



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Evolución de la telefonía a I3D en la parte de voz en el ámbito de
la Defensa*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Manuel Mena Hernández

DIRECTORES: Francisco Troncoso Pastoriza

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Evolución de la telefonía a I3D en la parte de voz en el ámbito de
la Defensa*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_deVigo

RESUMEN

La historia de la telefonía se inicia a finales del siglo XIX con la invención del teléfono por Alexander Graham Bell. Este sistema permitía la transmisión de la voz humana a través de cables de cobre con la ayuda de señales eléctricas continuas. En aquel entonces, las llamadas se conectaban manualmente por operadores. Además, presentaban limitaciones en calidad y capacidad de poder realizar múltiples llamadas simultáneas.

Con el transcurrir del tiempo, la tecnología fue avanzando lo que supuso una mejora en la eficiencia y calidad en las comunicaciones. Ya en el siglo pasado, la telefonía digital comenzó a reemplazar las conexiones analógicas, es decir, se inició la digitalización. De tal forma que, las señales de voz comenzaron a digitalizarse comprimiéndose y transmitiéndose en forma de bits. Se logró mejorar la calidad del sonido y la optimización en el uso de las líneas telefónicas. De hecho, las centrales telefónicas pasaron a ser digitales y fueron capaces de gestionar, de manera más eficiente las llamadas.

Sin embargo, esto no era el techo para esta tecnología. Llegó Internet y la telefonía se volvió a reinventar. Apareció VoIP (Voice over IP) permitiendo llamadas telefónicas a través de redes de datos usando el protocolo de internet IP. Este avance permitió la reducción de coste en las llamadas, integración de otros servicios digitales como las videollamadas y la mensajería instantánea entre otros.

En este momento, ya existen dos tipos de telefonía; fija y móvil. Ambas están conviviendo con una evolución distinta. Mientras que la telefonía fija ha experimentado la adaptación de nuevos servicios, la móvil, además de lo anterior, ha ido evolucionando desde el 1G hasta el actual 5G.

Este Trabajo Fin de Máster se centrará en la evolución de la telefonía en las Fuerzas Armadas durante estos últimos años hacia la I3D, qué software, hardware, protocolos, etc., intervienen, cómo se producen las llamadas entre los nodos, ya sean permanentes o desplegables, qué implica evolucionar hacia la virtualización y cómo se relacionan las distintas tecnologías entre sí.

PALABRAS CLAVE

Voz sobre IP, nodo permanente, nodo desplegable, telefonía analógica, telefonía digital, comunicaciones unificadas.

AGRADECIMIENTOS

A mi familia.

CONTENIDO

Contenido	1
Índice de Figuras	5
Índice de Tablas.....	7
1 Introducción y objetivos	9
1.1 Motivación del Trabajo de Fin de Máster	9
1.2 Objetivos del TFM	10
1.3 Estructura del TFM	10
2 Estado del arte	12
2.1 Historia VoIP	12
2.2 Tecnologías fundamentales para la telefonía/categorización de la telefonía	12
2.2.1 Telefonía analógica, digital e IP	12
2.2.2 Telefonía fija.....	14
2.2.3 Telefonía móvil.....	15
2.3 Paso de la voz a Internet	15
2.4 Fundamentos físicos para transmitir	15
2.4.1 Muestreo	16
2.4.2 Cuantificación.....	16
2.4.3 Codificación y compresión	16
2.4.4 Codificador-decodificador	17
2.4.5 Tipo de conexión	17
2.4.6 Procesamiento de una llamada.....	18
2.4.7 Transporte de voz sobre paquetes	19
2.5 Dominios.....	19
2.6 Protocolos de comunicación	19
2.6.1 Protocolo IP	20
2.6.2 Protocolos de encaminamiento	23
2.6.3 Protocolos de control	24
2.6.4 Protocolo RTP	25
2.6.5 Protocolo de transporte en VoIP	25
2.6.6 Protocolos de aplicación en VoIP	26
2.6.7 Protocolo de señalización	26
2.6.8 Protocolo de seguridad	30
2.6.9 Protocolo de gestión en telefonía.....	32
2.6.10 Calidad de la voz	33

2.6.11 Técnicas de evaluación de la calidad de la voz	37
2.6.12 Calidad de servicio de una red	38
2.7 Tráfico de red	39
2.7.1 Marcado y clasificación del tráfico de red	39
2.7.2 Técnicas LST	40
2.7.3 Control de congestión	41
2.7.4 Gestión de ancho de banda	43
2.7.5 Prevención de la congestión	45
2.7.6 Adaptación del tráfico y funciones de policía	46
2.7.7 Control de admisión	47
2.8 Infraestructura de comunicaciones	47
2.8.1 Backbones telefónicos tradicionales vs IP	47
2.8.2 Redes corporativas de voz	49
2.8.3 Centros RCT	49
2.8.4 Centros ATM	50
2.8.5 Estándar E1	52
2.8.6 Centrales I3D	52
2.8.7 MXONE	53
2.8.8 Gateway	53
2.8.9 Media Gateway	54
2.8.10 NGN	55
2.8.11 Call Manager	55
2.8.12 Teléfonos software o softphone	56
2.8.13 PBX	56
2.8.1 PSTN	57
2.8.2 SBC	58
2.9 Mecanismos de seguridad	58
2.9.1 Intrusion Detection Systems (IDS)	58
2.9.2 Intrusion Prevention Systems (IPS)	58
2.9.3 Firewall	59
3 Desarrollo del TFM	60
3.1 Situación actual	60
3.2 Arquitecturas	62
3.2.1 Arquitectura de telecomunicaciones de un nodo permanente de la I3D	62
3.2.2. Arquitectura de telecomunicaciones de un nodo desplegable de la I3D	68
3.2.3. Arquitectura servidor MXONE virtualizado	75

3.3 Implantación de los nodos permanentes en la I3D	76
3.3.1 Proceso de implantación en la I3D	76
3.3.2 Planificación y documentación previa	76
3.3.3 Instalación física y configuración inicial	77
3.3.4 Configuración avanzada	78
3.3.5 Plan de verificación y pruebas detallado.	78
3.3.6 Documentación de resultados.	82
3.3.7 Aprobación y despliegue.	82
3.3.8 Seguimiento del sistema una vez implementado.	82
3.3.9 Capacitación del personal.	83
3.3.10 Seguridad física.	83
3.3.11 Cumplimiento legal.	83
3.3.12 Plan de contingencia.	84
3.4 Despliegue de nodos desplegables	84
3.5 Procedimiento de llamadas	85
3.5.1 Procedimiento de llamada del nodo permanente de la I3D	85
3.5.1 Procedimiento de llamada del nodo desplegable de la I3D	89
4 Resultados	92
4.1 Proceso para la implementación de la I3D.....	92
4.2 Ejemplo análisis de costes implementación nodo permanente, nodo MXONE virtualizado y sin virtualizar	92
4.2.1 Costes asociados a la instalación del nodo permanente.....	93
4.2.2 Costes asociados para el servidor MXONE, SBC, firewalls y NGN virtualizados.....	94
4.2.3 Costes asociados para el servidor MXONE, SBC, firewalls y NGN sin virtualizar	96
4.2.4 Comparativa costes instalación nodo virtualizado vs nodo no virtualizado	98
4.3 Ejemplo análisis consumos energéticos y huella de carbono nodo MXONE virtualizado y sin virtualizar	98
4.3.1 Consumos energéticos nodo MXONE virtualizado y sin virtualizar	98
4.3.2 Cálculo de la huella de carbono nodo MXONE virtualizado y sin virtualizar	100
4.4 Implicaciones de la I3D	101
4.5 Retos futuros	102
5 Conclusiones y líneas futuras	105
6 Bibliografía.....	107
Anexo I: Subnetting.....	110
Anexo II: Ejemplo creación subredes	111
Anexo III: Ejemplo división red principal en subredes.....	113

Anexo IV: Streaming; cómo ve el usuario el contenido multimedia	114
Anexo V: Secuencia en un establecimiento de llamada	115
Anexo VI: Funciones que realizan xml, cgi, tcl, c++	116
Anexo VII: Comunicación MGC y MG	117
Anexo VIII: Llamada telefonía tradicional red ip	119
Anexo IX: Comparación señal original y degradada	120
Anexo X: Ejemplo tráfico voz IP, video y datos.....	121
Anexo XI: Ejemplo distribución ancho de banda en función del peso	122
Anexo XII: Mecanismo control de flujo redes ip a nivel transporte	123
Anexo XIII: Funcionamiento WRED en caso de congestión.....	124
Anexo XIV: Cómo implementar ECN en el campo ToS	125

ÍNDICE DE FIGURAS

Figura 2-1 Modelo red VoIP (Fuente: Libro infraestructuras de redes de datos y sistemas de telefonía) [7].....	30
Figura 2-2 Calidad de la voz (imagen propia).....	35
Figura 2-3 Fuentes de ruido (Fuente: Libro infraestructuras de redes de datos y sistemas de telefonía) [7].....	37
Figura 2-4 Elementos 5620 NM (Fuente: [20]).....	50
Figura 2-5 Operator position (Fuente:[20])position (Fuente: [20]).....	51
Figura 2-6 Media Gateway Unit, MGU2 (Fuente: [23])	54
Figura 2-7 Gateway en la red IP (Fuente: [24])	54
Figura 2-8 Central PBX (Fuente: [25])	57
Figura 2-9 PSTN (Fuente: [26])	57
Figura 3-1 Red de telefonía (imagen propia)	61
Figura 3-2 Red ATM e I3D (imagen propia)	61
Figura 3-3 Fuente: mitel teléfono serie 6900 [29].....	63
Figura 3-4 Nodo permanente (imagen propia)	64
Figura 3-5 Firewall (Fuente: Tonitrus [30])	69
Figura 3-6 Switch (Fuente: instaladores de telecom hoy [31])	69
Figura 3-7 Teléfono GXP1610 GRANDSTREAM (Fuente: grandstream[32])	69
Figura 3-8 Nodo desplegable con call manager (imagen propia).....	70
Figura 3-9 Nodo desplegable sin call manager (imagen propia).....	74
Figura 3-10 Distribución equipos de la MXONE (imagen propia).....	76
Figura 3-11 Alta número de teléfono 1 (imagen propia).....	77
Figura 3-12 Alta número de teléfono 2 (imagen propia).....	77
Figura 3-13 Diagrama de plazos proyecto 1 (imagen propia).....	80
Figura 3-14 Diagrama de plazos proyecto 2 (imagen propia).....	81
Figura 3-15 Diagrama de plazos proyecto 3 (imagen propia).....	81
Figura 3-16 Diagrama de plazos proyecto 4 (imagen propia).....	81
Figura 3-17 Diagrama de Gantt 5 (imagen propia)	84
Figura 3-18 Arquitectura nodo desplegable (imagen propia).....	85
Figura 3-19 Llamada desde teléfono en nodo permanente (imagen propia)	86
Figura 3-20 Llamada desde teléfono en nodo permanente a red ATM (imagen propia)	87
Figura 3-21 Llamada desde teléfono en nodo permanente a red pública (imagen propia)	88
Figura 3-22 Llamada desde teléfono en nodo desplegable a otro en nodo permanente (imagen propia).....	89

Figura 3-23 Llamada desde teléfono en nodo desplegable a otro en red ATM (imagen propia).....	90
Figura 3-24 Llamada desde teléfono en nodo desplegable a otro en red pública (imagen propia)..	91
Figura A1-1 Dirección IP y máscara de subred.....	110
Figura A1-2 Nueva máscara de subred	110
Figura A1-3 Subredes resultantes.....	110
Figura A2-1 Subredes A y B	111
Figura A2-1 Subredes C y D	112
Figura A7-1 Comando AuditEndpoint	117
Figura A7-2 Comando EndpointConfiguration.....	117
Figura A7-3 Comando ModifyConnection	117
Figura A7-4 Comando DeleteConnection	118
Figura A7-5 Comando CreateConnection	118

ÍNDICE DE TABLAS

Tabla 2-1 Valores MTU en función de la red.....	21
Tabla 2-2 Protocolos de encaminados y encaminamiento	23
Tabla 2-3 Protocolos	28
Tabla 2-4 Estándares	37
Tabla 2-5 Clasificación del tráfico de red en función del nivel.	39
Tabla 3-1 Equipos nodo permanente	64
Tabla 3-2 Inventarios equipos de red nodo permanente.....	64
Tabla 3-3 VLAN asignadas	65
Tabla 3-4 Relación switches nodo permanente	66
Tabla 3-5 Relación de switches y VLAN asignados	66
Tabla 3-6 Designación de puertos del switch de core	67
Tabla 3-7 Designación de puertos del switch de acceso 01	67
Tabla 3-8 Designación de puertos el Media Gateway	68
Tabla 3-9 Designación de puertos de los switches de acceso 02, 03 y 04	68
Tabla 3-10 Designación de puertos de los switches de acceso 05, 06 y 07	68
Tabla 3-11 Relación de equipos con sus direcciones IP y VLAN	71
Tabla 3-12 Relación de VLAN con sus direcciones IP y observaciones	71
Tabla 3-13 Designación de puertos del switch de core	72
Tabla 3-14 Designación de puertos de los switches de acceso 01, 02 y 03	72
Tabla 3-15 Designación de puertos del call manager.....	73
Tabla 3-16 Códec	73
Tabla 3-17 Modelo de teléfono con asignación de extensión telefónica y DDI	73
Tabla 3-18 Inventario equipamiento de red en nodo desplegable	74
Tabla 3-19 Relación de VLAN con sus direcciones IP y observaciones	75
Tabla 3-20 Destinatarios a los que puede llamar teléfonos I3D.....	80
Tabla 4-1 Precio adquisición, instalación y mano de obra nodo permanente	93
Tabla 4-2 Inventarios equipos de red nodo permanente.....	94
Tabla 4-3 Precio adquisición, instalación y mano de obra nodo virtualizado.....	95
Tabla 4-4 Coste mantenimiento nodo virtualizado durante un periodo de 10 años	96
Tabla 4-5 Precio adquisición, instalación y mano de obra nodo no virtualizado.....	97
Tabla 4-6 Coste mantenimiento nodo no virtualizado durante un periodo de 10 años	97
Tabla 4-7 Consumo de energía en un año sin virtualización.....	99
Tabla 4-8 Consumo de energía en un año con virtualización	99

Tabla 4-9 Variación de consumo de energía en un año virtualización/sin virtualización.....100

Tabla 4-10 Variación de la emisión de CO₂ en un año virtualización/sin virtualización 100

Tabla 0-1 Anexo II ejemplo de creación de subredes 111

Tabla 0-1 Anexo III ejemplo división red principal en subredes 113

Tabla 0-1 Anexo XIV implementar ECN en el campo ToS.....125

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación del Trabajo de Fin de Máster

A finales del s. XIX apareció un gran invento denominado teléfono. Éste logró la comunicación entre dos usuarios a distancia. Una vez que fue mostrado al mundo logró aumentar en gran medida su demanda. Para satisfacer esta necesidad se tuvieron que crear redes que, con el paso del tiempo, llegaron a ser la infraestructura RCT¹. Esta red permite hacer llamadas por conmutación de circuitos.

Con el paso del tiempo, la telefonía se convirtió en un medio para las actividades comerciales y personales que supuso un cambio en la forma de interactuar de los ciudadanos, formando la base de las telecomunicaciones que conocemos en la actualidad.

Desafortunadamente para RCT, ha sido sustituida gracias a los avances tecnológicos que ofrece VoIP. No solo porque sus costes disminuyen respecto al primero sino también porque tanto la voz como los datos pueden conectarse a la misma red de ordenadores, teléfonos móviles, tabletas, teléfonos IP., con una reducción de costes de mantenimiento y mayor flexibilidad.

En la actualidad, las empresas, ya sean grandes o pequeñas, utilizan sus propias redes que son privadas y se pueden conectar mediante una red denominada MPLS² con la ayuda de firewalls, estas redes pueden proteger sus redes y teléfonos que se conectan internamente a switches que permiten su conexión al interior y exterior de su organización. Esta tecnología ofrece comunicación encriptada y protegida, con baja latencia y es capaz de priorizar el tráfico tanto para voz como para datos.

