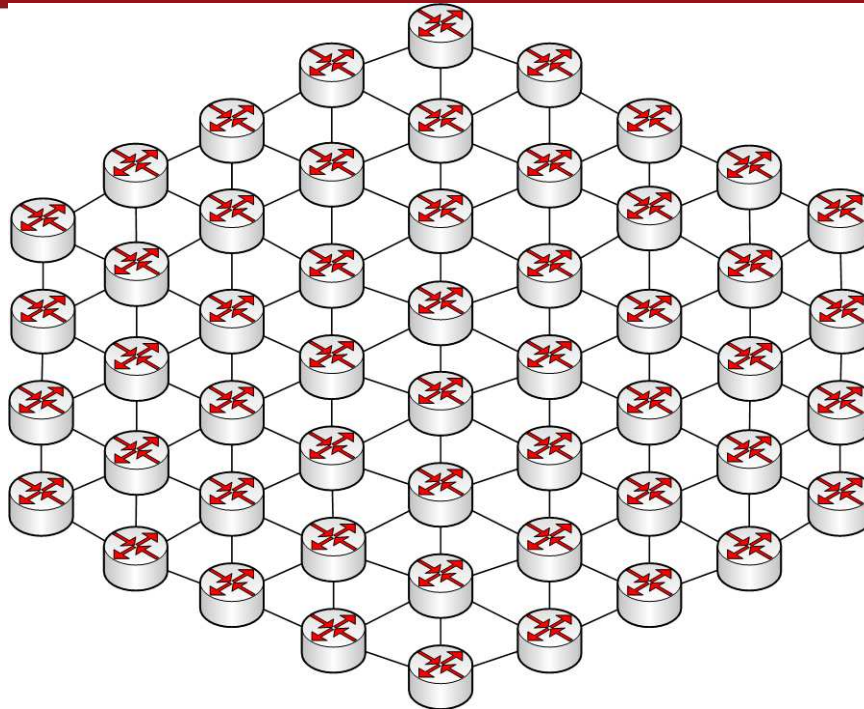


FIGURA 4-1: TOPOLOGÍA DE RED A SIMULAR

Debido a que el objetivo de esta simulación es comparar las arquitecturas IP y MPLS, se empleará una muestra significativa de tráfico transmitido a través del core. Así, la simulación, contará con diferentes tipos de tráfico como HTTP, FTP, SIP, RTP y UDP. Estos se simularán mediante diferentes hosts los cuales generarán tráfico de diferentes aplicaciones como llamadas telefónicas, descarga de archivos, acceso a páginas web y *videostreaming*. En la tabla 4-1 se puede observar el número de hosts empleados en la simulación.

TABLA 4-1: TRÁFICO A SIMULAR

CANTIDAD	TIPO DE EQUIPO	APLICACIÓN	INFORMACIÓN
1	Servidor	SIP	8 minutos de comunicación
1	Host	SIP	
1	Servidor	FTP	20Mb
1	Host	FTP	
1	Servidor	HTTP	10 peticiones Máximo de 45KB/petición
1	Host	HTTP	
2	Host	RTP	8 minutos de comunicación
1	Servidor	<i>VideoStreaming</i>	10 MB
1	Host	<i>VideoStreaming</i>	

Asimismo, los parámetros de QoS tomados en cuenta para la comparación serán los definidos en las recomendaciones Y.1540 y Y.1541 de la ITU-T indicadas en la sección 3.2. Por otro lado, las aplicaciones indicadas anteriormente, se implementaron según los protocolos indicados en la tabla 4-2.

TABLA 4-2: PROTOCOLOS IMPLEMENTADOS

APLICACIÓN	PROTOCOLO IMPLEMENTADO
SIP	TCP
FTP	TCP
HTTP	TCP
RTP	UDP
<i>VideoStreaming</i>	UDP

Cabe recalcar que los enlaces entre los nodos de red tendrán una capacidad de 2 Mbps ya que este es el mínimo indicado por la ITU-T para garantizar QoS como se indicó en el capítulo 3. Además, las conexiones host – router serán enlaces Ethernet, es decir, 10 Mbps.

La configuración de los nodos y el protocolo de enrutamiento a utilizar dependerán de la arquitectura empleada en la simulación. Por otro lado, el tiempo de simulación será de 15 minutos donde todas las aplicaciones generarán tráfico simultáneamente y el tipo de colas empleado en los enlaces es del tipo FIFO (*First In First Out*).

En la tabla 4-3, se pueden observar los parámetros de simulación.

TABLA 4-3: PARÁMETROS DE SIMULACIÓN

	CANTIDAD	VELOCIDAD (Mbps)	TIPO DE COLA	DURACIÓN (min)
Host	8	10	FIFO	--
Routers	12	--	FIFO	--
Enlaces	--	2	FIFO	--
Simulación	--	--	--	15

El escenario de simulación será el mostrado en la figura 4-2. La selección de esta topología se realizó en base a la cantidad de nodos de red y nodos generadores de tráfico. Asimismo, se tomó en cuenta la cantidad de tráfico que se simulará. Todo esto hace posible la simulación de un escenario real con tráfico que usualmente se encuentra presente en la red.

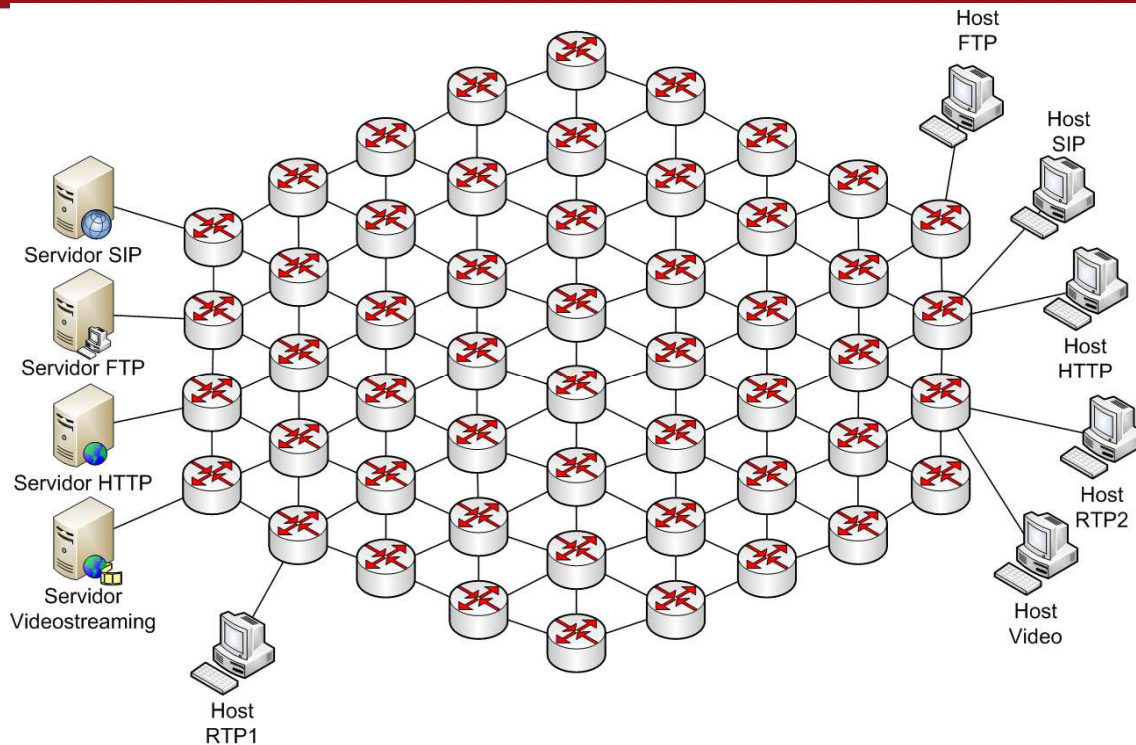


FIGURA 4-2: TOPOLOGÍA DE SIMULACIÓN FINAL

El tráfico se transmite de la siguiente forma:

- HTTP: de Servidor HTTP a Host HTTP.
- FTP: de Host FTP a Servidor FTP.
- SIP: de Host SIP a Servidor SIP.
- *Videostreaming*: de Servidor UDP a Host UDP.
- RTP: de Host RTP2 a Host RTP1

Los parámetros de simulación descritos se pueden verificar en el Anexo 2.

A continuación se describen las simulaciones realizadas así como los resultados obtenidos.

4.2.2. Simulación IP *Best Effort*

De acuerdo a la topología de simulación propuesta para la simulación, la red utilizada para las pruebas de desempeño de la arquitectura IP *Best Effort* se muestra en la figura 4-3.

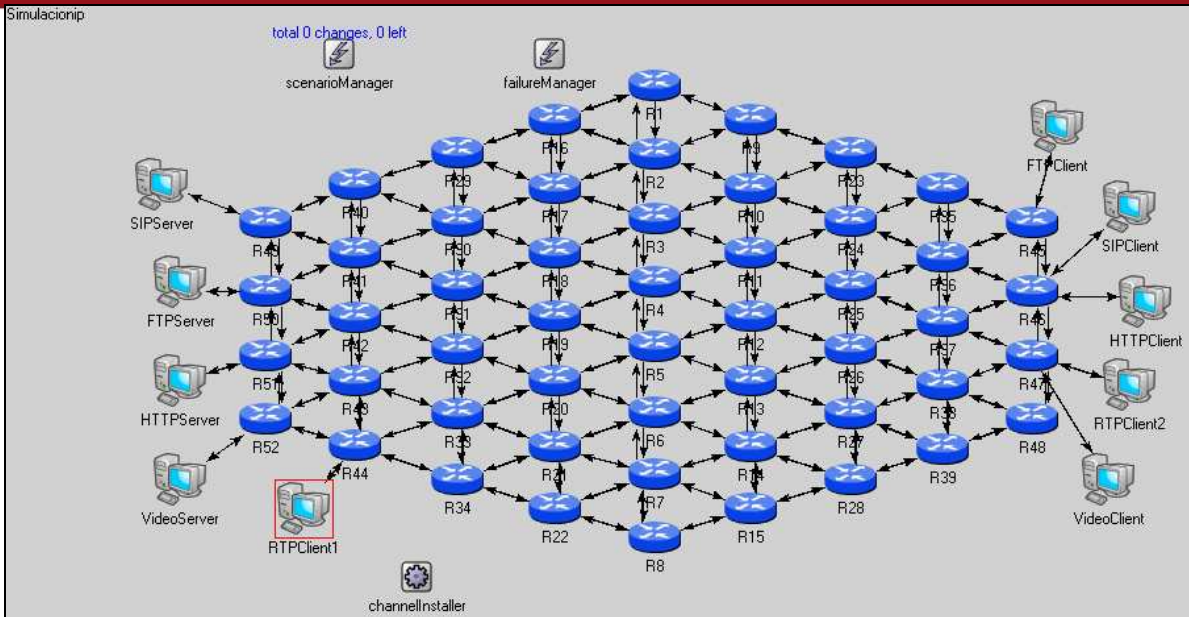


FIGURA 4-3: RED DE SIMULACIÓN IP BEST EFFORT

Para esta arquitectura, se emplearon 52 routers, 10 hosts y, además, el protocolo de enrutamiento OSPF ya que es el más utilizado por los operadores para la distribución de rutas actualmente.

Al inicio de la simulación, se tiene un intercambio de mensajes HELLO y Link Update para la distribución de rutas mediante el protocolo OSPF (ver figura 4-4).

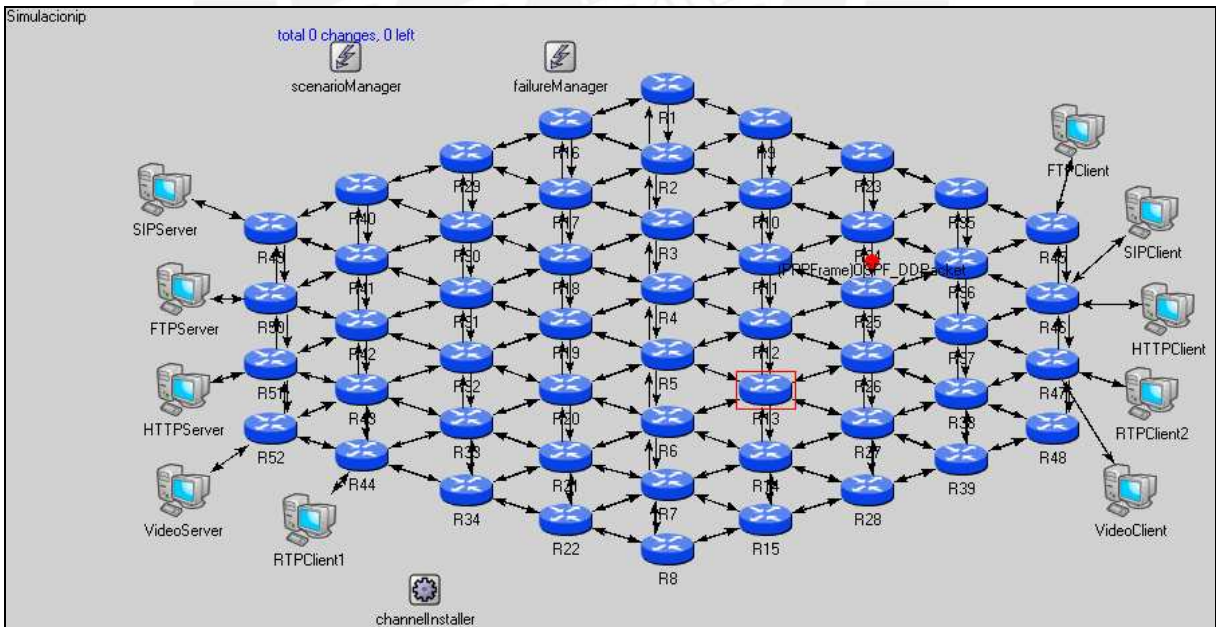


FIGURA 4-4: INTERCAMBIO MENSAJES OSPF

Luego, en el minuto 2, empieza la transmisión de los paquetes correspondientes a todas las aplicaciones previamente configuradas.

Al finalizar la simulación luego de 15 minutos, se obtienen diferentes valores para cada aplicación. A continuación, se mostrarán los resultados de retardo de las diferentes aplicaciones implementadas (figuras 4-5, 4-6, 4-7, 4-8 y 4-9).