Los inconvenientes que presentan este tipo de tecnología son los costes, es decir, es más caro que otros métodos de conexión como VPNs³ sobre Internet. De hecho, MPLS es un servicio gestionado por los proveedores con las tarifas adicionales por la gestión y el mantenimiento de la red. Aquellas organizaciones que tengan la intención de combinar diferentes tecnologías como son 4G/5G con MPLS pueden tener dificultades dado que tratan de manera distinta el envío de la información. Otro inconveniente es la complejidad de utilizar los firewalls con las redes MPLS. De hecho, se tienen que configurar adecuadamente con reglas dado que, de no hacerse así, podrían causar vulnerabilidades de seguridad.

Este Trabajo de Fin de Máster busca mostrar, a nivel de las Fuerzas Armadas, en qué situación tecnológica nos encontramos actualmente, y qué elementos hardware, software, protocolos, etc., nos

¹ RCT: Red de Telefonía Conmutada.

² MPLS: *Multiprotocol Label Switching*

³ VPN: *Virtual Private Network*

permiten la comunicación entre las distintas unidades que se encuentran tanto en España como en Zona de Operaciones.

En definitiva, lo que se trata es mostrar cómo se encaminan las llamadas, qué elementos ayudan a que se puedan realizar, cómo se está evolucionando hacia la I3D⁴ en telefonía y qué futuro se puede presentar.

1.2 Objetivos del TFM

En la actualidad, la tecnología, y en concreto la telefonía, ha crecido tanto que no sólo permite mantener una conversión telefónica sino también utilizar una serie de aplicaciones en nuestros dispositivos móviles que nos ayudan a cumplir las tareas que tenemos encomendadas o por simple ocio.

El objetivo principal de este trabajo es mostrar la situación de la telefonía en las Fuerzas Armadas y cómo se relacionan el mundo de las redes ATM⁵ con la I3D, las nuevas arquitecturas que se están implementando, denominadas nodos permanentes y desplegables, cómo transitan las llamadas entre las redes ATM y la nueva I3D y el futuro que se vislumbra. Otro aspecto para reseñar es cómo se dan los pasos a seguir para una correcta implementación de la I3D en las unidades, reemplazando las centralitas que pertenecen a la red de ATM.

Para ello, se tendrán en cuenta los siguientes puntos:

- Situación actual de la telefonía en las fuerzas armadas.
- Exposición de las telefonías analógicas, digitales e IP⁶, fija y móvil.
- Explicación de los fundamentos físicos que permiten las conversiones analógico-digitales, codificación y compresión, tipos de conexiones, procesamiento de llamadas, etc.
- Explicación sobre los protocolos que permiten la comunicación entre redes de distinta naturaleza, tipos de tráfico de red, cómo gestionar los anchos de banda, el control de congestión, adaptación del tráfico, etc.
- Mostrar qué elementos participan en las llamadas telefónicas, así como se dan éstas en diversos casos, partiendo de usuario que se encuentra en la I3D.
- En telefonía, qué pruebas se realizan para la implantación de la I3D tanto en nodos permanentes como en desplegables.
- Se mostrará un análisis de la implantación de la I3D.
- Se explicará, desde el punto de vista actual, cómo puede ser el futuro de la telefonía.

1.3 Estructura del TFM

La estructura se establece en estos capítulos:

En el capítulo 1 se muestra la motivación de este trabajo y los objetivos a alcanzar.

En el capítulo 2 se hace una pequeña introducción en la historia de VoIP⁷. Según se va avanzando en el capítulo se muestra qué tipos de telefonía han ido introduciéndose conforme mejoraba la tecnología. Además, qué tecnologías han sido necesarias implementar para garantizar las comunicaciones entre distintas tecnologías junto con los protocolos que los acompañan. Se muestra también los equipos físicos involucrados e instalados que ayudan al encaminamiento de las llamadas y los mecanismos de seguridad que eviten ataques no deseados.

⁴ I3D: Infraestructura Integral de Información de la Defensa

⁵ ATM: *Asynchronous Transfer Mode*

⁶ IP: *Internet Protocol*

⁷ VoIP: Voz sobre IP

El capítulo 3 se puede dividir en seis partes: inicialmente, se da una visión de la situación actual; a continuación, se muestran las arquitecturas en I3D, nodos desplegados y permanentes; en la tercera parte, se enseña el proceso de implantación en la I3D; seguidamente, se presenta un despliegue de nodos desplegados; en la quinta parte, se indica cómo se encaminan las llamadas y, cómo se trabaja para conectar los teléfonos de estos nodos con la MXONE y que logren conectarse a la red; finalmente, se indican los retos futuros.

En el capítulo 4 se pueden ver los resultados a los que han sido sometidos los sistemas para garantizar su correcto funcionamiento, tanto para nodos permanentes como desplegados. Además, todo esto supone un proceso de ingeniería sin el que no sería posible llegar a buen fin. Ciertamente, que el objetivo es cumplir con el 100% de los requisitos fijados, pero conforme se van realizando las instalaciones se puede observar aquellos puntos débiles que deberán mejorarse en posteriores acuerdos.

Finalmente, en el capítulo 5 se presentan las conclusiones obtenidas y las acciones que se desean realizar en la I3D en un futuro.

2 ESTADO DEL ARTE

2.1 Historia VoIP

En 1995, un grupo de jóvenes de origen israelí crearon VoIP. Hasta aquel momento la comunicación era entre ordenadores. La empresa *Vocaltec, Inc.*, lanzó un producto denominado *softphone*⁸ que disponía de una tarjeta de audio, micrófono y modem. El funcionamiento de este software consistía en comprimir la señal de voz, a través de paquetes de voz que eran enviados por Internet. Inicialmente, fue un fracaso debido a que obligaba a los dos ordenadores a tener el mismo software y hardware.

En 1997, *Jeff Pulver*, unifica a usuarios, fabricantes involucrados en la tecnología VON⁹ en la feria anual sobre VoIP. En 1998, se comenzaron a fabricar los primeros adaptadores telefónicos (ATA) y *Gateway* que permitieron la comunicación entre un teléfono y un PC.

En 1999, *CISCO* empezó a poner en venta las primeras unidades para VoIP, con los protocolos de señalización H.323.

En 2000, el estudiante *Mark Spencer* de la *Universidad de Auburn* crea *Asterik* que es la primera central telefónica basada en Linux con un código fuente abierto. Permite una solución freeware para empresas y soluciones IP-PBX¹⁰.

En 2002 surge el protocolo de señalización SIP (*Session Initiation Protocol*) que comenzó a desplazar a H.323.

En 2003 dos universitarios, *Jan Friis* y *Niklas Zennstrom*, crearon *softphone* fácilmente instalable en cualquier PC que atravesaba todos los firewalls y routers incluso los corporativos. Este producto es *Skype*, que en 2005 llegó a contar con 50 millones de usuarios [1].

2.2 Tecnologías fundamentales para la telefonía/categorización de la telefonía

2.2.1 Telefonía analógica, digital e IP

Se puede afirmar que se pueden hacer llamadas telefónicas con tres tipos de tecnologías diferentes; telefonía analógica, digital y voz IP.

⁸ Softphone: *Internet Phone Software*

⁹ VON: *Voice On the Net*

¹⁰ IP-PBX: *Internet Protocol Private Branch Exchange*

2.2.1.1 Telefonía analógica

La centralita analógica, conocida como clásica o tradicional, está basada en tecnología analógica, es decir, las llamadas son conmutadas y redirigidas mediante la propia electrónica de la centralita. Los teléfonos están conectados a un par de hilos (RJ9) [2] y se usará líneas de telefonía básica RTB para conectarse al exterior.

La voz y los datos se transmiten por las señales analógicas con la limitación de su ancho de banda. El micrófono, que lleva el teléfono en su interior, convierte las ondas sonoras en eléctricas que finalmente viajan por el cableado de cobre. La señal generada se representa de forma continua cuyos parámetros como son la amplitud y frecuencia dependerá de la persona que los genere. Toda llamada podrá verse afectada por la distancia entre los interlocutores, las interferencias, la degradación de la señal y el ruido de la línea. Es decir, a mayor distancia mayor atenuación. La tecnología PSTN¹¹ o conmutación de circuitos se caracteriza por tener una conexión física dedicada entre los dos usuarios y estará activa hasta la finalización de la llamada. Estas llamadas podrán pasar por diferentes centrales ATM. Cuando la señal alcance al teléfono del receptor, el altavoz convertirá la señal eléctrica en sonora. Esta tecnología ofrece, como funciones básicas, la llamada en espera, transferencias de llamadas e identificación de llamadas.

Aunque esta tecnología está siendo reemplazada se sigue utilizando en zonas remotas o en lugares donde las tecnologías IP no han llegado.

2.2.1.2 Telefonía digital

Se le puede considerar una evolución de la telefonía tradicional o analógica. De tal forma que se pueden utilizar las líneas tradicionales como ISDN o PSTN usando la modulación digital para convertir las señales de voz en formato digital usando las líneas conmutadas citadas anteriormente. Gracias a la modulación por impulsos codificados o PCM¹² se puede convertir la señal de la voz en formato digital. El hecho de que las llamadas sean dedicadas implica que no les influya el tráfico de datos de la red y que la calidad de la voz no se vea afectada. Sin embargo, debido a que las llamadas son dedicadas implica que los costes aumenten. De hecho, si las comunicaciones son a larga distancia, aumentará su coste debido a que dependen de diferentes compañías telefónicas. Además, puede utilizar conmutación de circuitos o conmutación de paquetes (en redes digitales).

En el caso de ser necesario aumentar el número de líneas se tendrá que adquirir hardware adicional con los costes económicos que supone. Por tanto, existe un problema de limitación de número de canales disponibles.

Estas líneas forman parte de la RDSI o ISDN¹³ que ofrece servicios. De tal manera que, la voz y los datos pueden viajar simultáneamente con una capacidad de 128kbps (subida y bajada) y dos canales de voz de 64kbps. Además, cada canal dispone de una numeración DDI¹⁴ para llamar y recibir llamadas. Es decir, es una funcionalidad que permite a los usuarios tener un número de teléfono público y directo sin pasar por una centralita.

Las centralitas se les puede comparar con los servidores (ordenadores) que puede admitir diversos tipos de líneas de entrada (RDSI, RTB) incluso enlaces móviles GSM¹⁵, fax, módem, etc. Siendo ampliables en caso necesario y los teléfonos se conectarán por cable RJ11 o RJ45. Además, si se quiere establecer una comunicación entre un teléfono que se encuentra en la red tradicional con otro que esté en la red de telefonía digital, se requiere de adaptadores para convertir la señal analógica en digital.

¹¹ PSTN: Red Telefónica Conmutada Pública, *Public Switched Telephone Network*

¹² PCM: *Pulse Code Modulation*

¹³ ISDN: Red Digital de Servicios Integrados

¹⁴ DDI: *Direct Dial In*

¹⁵ GSM: *Global System for Mobile Communications*

2.2.1.3 Telefonía IP

La telefonía IP, a diferencia de las dos anteriores, utiliza las redes de datos para transmitir las llamadas en paquetes IP que circulan en la red sin que existan líneas dedicadas entre el origen y el destino. Esto último, implica costes más bajos e integrar otros servicios con el inconveniente de que la calidad de la voz dependa de las condiciones en las que se encuentre la red, de los equipos que se instalen y del operador que se contrate. Además, su infraestructura no depende de las dos tecnologías anteriores, pero se sirve de ellas, como son infraestructuras para funcionar. Es decir, en este caso no existen líneas físicas dedicadas para mantener la conversión, sino que son las conexiones de datos (fibra óptica, ADSL, LAN...) que nos permiten realizar este tipo de llamadas. Por lo que no existe limitación en el número de llamadas simultáneas. Además, los números de teléfonos se alojan en la nube de nuestro operador de telecomunicaciones. Podemos usar tantos números como queramos contratar y del lugar geográfico que queramos. Por lo que se pueden crear redes de organizaciones, aunque estén ubicadas lejos físicamente.

Actualmente, se ofrecen centrales IP, como MXONE, que se asemejan a las centralitas digitales que agrupan las líneas de teléfonos, aunque estén ubicados físicamente alejados, en una única central. Cada una de estas ubicaciones dispondrán de switches, donde se conectarán los teléfonos, y dependerán de la central IP (MXONE). Para este caso, ya no será necesario realizar nuevos cableados, sino que se utilizará por las redes de IP compartiéndolo con los ordenadores. El teléfono se podrá conectar en cualquier puerto de la red manteniendo su numeración.

No importa donde se encuentren los usuarios mientras tengan conexión a Internet para utilizar los servicios de video llamadas, mensajería instantánea, etc. Además, es posible establecer comunicaciones telefónicas entre redes distintas, es decir, una llamada puede iniciarse en una red IP, pasar a través de una red tradicional (PSTN), basada en TDM¹⁶.

2.2.2 Telefonía fija

Teniendo en cuenta el reglamento de la Ley General de Telecomunicaciones el uso del servicio telefónico es considerado como universal, protegiendo a los usuarios y con capacidad de acceso a Internet. Por ello, se establece una legislación aplicable a todos los ciudadanos y con unos costes que pueden ser asumidos por la sociedad.

Se ofrece un servicio a millones de usuarios usando conmutación de circuitos utilizando la señalización SS7¹⁷. Para evitar que existan problemas con la numeración se implementó un plan de numeración universal, denominado E.164 [3], y que determina qué numeración debe tener cada localización geográfica. Debido a la introducción de las tecnologías como Xdsl y FTTH¹⁸ los usuarios disponen de un gran ancho de banda para acceder a Internet. Siendo ideal para aquellas aplicaciones que necesiten una gran capacidad de datos como es el *streaming* en video en alta definición, juegos en línea y aplicaciones de realidad virtual.

La tecnología ADSL¹⁹ logra que las líneas de cobre existentes puedan convertir la voz en paquetes de datos. Además, si realizamos una comparativa entre FTTH y ADSL se llega a la conclusión de que es necesario realizar una nueva infraestructura de fibra óptica que alcance al usuario final. Por otro lado, ADSL utiliza los cables de cobre existentes. Si hablamos de velocidades, FTTH ofrece velocidades mucho más altas que ADSL, ofreciendo el primero mucho más ancho de banda con una conexión más estable, a mayores distancias sin degradación significativa de la calidad de servicio (QoS).

¹⁶ TDM: *Time Division Multiplexing*

¹⁷ SS7: *Signaling System No.7*

¹⁸ FTTH: *Fiber to the Home*

¹⁹ ADSL: *Asymmetric Digital Subscriber Line*

Es necesario precisar que, actualmente, la operadora Telefónica está retirando el cobre desplegado en España.

2.2.3 Telefonía móvil

Esta viene a complementar a la telefonía fija, es decir, una de ellas permite la movilidad del usuario mientras la otra se centra en aquellas situaciones donde la comunicación se produce, por parte de uno de los interlocutores, en estático. Hace años, la telefonía inalámbrica fue una solución denominada DECT²⁰. El usuario usaba un teléfono que se conectaba a una base a través de un enlace radio y a su vez, a la red. Sin embargo, el alcance entre la base y el teléfono se limitaba a 300 metros. Afortunadamente, con las tecnologías AMPS²¹ en América o TACS²² que permitían que entre la señalización analógica y la conmutación de circuitos la comunicación de la voz sin datos denominado 1G. Seguidamente, apareció 2G que sí permitió la transmisión de la voz y los datos asociado con la tecnología GSM. Posteriormente, se unió UMTS²³ para 3G y LTE²⁴ para 4G. Estos dos últimos permitió el envío de datos, imágenes, videos y juegos en tiempo real. Es importante reseñar que 3.5G utilizó HSPA²⁵ para alcanzar hasta los 42 Mbps.

Por tanto, si realizamos una comparativa con la telefonía fija, se puede llegar a la conclusión en de que la telefonía fija depende de una conexión fija pero la calidad de las llamadas es superior a las de móvil. Sin embargo, la telefonía móvil entrega más funcionalidades que la telefonía fija.

2.3 Paso de la voz a Internet

Gracias a Internet la telefonía ha mejorado desde su variante fija a móvil. Es decir, se han desarrollados tecnologías en Internet que han permitido a la voz y los datos convivir en la misma infraestructura.

Es necesario indicar que las redes de conmutación de circuitos establecen un camino entre dos extremos. Siendo ineficiente para una transmisión de datos si éstos se envían cada cierto periodo de tiempo teniendo el sistema sin utilizar durante largos periodos de tiempo. Mientras que, para las redes de conmutación de paquetes, la información se divide en fragmentos pequeños que se envían por distintos caminos de la red sin reserva de los caminos por donde debe transitar la información. Para este último caso, pueden darse casos de retardos, pérdidas y *jitter* que son perjudiciales para la calidad de la voz.

Debido a la evolución tecnológica, el protocolo IP junto con TCP²⁶ se empezó a utilizar en conmutación de paquetes para el transporte. Una característica importante para que se utilice este protocolo es la flexibilidad al proporcionar el uso de servicios, aplicaciones y tecnologías. Sin embargo, el protocolo *IP* no fue concebido para el transporte de información multimedia en tiempo real. Por ello, es imprescindible utilizar mecanismos que ayuden a este servicio de tipo *BEST EFFORT* (Ver punto 2.6.1. Protocolo IP).

2.4 Fundamentos físicos para transmitir

La voz del ser humano genera una onda comprendida entre los 20 Hz y los 20 KHz de frecuencia. Dentro de este tramo, se selecciona un espectro comprendido entre los 300 y 3.400 Hz denominado ancho de banda telefónico que es el utilizado en telefonía sin considerar el resto de las frecuencias.

²⁰ DECT: *Digital Enhanced Cordless Telephony*

²¹ AMPS: *Analog Mobile Phone System*

²² TACS: *Total Communication Systems*

²³ UMTS: *Universal Mobile Telecommunications System*

²⁴ LTE: *Long Term Evolution*

²⁵ HSPA: *High-Speed Packet Access*

²⁶ TCP: *Transport Control Protocol*

El proceso natural es el siguiente: “La señal de voz consiste en una señal analógica, que es continua en el tiempo como en la amplitud. Sin embargo, este tipo de señales no pueden transmitirse por sistemas digitales por lo que habría que cambiarle el formato y convertirla en una señal digital. Este cambio de formato implica el muestreo de la señal (discretización temporal) y la posterior cuantificación de las muestras obtenidas (discretización en amplitud). Posteriormente, las muestras de voz cuantificadas habrán de ser codificadas adecuadamente para su transmisión por el canal de comunicaciones.” [4]

2.4.1 Muestreo

Como la señal analógica varía a lo largo del tiempo, lo que pretende realizar el muestreo es coger valores de esta señal a intervalos regulares con el objetivo de evitar perder información. Para reducir la pérdida de información hay que basarse en el *teorema de Nyquist* que afirma que la frecuencia con la que ha de recogerse las muestras (f_s) de una señal debe ser, al menos, del doble de su ancho de banda (f_n).

$$f_s > 2 \cdot f_n$$

En el caso de que la frecuencia de muestreo (f_s) cumpla con la condición ocurrirá que las frecuencias se superpongan y la señal se distorsione. A esto último se le denomina fenómeno *aliasing*.

2.4.2 Cuantificación

A continuación del muestreo de la señal se produce la cuantificación. En este punto, la señal consiste en un conjunto discreto de valores recogidos en ciertos instantes de tiempo con valores continuos de amplitud. En el proceso de cuantificación, a cada una de las muestras se le asigna un valor entre M posibles (señal en escalones). Por ello se le denomina proceso cuantificación. Además, se introduce un valor de error (ruido de cuantificación) que viene como consecuencia de que ciertos valores de la señal se ajustan a los niveles discretos más cercanos. A modo de ejemplo, una muestra de la señal con valor de 3,75 pasará a tener un valor 4 en un proceso de cuantificación en el que sólo se manejen valores enteros.

Mediante este proceso, cada muestra de la señal queda representada en un número finito de bits con un total de M posibles valores diferentes. El resultado es la representación digital de la señal. Al realizar el proceso de cuantificación, se divide el rango dinámico de la señal (conjunto de valores que puede tomar la señal) en M niveles de tamaño Δ (intervalo de cuantificación).

2.4.3 Codificación y compresión

Una vez que se ha digitalizado la voz es necesaria adaptarla para transmitirla por una canal de comunicaciones concreto. La codificación, digitalización y compresión, consiste en asignar un código binario a cada uno de los valores discretos de la señal.

En el caso de la telefonía, se ha utilizado PCM como modulación. Para concretar, las muestras de voz son de 8bits y como se dan 8.000 muestras por segundo, es decir, la frecuencia de muestreo es de 8kbps. El producto de 8.000 muestras por segundo por 8 bits, que son las muestras de voz, corresponde con la velocidad de un canal (64kbps). Este valor es el utilizado por la codificación G.711.

Lo anterior, como ya se ha citado corresponde con G.711. Sin embargo, para poder conocer el valor del ancho de banda de un codificador se utiliza el concepto régimen binario. Es decir, es el producto de la frecuencia de muestreo (f_s) por el número de bits usados al codificar cada muestra N.

$$R_b = N f_s$$

Puede darse el caso de que la red presente un ancho de banda limitado y sea necesario adaptarse a esta circunstancia por lo que se deberá utilizar otra codificación como puede ser G.721. El inconveniente es que ofrecerá una menor calidad. Una vez se digitalice la señal de voz de entrada con

PCM, a 64kbps, el objetivo de G.721 es lograr reducirlo a 32 o 24kbps. A partir de aquí, se procede a la compresión con ADPCM²⁷. Debe quedar claro que con PCM se transmitía cada muestra completa, mientras con ADPCM codifica la muestra actual y su valor esperado. Es decir, el valor esperado se obtiene con la información de las muestras anteriores. Pueden darse dos casos; predicción adaptativa y cuantificación adaptativa. En el caso de la predicción adaptativa, si las últimas muestras tienen un patrón creciente, se predice que la siguiente muestra también sea creciente. Para el segundo caso, si la diferencia entre el valor real y el predicho se cuantifica con menos bits. A continuación, vendrá la señal comprimida con menos información, es decir, menos bits por muestra (32 o 24 kbps) para reconstruir la señal. El hecho de lograr disminuir el ancho de banda implica un aumento del retardo y disminución de la calidad.

El proceso de compresión implica usar recursos computacionales, es decir, existe un elemento denominado DSP²⁸ que realiza cálculos que hacen consumir ciclos de la CPU. En caso de no realizarse el proceso de compresión no habría consumo de ciclos de CPU.

Una vez realizada la codificación de la señal se empaqueta y transmite por la red.

2.4.4 Codificador-decodificador

Una vez explicado el proceso de muestreo, cuantificación y codificación es necesario indicar que, en caso necesario, se debe llegar a un compromiso entre el ancho de banda y la calidad de servicio.

Existen varios tipos de códecs. Por ejemplo, G.729 se caracteriza por reducir el ancho de banda, pero presentan el problema de pérdida de paquetes. Para solucionar esto último, utilizan técnicas de interpolación. Existe otro caso que es G. 723.1, y siendo similar a G.729, además incluye la capacidad compresión por supresión de silencios y VAD²⁹. Esta supresión afecta al funcionamiento de los módems de los usuarios dado que éstos están acostumbrados a trabajar sobre un caudal de datos constantes. Como solución a esto último, se puede implementar en los Gateways ciertas funciones que lo inhabiliten, pero aumenta el uso de ancho de banda al transmitir datos, aunque haya silencios. Finalmente, al códec G.723.1 se le conoce como caudal variable ofreciendo servicios como el modelo DiffServ³⁰ de Internet o los servicios UBR³¹ o ABR³² de ATM, mientras que a G.711 es de caudal constante.

En el caso del códec G.729, al igual que G.711, es de caudal constante y ofrece servicios orientados a conexión como son RSVP (*Resource Reservation Protocol*) o circuitos CBR³³ de ATM.

2.4.5 Tipo de conexión

La salida de códec es una secuencia de datos que se convierte en paquetes IP y se transporta a través de la red IP hasta su destino, realizando el proceso inverso.

Si quisiéramos conectar a todos los usuarios sería necesario que el número de conexiones siguiese la siguiente expresión matemática:

$$C = \left(\frac{n}{2}\right) = n(n-1)/2$$

siendo: c el número de conexiones y n el número de abonados.

Este resultado es inviable si tomamos como ejemplo a un número de abonados igual a 1millón. Para esto sería necesario un total de 500.000.000 de conexiones. Para solucionarlo se decidió agrupar a

²⁷ ADPCM: *Adaptive Differential Pulse-Code Modulation*

²⁸ DSP: *Procesador Digital de Señales*

²⁹ VAD: *Voice Activity Detection*

³⁰ DiffServ: *Differentiated Services*

³¹ UBR: *Unspecified Bit Rate*

³² ABR: *Available Bit Rate*

³³ CBR: *Constant Bit Rate*

los abonados en los nodos de conmutación o centrales para reducir el número de conexiones. Estas centrales se conectarán siguiendo una estructura jerárquica en una red mallada.

Este sistema tiende a simplificarse conforme las centrales tienen el mismo hardware [4] y lo que las diferencia es el software distinguiendo entre centrales de abonados y las centrales de tránsito. De tal forma que, para conectar a dos abonados de una central con otro de otra central distinta, es necesario recorrer el árbol jerárquico completo. Si se hace esto último es ineficiente y consume muchos recursos. Para evitarlo, la solución consiste en superponer a la red jerárquica, una red complementaria en la que existen enlaces directos entre centrales donde existe un tráfico frecuente. Por ello, se introduce un plan de encaminamiento que indique la ruta óptima para enlazar abonados y que, en caso de haber al menos dos caminos, habrá un camino por la red jerárquica y otro por la red complementaria.

Es necesario indicar que la comunicación entre el usuario y su central local se realiza a dos hilos mientras que entre las centrales (*transporte y conmutación*) se realiza a cuatro hilos, es decir, dos hilos para la transmisión y dos para la recepción con bobinas híbridas.

Las centrales de conmutación ayudan a la interconexión de usuarios a través de un conmutador. De tal manera que, ante una serie de entradas o salidas se utiliza un algoritmo que transfiere las señales entre abonados. Estas conexiones se pueden realizar a través de un camino físico (conmutación espacial) como por instantes de tiempo dentro de un camino físico (conmutación temporal). Es decir, un conmutador está formado por varias etapas que cada una de ellas pueden realizar conmutación temporal o espacial. Es necesario indicar que la conmutación temporal precisa del uso de la tecnología digital. De tal manera que, el conmutador se encarga del control de las entradas y salidas de las señales que se dan en el mismo canal en distintos momentos temporales. Las señales digitales se organizan de tal manera que los bits se agrupan en tramas y, las tramas están compuestas por canales que pueden ser de señalización, de control o datos.

Los canales de datos, que contienen las conversaciones de los usuarios, se les asigna un canal o intervalo de canal. Para el caso de que dos usuarios se conecten telefónicamente, se realizará de tal manera que el usuario1 escuchará al usuario2 leyendo las muestras del canal 2, mientras que el usuario 2 leerá las muestras del canal 1. Un ejemplo para este caso es la trama PCM 30+2 que a continuación se indica.

2.4.6 Procesamiento de una llamada

El proceso de establecimiento de la conexión comienza cuando el usuario descuelga el teléfono y el circuito se cierra, *off hook*, permitiendo el paso de una corriente denominada corriente en bucle. La central envía al abonado un tono de invitación a marcar. Este caso se da en la telefonía tradicional, digital e IP.

Existen dos tipos de marcación; por tonos y por pulsos. La marcación por tonos, son los sonidos generados por un teléfono cuando se presionan los números y se denomina marcación multifrecuencia o DTMF (*Dual Tone Multi Frequency*). Cuando el usuario presiona los números, el equipo de los nodos escuchan los tonos y entienden su significado para decodificarlos en comandos. El comando dirá al nodo donde encaminar la llamada. Mientras que la marcación por pulsos se aprovecha la corriente de bucle para enviar los dígitos del número de teléfono. Por lo que es necesario dejar tiempos entre dígitos consecutivos. Este tipo de marcación está en desuso dado que puede dar lugar a errores.

Los tonos que existen son:

- Tono de llamada: Indica que el teléfono al que se está llamando está sonando.
- Tono de ocupado: Indica que el abonado de destino está descolgado.
- Tono rápido: La central no tiene recursos para cursar una nueva llamada.
- Mensajes de información: Cuando el número marcado no es correcto.

El destinatario de la llamada recibe un voltaje (A/C) suficientemente alto para que suene su teléfono. Y en el caso de que finalice la llamada, al colgar uno de los dos extremos, el abonado que no ha colgado recibe un tono, igual que el tono de ocupado, que indica que ha finalizado la comunicación.

2.4.7 Transporte de voz sobre paquetes

Para lograr un transporte de la voz sobre paquetes es necesario llevar a cabo una serie de procesos tales como la digitalización de la voz y convertirla en paquetes (tramas o celdas) en el protocolo que en este caso es IP. Además, para el caso de la telefonía es preciso realizar las funciones de señalización de la llamada, reenvío de llamadas, mensajería, etc. A esto, hay que añadirle routers, switches, hubs en VoIP, teléfonos IP, pasarelas y elementos para el control de llamadas y de señalización. Además, es necesario indicar que, a parte de la VoIP, existen otros servicios como:

- ToIP: Telefonía sobre IP.
- VoFR: Servicios de telefonía prestados sobre redes soportados por circuitos Frame Relay, para la transmisión de datos.
- MoIP: Servicios multimedia, voz, datos e imágenes prestados sobre redes IP.
- FoIP: Servicios de transmisión de fax prestados sobre redes IP.

Los teléfonos IP son los equipos que utilizan los usuarios para comunicarse. Se les puede asimilar a los teléfonos convencionales con una pequeña pantalla y conexión a la red con un conector RJ-45 que es lo utilizado en una red Ethernet.

Es importante señalar que existe un tipo de teléfono IP denominado *softphone* que funciona sobre un ordenador, es decir, se utilizar al ordenador como si fuese un teléfono. Se definirá con más detalle en el punto 2.8.12.

2.5 Dominios

En Internet los dominios se pueden clasificar como genéricos *Generic Top Level Domain* y territoriales *Country Code Top Level Domain*. Los primeros son com, .net, .edu, .gov, .info, .biz, etc., mientras que los segundos están formados son .es, .it, etc., que hacen referencias normalmente a los países.

2.6 Protocolos de comunicación

En este punto se van a tratar de una serie de protocolo que van a mostrar cómo se relacionan los distintos elementos que ayudan a la voz en su funcionamiento.

Se va a mostrar qué es el protocolo IP, el formato de paquete, estructura y direccionamiento que usa. El encaminamiento nos muestra cómo los nodos utilizan las tablas para enviar enviarse entre sí los paquetes para llegar al destinatario correcto. Los controles que se van a encargar de avisar de errores en el encaminamiento y los elementos que ayudan, como RTP³⁴, a la entrega de audio y video a través de redes IP. Otros elementos, nos ayudan a de iniciar, modificar y finalizar las sesiones multimedia negociando los códecs para establecer las conversaciones entre los distintos intervinientes.

En este punto, también se van a tratar los mecanismos para reducir las pérdidas de paquetes, *jitter*, retardo que se puedan dar en la red.

Todo lo anterior, debe estar supeditado a unas reglas de seguridad que minimicen el impacto de amenazas que traten de evitar el correcto funcionamiento de los distintos servicios que se ofrezcan.

Finalmente, la calidad de servicio de una red define la capacidad enviar información desde una fuente a otra de forma óptima.

³⁴ RTP: *Real-time Transport Protocol*

Todo lo citado en este apartado, deben ir de la mano para garantizar un correcto funcionamiento de la red que afectará al servicio de telefonía.

2.6.1 Protocolo IP

El protocolo IP pertenece al nivel de red ofreciendo un servicio sin garantía de servicio o *Best Effort* [4]. *Best Effort* quiere decir que el protocolo IP intenta entregar los paquetes de datos en su destino con el mejor esfuerzo, pero no da garantía de que se produzca la entrega, el orden de entrega o el tiempo que tardará en realizarse la tarea. Lo que implica que no integra mecanismos de calidad de servicio (QoS) en el protocolo IP.

Las redes IP son de tipo datagrama donde la información se divide en fragmentos más pequeños, paquetes o datagramas, que se envía de forma independiente. Con un servicio sin conexión y sin dialogo previamente establecido entre los extremos. Esto último, resulta crítico para el transporte de paquetes en tiempo real como la voz al transmitirse por caminos independientes. Esto implica que los paquetes se tengan que reordenar en el destino.

2.6.1.1 Formato del paquete

Es la unidad de información a nivel de IP que encapsula la parte de la capa de transporte, los datos de control y los datos de usuario. Dado que ya conocemos que los paquetes circularán por la red de forma desordenada, podrán reconstruirse con la ayuda de los campos DF, MF y OFFSET. El parámetro DF significa *Don't Fragment* (no fragmentar), MF quiere decir *More Fragments* (más fragmentos) y OFFSET.