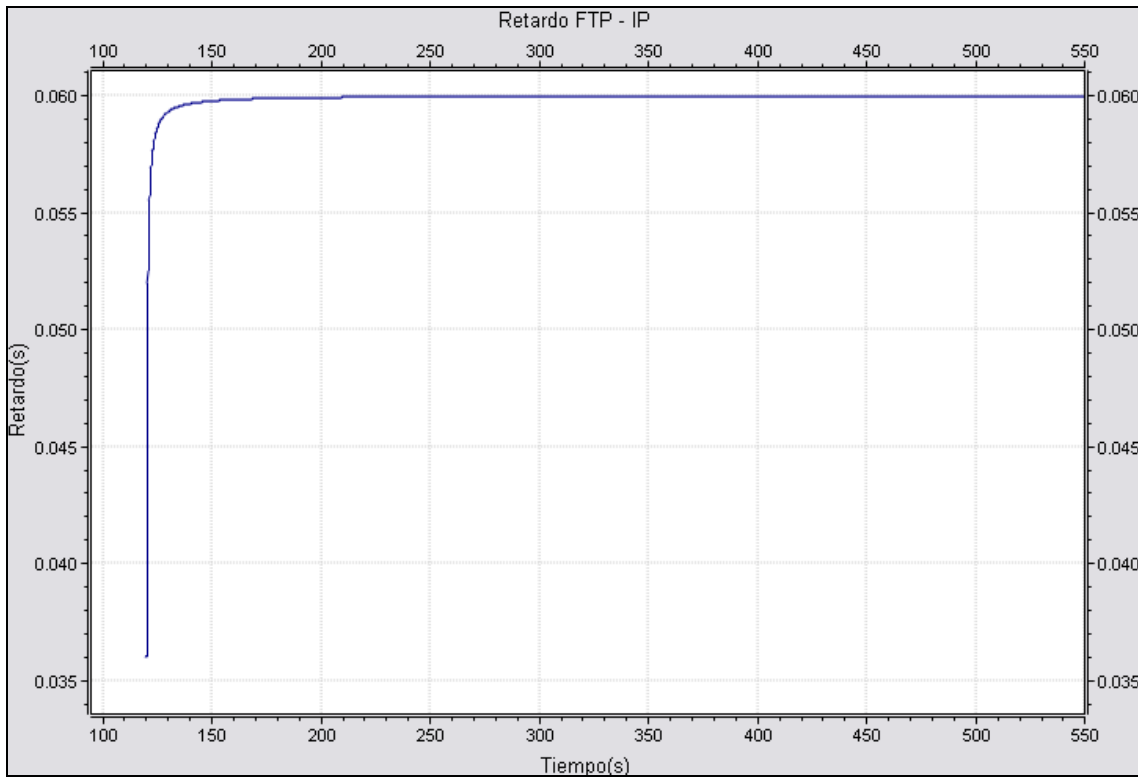


FIGURA 4-5: FTP RETARDO

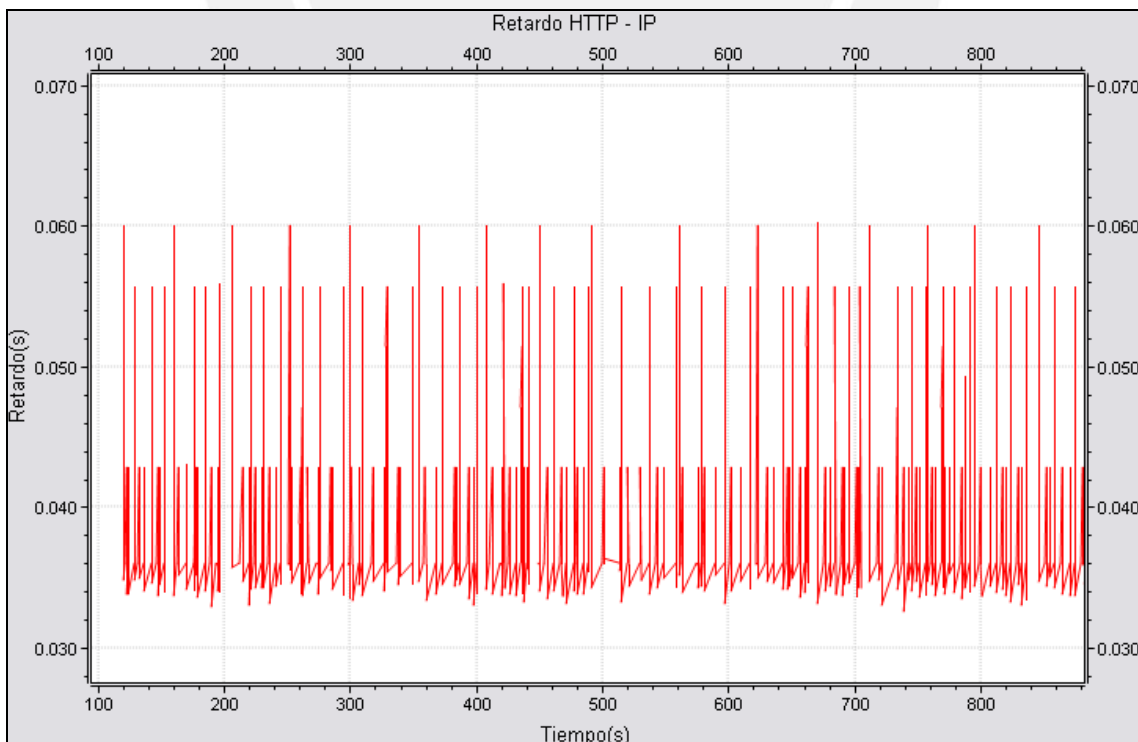


FIGURA 4-6: HTTP RETARDO

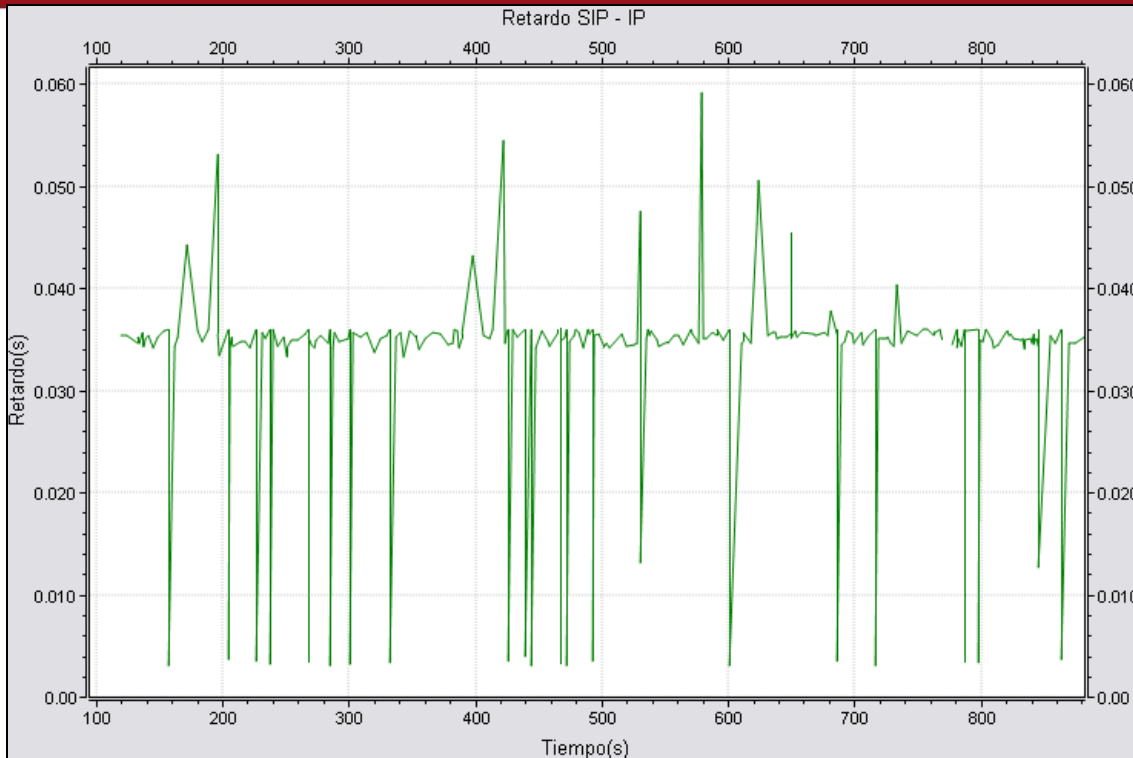


FIGURA 4-7: SIP RETARDO

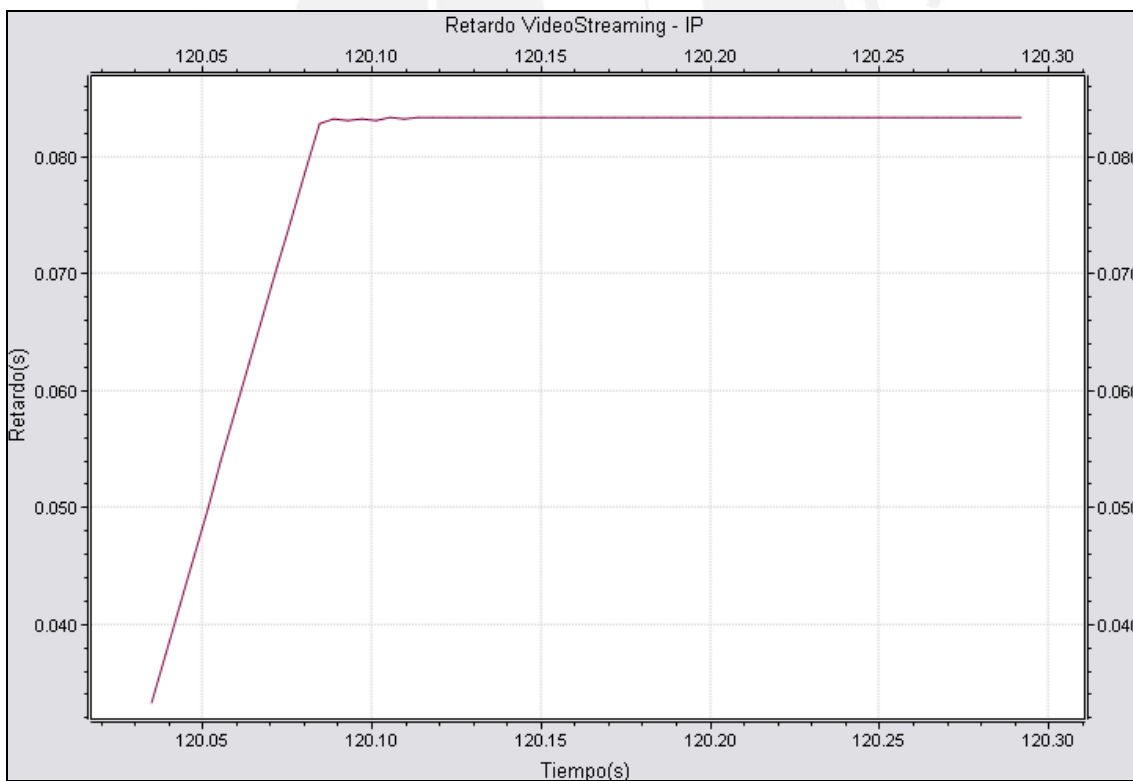


FIGURA 4-8: VIDEOSTREAMING RETARDO

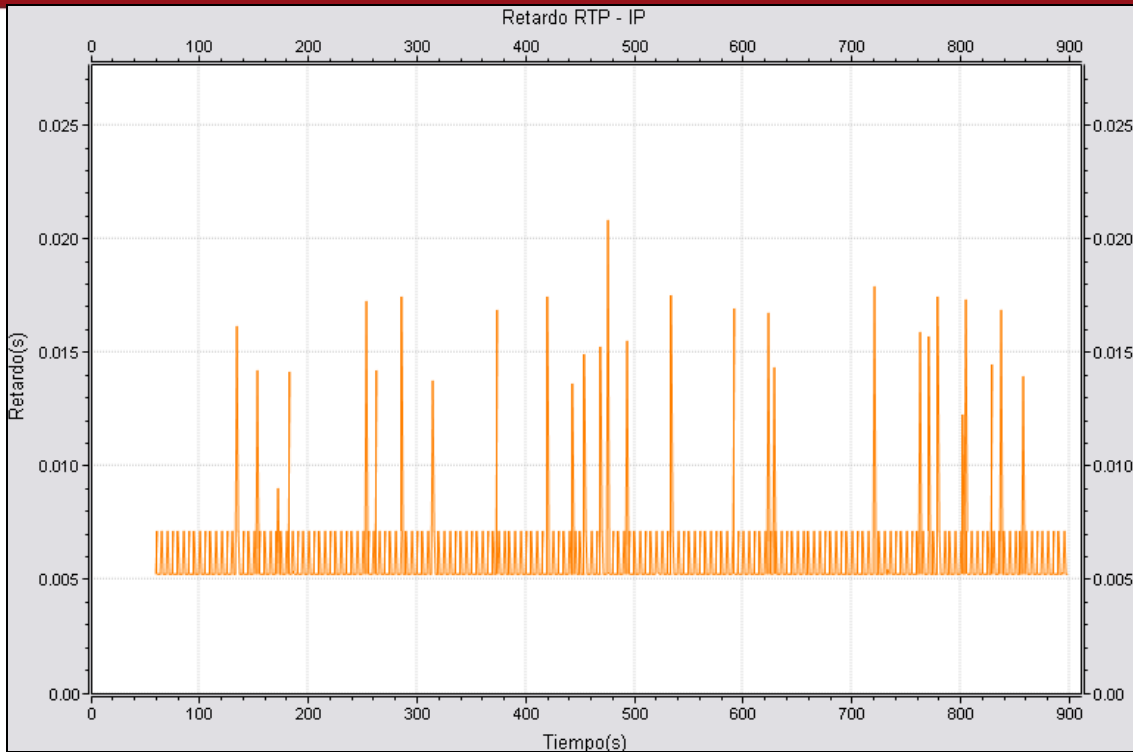


FIGURA 4-9: RTP RETARDO

En la tabla 4-4, se muestran los valores de retardo y *jitter* para los cuatro protocolos implementados.

TABLA 4-4: RESULTADOS IP BEST EFFORT

APLICACIÓN	RETARDO (ms)			JITTER (ms)
	MIN	PROM	MAX	
FTP	35.98	59.96	60.09	0.78
SIP	3.06	33.09	59.06	77.56
HTTP	32.52	39.34	60.09	120.03
Video	33.3	78.15	83.42	0.8
RTP	5.24	5.95	20.77	1.97

4.2.3. Simulación MPLS RSVP-TE

Para el caso de MPLS la red utilizada para las pruebas de desempeño se muestra en la figura 4-10. Para estas pruebas, se implementará el protocolo de distribución de etiquetas RSVP-TE ya que proporciona la reserva de recursos e Ingeniería de Tráfico.

El protocolo de enrutamiento utilizado, al igual que las pruebas de IP *Best Effort*, fue OSPF.