DF indica si el paquete puede ser fragmentado, es decir, si el valor del bit es igual a 1 indica que el paquete no debe ser fragmentado. Si es igual a 0 sí puede ser fragmentado. Esto sirve para asegurar que el paquete llega intacto y emplea herramientas de diagnóstico como hacer un ping o traceroute para determinar el tamaño máximo de la unidad de transmisión/ MTU³⁵ entre dos dispositivos. Es necesario matizar que el tamaño máximo del paquete se le denomina MTU. Y si el router necesita fragmentar un paquete cuyo valor del bit DF es igual a 1, lo que ocurrirá es que el router descartará el paquete enviando un mensaje *ICMP*³⁶ al origen del paquete informando del asunto.

MF indica si hay más fragmentos de un paquete por venir. Si el valor del bit es igual a 1 quiere decir que el paquete es un fragmento. Además, se utiliza para reensamblar paquetes, es decir, el último fragmento vendrá con un valor igual a 0 para indicar que ya no hay más fragmentos. Por tanto, ya se podría empezar a iniciar el proceso de ensamblaje.

Normalmente, se utiliza OFFSET para determinar la posición del fragmento en el datagrama original. Además, nos sirve para colocar los fragmentos en el lugar correcto.

Existe un contador de salto TTL³⁷ que ayuda a que los paquetes no viajen de forma continua por la red. Para ello, se introduce un valor inicial de 255 que irá decreciendo en una unidad por cada nodo que pasa. En el momento que alcance el valor cero, será descartado en ese nodo.

2.6.1.2 Fragmentación

Si el tamaño del paquete es mayor que el valor de la trama se tendrá que dividir en fragmentos más pequeños para ser enviado. En la siguiente tabla se muestre los valores del MTU en función de la red.

³⁵ MTU: *Maximum Transfer Unit*

³⁶ ICMP: *Internet Control Message Protocol*

³⁷ TTL: *Time To Live*,

Protocolo a nivel de enlace	MTU (bytes)
PPP	1500
SLIP	1006 (limite original)
X.25	1600 (RFC 1356)
Frame Relay	1500
Ethernet	4352
FDDI	Datos en col 2
Classical IP over ATM	9180

Tabla 2-1 Valores MTU en función de la red.

2.6.1.3 Direccionamiento

Todas las redes deben disponer las características de direccionamiento, encaminamiento y señalización. El direccionamiento nos ayuda a determinar el origen y el destino de las llamadas telefónicas. Mientras que las cabeceras IP nos sirven para asociar las clases de servicio a cada una de las llamadas en función de la prioridad. Por parte del encaminamiento, muestra el camino más apropiado para que el paquete alcance su destino. Finalmente, la señalización avisa a los elementos de red y a las estaciones finales su establecimiento de conexión y registro de eventos.

Otro aspecto importante a tener en cuenta es que el direccionamiento permite identificar a todos los elementos que se conectan a la red. Para realizar esto último, en IPv4, a cada uno de los equipos se le identifica con 4 bytes, denominado dirección de red o dirección IP.

Es necesario indicar que una dirección IP genérica se divide en dos partes; identificador de red y el identificador del host dentro de la subred. La división en clases se realiza en función del tamaño de la red para determinar el número de estaciones que habrá en la red.

Conforme pasaba el tiempo, el número de dispositivos que se conectaban a la red iba creciendo por lo que fue necesario definir rangos de direcciones privadas reutilizables. Estas direcciones privadas no son accesibles desde internet. De hecho, para que estas direcciones privadas puedan acceder a internet se utiliza un mecanismo de traducción de dirección de red denominado NAT³⁸, es decir, la norma RFC 3022 permite a las empresas solicitar direcciones públicas menor que el número de equipos que se quieren conectar a internet. De tal manera, que los equipos servidores dispondrán de IP pública mientras que el resto de los equipos tendrán asignada una IP privada.

El NAT puede implementarse en los routers de tal forma que sirve de frontera entre una red interior o LAN y el exterior como único punto de comunicación. NAT sólo traduce paquetes IP a ICMP o a los protocolos de transporte TCP y UDP. Por ejemplo, para un sistema donde se desee disponer de menos de 255 ordenadores precisará una red de clase C. En caso de necesitar de más ordenadores necesitaría una red de clase B. Tener un sistema de redes basado en clases es un inconveniente en el caso de necesitar 500 ordenadores y que le sobre 65.536 direcciones. ¿cómo podemos resolver esto? Utilizando subredes (*subnetting*), VLSM³⁹ o CIDR⁴⁰ [5]. En el Anexo se presenta un ejemplo de subnetting

³⁸ NAT: *Network Address Translation*

³⁹ VLSM: *Variable Length Subnet Mask*

⁴⁰ CIDR: *Classless InterDomain Routing*

2.6.1.4 VLISM

Es una técnica de tipo subneteo que permite utilizar diferentes longitudes de máscara de subred dentro de una misma red principal. Es decir, maximiza el uso eficiente del espacio de direcciones de direcciones IP de tal forma que cada subred tenga una máscara de subred se ajuste a las necesidades de tamaño. Se da una serie de pasos como determinar las necesidades de la red donde se evalúa cuántas subredes se necesitan y cuántos hosts requiere cada subred. Por otra parte, asignar la red principal donde se comienza con una dirección IP de red principal y una máscara de subred. Finalmente, se realiza un Subneteo iterativo donde se asigna a subredes más grandes primero (aquellas con más *hosts*) y luego subdividir las subredes restantes para ajustarse a las necesidades más pequeñas.

En el Anexo se presenta un ejemplo para ver cómo se aplica en este caso.

2.6.1.5 CIDR

Es un método denominado *Classless InterDomain Routing* que asigna y especifica direcciones IP y encamina IP que reemplaza a las clases A, B, C. De hecho, combina 32 bits en notación decimal. Un ejemplo sería la dirección 192.168.1.1.

A mayor número de ordenadores que se conectan a la red, aumenta la complejidad y se produce la necesidad de situar los equipos en subredes utilizándose la máscara de subred para dividir la red en subredes (subnetting). A esto se le denomina FLSM⁴¹, es decir, todas las subredes creadas a partir de una red principal tienen la misma longitud de máscara de subred y, por lo tanto, el mismo número de direcciones IP disponibles. En el Anexo se puede ver un ejemplo de FLSM.

Las diferencias que existen entre VLISM y FLSM es que en FLSM todas las subredes tienen la misma longitud de máscara. Es más fácil de implementar y administrar Mientras que para VLISM las subredes pueden tener diferentes longitudes de máscara. Más flexible y optimizado, pero más complejo de planificar y administrar.

2.6.1.6 ENUM

Es un protocolo denominado *Electronic Number Mapping* que define una arquitectura y un protocolo basados en el DNS para hacer corresponder los números de teléfono con los URL⁴². De esta forma, es posible contactar un teléfono con servicio de telefonía sobre IP (VoIP) desde un teléfono tradicional. ENUM [4] establece una correspondencia entre la ITU-T y el Plan Internacional de Numeración E.164.

Se puede afirmar que cada equipo en Internet está localizado con un único número, su dirección IP, etc. Lo usual no es encontrar la web de una empresa por su número de teléfono. Sino que lo que hace es traducir los números de teléfono a algo parecido a los dominios que serán convertidos en direcciones IP. De esta forma, surgió ENUM que hacer la traducción de un número que podría ser +34 91 1234567 en un dominio de tipo 7.6.5.4.3.2.1.1.9.4.3. e164 arpa.

Es necesario aclarar que E.164 es un estándar internacional de número de teléfono gestionado por la ITU. Y Arpa es un dominio de primer nivel que pertenece a la Agencia para Proyectos Avanzados de Investigación de Estados Unidos.

ENUM ofrece teléfonos con los servicios de correo electrónico, mensajerías, acceso a la web utilizando del sistema de nombres de dominio de internet (DNS). Es decir, se puede acceder a internet tecleando el nombre de la dirección de la página web de tal forma que ENUM lo hará exactamente igual que el DNS. Una de las ventajas que ofrece ENUM es que desde un mismo teléfono los usuarios pueden tener los datos de otros usuarios con sus respectivos correos electrónicos y otros datos en las bases de datos internacionales públicos.

⁴¹ FLSM: *Fixed Length Subnet Masks*

⁴² URL: *Uniform Resource Locators*

Para un teléfono IP ya no es necesario tener el teléfono de la otra persona sino con conocer el destino es suficiente. Una de las ventajas que ofrece ENUM es poder encaminar llamadas a números de teléfonos virtuales dirigidos a ordenadores. Además, permite que un número de teléfono en un punto de contacto único para una persona o empresa. Permite que no solo llamar a esta persona sino también enviarle correos electrónicos. Reenviar las llamadas a teléfono fijos, acceder a información sobre una empresa a través de la web.

Desafortunadamente, a pesar de su potencial, la implantación de ENUM ha sido limitada. Solamente ha sido adoptado en algunos países. Esto fue debido a la falta de un consenso global sobre la implementación y el uso ha dificultado su adopción. Otro inconveniente es que existe preocupación por la seguridad de los números telefónicos lo que ha limitado la adopción de *Public* ENUM.

Tecnologías como SIP y otros métodos de encaminamiento de llamadas en redes IP compiten con ENUM, ofreciendo soluciones alternativas que en algunos casos son más fáciles de implementar.

2.6.2 Protocolos de encaminamiento

El encaminamiento corresponde al nivel de red seleccionando la ruta que deben seguir los paquetes hasta su destino. Se deben distinguir dos tipos de protocolos [4]:

- Protocolos encaminados o de transporte
- Protocolos de encaminamiento

Los protocolos de encaminamiento son los que generan las aplicaciones y servicios de red. Mientras que los protocolos de encaminado [4] son los utilizados para la gestión de las tablas de encaminamiento de los nodos de la red y toman las decisiones que se reflejan en estas tablas. Es necesario indicar que, para lograr lo anterior, al intercambiar información con otros routers permite determinar cuáles son las rutas óptimas.

Encaminados o de transporte	Encaminamiento
IP, IPX, CLNP, XNS	IGRIP, RIP, OSPF, EGP, ES-IS, IS-IS

Tabla 2-2 Protocolos de encaminados y encaminamiento

La diferencia entre ellos es el algoritmo utilizado. Es decir, consiste en el algoritmo que se utiliza para actualizar las tablas de almacenamiento de cada nodo de la red. Un caso de algoritmo de encaminamiento estático son los de inundación en el que el paquete entrante se retransmite por todos los enlaces de salida. En este caso, se añade un mecanismo como es el contador de salto que disminuya en una unidad al pasar por cada nodo y al llegar el valor cero, el paquete se descarta.

Los protocolos de encaminamiento se caracterizan porque mueven los paquetes de datos en la red teniendo en cuenta las tablas de encaminamiento [4] que se actualizan en función de las condiciones de la red, es decir, los algoritmos se adaptan ante situaciones cambiantes en la red y determinado por el protocolo de encaminado. Cada router posee una tabla o vector con la distancia mínima hasta el posible destino. De hecho, los routers recalculan las tablas de distancias en función de la información recibida.

Dependiendo de cómo se manejen los datos de las tablas de encaminamiento, podemos distinguir entre algoritmos de encaminamiento estáticos o dinámicos. Los primeros son valores estáticos y ya están definidos al configurar el router y los segundos son valores dinámicos y se actualizan durante el funcionamiento del equipo.

Actualmente, uno de los algoritmos más utilizados es el de Dijkstra que es el protocolo de *routing* de Internet que consisten en seleccionar el camino más corto OSPF⁴³ [4]. En el caso de que se

⁴³ OSPF: *Open Shortest Path First*

produzca entre sistemas distintos se utiliza BGP⁴⁴ mientras que, si se da dentro de un sistema autónomo, como una organización, se emplea OSPF.

2.6.3 Protocolos de control

A continuación, se van a definir los protocolos ARP⁴⁵, ICMP y DHCP⁴⁶.

2.6.3.1 ARP

Todo equipo conectado a la red tiene dos direcciones [4]; una dirección lógica IP, que identifica los dispositivos en la capa de red, y otra física MAC. La dirección IP puede variar mientras que la física no se puede alterar.

Para enviar un paquete, es necesario conocer la dirección IP y su dirección física o MAC. En el caso de no conocerse, se ejecuta el prototipo ARP⁴⁷ conociendo la dirección de red IP. De tal forma que el de origen un paquete ARP request que se difunde a todos los equipos de la red y de la dirección IP del equipo cuya dirección física se quiere obtener. Este paquete es recibido por todas las estaciones de la red y únicamente contestará aquella cuya dirección IP coincide con la dirección IP del paquete ARP request. La respuesta que se genera es la ARP reply dando su dirección física MAC.

2.6.3.2 ICMP

Este protocolo avisa de errores en el encaminamiento [4]. En el momento en el que el router detecta un error de encaminamiento envía un paquete ICMP con la dirección IP destino que originó el paquete.

Para este caso, se limita a informar de que se ha producido un error sin sugerir acciones a realizar dado que esto corresponde a los protocolos encaminados (por ejemplo, IP, IPX, CLNP, XNS).

Existen otros tipos de ICMP que nos informan de situaciones tales como cuando un router que no tiene definida una ruta hacia el destino al que denominamos *Destination Unreachable*. O bien, cuando un router descarta un paquete porque su contador de saltos es cero y al que denominamos *Time exceeded for a datagram*.

Es necesario indicar que cuando realizamos un ping utilizan mensajes ICMP para testear la red, comprobar si el sistema está encendido y conectado. Para ello, se consigue enviando a dicha máquina paquetes ICMP y, en caso de estar operativo, responderá con otro paquete ICMP.

2.6.3.3 DHCP

Es el protocolo de red en el que un servidor da los parámetros de configuración a los equipos conectados [4]. Estos parámetros son máscara, puerta de enlace, etc. Además, incluye la asignación de dirección de IP. En el caso de no disponer de DHCP, las IP se deberán configurar manualmente en cada equipo. En el caso de que un equipo tenga que llevarse a otra red, habrá que darle una nueva IP. Este sistema es de gran ayuda dado que permite al gestor distribuir las direcciones IP de forma automática.

El protocolo DHCP ofrece tres maneras de asignación de IP:

- Manual: Existe una tabla con direcciones MAC. Sólo los ordenadores y teléfonos que estén incluidos con su MAC en la tabla se les podrá asignar una IP.
- Automática: El administrador de la red determinará las direcciones IP que se le asignará a los equipos de forma permanente.

⁴⁴ BGP: *Border Gateway Protocol*

⁴⁵ ARP: *Address Resolution Protocol*

⁴⁶ DHCP: *Dynamic Host Configuration Protocol*

⁴⁷ ARP: *Address Resolution Protocol*

- Dinámica: El administrador de la red ofrecerá un rango de IP y cada equipo conectado solicitará su dirección IP al servidor. Este método no permite la que los equipos siempre tengan la misma dirección IP. La ventaja de este método es que puedes añadir máquinas a la red en cualquier momento. De tal forma que, DHCP actualiza las nuevas direcciones IP al DNS asociado junto con sus servidores asociados cumpliendo con la normativa RFC 2136.

2.6.4 Protocolo RTP

Es importante indicar que un protocolo en tiempo real (RTP) [4] es un protocolo de red para la entrega de audio y video a través de redes IP. Como ejemplo, sería una combinación de telefonía, aplicaciones de videoconferencia, etc. Además, RTP se ejecuta a través del protocolo de datagramas de usuario (UDP) junto con el protocolo de control RTP (*RTCP*). De tal manera que, RTP transporta los flujos de medios como audio y video mientras que *RTCP*⁴⁸ sirve para monitorizar las estadísticas de transmisión y la calidad de servicio (QoS). Utilizamos RTP junto con un protocolo de señalización como el protocolo de inicio de sesión (SIP) que establece las conexiones a través de la red.

2.6.5 Protocolo de transporte en VoIP

Puede darse el caso de que durante el envío de paquetes sea necesario fragmentarlos y reensamblarlos. Esto provocará pérdidas, retardos, jitter, por lo que será necesario introducir mecanismos para reducirlos.

Para el intercambio de audio y video en tiempo real se utilizan los protocolos determinados en RFC 1889 y RTP y RTCP para el control de intercambio. Estos dos últimos utilizan UDP por su simplicidad ya que TCP ofrece un retardo muy elevado. Sin embargo, UDP no garantiza la entrega ordenada ni corrección de errores, pero es preferido en aplicaciones de streaming y VoIP por su menor sobrecarga y latencia.