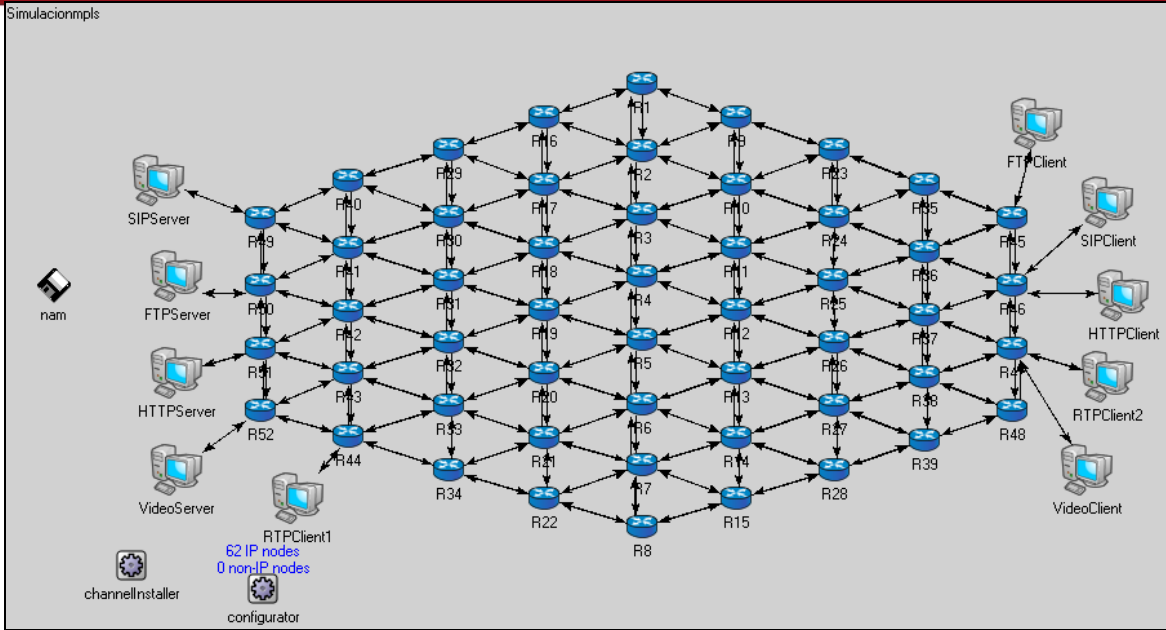


FIGURA 4-10: RED DE SIMULACIÓN MPLS RSVP-TE

Al inicio de la simulación, se observa el intercambio de mensajes OSPF para la distribución de rutas (ver figura 4-11). Luego empieza el intercambio de etiquetas entre los routers MPLS mediante el protocolo RSVP-TE.

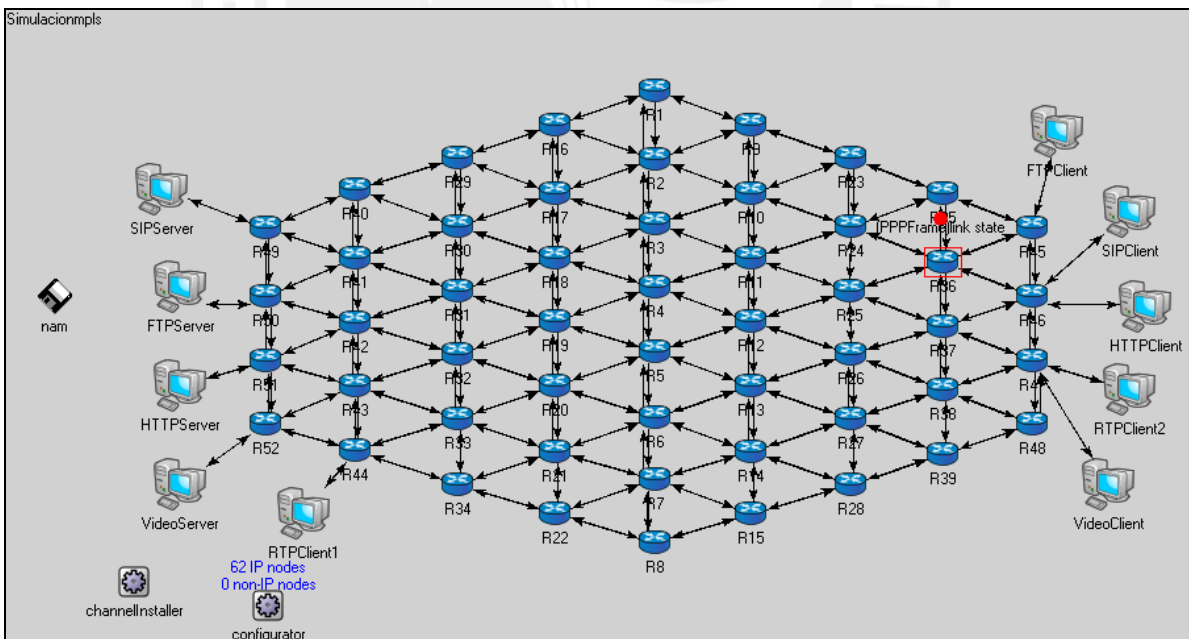


FIGURA 4-11: INTERCAMBIO DE MENSAJES OSPF

A partir del segundo minuto, empieza la generación de tráfico por parte de los hosts según las aplicaciones previamente configuradas.

Al finalizar la simulación luego de 15 minutos, se obtienen diferentes valores para cada una de las aplicaciones. A continuación, se mostrarán los resultados de retardo de las diferentes aplicaciones implementadas (figuras 4-12, 4-13, 4-14, 4-15 y 4-16).

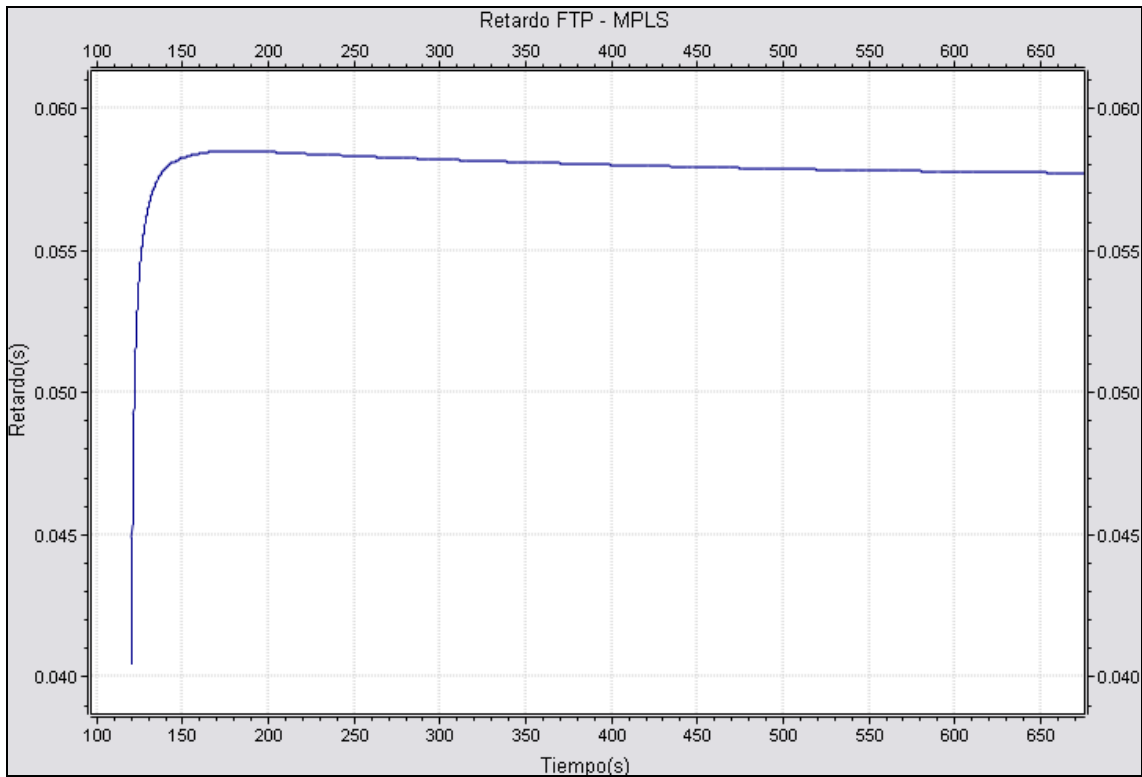


FIGURA 4-12: FTP RETARDO

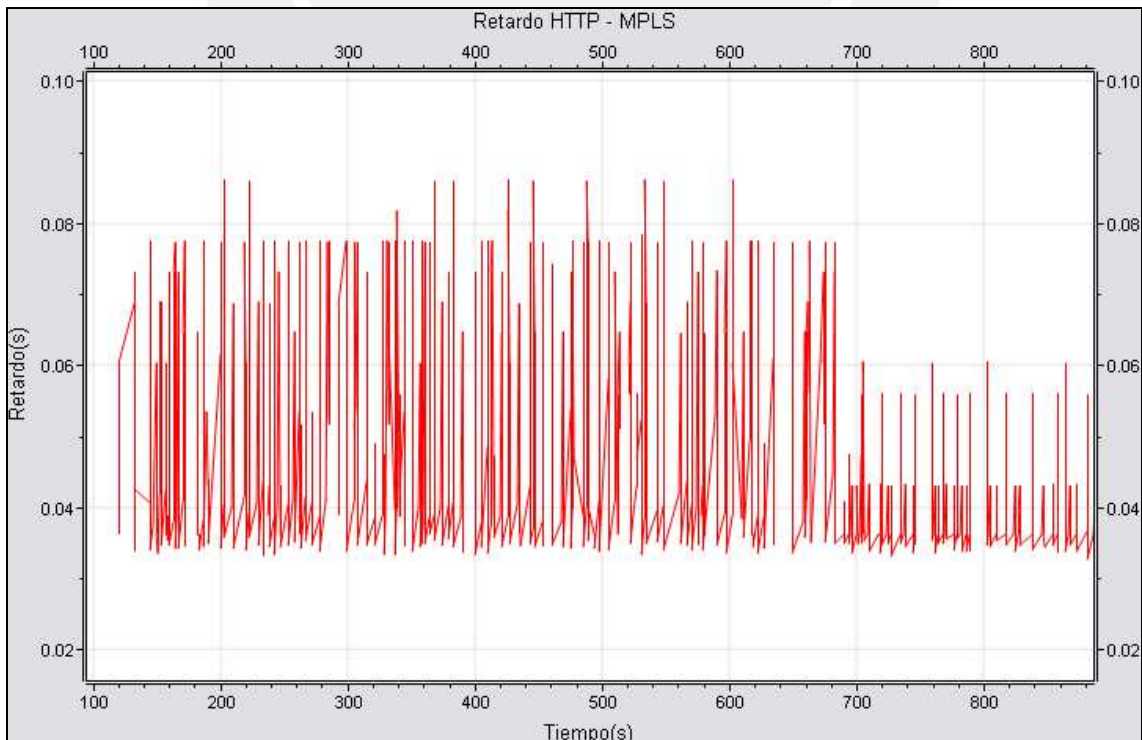


FIGURA 4-13: HTTP RETARDO

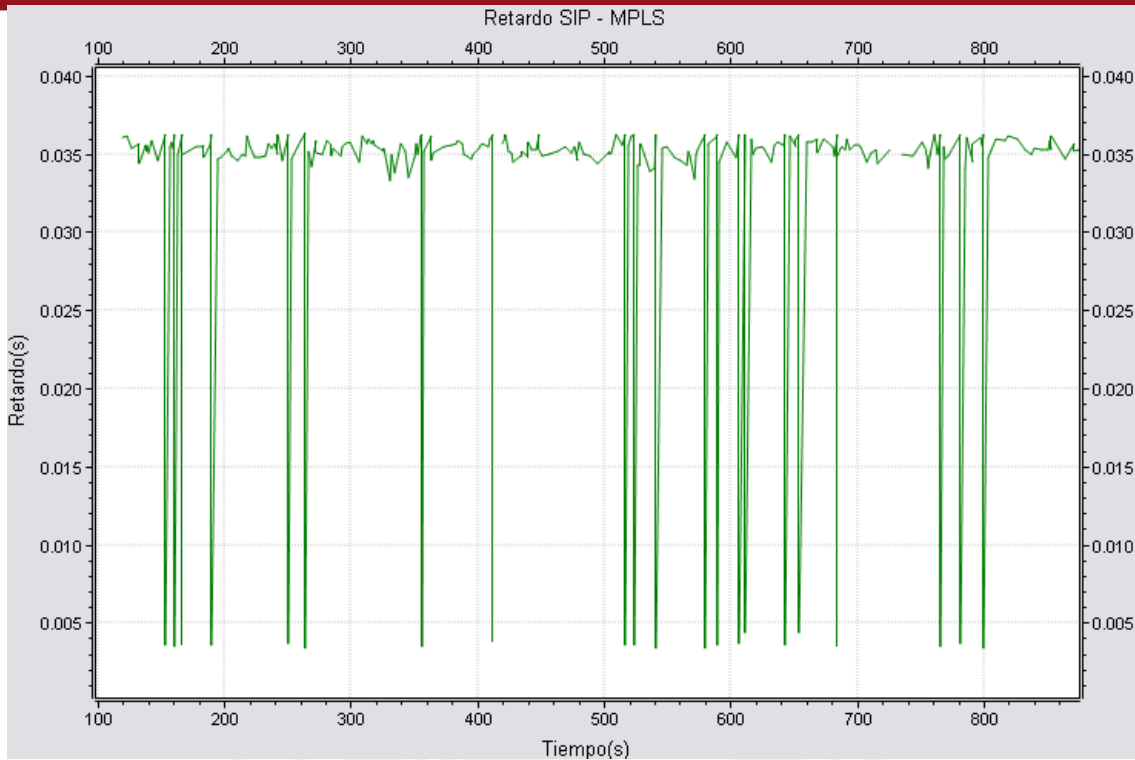


FIGURA 4-14: SIP RETARDO

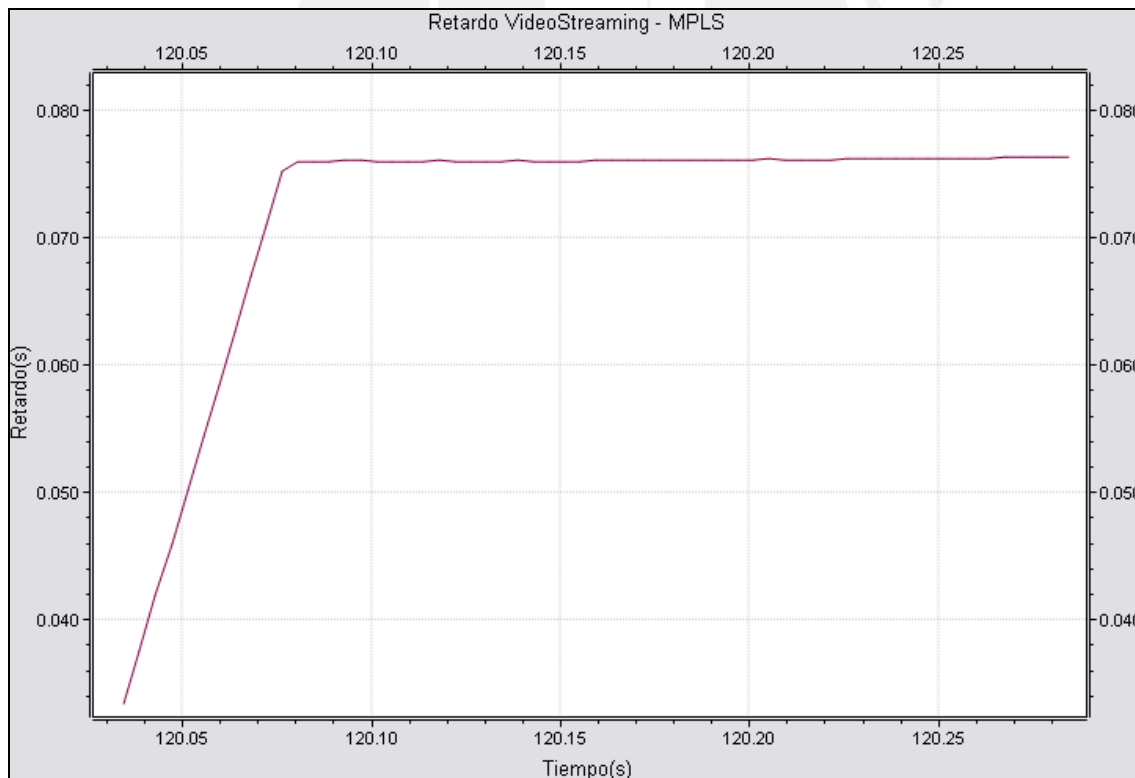


FIGURA 4-15: VIDEOSTREAMING RETARDO

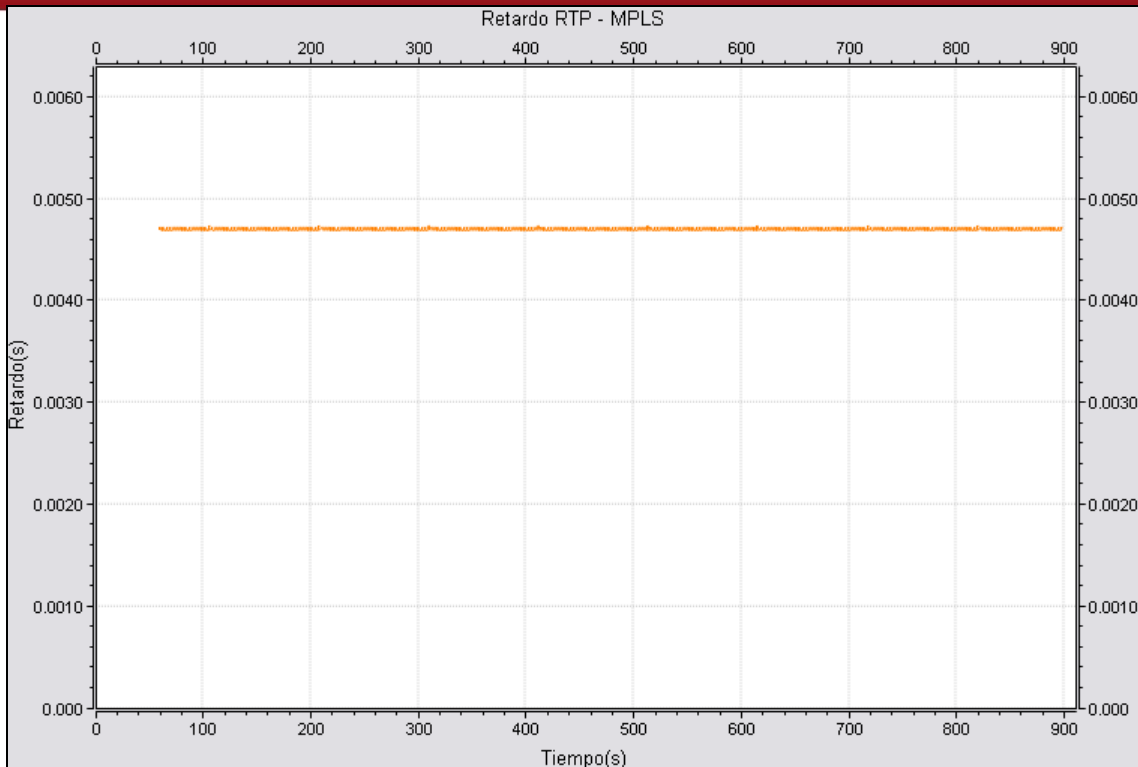


FIGURA 4-16: RTP RETARDO

En la tabla 4-5, se muestran los valores de retardo, pérdida de paquetes y jitter para los cuatro protocolos implementados.

TABLA 4-5: RESULTADOS MPLS

APLICACIÓN	RETARDO (ms)			JITTER (ms)
	MIN	PROM	MAX	
FTP	40.42	57.41	58.41	4.38
SIP	3.31	32.85	36.31	75.27
HTTP	32.73	47.58	86.11	99.29
Video	33.41	72.16	76.35	0.71
RTP	4.68	4.69	4.72	0.01

4.3. RESULTADOS

De los resultados obtenidos en las secciones 4.2.2 y 4.2.3 (ver tablas 4-4 y 4-5), se puede observar que MPLS presenta las mejores prestaciones de red para los diferentes tipos de tráfico simulado.

La arquitectura MPLS obtuvo valores de retardo y *jitter* menores que la arquitectura IP *Best Effort*. Por lo tanto, con MPLS RSVP-TE se pueden ofrecer los requerimientos

que necesitan las aplicaciones actualmente, cumpliendo con las recomendaciones Y.1540 y Y.1541 de la ITU-T.

Por otro lado, se pudo comprobar que se hace necesario de un protocolo de enrutamiento lo suficientemente eficiente para la distribución de rutas IP los cuales serán empleados para la distribución de etiquetas.

Para el caso particular del tráfico UDP, se observa que los valores de retardo y *jitter* permiten la transmisión adecuada de aplicaciones en tiempo real como VoIP o videoconferencias.



CAPÍTULO 5

PROPUESTA DE MIGRACIÓN

5.1. ESCENARIO INICIAL DE MIGRACIÓN

Para la presente Tesis, el escenario inicial de migración consiste en:

- Una red NGN con *core* IP formado por 52 routers distribuidos a lo largo del territorio peruano (ver figura 5-1).
- El servicio será brindado por un solo operador.
- El acceso de los usuarios se da por medio de Centrales TDM de Clase 5 o redes ADSL, pudiéndose tener usuarios POTS, ISDN o xDSL ya sean para servicios de voz o datos.

Este escenario descrito se muestra en la figura 5-2.

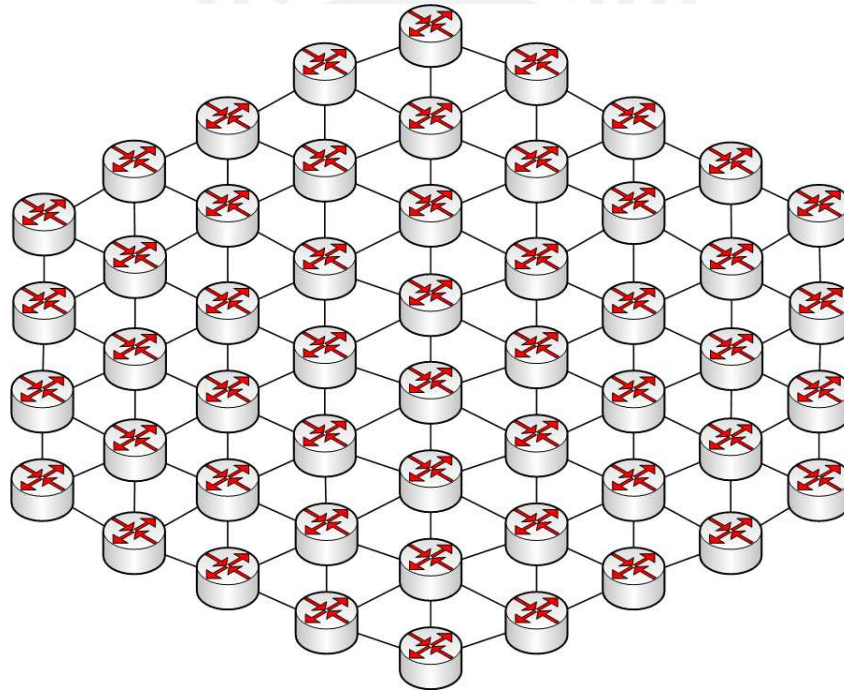


FIGURA 5-1: CORE IP INICIAL

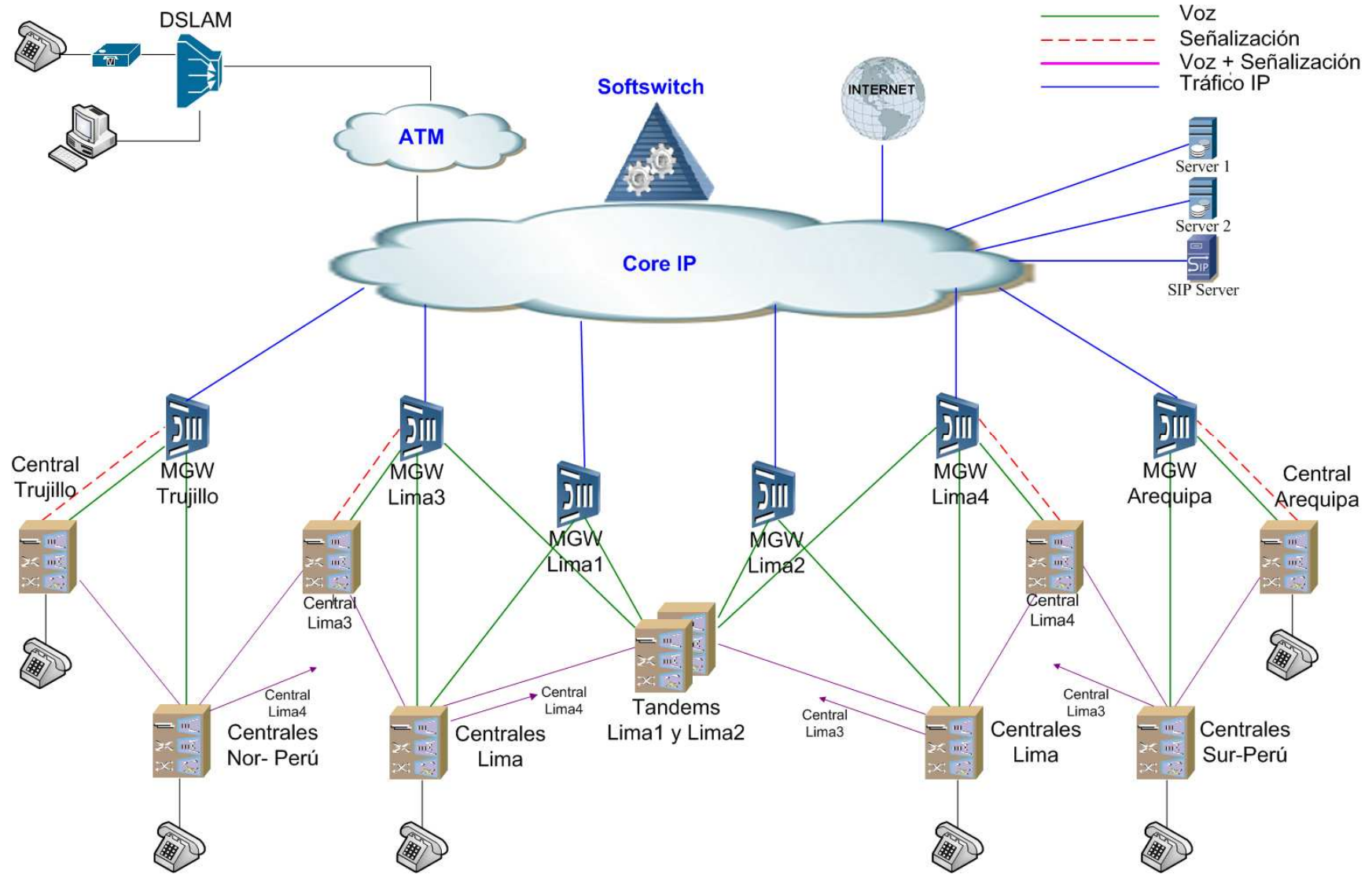


FIGURA 5-2: ESCENARIO INICIAL DE MIGRACIÓN

Como se puede observar, gran parte del tráfico de señalización se transmite a través del *core* IP; sin embargo, aún se mantienen los enlaces de señalización entre las centrales TDM de la red PSTN original.

El conjunto de 52 routers es el que finalmente será la red de estudio sobre el cual se compararán las arquitecturas IP y MPLS para la provisión de QoS en el *core* de la red NGN.

Las razones para este escenario inicial son las siguientes:

- Las redes NGN actuales en nuestro país presentan un *core* IP sin calidad de servicio.
- La Tesis se basa en la red un solo operador debido a que los objetivos de la Tesis no implican el estudio de la calidad de servicio entre redes de diferentes operadores.
- Actualmente, los operadores brindan el acceso a su *core* mediante centrales TDM de Clase 5 o tecnología ADSL. Si bien es cierto que el número de usuarios de acceso ADSL ha aumentado, el servicio de telefonía a través de esta tecnología de acceso aún no es implementado masivamente por los operadores; sin embargo, estos usuarios sí tienen acceso a servicios de datos.

Con estas definiciones previas, se ubicará la red NGN de estudio en el escenario peruano actual.

5.1.1. Demanda actual de enlaces y tráfico

De acuerdo a los datos presentados por OSIPTEL en sus estadísticas de telefonía fija y acceso a Internet, se obtienen los resultados de las tablas 5-1 y 5-2.

TABLA 5-1: ENLACES Y TRÁFICO SECTOR RESIDENCIAL

RESIDENCIAL	Número de clientes	E1's	BW (Gbps)	Tasa de crecimiento anual	E1's futuro	BW Futuro (Gbps)
Telefonía fija	3.000.000	20000	40	2%	20400	40.8
ADSL	850000	--	90	25%	--	112.5

TABLA 5-2: ENLACES Y TRÁFICO SECTOR EMPRESARIAL

EMPRESARIAL	E1's	BW (Gbps)
ISDN (PRI)	15000	30
Internet	--	10

Por tal motivo, debido al crecimiento del tráfico tanto de voz como de datos, se hace necesario el manejo de calidad de servicio en el *core* de la red NGN.