Cuando se utiliza la voz sobre paquetes, los puertos UDP elegidos por cada extremo deben ser notificados entre ellos con la ayuda de un *mecanismo de señalización*.

El *protocolo* RTP es utilizado tanto para audio como para video en tiempo real sobre redes IP con pérdidas que se pueden producir en la red durante la comunicación. Además, no garantiza la entrega de los paquetes en tiempo real pero sí ofrece los recursos para una entrega sincronizada. A nivel de estructura de paquetes, los RTP se caracterizan porque sus paquetes están divididos en dos partes o bloques. Una de estas partes contiene la cabecera con la información que debe ser rehecho realizado por el *códec* del emisor. La segunda parte contiene el flujo de bits. A parte de lo anterior, es necesario aclarar que RTP identifica el tipo de información transportada, marcas temporales (*time stamp*), números de secuencia y control de llegada de paquetes. Lo anterior, sirve a los receptores para reconstruir el flujo de paquetes. Para esta reconstrucción, las pérdidas, retardos y jitter deben ser consideradas. Es decir, RTP ofrece al receptor las herramientas para recuperar la información. Una opción es comprimir las cabeceras usando *cRTP*⁴⁹ pero, asumir esta opción provocará introducir un retardo adicional por la compresión a pesar de aumentar la eficiencia en el transporte.

Finalmente, el protocolo RTSP pertenece al nivel de aplicación, a diferencia de RTP y RTCP que trabajan en la *capa de transporte*, indica cómo se realiza el *streaming*.

Streaming es la capacidad de enviar el contenido multimedia tal que se puedan ver mientras están siendo transmitidos sin necesidad de descargarlos. De tal manera que el usuario al recibir un número suficiente de paquetes comienza la reproducción y, a la vez ir descomprimiendo otros paquetes para

⁴⁸ RTCP: *Real Time Control Protocol*

⁴⁹ cRTP: *compressed RTP*

reproducirlo a continuación. A parte de lo anterior, el servidor posee la información sobre el estado de cada cliente que posee en ese momento. En el Anexo se puede ver un ejemplo.

Se puede utilizar TSP en una variedad de aplicaciones que usamos a diario, tales como streaming de video y audio como son youtube, Netflix. Video vigilancia como cámaras IP y CCTV⁵⁰ para transmitir video en tiempo real, videoconferencias para celebrar reuniones, formación online, etc.

2.6.6 Protocolos de aplicación en VoIP

Las normas son los protocolos que garanticen la interoperabilidad, en la VoIP, entre todos los participantes.

Los protocolos VoIP están situados en la capa de aplicación de la pila TCP/IP.

Gracias a los protocolos SIP y H.323 el usuario puede iniciar la llamada. SIP se encarga de localizar al destinatario y negociar los parámetros de la sesión evitando que la sobrecarga de la red. Además, utiliza TCP para garantizar que la entrega de paquetes sea fiable. Mientras que H.323 funciona de manera similar a SIP, pero utiliza mensajes y estructuras de señalización diferentes para realizar la llamada.

En la fase que se produce la conversación entran a jugar las funciones RTP y RTCP. Para el primer caso, RTP, es el responsable de entregar datos de audio y video, sincroniza los datos, detecta los paquetes que se pierden y corrige los errores. Todo ello, en tiempo real.

Finalmente, en la fase de terminar la llamada, también se utilizan los protocolos SIP y H.323 con las mismas características antes citadas.

2.6.7 Protocolo de señalización

Previamente a explicar los protocolos de señalización, es necesario señalar que existen un par de métodos denominados canal asociado o CAS⁵¹ y señalización por canal común (CSS) [4].

En la señalización por canal asociado CAS es común en sistemas de telefonía tradicional (telefonía analógica) y algunos sistemas digitales más antiguos como TDM. Su funcionamiento consiste en que la información de señalización (conexión y liberar llamadas) discurre por el mismo circuito por donde se produce la comunicación de voz. Como ejemplo se encuentra la señalización por tonos multifrecuencia (DTMF). Este caso no es aplicable a IP dado que no es posible la transmisión de voz y datos a la vez.

En la señalización por canal común CCS⁵² se designa un canal para enviar la información de señalización y separado de varios canales de voz. De hecho, el sistema de señalización SS7 es un protocolo por canal común (CCS).

En telefonía digital (TDM) se emplea en redes ISDN y telefonía móvil.

CSS es utilizado para enviar información de señalización que es utilizado por la parte de voz de IP, H. 323 y SIP. Además, H.323 utiliza el control de llamadas con la ayuda de los protocolos H.225 y H.245.

En el caso que se tenga que decidir entre CAS y CSS, dependerá del tipo de red.

Una vez explicado lo anterior, es necesario indicar que los protocolos de señalización se utilizan para garantizar que las llamadas se realicen correctamente.

El protocolo de señalización utilizado en redes PSTN es SS7. Las funciones que tiene asignadas son el establecimiento y terminación de llamadas, facturación, y el desvío de llamadas.

⁵⁰ CCTV: *Closed Circuit Televisión*

⁵¹ CAS: *Channel Associated Signaling*

⁵² CCS: *Common Channel Signaling*

En el caso de redes de voz sobre paquetes existen dos protocolos de señalización: protocolo de señalización entre terminales y protocolos de señalización en la red IP. Para los primeros, los protocolos que permite la voz, video y audio corresponden con H.323 y el SIP. Mientras que para la señalización se centralizan en un controlador que establece un diálogo con las pasarelas y las controla remotamente. Los más extendidos son MGCP⁵³ (equivalente a H.248 denominado Megaco) y SIGTRAN⁵⁴.

A continuación, se van a describir con más detalle los protocolos en función a la red que pertenezcan.

2.6.7.1 Redes digitales

El sistema SS7, que se utiliza para identificar y encaminar llamadas utilizando los protocolos como Punto de Conmutación de Señalización SSP⁵⁵, Punto de Transferencia de Señalización STP (*Signaling Transfer Point*) y Punto de Control de Señalización SCP⁵⁶. Además, SS7 utiliza una arquitectura redundante donde se incluyen los siguientes protocolos:

- MTP⁵⁷. Asegura la entrega fiable de los mensajes dentro de la red.
- TCAP (*Transaction Capabilities Application Part*). Permite la comunicación para realizar consultas en bases de datos.
- ISUP (*ISDN User Part o PSTN*). Maneja la señalización para establecer y finalizar llamadas.

En el caso de que se quiera realizar una llamada telefónica desde una red tradicional (PSTN) a una red IP, la señalización en esta red será SS7 de tal forma que *Signal Gateway* (SG), que es un tipo de Gateway que garantiza a SS7 la comunicación entre las redes PSTN con IP, reciba la petición que transformará en el formato que sea comprensible por IP usando el protocolo SIGTRAN. Seguidamente, SG enviará la señal convertida al MGC⁵⁸ a través de la red IP. Además, MGC consultará su base de datos para obtener la dirección IP asociada al número de teléfono marcado por la persona que inició la llamada que serán enviados a SG y *Media Gateway* (MG). El MG recibe las instrucciones del MGC sobre cómo manejar los medios (audio) de la llamada y convierte el flujo de medios de la red telefónica tradicional (PCM) al formato utilizado en la red IP (como puede ser G.711, G.729). Seguidamente, MG establece una conexión de medios (*Real-time Transport Protocol*) con el destino en la red IP. De tal forma que, la señalización SIP, que contiene la información sobre la llamada, se envía desde el MGC al destinatario en la red IP y el flujo de medios (voz) convertido se transmite a través de la red IP utilizando RTP. Finalmente, el destinatario que se encuentra en la red IP recibe la señalización SIP y RTP estableciéndose la llamada y permitiendo al usuario establecer una comunicación con el usuario que está en la red telefónica tradicional.

En el caso de que SS7 desee introducir mayor seguridad, tendrá que utilizar el protocolo de transmisión de señalización SCTP⁵⁹.

2.6.7.2 Redes de voz sobre IP

Existen una serie de protocolos que a continuación se van a definir, pero es necesario aclarar que H.323 y STP es la señalización entre terminales. Mientras que MGCP y SIGTRAN es la señalización en la red IP.

⁵³ MGCP: *Media Gateway Control Protocol*

⁵⁴ SIGTRAN: *Signaling Transport*

⁵⁵ SSP: *Signaling Switching Point*

⁵⁶ SCP: *Signaling Control Point*

⁵⁷ MTP: *Message Transfer Part*

⁵⁸ MGC: *Media Gateway Controller*

⁵⁹ SCTP: *Stream Control Transmission Protocol*

H.323

Es un estándar empleado para el envío de voz, video y datos sobre redes de paquetes y en la siguiente tabla se muestran protocolos con los que trabaja [6]:

Protocolo	Función
H.225	Empaqueta, sincroniza e inicia las llamadas usando mensajes de señalización Q.931 en la RDSI.
H.245	Se usa para la negociación y el manejo de los canales lógicos y el control de las llamadas.
Q.931	Dirige el inicio y fin de las llamadas.
H.235	Realiza la autenticación y funciones de seguridad
H.261	Realiza compresión de en redes en conmutadas.
H.263	Es una mejora del estándar H.261 para la compresión de video.
G.711	Es uno de los códec más comunes para la transmisión de voz en redes telefónicas tradicionales y VoIP. Proporciona una calidad de voz de alta fidelidad utilizando PCM.
RAS	Se encarga de la gestión de registros, admisión y el estado de los terminales en una red H.323. Gestiona la inscripción de terminales, la solicitud de ancho de banda, y la supervisión del estado de la red.
G.723	Estándar de compresión de audio utilizado en aplicaciones de VoIP.
T.120	Sirve para la transmisión de datos en tiempo real donde se ven como documentos y gráficos, durante una conferencia. Incluye varios subprotocolos, como T.122 y T.126.

Tabla 2-3 Protocolos

Una red H.323 está formada por cuatro elementos que son terminales, pasarelas, gatekeepers y unidades de control y que a continuación se expone:

- Teléfonos analógicos, redes GSM, RDSI, IP, ordenadores que permiten conversaciones.
- Los Gateway (pasarelas) permiten la conexión entre las redes de telefonía PSTN con las redes IP. Los datos, formados por señalización SIP y audio en formato RTP, irán encapsulados en la red IP. La voz comprimida en el códec, como pueden ser G.711 O G.729, en la red IP, pasará, gracias a la transcodificación de audio a un formato sin comprimir en el Gateway para enviarse como celdas ATM. El siguiente proceso será la conversión de protocolos que consiste en que la señalización SIP, de IP, se convierte en ISUP que es el protocolo de la red de ATM.
- Los gatekeepers se usan para la gestión y control de llamadas VoIP, control del ancho de banda, conversión de las direcciones IP a numeración telefónica, entre otras. Los teléfonos se registrarán en el gatekeeper con la ayuda del protocolo de señalización RAS (*Registration, Admission, and Status*). De esta manera, se puede se logra identificar a los usuarios y las direcciones IP que tienen asignadas. Así, podrá monitorizar las llamadas que hace el usuario, determinara la mejor ruta por donde debe transitar una llama y autorizar las llamadas basándose en políticas preestablecidas.

- La unidad de control multipunto *MCU*⁶⁰ es un dispositivo o software que ofrece la posibilidad de realizar conferencias, donde más de dos participantes pueden comunicarse simultáneamente en una misma sesión. Las señales de audio pasan por un proceso de digitalización y compresión gracias a los algoritmos tales como el G.711 o G.723. Mientras que la señal de video se trata con H.261 o H.263 y los datos se ajustan al estándar T.120.

2.6.7.3 SIP

Es un protocolo [4], que pertenece a la capa de aplicación, que permite iniciar y terminar las conversaciones entre usuarios que pueden ser de voz o de video. Además, se le considera una alternativa a H.323. Se caracteriza por utilizar al protocolo SDP⁶¹ para matizar las características tales como direcciones y puertos que intervendrán en la comunicación. Es necesario indicar que puede utilizarse juntamente con MGCP o H.248.

Además, existen una serie de servidores que están en la arquitectura SIP y que se utilizan para manejar diferentes aspectos de la señalización y gestión de sesiones [6].

- Servidor *Register*: Maneja las solicitudes de registro de los usuarios SIP y permite a los dispositivos SIP (como teléfonos IP y softphone) registrar su ubicación (dirección IP y puerto) con la red.
- Servidor *Proxy*: Se utiliza cuando un usuario quiere establecer una comunicación con otro usuario.
- Servidor *Redirect*: Este servidor no reenvía las solicitudes directamente, sino que informa al cliente sobre la ubicación alternativa del destinatario con el que quiere contactar.
- Servidor *Location*: Tiene una base de datos de información sobre la ubicación de los usuarios SIP registrados y permite a otros servidores SIP encontrar la dirección IP.

Para el registro y establecimiento de llamadas se pueden usar las aplicaciones XML, CGI en Perl, TCL o C++ cuyas funciones se describen en el Anexo VI.

Las ventajas que presenta SIP frente a H.323 es el establecimiento de llamada en SIP es mucho más simple que H.323. SIP permite una arquitectura descentralizada con nuevas funcionalidades logrando que los usuarios puedan registrarse en diferentes ubicaciones y equipos, implementando servidores proxy y de registro. Por el contrario, H.323 es más centralizado.

2.6.7.4 MGCP

Es un protocolo [4] utilizado en las redes de telefonía IP para gestionar y controlar los *Gateway* de medios que conectan la red de telefonía tradicional (PSTN) con la red IP (voz sobre paquetes).

A pesar de que MGCP controla las conexiones, el transporte real de datos multimedia (voz, video) se realiza con la ayuda del protocolo como RTP.

Es necesario aclarar que el cliente utiliza una entidad lógica central denominada *Call Agent*, que actúa como un servidor que hace funciones de control y gestión de la red, que envía comandos, y el Media Gateway actúa como el servidor que ejecuta estos comandos. Su papel se basa en la señalización y el control de llamadas en el establecimiento, mantenimiento y terminación de sesiones. Interaccionando con los Media Gateway enviando comandos utilizando protocolos como MGCP o H.248/MEGACO. En el Anexo se presenta los comandos que permiten la comunicación entre los MGC y los MG.

⁶⁰ MCU: *Multiconference Control Unit*

⁶¹ SDP: *Session Description Protocol*

Puede darse el caso de que un par de teléfonos estén en pasarelas que se ubiquen en controladores (MGC) distintos. La información intercambiada entre ellos se dará con la ayuda de un protocolo de señalización que sincronice el establecimiento de la llamada entre los usuarios.

2.6.7.5 SIGTRAN

Es un conjunto de protocolos que se usan para transportar la señalización de las redes de telecomunicaciones tradicionales, como es SS7, sobre redes IP. Su objetivo es permitir que las redes IP dirijan la señalización tradicional de la PSTN con alta fiabilidad y eficiencia.

Este estándar posee tres componentes [4]: pasarela de medios (MG), Controlador de pasarelas de medios (MGC) y Pasarela de señalización (SG). En el primer caso, pasarela de medios, se considera el punto de terminación de las llamadas de la red telefónica convencional. Realiza la compresión y empaquetamiento de la voz y entrega los paquetes a la red IP. En el caso inverso, las llamadas desde la red IP a la red telefónica convencional lo que realiza la pasarela es transportar la señalización Q.931 a MGC en llamadas RDSI o como SS7. Para el segundo caso, controlador de pasarelas de medios, se responsabiliza del registro y gestión de los recursos de la MG, de las decisiones de encaminamiento, etc. Además, contiene una base de datos en la que se encuentran las direcciones IP y los números de teléfono en formato E.164. Por último, la pasarela de señalización que está situado en las fronteras de la red IP, intercambia señalización SS7 con la red telefónica creando paquetes de señalización con formato SIGTRAN y se envía por red IP. Estos paquetes tienen destino MGC. Por tanto, el paso de una red telefónica a una red IP es muy compleja ya que la señalización por un canal común es responsabilidad del controlador. Además, SIGTRAN controla la señalización entre las pasarelas (MG, SG) y su controlador. Mientras que MGC controla los terminales de usuario con alguno de los protocolos H.323 o SIP. En el Anexo se puede ver un ejemplo de una llamada desde telefonía tradicional a un teléfono IP y, viceversa.