5.2. PROPUESTA FINAL

En esta sección describen los requerimientos y etapas necesarios para la migración del *core* NGN de IP a MPLS.

5.2.1. Aspectos Técnicos

El objetivo principal de la presente Tesis es brindar una propuesta técnica para la migración antes mencionada; por este motivo, se describen a continuación los aspectos técnicos necesarios para cumplir con esta tarea.

5.2.1.1. Verificación de routers

Antes de la migración, se debe verificar si los routers empleados en el *core* IP soportan MPLS. Si estos lo soportan, se podrá continuar el análisis técnico. Sin embargo, si no es así, se debe consultar al proveedor de los equipos (Cisco, Juniper, Huawei o Alcatel - Lucent) para consultar si es posible hacer un *upgrade* al sistema operativo de estos o, en su defecto, realizar la compra de nuevos routers.

En la actualidad, la mayoría de routers utilizados en las redes *core* soportan MPLS o requieren un *upgrade* para poder hacerlo. Por este motivo, la compra de nuevos equipos queda casi descartada evitando así, el aumento de los costos.

5.2.1.2. Distribución de etiquetas

Como se sabe, MPLS emplea etiquetas para el establecimiento de los LSPs a través de la red. En consecuencia, se necesita un protocolo de señalización que permita el intercambio de estas etiquetas con el objetivo de que todos los routers sepan qué etiqueta colocar a los paquetes según sus características. Entre estos protocolos de señalización se tienen LDP y RSVP-TE.

Para esta propuesta de migración, se hará uso del protocolo RSVP-TE que, a diferencia de LDP, permite Ingeniería de Tráfico y el re-enrutamiento de los trayectos LSP mencionado en la sección 3.4.4. Asimismo, se emplearán caminos explícitos.

5.2.1.3. Protocolo de enrutamiento

Se empleará el protocolo OSPF como protocolo de enrutamiento debido a que no satura el BW de los enlaces y por su fácil configuración. Cabe recalcar que, como se está trabajando en la red de un solo proveedor, se tiene un solo sistema autónomo por lo que sólo se requiere un protocolo de enrutamiento IGP como OSPF. Asimismo, se utilizarán tres áreas OSPF y las extensiones de Ingeniería de Tráfico para este protocolo.

5.2.1.4. Routers especiales

Para el mejor funcionamiento de la red, se designarán routers especiales los cuales tendrán una función específica.

- Router *Access* (RA): router al cual se conectan los usuarios de VoIP o Internet con acceso ADSL. Estos equipos poseen las configuraciones necesarias para su provisión y adecuado enrutamiento hacia los MGWs o a la red de redes respectivamente.
- Router *Gateway* (RGW): este equipo es utilizado para la conexión con los MGWs permitiendo el acceso a los usuarios de telefonía tradicional TDM. Por otro lado, el Softswitch NGN también se conecta al *core* MPLS a través de un RGW.
- Router Toll Gate (RTG): router que permite la conexión con la red internacional para transportar el tráfico correspondiente.
- Router NAP (RNAP): opera como punto de interconexión con otros operadores.
- Router Satelital (Satelital): permite la conexión de los equipos que se encuentran en zonas donde sólo se tiene comunicación vía enlaces satelitales como las ciudades de Iquitos, Puerto Maldonado y Pucalpa.
- Router *Core* (RC): router interno a la red MPLS. No tiene interconexión de acceso directa con las redes de acceso o MGWs ya que es empleado para la comunicación entre los diferentes routers de borde como RA, RGW, RTG, RNAP o Satelital.

5.2.1.5. Distribución de routers en el territorio peruano

En esta etapa se distribuirán los 52 routers a lo largo del territorio peruano según el escenario inicial de migración mostrado en la sección 5.1. En este escenario, se tienen MGWs en tres zonas diferentes del país: Trujillo, Lima y Arequipa, por lo que el *core* MPLS propuesto estará conformado por las zonas Norte, Centro y Sur donde los nodos principales estarán ubicados en las ciudades de Trujillo, Lima y Arequipa respectivamente. A estos nodos se conectarán los demás nodos RA y RGW que conforman la red según la zona a la que pertenezcan a excepción de los routers ubicados en las ciudades de Iquitos, Puerto Maldonado y Pucalpa lo cuales se conectan al router Satelital localizado en Lima.

Por otro lado, se tendrá un *mini-core* formado por cuatro routers ubicados en Lima. Estos estarán interconectados con los routers ubicados en Trujillo y Arequipa así como los routers restantes de Lima. Además, este *mini-core* tendrá conexión con los routers TG, NAP y Satelital y el Softswitch ubicado en Lima.

5.2.1.6. Justificación de ubicación de nodos y subnodos de la red

Según las estadísticas publicadas por OSIPTEL [OSI2009], los departamentos que concentran el mayor tráfico de telefonía e Internet son Lima, La Libertad y Arequipa. Por

este motivo, estos son los departamentos en donde se encuentran los nodos más importantes del core NGN. Los demás nodos se encuentran en las ciudades cercanas a estas teniendo conexiones redundantes con sus respectivos nodos.

5.2.1.7. Enlaces

Se emplearán los mismos enlaces físicos existentes en el escenario inicial de migración; por lo tanto, no se implementarán nuevos enlaces físicos. Se tienen los siguientes:

- Fibra Óptica: utilizada en los enlaces router-router, router-MGW y router-Softswitch.
- Cobre: utilizado para la conexión con la red ATM. También es empleado en la interconexión con los diferentes servidores de la red NGN.
- Satelital: empleado para la comunicación con ciudades con las cuales, por la geografía del territorio peruano, no se tiene enlace alámbrico. Por ejemplo, las ciudades de Iquitos, Puerto Maldonado y Pucallpa tienen acceso a la red NGN mediante enlaces satelitales.

5.2.1.8. Conexiones con otros equipos NGN

Se hará una reestructuración de tal forma que se tengan los routers RA y RGW descritos anteriormente. Se tendrán RA ubicados en diferentes ciudades del Perú. Los RGW estarán localizados en Trujillo, Lima y Arequipa ya que, en estas ciudades, se encuentran los diferentes MGWs que permiten la interconexión con las centrales TDM así como el Softswitch que se encuentra en Lima.

5.2.1.9. Direccionamiento IP

Se utilizarán tres rangos de direcciones IP privadas y un rango de direcciones IP públicas. Estas direcciones públicas serán las otorgadas por la LACNIC (*Latin American and Caribbean Internet Addresses Registry*) y serán utilizadas en los routers RTG.

TABLA 5-3: DIRECCIONES IP

TIPO	RANGO	MÁSCARA	CLASE
Privada	10.0.0.0	255.0.0.0	A
	172.10.0.0	255.255.0.0	B
	172.20.0.0	255.255.0.0	B
Pública	Rango brindado por LACNIC		

5.2.1.10. Clasificación de tipos de servicios

Los servicios de datos pueden ser clasificados mapeando el valor del campo DSCP de la cabecera IP en el campo EXP de la cabecera MPLS obteniéndose los siguientes tipos de servicio:

- Premium: para tráfico con QoS muy alto (DSCP = 46).
- Gold: para tráfico con QoS alto (DSCP = 10, 12 o 14).
- Silver: para tráfico con QoS medio alto (DSCP = 18, 22 o 25).
- Bronce: para tráfico con QoS medio bajo (DSCP = 26, 28 o 30).
- Best Effort: para tráfico sin QoS (DSCP = 0).

5.2.1.11. Gestión de equipos

La gestión de toda la red se realizará desde el NOC en Lima para lo cual se hará uso de diferentes protocolos según el equipo a gestionar. Entre dichos protocolos se tienen:

- TELNET: empleado para el acceso a algunos servidores de la red.
- SSH: este protocolo se utiliza para el acceso a equipos como MGWs, Softswitch y algunos servidores de la red.
- HTTP: además de los dos primeros protocolos mencionados, algunos equipos permiten el acceso vía HTTP proveyendo una interfaz gráfica más amigable.
- SNMP: empleado para la obtención de datos estadísticos como BW en los diferentes enlaces.
- TACACS: utilizado para el acceso a los equipos de red mediante la autenticación de usuario. Cada persona autorizada a gestionar los diferentes routers de la red, tendrán un usuario TACACS con el cual se tendrá acceso a cada uno de los routers del *core*. Este protocolo permite dar restricciones según el tipo de usuario que se tenga así como el registro de modificaciones realizadas en los equipos.

Además de los protocolos de gestión, es necesario recalcar que los routers poseerán interfaces loopbacks para la gestión de los mismos.

Por otro lado, debido a que se llevarán a cabo *upgrades* en los nodos, también deberá cambiarse la versión de la plataforma de gestión brindada por el proveedor de los equipos para poder soportar las nuevas funcionalidades de los diferentes nodos. En consecuencia, tanto el servidor como los clientes del gestor deberán ser actualizados.

5.2.2. Escenario final

A continuación se detallan las configuraciones que se realizarán en la red según los aspectos técnicos mencionados anteriormente.

5.2.2.1. Distribución de routers

Se nombrarán los routers según su ubicación física y su funcionalidad según lo descrito en la sección 5.2.1. Al finalizar esta tarea se tendrá lo siguiente:

TABLA 5-4: NOMBRAMIENTO DE ROUTERS

ZONA	ROUTER	UBICACIÓN	FUNCIONALIDAD
NORTE	TRUJILLO	Trujillo	RC
	TRU1	Trujillo	RGW
	TRU2	Trujillo	RA
	TRU3	Trujillo	RA
	PIU	Piura	RA
	CHM	Chimbote	RA
	CHI	Chiclayo	RA
	CAJ	Cajamarca	RA
	TPO	Tarapoto	RA
	HRZ	Huaraz	RA
CENTRO	LIM01	Lima	RA
	LIM02	Lima	RA
	LIM03	Lima	RA
	LIM04	Lima	RA
	LIM05	Lima	RGW
	LIM06	Lima	RGW
	LIM07	Lima	RA
	LIM08	Lima	RA
	LIM09	Lima	RA
	LIM10	Lima	RA
	LIM11	Lima	RA
	LIM12	Lima	RGW
	LIM13	Lima	RGW
	LIM14	Lima	RA
LIMA1	Lima	RC	

	LIMA2	Lima	RC
	LIMA3	Lima	RC
	LIMA4	Lima	RC
	LIMA5	Lima	RC
	LIMNAP1	Lima	RNAP
	LIMNAP2	Lima	RNAP
	LIMTG1	Lima	RTG
	LIMTG2	Lima	RTG
	SATELITAL	Lima	Satelital
	HCH	Huacho	RA
	ICA	Ica	RA
	CHN	Chincha	RA
	HYO1	Huancayo	RA
	HYO2	Huancayo	RA
	PUCP	Pucallpa	RA
	PTM	Puerto Maldonado	RA
	IQUI	Iquitos	RA
SUR	AREQUIPA	Arequipa	RC
	AQP1	Arequipa	RGW
	AQP2	Arequipa	RA
	AQP3	Arequipa	RA
	AQP4	Arequipa	RA
	JUL1	Juliaca	RA
	JUL2	Juliaca	RA
	TACNA1	Tacna	RA
	TACNA2	Tacna	RA
	CUSCO	Cusco	RA

Como se puede observar, los routers están distribuidos en todo el territorio peruano teniéndose tres puntos principales de acceso que son Trujillo, Lima y Arequipa. Además se tiene un router para los enlaces satelitales.

A continuación, en la figura 5-3, se muestra dicha distribución a lo largo del territorio peruano.

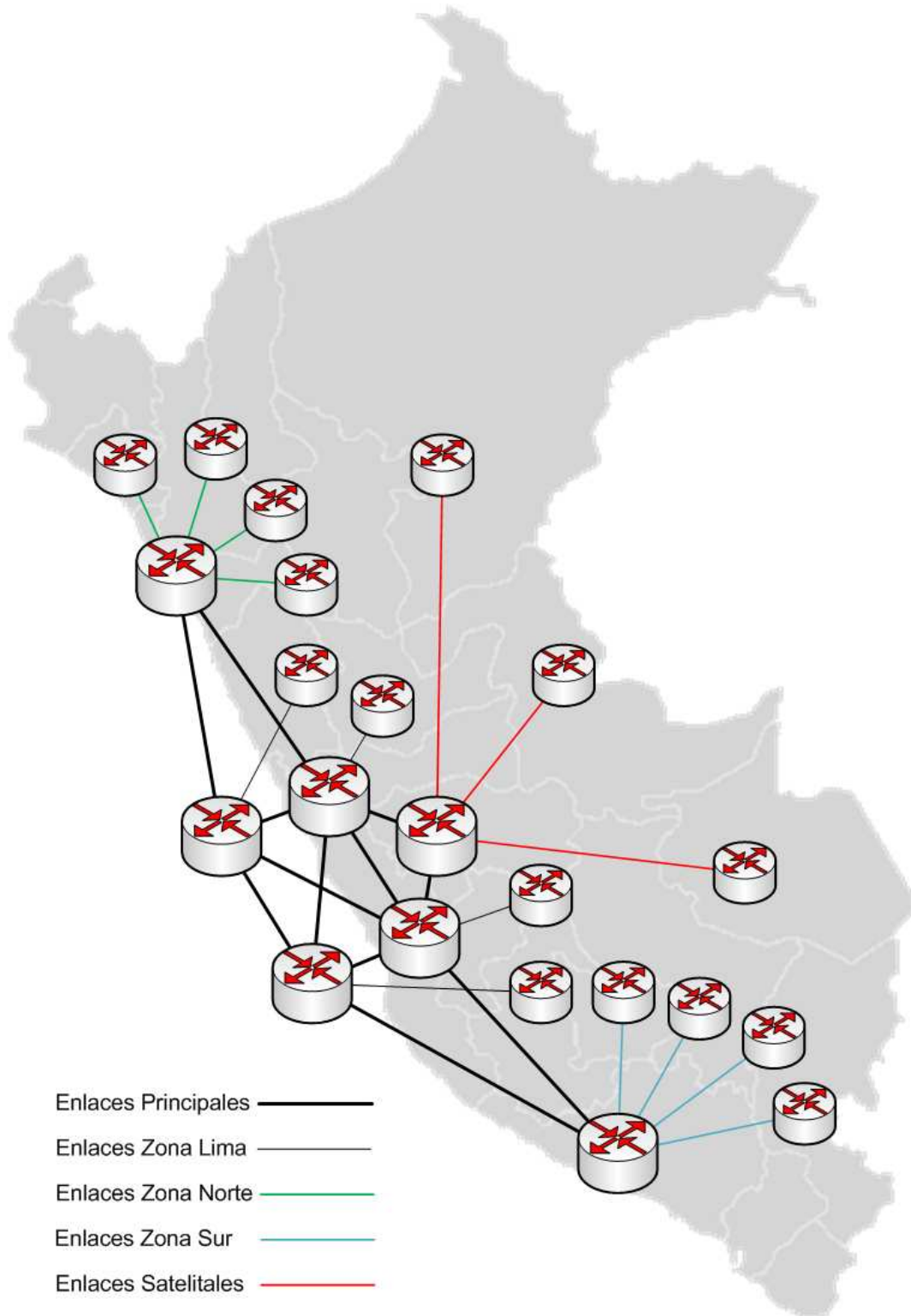


FIGURA 5-3: DISTRIBUCIÓN DE ROUTERS

En la figura 5-4, se puede observar el diagrama detallado de la red propuesta. En este diagrama se pueden observar todos los routers descritos anteriormente y la conexión correspondiente para cada uno de ellos.

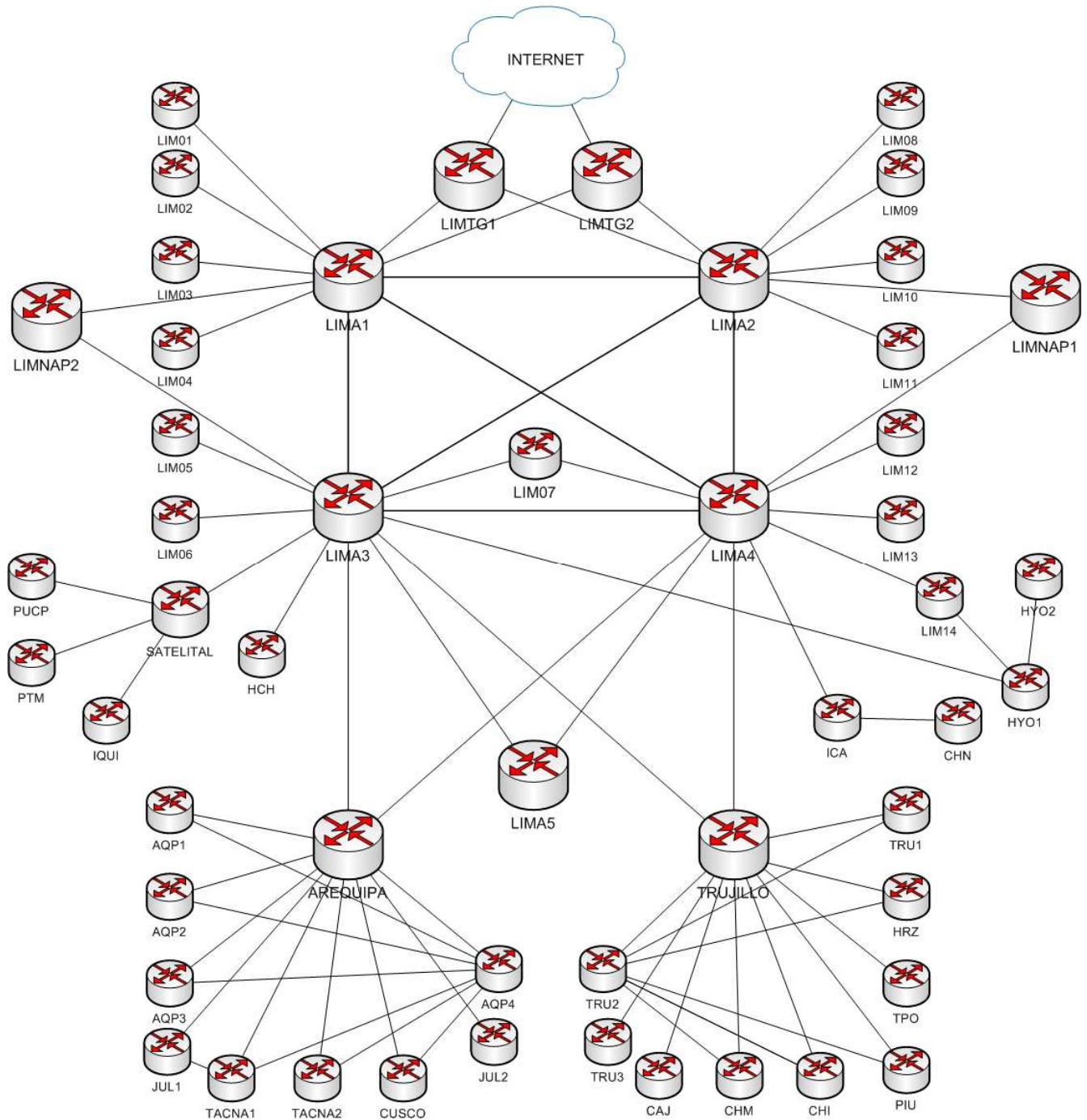


FIGURA 5-4: CORE MPLS FINAL

En la figura 5-5, se muestra la conexión del core con los equipos de los niveles restantes de la red NGN.

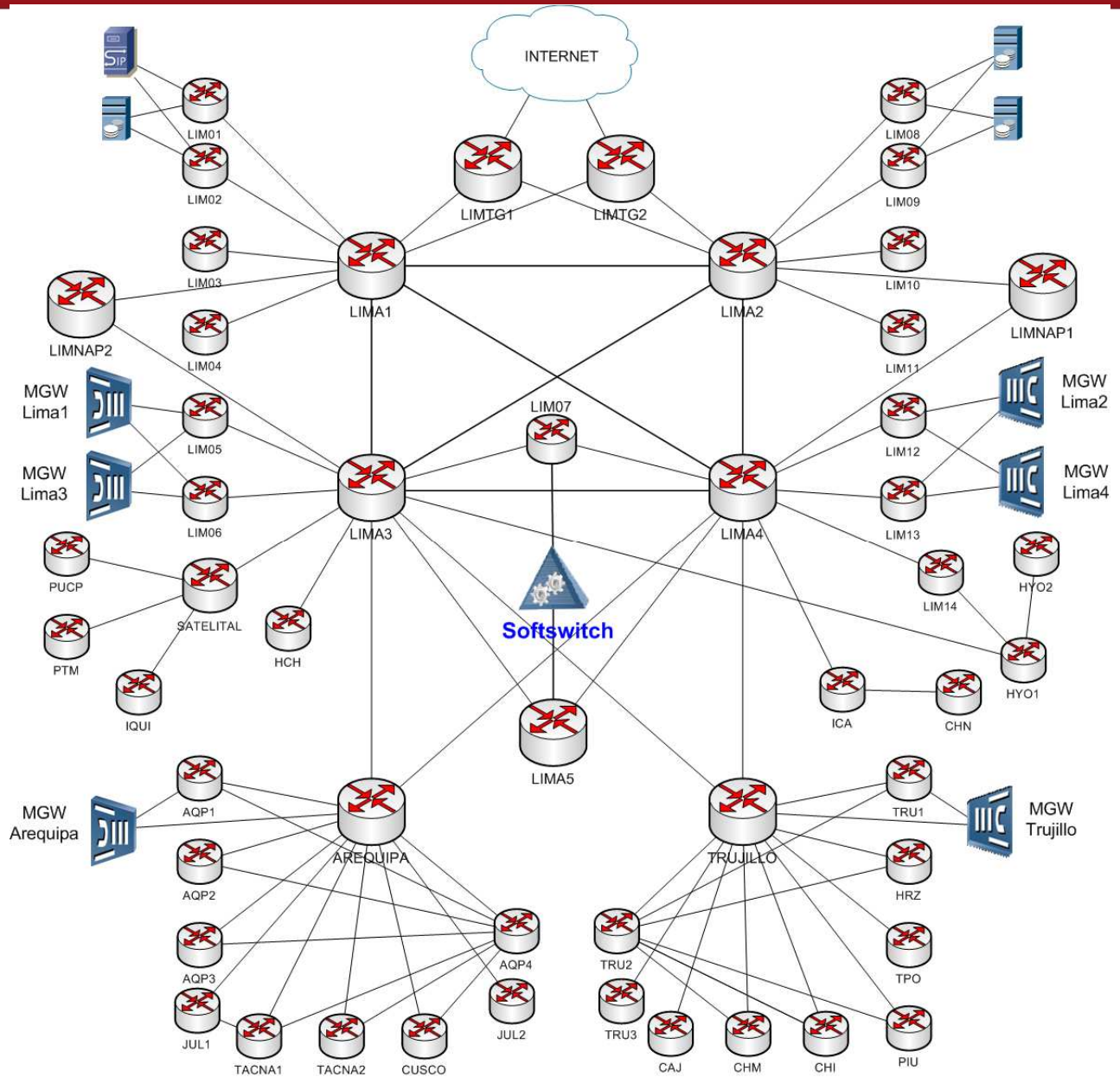


FIGURA 5-5: CORE NGN FINAL

5.2.2.2. Direccionamiento IP

Como se mencionó en la sección 5.2.1.9 (Direccionamiento IP), se emplearán tres rangos de direcciones IP privadas, una de clase A (10.0.0.0) y dos de clase B (172.10.0.0 y 172.20.0.0). El rango 10.0.0.0 será utilizado para en las interfaces de los diferentes routers de red. Por otro lado, los rangos 172.10.0.0 y 172.20.0.0 serán empleados en los servidores de red y en las interfaces *loopback* para la gestión de todos los equipos respectivamente.

Además, el rango 10.0.0.0 será dividido en tres rangos diferentes con el objetivo de direccionar las diferentes zonas Norte, Centro y Sur.

A continuación, en la tabla 5-5, se muestran los diferentes rangos empleados.

TABLA 5-5: DIRECCIONAMIENTO IP

UTILIZACIÓN	RED	MÁSCARA
Routers Zona Centro	10.10.0.0	255.255.0.0
Routers Zona Norte	10.20.0.0	255.255.0.0
Routers Zona Sur	10.30.0.0	255.255.0.0
Servidores	172.10.0.0	255.255.0.0
<i>Loopbacks</i> de Gestión	172.20.0.0	255.255.0.0

En la figura 5-6, se muestra el diagrama de red NGN donde se indica los rangos de direcciones IP a los que pertenece cada enlace.



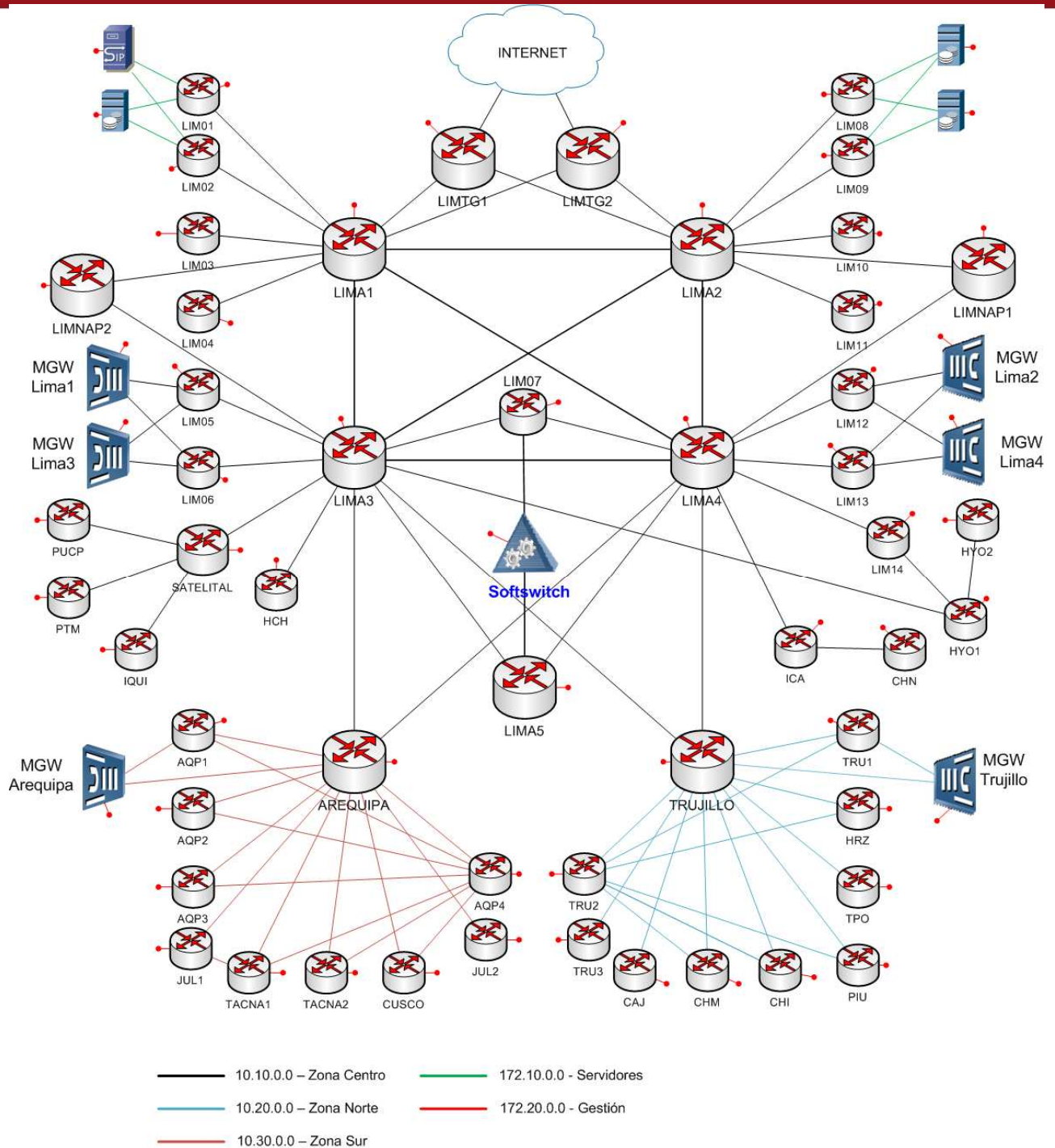


FIGURA 5-6: DIRECCIONAMIENTO IP

5.2.2.3. Protocolo de enrutamiento

En esta red, como se mencionó en la sección 5.2.1.3, se empleará el protocolo OSPF con tres áreas configuradas. Estas áreas serán las indicadas en la tabla 5-6 según la zona de distribución en el territorio peruano (Norte, Centro o Sur).

TABLA 5-6: ÁREAS OSPF

ÁREA	ZONA
Área 0	Centro
Área 1	Norte
Área 2	Sur

Según esta configuración, el diagrama de red sería el mostrado en la figura 5-7.