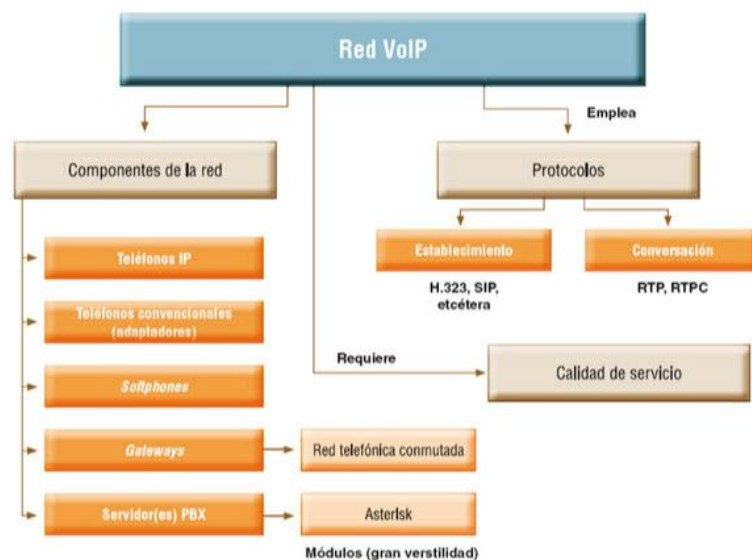


Figura 2-1 Modelo red VoIP (Fuente: Libro infraestructuras de redes de datos y sistemas de telefonía) [7]

2.6.8 Protocolo de seguridad

Es importante tener en cuenta que la seguridad es un elemento esencial tanto para la telefonía tradicional como en la red VoIP. Por ello, se deben proteger las redes donde se envía la información y los equipos que lo forman.

Las llamadas pueden ser intervenidas y ser modificadas mediante técnicas como robo de identidad, redireccionamiento de llamadas haciendo que la integridad esté en riesgo.

Las redes VoIP están expuestas a una pérdida de energía eléctrica que puede provocar que el sistema se caiga y perdiendo su disponibilidad. Además, pueden sufrir ataques por denegación de servicio impidiendo la comunicación de voz o datos.

Los teléfonos, al estar equipados con un software pueden sufrir ataques como se dan en los ordenadores. Por lo que se igualan a los ordenadores a nivel de vulnerabilidad. Respecto al resto de los equipos deben estar configurados adecuadamente. De hecho, al ir añadiendo nuevos equipos será necesario ir actualizando al igual que al resto ya instalados previamente.

En el momento de conectarnos a Internet debemos ser conscientes de que no hay reserva de ancho de banda. Por lo que es posible que al realizar llamadas sobre IP pueda verse afectada por la pérdida de paquetes. Por ello, la única solución es la encriptación para evitar que la captura de las conversaciones. Sin embargo, consume ancho de banda. A pesar de esto último, existen varios tipos de encriptación, lo importante es elegir un algoritmo de encriptación adecuado. Se están obteniendo mejores algoritmos que al instalarse en los routers y conmutadores están reduciendo y la pérdida de paquetes y tiempos obteniendo mejoras en la calidad de servicio.

Las redes de conmutación de paquetes utilizan 8 kbps de ancho de banda para la realización de llamadas de voz con una buena calidad. Para el caso de las redes de conmutación de paquetes, se necesitan 64 kbps.

Respecto a la seguridad para la telefonía tradicional, en concreto SS7, presenta las siguientes funciones:

- MTP: Aparte de otras funciones, se encarga de la autenticidad y el orden de los mensajes.
- SCCP (*Signaling Connection Control Part*): Proporciona direccionamiento y encaminamiento seguro de los mensajes de señalización.
- TCAP: Facilita servicios avanzados como autenticación y autorización a través de consultas de base de datos.
- ISUP: Gestiona la configuración, el mantenimiento y la finalización de llamadas, asegurando que la señalización se transmita de manera segura.

Para el caso de la Red Digital de Servicios Integrados (RDSI o ISDN) presenta:

- Q.931: Protocolo de señalización para el establecimiento y la finalización de conexiones, con capacidades para manejo de errores.
- Q.932: Proporciona control de calidad de servicio y manejo de errores para asegurar la integridad de la señalización.

Para el caso de la seguridad de la telefonía VoIP:

- Se puede utilizar TLS (*Transport Layer Security*) [8] para la encriptación de la señal. De esta forma, se lograría proteger la comunicación contra intercepciones y modificaciones. Por otra parte, está SRTP que encripta el contenido de la comunicación dando confidencialidad e integridad de los datos durante la comunicación.
- También se puede hacer referencia a SCTP⁶² que da más seguridad y confiabilidad que TCP y es usado para el transporte de señalización SS7 sobre IP.
- Otro de los protocolos que pueden ser utilizados es ZRTP⁶³ que encripta la voz de tal manera que no existe un intercambio de claves en la red.

⁶² SCTP: *Stream Control Transmission Protocol*

⁶³ ZRTP: *Z and Real-Time Transport Protocol*

Respecto a los protocolos de autenticación y seguridad:

- Una de las opciones que se puede tomar es RADIUS⁶⁴ “es un protocolo estándar de Internet que proporciona servicios centralizados de gestión de autenticación, contabilidad e IP para los usuarios de acceso remoto en una red de acceso telefónico distribuida.” [9]
- Otra opción más avanzada que la anterior es DIAMETER [10]. Ésta ofrece servicio de autenticación para acceder a redes de tipo 3G, multimedia IP y LTE/4G. En este sentido, decide a qué servicios puede acceder un usuario a qué coste y qué calidad de servicio necesita.
- Además de las dos anteriores está Ipsec que define una serie de reglas para configurar conexiones seguras. En ésta se agrega un cifrado y una autenticación. “Admite varios tipos de cifrado como AES, Triple DES, etc.” [11]

La seguridad en las redes también queda protegida utilizando los siguientes elementos:

- Los firewalls, definido en el punto 2.9.3, es una barrera que se sitúa y protege a la red interna de las amenazas de las redes externas.
- Por otra parte, están los SBC⁶⁵ que no dejan de ser dispositivos que se introducen en la frontera entre las redes de las organizaciones y las redes públicas.
- Además, están los *Intrusion Detection System* (IDS) e *Intrusion Prevention System* (IPS). El primero, detecta accesos no autorizados a una red mediante la monitorización usando una base de datos con los posibles ataques que puede recibir. El segundo, realiza la misma función que el anterior, pero añade una actuación lanzando alarmas, descartando paquetes, realizando desconexiones, etc. Ambos sistemas se integran con cortafuegos.

Los ataques más comunes a los que hace frente los IDS e IPS, son los siguientes:

- *IP Flooding*: Consiste en ataques que buscan inundar el servidor SIP con mensajes SIP para interrumpir el servicio. Para un IDS puede detectar un volumen anormalmente alto de mensajes SIP y generar alertas. Mientras que para IPS puede bloquear automáticamente la dirección IP del atacante para detener el ataque.
- Registro No Autorizado: Son intentos de registrar dispositivos no autorizados en la red para interceptar o redirigir llamadas.
- *Eavesdropping* o escucha clandestina [12]: Es la captura de paquetes RTP para escuchar conversaciones privadas. Un IDS puede analizar flujos RTP para detectar paquetes anómalos. Mientras que un IPS puede aplicar encriptación SRTP para proteger el tráfico de voz.

2.6.9 Protocolo de gestión en telefonía

Los protocolos de gestión en telefonía son esenciales para supervisar, controlar y optimizar las redes de comunicación. Estos protocolos permiten la recopilación de datos de rendimiento, la detección de problemas y la ejecución de acciones correctivas.

Conforme va aumentando la complejidad de VoIP, se hace necesario disponer [6] de herramientas de gestión que permitan medir las prestaciones que ofrece la red en tiempo real e información sobre fallos.

⁶⁴ RADIUS: *Remote Authentication Dial In User Service*

⁶⁵ SBC: *Session Border Controller*

Para responder a esta situación, *RFC 3611* definió una extensión del protocolo *RTCP* denominado *RTCP XR (RTCP Reporting Extension)* donde se incluyó un software adicional [6] en pasarelas y teléfonos IP para que durante el intercambio de mensajes entre estos dispositivos los equipos de gestión de red puedan capturarlos, interpretarlo, analizarlos y tomar las medidas necesarias.

Los *mensajes RTCP XP* contienen información sobre las decisiones que se deben tomar [6]:

- Pérdida, el retardo y mediciones sobre la voz, nivel de la señal de ruido o pérdida del eco.
- Calidad de la voz.
- Configuración de los buffers de supresión de *jitter*, latencia y de los algoritmos de recuperación frente a las pérdidas en los puntos finales.
- Realiza un diagnóstico para determinar si existe una disminución de la calidad debido a problemas de configuración de los puntos finales o es por causa de un mal funcionamiento de la red.
- Tomar las acciones correctivas sobre los equipos de gestión en función de los informes.

2.6.10 Calidad de la voz

La calidad de servicio (*Quality of Service*) es aplicable al usuario o de la red. Para un usuario es cómo se escuchan los interlocutores en una conversación telefónica. Mientras que, para la red, son los parámetros como retardo, *jitter*, ancho de banda y pérdidas.

Tanto si se utilizan redes de conmutación de circuitos o de paquetes ambas deben ofrecer una calidad de servicio similar.

En la telefonía tradicional se establecen conversaciones por pares de usuarios en canales dedicados. La calidad de esas conversaciones se mide con un ancho de banda es idóneo. Cuando ya estamos en la telefonía IP y se da el aumento del número de paquetes que circulan por la red, supone que la calidad de la voz se vea afectada. La calidad de servicio de la voz que está regulada por la norma E.420.

La tasa de conectividad es la probabilidad por la que una red pueda realizar una llamada. Mientras que la inteligibilidad de la voz es la capacidad por la que cada interlocutor sea capaz de entender las palabras de la otra persona con la que está hablando. Aquí aparece un nuevo concepto que es la claridad de la voz que depende de la distorsión introducida por la red durante la conversación. En las conversaciones cuyas frecuencias se encuentren entre los 200 y 800 Hz serán más comprensibles, mientras que para el intervalo de 1000 a 1200 Hz son de menor calidad. Finalmente, la codificación de la voz convierte las señales de voz analógicas en digitales que son transmitidos. Es necesario tener en cuenta que la tasa de error es la proporción de bits que se reciben incorrectamente tomando en consideración el número total de bits transmitidos. Una muestra con un valor de alta tasa binaria implica una mejor calidad e inteligibilidad. Por el contrario, una baja tasa binaria afecta negativamente la calidad e inteligibilidad. Una baja tasa de error permite recibir la señal de voz casi sin errores. Mientras que una alta tasa de error introduce distorsiones y pérdidas de información en la señal de voz.

A continuación, se van a describir con más profundidad los conceptos de disponibilidad, *jitter*, pérdidas, eco, ancho de banda y ruido.

La disponibilidad [3] es la capacidad de que un sistema telefónico esté operativo y accesible cuando se necesita en tanto por ciento. La telefonía basada en RTPC o la RDSI ofrece una disponibilidad muy elevada que puede estimarse en un 99,99%. Sin embargo, para las redes de datos, este valor, no alcanza estos niveles tan elevados. Para todo sistema que se quiera diseñar debe tener en cuenta el tiempo que debe estar operativo el sistema teniendo en cuenta los fallos inesperados con el coste asociado. Los elementos más críticos, para VoIP, son los servidores, las pasarelas y los

terminales de usuario. En el caso de que exista un error en uno de los sistemas, otro similar asumirá la carga de trabajo manteniendo el servicio disponible. Por lo tanto, cualquier parte del sistema que resulte crítica será necesario que esté replicado. El hecho de pensar que todo debe estar replicado es económica inviable por ello, la mejor solución es replicar lo que se considere como elemento crítico como son los servidores del control de llamadas, la señalización y las pasarelas. Es necesario indicar que existen ciertos casos en los que cuando la red de conmutación de paquetes no es capaz de dar el servicio adecuado, por lo que se utiliza la red RTPC o RDSI para encaminar las llamadas. A esto se le denomina encaminamiento *backup*.

Otro sistema que nos puede ayudar para la falta de servicio por una caída de los sistemas de alimentación es utilizar sistemas de alimentación ininterrumpida (SAI). Estos sistemas, de pequeña potencia, constan de una batería de 220 V/50Hz para alimentar al equipo durante un cierto tiempo. Este tiempo permitirá cerrar aplicaciones y guardar la información para evitar su pérdida. Existen otros que su funcionamiento se basa en generadores con motores de gasoil (grupo electrógeno) aumentando la autonomía del sistema.

Respecto al *jitter* se puede afirmar que en redes IP, al contrario que la conmutación de circuitos no es posible que todos los paquetes sigan el mismo camino. Esto implica que cada paquete llegará a su destino pasando por un número diferente de nodos que conllevará una variación del retardo de cada uno de ellos. A esta variación de retardo se denomina *jitter*. Para minimizar estas variaciones se utilizan los buffers de supervisión de *jitter*. Este método consiste en almacenar los paquetes que han llegado fuera de secuencia durante un cierto tiempo para reordenarlos correctamente. De hecho, cuanto mayor sea el *jitter* mayor tendrá que ser el tamaño del buffer de supresión de jitter para mantener la calidad. Esta supresión del *jitter* supone un incremento en el retardo por lo que es necesario encontrar una solución de compromiso entre el tamaño del buffer, el retardo y las pérdidas. En el caso de las pérdidas de paquetes, es necesario aclarar que se producen en los nodos como consecuencia de la congestión en los nodos. Esto implica una disminución de la calidad de la voz. Esta disminución de calidad aumenta al incrementarse la compresión del códec. ¿Cómo se puede solucionar? Este problema se puede solucionar mejorando la arquitectura de la red, es decir, instalando líneas y routers de mayor capacidad. Sin embargo, no es una solución definitiva dado que si se produce un aumento del tráfico volverá a incrementarse los retrasos. Existen grupos de técnicas para atenuar los retardos que son la corrección de errores *FEC (Forward Error Control)*, distribución de errores o la recuperación de errores (*Packet Loss Concealment*).

Relativo a la **corrección de errores** se incluye información de redundancia para recuperar el valor de un paquete perdido. El inconveniente es el retardo que, para decodificar un paquete, es necesario apoyarse en otros paquetes.

Si tenemos en cuenta la distribución de errores, que consiste en aleatorizar las pérdidas para dispersar sus efectos, es decir, es una estrategia para mejorar la robustez y la calidad de las transmisiones haciendo que la pérdida de paquetes no sea tan apreciable. El inconveniente que puede suponer un retardo puede suponer aumentar el gasto de ancho de banda.

Finalmente, la recuperación de errores que no deja de ser una técnica que consiste en sustituir un paquete por otro. De esta manera, intenta ocultar o compensar las pérdidas para que sean menos perceptibles para el usuario final. Existen una serie de técnicas como son la repetición de paquetes anteriores, interpolación, sustitución en silencio o algoritmos de predicción que cuanto más compleja sea la técnica utilizada mayor será el retardo añadido. Se suelen utilizar en servicios de streaming como Spotify, Netflix, Youtube.

Respecto al retardo se puede indicar que es el tiempo invertido por la señal de voz desde el origen al destino. Además, existen dos elementos que influyen sobre el retardo que son el retardo máximo aceptable y las fuentes que provocan el retardo. Para el retardo máximo aceptable se puede afirmar que es el umbral por encima del que la calidad de la voz es inaceptable. Según G.144 de ITU-T [13] el

umbral se encuentra en el intervalo 150 ms y 200 ms. Para el caso de comunicaciones por satélite se puede aceptar un retardo en torno a 400ms.

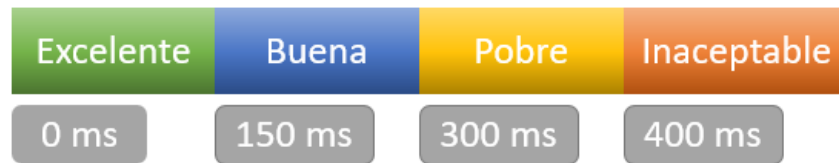


Figura 2-2 Calidad de la voz (imagen propia)

Respecto a las fuentes que lo provocan hay que considerar los siguientes:

- Digitalización de la voz al pasar de analógico a digital.
- Los códecs realizan la compresión que reduce el ancho de banda.
- Empaquetar las muestras de voz antes de su transmisión.
- Los retardos provocados dependen del tipo de códec utilizado.
- Los paquetes llegan a la pasarela y pasarán un tiempo en ésta, es decir, el retardo de serialización y se contará cada vez que el paquete atravesase un dispositivo *store-and-forward* como puede ser un router o un switch.
- Los paquetes llegarán hasta su destino en un cierto tiempo. Depende de las variables fija y variable. La variable fija corresponde al tiempo de propagación, es decir, es el tiempo que tarda la señal en alcanzar el destino. La parte variable son los encolados de los paquetes en los nodos que dependen de la carga de los nodos y su capacidad. El retardo en la red puede estar comprendido entre los 70 ms y 100 ms.

Ahora entramos en la parte del eco que ocurre tanto en las redes telefónicas tradicionales y la voz sobre paquetes. ¿Cuándo ocurre? Cuando el emisor escucha su voz junto a la voz del otro interlocutor. Existen varias causas que generan el eco como son el acoplamiento entre el micrófono y el auricular del teléfono o el eco eléctrico debido a la desadaptación de impedancias en el receptor. Para el caso del acoplamiento se puede solventar utilizando teléfonos de mayor calidad. Es necesario aclarar que en las redes telefónicas donde se utilizan dos pares de hilos, uno para transmisión y otro para recepción, que conectan los teléfonos de dos usuarios. La bobina híbrida se utiliza para conectar el teléfono del usuario con la central telefónica asociada realizándose la conversión de 2 hilos a 4 hilos que provoca que la señal incidente acompañe a la voz que llega al otro extremo dando lugar al eco. Es necesario indicar que es inevitable e imperceptible. En el caso de darse las dos siguientes circunstancias, es decir, una amplitud de la señal muy baja y el tiempo de retardo menor que 50 ms, entonces el eco quedará por debajo de la voz del emisor.

Para calcular el valor de la señal reflejada se utiliza la ecuación que se denomina *Eco Return Loss* (ERL) y debe ser mayor que 55dB. A continuación, se expone la citada ecuación [4]:

$$ERL = A - B$$

siendo A la amplitud de la señal de la fuente y B la amplitud del eco.

Es necesario indicar que el eco en redes de voz sobre paquetes se produce cuando se desea comunicar con un teléfono que se encuentra en una red analógica, denominado circuitos de conmutación, y no en digitales. Es decir, no existe el eco en las redes de datos o IP. Es importante aclarar que la voz sobre paquetes que interaccionan con teléfonos convencionales y PBX se produce una cierta cantidad de eco que habrá que limitar en la medida de lo posible. ¿Cómo se previene lo anterior? Utilizando canceladores de eco que realiza un filtrado adaptativo de la señal recibida, que incluye la voz y el eco, que valora el valor del eco e intenta anularlo. Por lo que se deben seguir las

recomendaciones de la ITU-T para la cancelación del eco empleando filtros adaptativos según las recomendaciones G.165 y G.168.

Para el caso del ancho de banda (BW , *bandwidth*) de una red es la cantidad máxima de información que la red capaz de transportar por unidad de tiempo. La ecuación [4] que refleja esta definición es la siguiente:

$$BW = \frac{BW_{VOZ} + BW_{VIDEO} + BW_{DATOS}}{0.75}$$

Se deja un 25% de margen para hacer frente a picos de tráfico y con ello, al ofrecer un ancho de banda considerable disminuye la probabilidad de *jitter*. Esto no quiere decir que no aparezca este problema.

Relativo al ancho de banda, se pueden tener dos escenarios. Una comunicación de voz sin comprimir o comprimida. Para la primera de ellas, sin comprimir, supone un consumo de 64kbps. Para el segundo caso, se aumenta la eficiencia de utilización del ancho de banda al aumentar el número de comunicaciones. Y, aunque no haya una correspondencia entre el ancho de banda y la calidad de la voz, lo que es seguro que cuanto mayor sea la compresión, menor es la calidad de la voz transmitida al sufrir problemas de retardo y a pérdidas.

Existe un mecanismo denominado supresión de silencios VAD que es utilizado para la compresión del ancho de banda. Este tiene en consideración que en torno al 60% de las conversaciones ocupan silencios. Por tanto, se aprovechan estos instantes para introducir tráfico de otras llamadas telefónicas. Con esto se logra reducir en un 60% en flujo de paquetes. El inconveniente de este método provoca el efecto *clipping*, es decir, la voz de la persona que está hablando parece que está recortada. Además, provoca pérdidas, *jitter* y latencia.

Finalmente, el ruido, que son los factores que degradan la calidad de la transmisión de información entre dos o más interlocutores. En la telefonía IP pueden existir distintas fuentes de ruido; se resumen en la siguiente Figura 2-3 [7] y pueden estar organizadas según los niveles de la red en los que se producen.

El ruido de fondo es una fuente de ruido común a la telefonía tradicional y a la telefonía IP. Cuando en un ambiente ruidoso colocamos nuestra mano alrededor del micrófono del teléfono, estamos efectuando un método para la atenuación del ruido. Existen también métodos electrónicos para hacerlo, que suelen ser comunes a la telefonía convencional y a la telefonía IP. Por otro lado, la saturación de la señal se produce cuando el nivel de la señal sonora es superior al que la onda portadora puede modular. En las fases de amplificación o de codificación de la señal, esta puede distorsionarse, perdiendo parte de su información. En la red pueden producirse pérdidas de paquetes, debido a los errores en alguno de los medios de transmisión o a la congestión de la red. Mientras que, en la capa física, las interferencias procedentes de diversas fuentes electromagnéticas son una importante causa de ruido.

Aplicación	Ruido de fondo		Saturación	
Transporte	Distorsión de la amplificación	Distorsión de la codificación		
Red		Pérdida de paquetes	Jitter	Retardos
Enlace de datos	Atenuación de la señal			
Física		Interferencias eléctricas (estáticas)		

Figura 2-3 Fuentes de ruido (Fuente: Libro infraestructuras de redes de datos y sistemas de telefonía) [7]

Dentro de la calidad del servicio (*Quality of Service* o *QoS*) existen un conjunto de estándares [7] para la reserva de ancho de banda en la red y el orden de prioridad de los paquetes. Estos estándares se elegirán en función de una serie de reglas tales como:

- Si el tráfico de red es principalmente de datos, y solo se transmite un treinta por ciento de voz o menos, puede usarse un sistema de priorización de paquetes como 802.1p.
- Para redes extensas (centenares de nodos de voz) y con un tráfico medio, puede usarse *DiffServ*.
- Para redes muy extensas (miles de nodos de voz) o con una gran densidad de tráfico, es preferible emplear RSVP.

En la tabla 2-4 se citan el nombre y el ámbito de aplicación de los estándares [14] más relevantes.

Nombre	Aplicación
802.1p	Ethernet con un solo segmento
802.1p VLAN	Redes Ethernet privadas
DiffServ	Redes compuestas de varios segmentos
RSVP	Redes compuestas de varios segmentos con un ancho de banda limitado
MPLS	Redes de alto rendimiento

Tabla 2-4 Estándares

2.6.11 Técnicas de evaluación de la calidad de la voz

Existe una variedad de técnicas como el modelado perceptual de la voz, ITU-T P800, P861 y *modelo E* que determinan la calidad de la voz.

El tipo ITU-T. *P800 (Escala MOS, Mean Opinion Score)* es un mecanismo tradicional que recibe el nombre de *Test ACR (Absolute Category Rating [15])*. Se reúne a una serie de usuarios para que opinen de la calidad de la voz en un determinado sistema de transmisión de la voz. En este caso, no hay una comparación con una señal de referencia. La escala de MOS tiene un valor mínimo de 1 y máximo de 5 que a continuación se expone [4].

- 5: Excelente (sin distorsión perceptible)
- 4: Bueno (distorsión perceptible pero no molesta)
- 3: Aceptable (distorsión perceptible y ligeramente molesta)
- 2: Malo (distorsión perceptible y molesta)

- 1: Inaceptable (distorsión severa)

El Modelado perceptual de la voz es una técnica que introduce una señal de referencia y de la señal de entrada que es la que se evalúa. De ambas, se proporciona una representación paramétrica.

Relativo a ITU-T. P861 [16] se puede afirmar que es un análisis objetivo de los códec de voz basado en un algoritmo denominado *PSQM*⁶⁶. *PSQM* compara una señal de referencia (original) con una señal degradada (procesada). Este proceso se muestra en el Anexo .

El Modelo E es un modelo de aproximación matemática que evalúa las características de la transmisión de la red de voz sobre paquetes tomando en cuenta la función de *retardo*, el *jitter*, las *pérdidas* y otras características de la red.

Este modelo está especificado en la recomendación de la ITU-T G.107 [17] y utiliza la siguiente fórmula [4]:

$$R = R_0 - I_s - I_d - I_e + A$$

Donde:

- R: Factor de transmisión.
 - R0 Factores básicos de la calidad de la voz, incluyendo el ruido de fondo. Relación señal ruido.
 - Is: Factores que afectan la calidad de la señal, como la distorsión de la señal de voz, efectos de filtrado y otras degradaciones de la señal.
 - Id: Factores de retardos (delay) que afectan la interacción conversacional.
 - Ie: Factores de equipo, que incluyen la compresión y otros efectos de la transmisión digital.
 - A: Factores de ventaja. Representa la mejora en la calidad considerando que los usuarios son más tolerantes a la degradación de los teléfonos móviles debido a la ventaja que supone la movilidad.

Se llega a las siguientes conclusiones:

- El retardo (Id) es uno de los factores más importantes cuando se estudia la calidad de la voz.
- En torno a los 175 ms un aumento del retardo supone una disminución drástica de la calidad de la voz.
- Cuanto mayor sea el valor de Ie mayor es la disminución de la calidad.
- La relación entre la escala de MOS y el factor de transmisión R es [4]:

$$MOS = \begin{cases} 1 & R < 0 \\ 1 + 0,035 * R + 7 * R * (R - 60) * (100 - R) * 10^{-6} & 0 < R < 100 \\ 4,5 & R > 100 \end{cases}$$

2.6.12 Calidad de servicio de una red

La calidad de servicio de una red se puede definir como la capacidad de transportar la información desde una fuente a otra.

El principal problema para diseñar una red es que no todos los componentes de las fuentes de tráfico, como puede ser el teléfono, entre otros, muestran el mismo comportamiento. Estos componentes o se pueden distinguir entre; fuentes de tráfico de tiempo real y fuentes de tráfico de

⁶⁶ PSQM: *Perceptual Speech Quality Measure*

tiempo no real [4]. Las primeras se caracterizan por tener bajo retardo, baja tolerancia al *jitter*, ancho de banda apropiado y *tasa de pérdidas baja*. Respecto a las segundas, se valora una baja tasa de pérdidas sobre el resto de los parámetros, siendo lo más importante, la veracidad de la información y no el tiempo en que tarde en llegar al destino.

La calidad de servicio se puede ver desde distintos puntos de vista. Un punto de vista puede ser ofrecer unas prestaciones en función de cada fuente generadora de tráfico. En este caso, primero se clasificará el tráfico gestionando el ancho de banda, controlando la congestión dando prioridades a las fuentes. Otro punto de vista es fragmentar el tráfico, gestionar la congestión, adaptación del tráfico y control de admisión.

Es necesario indicar que cada nodo es distinto, es decir, no se pueden aplicar todas las herramientas a cada uno de ellos. De tal manera que, para *clasificar el tráfico* o control de admisión se realizan en los *bordes de la red*. Mientras que las *técnicas de congestión* se dan en los routers del *backbone*.

2.7 Tráfico de red

2.7.1 Marcado y clasificación del tráfico de red

Para cumplir con la *calidad de servicio* es necesario introducir un servicio a cada tipo de tráfico. Para ello, se utilizan los mecanismos de *marcado y clasificación*.

El *marcado* está formado por una serie de herramientas, algoritmos, dentro del campo del paquete ya sea en la etiqueta, celda o en la trama. Una vez haya sido marcado por un nodo de la red, el resto de los nodos ya no tendrá la necesidad de analizarlos. Mientras que la *clasificación* consiste en ordenar los paquetes en función del tipo de tráfico. Una vez realizado esto, procede a aplicarles las políticas de servicio que corresponda.

Las herramientas de *clasificación* trabajan por capas del modelo de referencia OSI de la ISO [6]:

Nivel	Observaciones
Nivel 7	Identificadores de aplicación o URL
Nivel 4	Puertos TCP o UDP
Nivel 3	IPToS, DSCP,
Nivel 2	Dirección MAC, CoS, VLAN ID,
Nivel 1	Interfaz física, subinterfaz, PVC o puerto

Tabla 2-5 Clasificación del tráfico de red en función del nivel.

Las políticas de tráfico actúan sobre los paquetes que están identificados de forma correcta. A continuación, se va a describir qué son el etiquetado de las tramas VLAN e IP ToS.

Dentro del *etiquetado de las tramas* existe la opción de la separación del tráfico. Para ello, lo que se hace es corresponder a cada tráfico una o varias VLAN, esto implica la separación del tráfico. Este método consiste en agrupar *host* de diferentes segmentos de una misma LAN. Esto permitirá que los *hosts* puedan comunicarse entre sí como si estuvieran conectados al mismo sector físico.

Los inconvenientes que se puede dar es que al compartir el mismo medio de transmisión puede provocar problemas de falta de ancho de banda por sobrecarga. Como solución, se puede limitar los segmentos que puedan ofrecer los tráficos.

Una forma de aclarar las distribuciones de tráfico [6] como *multicast*, *broadcast* y *unicast* se puede afirmar que *multicast* permite la distribución del tráfico de red simultáneamente. Por ejemplo, realizar

una sesión de videoconferencia. Mientras que *broadcast* difunde información a todos los segmentos de la red incluso aquellos donde no hay usuarios como televisión, radio, publicidad por correo electrónico. Finalmente, *unicast* consiste en enviar datos a cada usuario interesados. Estos reciben una copia enviada por el emisor como puede ser la consulta individual de una página web.

Es necesario explicar que una *red ethernet* se pueden distinguir los *dominios de colisión* y *dominios broadcast*. Un *dominio de colisión* es una serie de estaciones que compiten por el control del medio de transmisión. Todas ellas están unidas al mismo *hub* o *repetidor*. Si aumentamos el número de estaciones implica una disminución de la prestación de la red al aumentar la probabilidad que varias estaciones soliciten el control de la transmisión al mismo tiempo. Para solventar este problema se puede acudir a *conmutadores LAN*, es decir, crear redes locales conmutadas. Un conmutador no deja de ser un reencaminador de tramas que recibe por un puerto de entrada que reenvía por uno o más puertos de salida utilizando el algoritmo *Spanning Tree*. De tal forma que, cada uno de los puertos sirven para segmentar la red conectando cada una de las estaciones a un hub y éste último al puerto de conmutador. Para el segundo caso, los *dominios broadcast* están por toda la subred delimitados por los routers que filtran estos tipos de tráfico. Pueden ser varias redes lógicas independientes cada una de ellas con sus dispositivos conectados al mismo switch de su red correspondiente. De tal forma que si un dispositivo envía un mensaje de broadcast al resto de dispositivos lo recibirán.

La alternativa a lo anterior son las VLAN o *Virtual LAN*. Éstas se definen por software, es decir, los dominios broadcast ofrecen una gran flexibilidad independientemente de la topología de la red. Además, implica seguridad al aislar el tráfico crítico y define niveles de acceso en función a la pertenencia a una VLAN concreta generando un mayor rendimiento de la red reduciendo el retardo de las comunicaciones. Puede darse el caso de que en una red existan varias redes VLAN. Para esta situación, existen un mecanismo que permite marcar las tramas que distinguen a qué VLAN pertenece cada trama para que el conmutador no tiene duda para reenviarla por los puertos de salida. Para cumplir todo esto, es necesario diferenciar dos tipos de enlaces de un conmutador: *las conexiones de enlace* que le conectan directamente a un hub o host y las *conexiones troncales* entre conmutadores.

Para etiquetar las tramas se realiza una ampliación de la trama MAC añadiendo nuevos campos. Esto está regulado por el estándar IEEE 802.1Q que indica la prioridad que se le da a cada trama y que viene determinado por el estándar IEEE 802.1p. Es necesario aclarar que IEEE 802.1p es un estándar de nivel 2 que marca y prioriza el tráfico de red a nivel MAC. Además, utiliza 3 bits del campo UP (User Priority).

La utilización del estándar *IEEE 802 1p* al implantar VLAN, ofrece una administración sencilla entre estaciones que se comunican simulando que están en la misma red y la restricción de tráfico en VLAN. El inconveniente es aumento de tráfico que se puede producir.

Una vez explicado *etiquetado de las tramas VLAN* pasamos a IP ToS. Tal y como se describe en la RFC 1349 en la cabecera de los paquetes IPv4 existen tres bits de precedencia utilizados para indicar la prioridad de usuario. Estos valores son procesados por los conmutadores y los routers de nivel 3. Existen ocho valores de los cuales se utiliza el valor 5 para la voz y el 4 para la videoconferencia y streaming de video, el valor 3 para la señalización de llamada, el 1 y el 2 para todas las aplicaciones de datos.