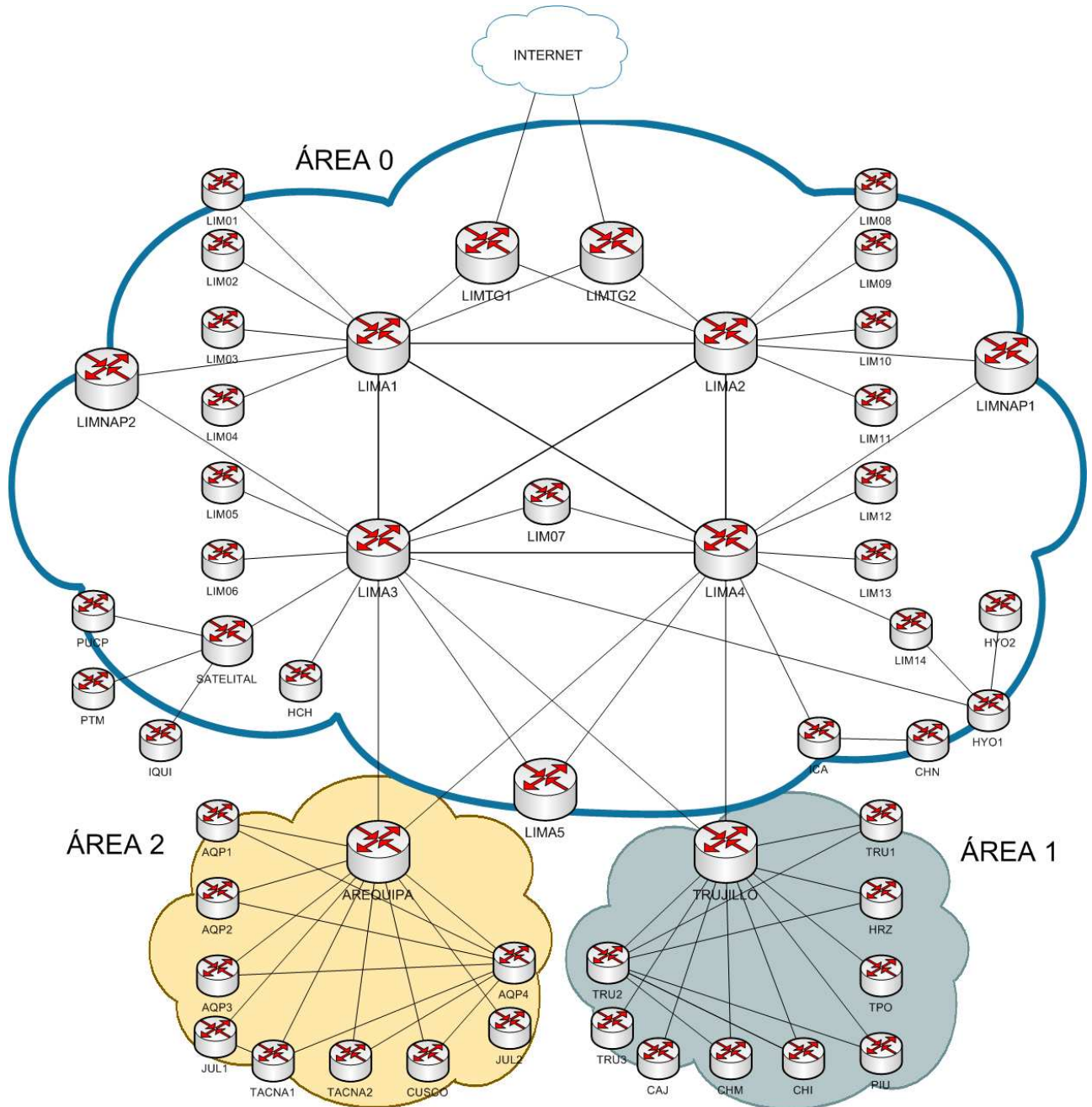


FIGURA 5-7: ÁREAS OSPF

5.2.2.4. Configuración de etiquetas

Debido a que los Edge LSR realizarán el marcado de paquetes según el FEC asignado a cada paquete IP, se debe realizar la configuración respectiva para estos routers de tal forma que puedan relacionar correctamente los flujos con un FEC adecuado. Como se mencionó en la sección 3.4.4.2 (Conceptos Previos), el FEC se asigna según las características del paquete IP. En esta propuesta, se tomarán en cuenta las características mostradas en la tabla 5-7.

TABLA 5-7: FEC

APLICACIÓN	FEC	IP RED ORIGEN	IP RED DESTINO
Tráfico Interno	A	10.0.0.0	10.0.0.0
Servicios Internos	B	--	172.10.0.0
Gestión	C	--	172.20.0.0

Como se puede observar, se definen tres FECs.

- El primero hace referencia a tráfico interno como señalización y tráfico de llamadas telefónicas.
- El segundo designa el FEC para el tráfico que tiene como destino los servidores internos de la red como servidores de *Billing*, Provisión y otras bases de datos.
- El tercer FEC se asigna a los flujos que tengan como objetivo la gestión de los equipos de red.

5.2.3. Plan de trabajo

En esta sección se detallan las etapas de migración así como los tiempos necesarios para esta.

5.2.3.1. Etapas de migración

Para la migración a MPLS se trabajará en cuatro etapas diferentes. En cada etapa se realizarán las configuraciones correspondientes siguiendo los aspectos técnicos descritos en las secciones 5.2.1 y 5.2.2 para las zonas Norte, Centro y Sur (ver tabla 5-8).

TABLA 5-8: DEFINICIÓN DE ETAPAS DE MIGRACIÓN

ETAPA	ZONA
1	Centro
2	Norte
3	Sur
4	Integración

En las tres primeras etapas, se designará un equipo de trabajo diferente para cada una de estas. Cada equipo estará liderado por un jefe de equipo los cuales se reunirán semanalmente para coordinar el avance de las etapas y solución de problemas comunes. Cada una de las tres primeras etapas se trabajará en paralelo y el objetivo principal será la formación de una red MPLS en cada zona donde los routers RC Lima 3, Lima 4, Trujillo y Arequipa también actuarán como *Edge LSR* (ver figura 5-8). Se trabajará de la siguiente manera:

- Para el caso en el que el tráfico tenga origen y destino en la misma zona, los paquetes se conmutarán según las etiquetas MPLS.
- Si el tráfico va de una zona a otra, el RC correspondiente se encargará de retirar cualquier etiqueta. En la zona destino, el paquete será transmitido según el protocolo de enrutamiento a nivel IP.

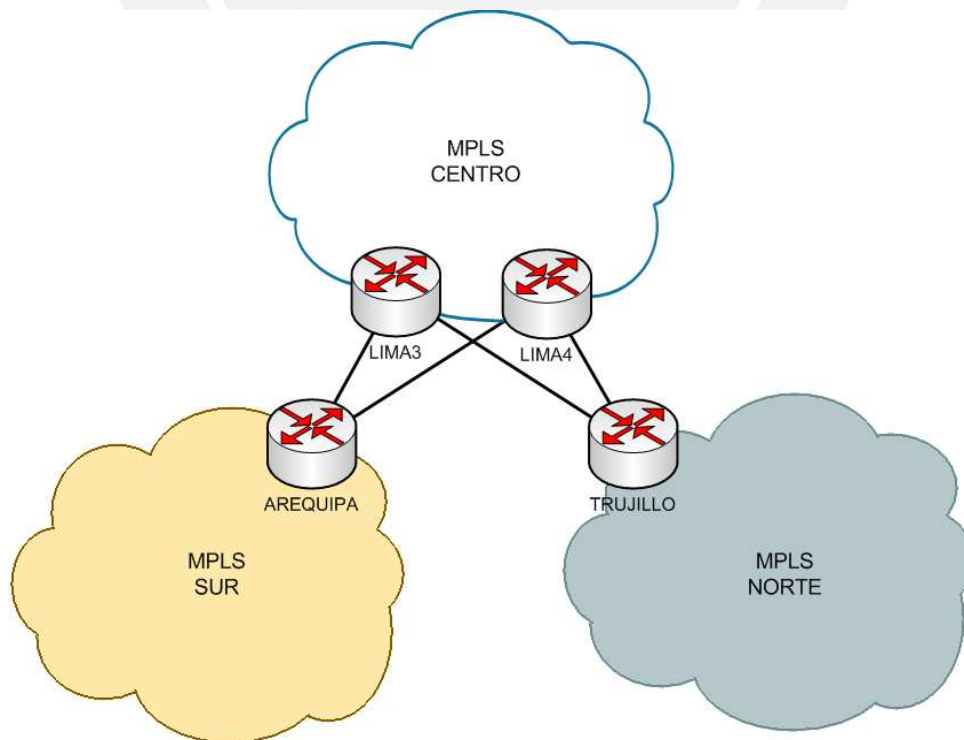


FIGURA 5-8: ETAPAS DE MIGRACIÓN

5.2.3.2. Desarrollo de las etapas

El desarrollo de cada una de las etapas, será realizado de la siguiente manera:

- Cuatro semanas de preparación del personal en capacitación técnica y definición de los objetivos de las diferentes etapas.
- Cuatro semanas de trabajo de investigación sobre las configuraciones necesarias en cada uno de los routers de la zona según el equipo de trabajo.
- Cuatro semanas dedicadas a la configuración de los equipos de cada zona. Estas configuraciones se realizarán en trabajos programados durante las madrugadas de los días de la semana en los que se presente la menor carga de tráfico en la red. Para el caso particular de la zona Centro, la tarea de configuración tomará en total seis semanas debido a que está formada por un mayor número de routers.
- Dos semanas para la coordinación entre los diferentes equipos de trabajo con el objetivo de definir los pasos a seguir para la integración final. En estas dos semanas, se corregirán posibles errores originados debido a las configuraciones realizadas.
- Dos semanas de trabajo para la integración final. En la primera semana se integrará la zona Centro con la zona Norte y, en la segunda, la zona Centro con la zona Sur.
- Por último, se realizarán verificaciones y continuarán haciendo pruebas respecto de las configuraciones realizadas por un periodo de cuatro semanas.

A continuación, en la figura 5-9, se puede observar el desarrollo de cada una de las etapas.

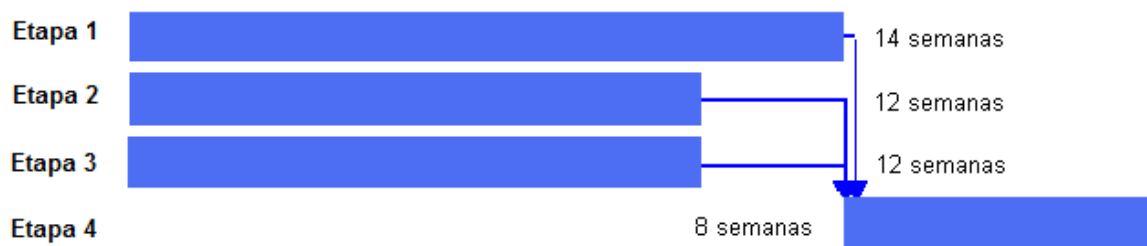


FIGURA 5-9: TIEMPOS ESTIMADOS

5.2.4. Propuesta Económica

En esta sección, se presenta una estimación del costo final para la propuesta de migración según los costos de *upgrades* y de personal.

5.2.4.1. Costo de *upgrades*

Debido a que, dentro de la propuesta de migración, se indica que los equipos sólo necesitan un *upgrade* de versión para soportar MPLS; se requiere calcular el costo para este proceso para cada uno de los 52 nodos de la red *core*.

A continuación, en la tabla 5-9, se muestra el detalle de costo de *upgrades* teniendo en cuenta un precio de *upgrade* por nodo de USD\$700.

TABLA 5-9: COSTO DE UPGRADES

ITEM	COSTO	NODOS	TOTAL (USD\$)
Nuevo Release	700	52	36400
COSTO DE UPGRADE			36400

5.2.4.2. Costo de personal

Además, se debe considerar el costo de personal el cual es calculado según el costo por hora-hombre y las semanas de trabajo mencionadas en la sección 5.2.3.2.

A continuación, en la tabla 5-10, se muestra el detalle de costo de personal, donde se toma en cuenta el precio de hora-hombre de USD\$55.

TABLA 5-10: COSTO DE PERSONAL

TAREA	SEMANAS	HORAS	PERSONAS	COSTO HORA-HOMBRE	TOTAL (USD\$)
Capacitación técnica y definición de objetivos	4	160	6	55	52800
Trabajo de investigación	4	160	6	55	52800
Configuración de equipos (zona centro)	6	240	2	55	26400
Configuración de equipos (zona norte)	4	160	2	55	17600
Configuración de equipos (zona sur)	4	160	2	55	17600
Coordinación entre equipos	2	80	6	55	26400
Integración final	2	80	3	55	13200
Verificación de migración	4	160	1	55	8800
COSTO DE PERSONAL					215600

5.2.4.3. Costo total

En la tabla 5-11, se obtiene el costo estimado de la propuesta de migración según los costos de *upgrades* y de personal.

TABLA 5-11: COSTO TOTAL

ITEM	COSTO (USD\$)
Upgrades	36400
Personal	215600
Total	252000

5.3. JUSTIFICACIÓN DE LA PROPUESTA

De los resultados obtenidos en la sección 4.3, se comprueba que MPLS es la arquitectura más idónea para ser implementada en el *core* de la red NGN ya que proporciona la QoS requerida por las diferentes aplicaciones que esta última transporta. Asimismo, se deben tomar en cuenta los protocolos de señalización empleados (como SIP, MGCP, SIGTRAN, entre otros) y protocolos utilizados para la gestión como SNMP.

Entre las diferentes ventajas que presenta MPLS para una red NGN, se tienen las siguientes [DIA2008B]:

- Velocidad: debido a que emplea conmutación por etiquetas, esta se hace de una manera más rápida en comparación con la conmutación realizada según la cabecera del protocolo IP.
- Escalabilidad: simplifica el proceso de señalización con respecto de otros protocolos de reserva de recursos.
- Gestión de QoS: la utilización de etiquetas, hace posible la definición de un túnel óptimo para cada aplicación según sus requerimientos.
- Seguridad: establecimiento de túneles.
- Migración: este protocolo es aplicable a cualquier protocolo de enrutamiento por lo que puede seguir siendo utilizado en caso de una futura migración a IPv6.

5.4. SERVICIOS A BRINDARSE

Como se ha indicado anteriormente, la red NGN tiene la capacidad de brindar diferentes tipos de servicios; por lo tanto, por esta, transitan diferentes tipos de aplicaciones. En el Perú, estas redes están siendo empleadas para servicios de voz, como telefonía, y datos, como acceso a Internet.

A continuación, se detallan los diferentes tipos de servicios que pueden ser implementados y brindados por estas redes [SEP2007] y [TEL2008].

5.4.1. Telefonía Local y LDN

Servicio de telefonía a nivel local ya sea mediante acceso tradicional o IP. En el primer caso se emplean MGWs para la conexión entre las centrales TDM y la red NGN. En el segundo, se emplean *gateways* residenciales en donde se conectan los teléfonos tradicionales o IP.

5.4.2. Telefonía LDI

Al igual que el servicio de Telefonía Local y LDN, el servicio de Telefonía LDI se realiza mediante acceso tradicional o IP. La diferencia del primero radica en que se emplean los routers o *gateways* que permiten la interconexión con algún *carrier* internacional para el transporte de las llamadas.

5.4.3. IP Centrex

Consiste en brindar funcionalidades de una PBX Virtual y telefonía entre las sucursales de una empresa utilizando un plan de numeración cerrado; es decir, mediante el marcado de anexos privados.

Con este, se pueden ofrecer diferentes servicios suplementarios como:

- Identificación de llamadas
- Conferencia tripartita
- Transferencia de llamadas
- Desvío de llamadas
- Rellamada
- Llamada en espera
- Agenda telefónica
- Casilla de voz
- Sala de conferencias

5.4.4. Primario IP

Este servicio permite la conectividad a la PSTN a través de la red NGN. Es usualmente utilizado por las empresas que poseen centrales telefónicas privadas ya que les ofrece 30 canales de voz. El acceso se realiza mediante enlaces PRI ISDN conectadas a las centrales telefónicas TDM o directamente a los MGWs.

5.4.5. Acceso Internet Residencial

Con las redes NGN, se pueden brindar acceso a Internet vía ADSL el cual es el más utilizado en el Perú. Por otro lado, también se pueden utilizar las conexiones *Dial-up*.

5.4.6. Acceso Internet Empresarial

Este tipo de servicio, a diferencia del Acceso Internet Residencial, requiere de enlaces dedicados para poder brindar mayor ancho de banda y seguridad.

5.4.7. Servicio de red privada de datos

Debido a que MPLS puede implementar redes privadas virtuales (VPN), este servicio se puede brindar de manera opcional en caso se decida realizar dicha implementación.



CAPÍTULO 6

CONCLUSIONES

Al culminar la presente Tesis, se puede concluir lo siguiente:

- Se realizó el estudio detallado de las redes NGN, sus componentes, los protocolos empleados y las normas de QoS (capítulos 2 y 3) verificándose que estas redes requieren de un *core* escalable y capaz de brindar QoS.
- Durante el desarrollo de la presente Tesis, se verificó que los actuales operadores peruanos de una red NGN poseen un *core* IP. Estas redes son empleadas para la provisión de diferentes servicios de voz y datos sin brindar la calidad de servicio adecuada.
- Como resultado de las pruebas de desempeño realizadas para la comparación entre las arquitecturas IP *Best Effort* y MPLS realizadas en el capítulo 4, se comprueba que la arquitectura capaz de brindar QoS a las redes NGN es MPLS.
- Se describió la red NGN con *core* IP que se propone migrar ubicándola en el escenario peruano, sección 5.1 (Escenario inicial de Migración).
- Se realizó la propuesta técnica de migración del *core* IP a MPLS de la red NGN descrita en el capítulo 5, sección 5.1 (Escenario inicial de Migración). En esta propuesta se detallaron los aspectos técnicos de la migración así como el plan propuesto para la migración y el tiempo necesario para cada etapa.

CAPÍTULO 7

RECOMENDACIONES Y TRABAJOS FUTUROS

7.1. RECOMENDACIONES

Después del estudio y las pruebas de desempeño realizados, se pueden dar las siguientes recomendaciones:

- Con respecto al protocolo a ser empleado en el *core* de una red NGN, es importante tomar en cuenta que MPLS es capaz de proporcionar la QoS necesaria por las diferentes aplicaciones que se brindan.
- Se recomienda verificar los tiempos necesarios por cada etapa de la migración propuesta de acuerdo al tamaño de la red y la cantidad de tráfico que se transporta.

7.2. TRABAJOS FUTUROS

- Estudio económico de la Propuesta de Migración: para que la propuesta de migración detallada en la presente Tesis pueda ser implementada por los actuales operadores NGN, se realizará el estudio económico de esta para verificar su rentabilidad.
- Evaluar el desempeño de la arquitectura MPLS LDP en el *core* de una red NGN.
- Actualización del paquete INET Framework para OMNeT++: durante el desarrollo de las pruebas de simulación se pudo verificar que este paquete presenta inestabilidad en algunos escenarios. Se hace necesario que esta herramienta soporte otros protocolos y tipos de tráfico para futuros estudios como la evaluación de DiffServ e IntServ así como los protocolos SCTP y SIGTRAN.
- Implementación de un taller para la enseñanza de OMNeT++: durante el desarrollo de las pruebas de simulación, se pudo confirmar que este simulador, a pesar de ser de código abierto, posee las herramientas suficientes para el estudio de los diferentes protocolos de red.

BIBLIOGRAFÍA

- [ASA2007] ASATANI, KOICHI. Presentación: "Next Generation Networks and QoS". International CQR Workshop, Japón. Mayo, 2007.
- [CIS2000] Cisco. Internetworking Technologies Handbook. Capítulo: "ISDN Overview". 2000.
- [CIS2006] Cisco. Documento: "E1 R2 Signaling Theory". Febrero, 2006.
URL: http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800943c2.shtml
Última fecha de consulta: Noviembre de 2008.
- [CHO2006] CHOI, TAESANG. Presentación: "Quality of Service in NGN". ITU-T Workshop on Next Generation Networks, Vietnam. Mayo, 2006.
- [ESC2007] Escuela Politécnica Nacional. "Convergencia hacia redes NGN". Quito, 2007.
- [DAR2008] DARROCH, JIM. "Introduction to SIGTRAN". Artesyn Communication Products, 2008.
- [DIA2007] DÍAZ ATAUCURI, DANIEL. Presentación: "MPLS". Redes de Banda Ancha, Pontificia Universidad Católica del Perú. Agosto, 2007.
- [DIA2008A] DÍAZ ATAUCURI, DANIEL. Presentación: "Internet de Servicios Integrados – IntServ". Redes de Banda Ancha, Pontificia Universidad Católica del Perú. Agosto, 2008.
- [DIA2008B] DÍAZ ATAUCURI, DANIEL. Presentación: "Multiprotocol Label Switching - MPLS". Redes de Banda Ancha, Pontificia Universidad Católica del Perú. Agosto, 2008.
- [DRY2004] DRYBURGH, LEE; HEWETT, JEFF. "Signaling System No. 7 (SS7/C7): Protocol, Architecture and Services. Cisco. Agosto, 2004.
- [GAL2008] GALLEGO, JOSÉ RAMÓN. Presentación: "QoS en Redes de Nueva Generación". Ingeniería Telemática, Universidad de Zaragoza. 2008.
- [GON2006] GONZALES SOTO, OSCAR. Presentación: "Concepto y Arquitectura de las redes NGN". Seminario regional sobre Costes y Tarifas para los países miembros del Grupo TAL, UIT. Río de Janeiro, Brasil. Mayo 2006.
- [GON2008] GONZALEZ, AGUSTÍN. Presentación: "Introducción a MPLS: Multi-Protocol Label Switching". Universidad de Maryland, Estados Unidos. 2008
- [GUP2007] GUPTA, LAV. Presentación: "Regulatory issues in Migraton to NGN". Telecom Regulatory Authority of India. Diciembre, 2007.
- [IMM2005] IMMONEN, MIA. Tesis de Maestría: "SIGTRAN: Signaling over IP – a step closer to an all-IP network". KTH Information and Communication Technology. Suecia, 2005.

- [ITU2004] ITU-T Recommendation Y.2001 "SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS". 2004.
- [ITU2005A] ITU-T, "NGN FG Proceedings Part I". 2005.
- [ITU2005B] ITU-T, "NGN FG Proceedings Part II". 2005.
- [ITU2005C] ITU-T, Definition of NGN
URL: <http://www.itu.int/ITU-T/ngn/definition.html>. 2005.
Última fecha de consulta: Octubre de 2008.
- [ITU2006A] ITU-T Recomendación Y.1541 "Network Performance Objectives for IP-based services, Series Y: Global Information Infrastructure, Internet protocol aspects and Next-Generation Networks", Febrero 2006.
- [ITU2006B] ITU-T Recomendación Y.1540 "IP packet transfer and availability performance parameters, Series Y: Global Information Infrastructure, Internet protocol aspects and Next-Generation Networks", Febrero 2006.
- [LIS2007] LI SALINA, JINGMING; SALINA, PASCAL. "Next Generation Networks Perspectives and Potentials". 2007.
- [LUH2005] LU, HUI-LAN. Presentación: "Quality of Service Standardization for Next Generation Networks". ITU-T NGN Technical Workshop, Korea. Marzo, 2005.
- [LUN2007] LUNA VICTORIA GARCÍA, IGOR. Trabajo de fin de carrera: "Medición y Tráfico en redes MPLS". Pontificia Universidad Católica del Perú, 2007.
- [MAR2002] MARTÍNEZ HELLÍN, AGUSTÍN; LÓPEZ ALMANSA, EUGENIO; RUEDA GARCÍA, JAVIER. "Arquitecturas de Redes de Nueva Generación: decisiones estratégicas". Alcatel, España. 2002.
- [NOR2007] Norwegian University of Science and Technology. Presentación: "NGN Architecture".
URL: www.item.ntnu.no/fag/ttm7/Lectures/6_2_NGN.ppt. 2007.
Última fecha de consulta: Octubre de 2008.
- [OEA2006] OEA. "Carpeta Técnica: Redes de Próxima generación". Comité Consultivo Permanente I: Normalización de Telecomunicaciones. 2006.
- [OSI2009] OSIPTEL. Sector Telecomunicaciones.
Estadísticas, Investigaciones y Publicaciones.
URL: www.osiptel.gob.pe
Última fecha de consulta: Octubre de 2009.
- [PER2003] Performance Technologies. "Tutorial on Signaling System 7 (SS7)". 2003.
- [QUI2007] QUINTANA CRUZ, DIEGO. Trabajo de fin de carrera: "Diseño e implementación de una red de telefonía IP con software libre en la RAAP". Pontificia Universidad Católica del Perú, 2007.

- [RFC3261] ROSENBERG J, SCHULZRINNE H. "SIP: Session Initiation Protocol". IETF, 2002. URL: <http://www.ietf.org/rfc/rfc3261.txt>
Última fecha de consulta: Abril de 2009.
- [RFC3372] VEMURI A, PETERSON J. "Session Initiation for Telephones (SIP-T): Context and Architectures". IETF, 2002. URL: <http://www.ietf.org/rfc/rfc3372.txt>
Consultado en Abril de 2009.
- [ROD2005] RODERA RODERA, SUSANA. Trabajo de fin de carrera: "Diseño e implementación de un Punto Neutro para VoIP". Universidad Politécnica de Catalunya. Setiembre, 2005.
- [REA2008] REAL MARTÍN, LUIS FERNANDO. Reportaje: "Desarrollo y Perspectiva desde ITU-T Arquitectura Funcional de NGN, Release 1". Antena de Telecomunicación. Marzo 2008.
- [RUS2006] RUSSELL, TRAVIS. "Signaling System #7". McGraw-Hill Professional Publishing. June, 2006
- [SEP2007] SEPÚLVEDA HERNAIZ, JUAN PABLO. Trabajo de fin de carrera: "Estudio sobre la Convergencia de redes y su factibilidad de implementación en Chile", Universidad Mayor. Agosto, 2007.
- [STA2001] STALLINGS, WILLIAM. Artículo: "MPLS", The Internet Protocol Journal. Setiembre, 2001.
- [STA2005] STAGNI, ALESSANDRO. Presentación: "Next Generation Networks and the end users expectations". Next Architecture – Next Generation Networks & Services – Italtel. Octubre, 2005.
- [STA2006] STASTNY, RICHARD. Presentación: "Next Generation Networks Evolution and Policy Considerations". ÖFEG, Budapest. Octubre 2006.
- [SUT2006] SUTHERLAND, KEVIN. Presentación: "Next Generation Networks (NGN) & the IP Multimedia Subsystem (IMS)". International Training Program, Gobierno de Australia. Setiembre 2006.
- [TEL2005A] Telefónica. Artículo: "Integración de infraestructuras Mediante NGN".
URL: http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_11.pdf. 2005.
Última fecha de consulta: Setiembre de 2008.
- [TEL2005B] Telefónica de España. Artículo: "La Próxima Generación de Redes, NGN, un trayecto hacia la convergencia"
URL: <http://sociedaddelainformacion.telefonica.es/jsp/articulos/detalle.jsp?elem=3188>. 2006.
Última fecha de consulta: Setiembre de 2008.

- [TEL2007] Telecommunication Engineering Centre. Technology White Paper: “NGN Architecture”. Ministerio de Comunicaciones y Tecnologías de Información, India.
URL: <http://www.tec.gov.in/technology%20updates/NGN%20Architecture.pdf>
Última fecha de consulta: Octubre de 2008.
- [TEL2008] Telefónica del Perú. Presentación: “NGN Conceptos y Aplicaciones”. Dirección Planificación e Ingeniería. Julio 2008.
- [TIL2007] TILAKARATNE. “Next Generation Network”. Independent Study. Department of Electronic & Telecommunication Engineering, University of Moratuwa. Sri Lanka, 2007.
URL: www.ent.mrt.ac.lk/~040388/Documents/Indipendent%20study040388.pdf
Última fecha de consulta: Noviembre de 2008.
- [VAN2005] VAN MEGGELEN, JIM; SMITH, JARED; MADSEN, LEIF. “Asterisk The future of Telephony”. O’Reilly Media, 2005.
- [VEL2008] VELARDE, EDGAR. Presentación: “Señalización”. Transmisión y Conmutación Digital, Pontificia Universidad Católica del Perú. Mayo, 2008.
- [VIL2008] VILCHEZ, LUIS. Artículo: “Redes NGN”. Blog TRIBYTE – Tecnología para el mundo. Octubre 2008.
URL: <http://tribyte.blogspot.com/2007/10/redes-ngn.html>
Última fecha de consulta: Noviembre de 2008.
- [VOI2009] VoIP Foro. “Ejemplo de llamada H.323”. Secciones Protocolos VoIP. 2009
URL: <http://www.voipforo.com/H323/H323ejemplo.php>
Última fecha de consulta: Mayo de 2009.
- [ZAM2005] ZAMORA, JOSÉ. Artículo: “NGN (Next Generation Networks): Mitos, realidades y posibilidades”. 2005.

ANEXOS

- Anexo 1: Instalación del simulador OMNET++ y el paquete INET Framework.
- Anexo 2: Archivos de configuración en OMNET++/INET Framework.
- Anexo 3: Archivos de simulación en OMNET++/INET Framework.