2.7.2 Técnicas LST⁶⁷

Las técnicas LST son un conjunto de herramientas y técnicas específicas diseñadas para gestionar, monitorear y optimizar dos extremos de un enlace punto a punto a través de una red WAN y que trabaja a nivel 2 y 3 de la pila de protocolos OSI de la ISO.

Se puede indicar que existen dos tipos de técnicas que son la compresión de cabeceras y la fragmentación y el entrelazado. En la primera, su objetivo es disminuir la cabeza del paquete IP. De

⁶⁷ LST: Link Specific Tools

hecho, la voz que está dentro de los paquetes es pequeños comparados las cabeceras RTP, UDP o IP aumentando el ancho de banda provocando que disminuya la eficiencia. Respecto a la fragmentación y el entrelazado de paquetes se utiliza para minimizar el retardo en los enlaces WAN de baja velocidad.

A continuación, se va a describir con más detalles que son la compresión de cabeceras y la fragmentación y el entrelazado.

Reducir las cabeceras puede verse desde dos puntos de vista. Un primer punto de vista es que se elimina todas aquellas informaciones redundantes. Para el segundo, se suprime ciertos campos para reducir el tamaño. Es una técnica que se aplica en redes donde el ancho de banda es limitado o el coste sea elevado ya sean en redes inalámbricas o móviles.

Esta compresión de tipo *cRTP* es para los enlaces de baja velocidad. Además, *cRTP* aprovecha que existen muy pocos campos que de la cabecera que varíen de un paquete a otro. Por ello, *cRTP* evita el envío de los campos de cabecera que no cambien y en su lugar envía una referencia que el otro extremo utilizará para localizar en memoria el valor de los campos no enviados.

Por otra parte, la fragmentación y entrelazado del tráfico es el tiempo que tarda cada uno de los nodos para el encolado lo que implica un aumento en el retardo de los paquetes. Independientemente del tipo de paquete que reciba el router, éste lo va procesando. De hecho, en el caso de que un paquete no prioritario llegar al router antes que un paquete con la categoría de prioritario, el primero deberá esperar hasta que finalice el procesamiento del prioritario. Esto es un inconveniente en el caso de paquetes no prioritarios con un tamaño grande.

Para solucionarlo, se podría determinar un tiempo de espera razonable, es decir, es lo que se conoce por fragmentación y entrelazado del tráfico TFI⁶⁸ [6]. El tamaño adecuado de los paquetes, en la fragmentación, depende del ancho de banda del enlace de salida (BW) y del jitter máximo permitido ($\delta_{m\acute{a}x}$). [4]

$$L = \delta_{m\acute{a}x} \cdot BW$$

2.7.3 Control de congestión

Se puede definir que la congestión se produce cuando los nodos no son capaces de asumir una mayor cantidad de paquetes. Esto implica que las aplicaciones de red ofrezcan soluciones al descartar paquetes sean descartados ofreciendo soluciones, lo que supone un aumento en el tiempo de servicio y una disminución en el rendimiento de la red.

Para reducir la congestión se utilizan las estrategias de encolado y planificación. El encolado consiste en que los nodos disponen de zonas de memoria donde se guardan los paquetes listos para ser reenviados. Serán enviados primero los que tengan mayor prioridad. Mientras que la planificación determina qué paquete será el próximo en enviar y el siguiente en espera para sucederle. A esto se le denomina disciplina de servicio del nodo.

Vamos a empezar con FIFO⁶⁹. De hecho, se la puede considerar como la más sencilla, en la que los paquetes entrantes se retransmiten en el mismo orden en que llegan. Todo aquel paquete que llegue sin que hubiese sitio en la cola, se descarta. Es el esquema que suele darse en muchos routers. FIFO no es adecuado para aplicaciones multimedia al no ser capaz de diferenciar entre diferentes tipos de tráfico.

A continuación, está PQ que consiste en utilizar colas de distinta prioridad y éstas se irán vaciando por orden decreciente de prioridad. El inconveniente que presenta es generar mucho tráfico en la cola

⁶⁸ TFI: *Traffic Fragmentation and Interleaving*

⁶⁹ FIFO: *First In, First Out*

de mayor prioridad y los de baja prioridad no se retransmitan generándose el fenómeno conocido como *traffic starvation*. Esto se evita utilizando el CQ que es el caso que viene a continuación.

CQ consiste en que en función del tipo de tráfico se le asigna un tipo de cola con un umbral mínimo de paquetes. Se establecen ciclos donde se enviarán estos paquetes. Así se garantiza un mínimo de envíos con la garantía de ancho de banda, que será estático, y un retardo aceptable.

WRR se puede utilizar para la gestión de tráfico de red y distribución de recursos en varios escenarios. En WRR la distribución de llamadas en gateways en VoIP, como los gateways se utilizan para convertir el tráfico de voz entre redes IP y redes tradicionales (PSTN), de acuerdo con su capacidad. Cuanto mayor sea la capacidad de los gateways mayor cantidad de llamadas podrá procesar, lo que asegura una distribución equitativa basada en su capacidad de procesamiento.

Como en telefonía existe una limitación en el ancho de banda, WRR asignará el ancho de banda teniendo en cuenta la prioridad asignada de forma justa.

En el caso de los SBCs, en concreto los WRR, pueden distribuir el tráfico de VoIP. Un SBC con más recursos (ancho de banda o capacidad de procesamiento) recibiría un mayor porcentaje del tráfico, mejorando la eficiencia y reduciendo la congestión.

Si nos centramos en los servidores SIP se emplea WRR para equilibrar la carga entre varios servidores de tipo SIP. Cuanto mayor sea la capacidad de un servidor mayor cantidad de solicitudes de configuración de llamadas podrá realizar.

WFQ realiza una calidad de servicio (QoS), dentro de los sistemas de telefonía VoIP, basada en el tráfico de la red, priorizando el tráfico de voz donde se obtenga los valores de latencia y jitter. WFQ asigna mayor peso a la voz que al tráfico web o correo electrónico. De esta manera, la VoIP y las videoconferencias dispongan el ancho de banda adecuado manteniendo la calidad. Además, minimiza el jitter y la latencia. En el Anexo X se puede ver un ejemplo.

CBWFQ proviene de *Weighted Fair Queueing* (WFQ) y el administrador de la red asignará prioridades y la gestión del ancho de banda para asegurar la calidad de servicio (QoS).

El administrador definirá una serie de reglas que afecte al tráfico clasificándolo por clases. Por ejemplo, se pueden crear clases separadas para tráfico de voz, video y tráfico de datos general.

Además, a cada clase se le asigna un ancho de banda mínimo garantizado y un peso. Este peso determina la prioridad relativa en la asignación del ancho de banda restante.

Otro aspecto por destacar es que los paquetes de cada clase se encolan en colas separadas y se programan para su transmisión según sus pesos y el ancho de banda garantizado. Esto asegura que las clases con mayor prioridad reciban un servicio preferente. En el Anexo se puede ver un ejemplo.

LLQ es una técnica para la gestión del tráfico en redes que asegura el tráfico de alta prioridad, como es la voz, basándose en CBWFQ y *cola de prioridad (PQ)* intentado obtener una latencia mínima. Hay que aclarar que, PQ está orientado para el tráfico en tiempo real, mientras que CBWFQ es idóneo para los datos. En el momento de que se tengan que enviar paquetes de tipo PQ será con una prioridad máxima.

Aquí surge el concepto de *Starvation* donde una o más colas de tráfico no reciben suficiente ancho de banda porque otras colas tienen prioridad. Esto implica que ciertos tipos de tráfico sufran un valor alto de latencia, pérdida de paquetes, o incluso falta total de transmisión. Para evitar Starvation será necesario asignar al grupo PQ un ancho de banda máximo, y la suma de ancho de banda de todas las aplicaciones no sobrepase un cierto valor umbral del ancho de banda disponible.

La cola de prioridad, de transmisión, se procesa antes que las demás. El tráfico en esta cola se transmite inmediatamente, sin esperar, asegurando la menor latencia posible. Mientras que el tráfico que no se considera crítico se clasifica y se encola utilizando CBWFQ, donde cada clase recibe un peso y un ancho de banda garantizado. Esto asegura que incluso el tráfico no prioritario se gestione de

manera justa y eficiente. Además, LLQ es el mecanismo de planificación más recomendado para aplicaciones VoIP y videoconferencia.

2.7.4 Gestión de ancho de banda

Para implantar una red es necesario determinar el tamaño del ancho de banda y, en caso de querer un aumento se ha de asumir que habrá un incremento del coste económico. Por ello, la elección del tamaño del ancho de banda debe ser lo más eficiente.

A continuación, vamos a ver con mayor detalle *Integrated Services* (IntServ), DiffServ y MPLS.

En el caso de *Integrated Services* (IntServ) se reservan recursos, como el ancho de banda, que en el camino por donde discurren los paquetes desde el origen y el destino utiliza el protocolo RSVP que señala y reserva la *calidad de servicio* (QoS) para cada flujo.

Es necesario añadir que, dado que RSVP es un protocolo *unidireccional* y, en caso de ser necesario aplicar la bidireccionalidad entre ambos extremos se deberá iniciar una reserva. En éste, se intercambian mensajes PATH y mensajes RESV. Los mensajes PATH son enviados del origen al destino y solicita la reserva de recursos en todos y cada uno de los nodos de la red que atraviesa el flujo de tráfico. Mientras que para RESV viajan en sentido inverso para confirmarlo o denegarlo.

RSVP determina dos tipos de servicio: servicio de carga controlada y servicio de carga garantizada. La primera proporciona al flujo una calidad de servicio de tipo *Soft QoS*, con mecanismos de control, que garantiza los recursos incluso aunque los nodos estén sobrecargados. El cliente debe proporcionar una estimación del tráfico que generará incluyéndolo en los mensajes PATH que envíe. En el caso de que se dé un servicio de carga garantizada, se determinará una calidad de servicio (QoS) requerida en ancho de banda, retardo extremo a extremo, etc., y que el camino de los nodos por donde transcurre el flujo sea capaz de soportar la QoS solicitada.

El problema de RSVP es su escalabilidad, es decir, todos los routers deben mantener información de estados de todos los flujos que lo atraviesan. Además, las reservas que se dan son del tipo *soft-state* con actualizaciones continuas en el tiempo. Esto último supone una sobrecarga en el tráfico de señalización.

En el caso de DiffServ, dependiendo del tipo de tráfico y las políticas establecidas, reduce la carga de los nodos en la red. Es necesario indicar que la diferenciación de los servicios se logra definiendo comportamientos específicos para cada clase de tráfico en cada nodo de la red que se denomina PHB (*Per Hop Behaviour*). Es decir, PHB es el comportamiento que se espera de un paquete cuando pasa por cada nodo (router o switch) en la red. Básicamente, determina cómo se trata el tráfico en cada salto.

Este modelo de DiffServ reduce la carga de procesamiento en los nodos de la red y no presenta problemas de escalabilidad que sí presenta IntServ. Además, DiffServ se divide en dominios con PHB idénticos. Los dominios se componen de subredes y el administrador designa recursos mediante el servicio SLA (*Service Level Agreement*). Hay que recordar que un servicio SLA es un contrato entre un proveedor de servicio y un cliente. En éste, se define los niveles de calidad de servicio, disponibilidad, rendimiento, tiempo de respuesta entre otros.

Existe un campo, que está situado en ToS⁷⁰ dentro del encabezado del paquete IP denominado DSCP (*DiffServ Code Point*), de tamaño 6 bits que indica la clase de servicio que se aplica al paquete.

Es necesario añadir que los nodos que pertenecen al dominio PHB se distinguen en dos clases: nodos extremos y nodos internos. Los nodos externos se caracterizan porque los paquetes que entran en la red son marcados por estos nodos. Una vez que llegan a los nodos internos seleccionan el PHB definido para cada flujo de datos. Es necesario indicar que los nodos externos, que pueden ser de

⁷⁰ ToS: *Type of Service*

entrada o de salida, deben garantizar que el tráfico que entre cumpla con el contrato TCA (Traffic Conditioning Agreement), donde se define las reglas y políticas para cumplir con la calidad de servicio (QoS) con otros dominios como es *DiffServ*. El tráfico entrante se clasifica en clases en función de las políticas definidas por la red y esto se hace en los bordes de la red, donde se conecta con otras redes. Las políticas de red, como el control de acceso y la gestión de ancho de banda, se suelen implementar en estos puntos. Por ejemplo, los firewalls y los routers de borde gestionan qué tipo de tráfico puede entrar o salir de la red. Respecto a los nodos de salida, realizan una preparación del tráfico previamente a enviarlo a otro dominio.

Dentro de un determinado dominio, los router, switches, etc se conectarán a otros, ya sean internos o externos, dentro de este ámbito. Todos ellos deben utilizar PHB pertinente para cada paquete tomando como referencia el BAC (*Bandwidth Aggregate Classifier*). BAC clasifica el tráfico de red en diferentes categorías o clases en función del ancho de banda. Así, permite a la red identificar y controlar los grupos de tráfico. Pueden crearse una clase para el tráfico de voz, otra para el tráfico de video y otra para el tráfico de datos.

Previamente, las rutas de encaminamiento de los paquetes de datos se basaban en las direcciones IP. Sin embargo, MPLS añade a los paquetes etiquetas que informan la ruta a seguir por el paquete. Por lo que el router analiza la cabecera y conoce la ruta siendo un proceso muy rápido basado únicamente en la etiqueta.

El funcionamiento básico se puede distinguir tres casos. Por una parte, la entrada a la red MPLS. En este caso, el paquete de datos entra en la red a través de un router de entrada. Este router añade una etiqueta al paquete basándose en la información de encaminamiento. Un segundo caso es el encaminamiento, es decir, los router intermedios (*Label Switch Routers*, LSR) en la red utiliza la etiqueta sin necesitar examinar el encabezado IP del paquete. El camino señalado por el conjunto de etiquetas recibe el nombre de LSP (*Label Switching Path*). Esto último, ayuda a acelerar el proceso. Además, para realizar la conmutación de etiquetas, los LSR forman en una tabla entradas que contienen un par de etiquetas de entrada/salida por cada entrada del LSR. Para el tercer caso, salida de la red MPLS cuando el paquete llega al router de salida (*Egress Router*), la etiqueta es eliminada y el paquete es enviado a su destino utilizando el encaminamiento IP tradicional. Es necesario aclarar que los nodos que pertenecen a la MPLS y se encuentran en la frontera de la red MPLS se les denomina LER⁷¹.

Es necesario indicar que las etiquetas deben encolarse y asignar a los paquetes un valor TTL (Time To Live) que indica el número de salto que podría efectuar el paquete antes de ser descartado. Es decir, cada vez que un paquete llega a un LSR, este decrementa el valor del TTL en una unidad que, en caso de llegar a cero, el paquete es eliminado.

Es necesario indicar que MPLS asigna a un LSP específico los recursos necesarios en cada LSR y en cada enlace que forma parte del LSP para cada tipo de tráfico. Para ello, utiliza un encaminamiento basado en restricciones CBR (*Constrained Based Routing*), para obtener los mejores caminos con unas condiciones de contorno dadas por unos valores concretos de calidad de servicio (QoS) ya sea retardo, jitter, pérdidas, etc. Estas herramientas son útiles y que permiten controlar el dimensionamiento y planificación de la red.

Se puede afirmar que MPLS mejora la calidad de servicio (QoS) clasificando y etiquetando el tráfico para priorizar aplicaciones críticas, usando rutas optimizadas disminuyendo la latencia y evitar la congestión. Además, implementa mecanismos de gestión de ancho de banda para asegurar que el tráfico importante siempre tenga la prioridad adecuada.

⁷¹ LER: *Layer Edge Router*

2.7.5 Prevención de la congestión

En este apartado se va a mostrar varios mecanismos de prevención de la congestión que son los que a continuación se muestran.

Para evitar que un emisor envíe demasiados datos al receptor se utiliza el control de flujo en TCP que se encuentra en el nivel de transporte. Por eso, se utiliza el sistema de ventanas (*Sliding Windows*) de tal que puede ajustarse de forma dinámica la cantidad de datos enviados en función de la capacidad del receptor en recibirlos y procesarlos. Este control de flujo posee dos ventanas, una de recepción (*Receive Window*) y otra ventana deslizante. La ventana de recepción es la que indica la cantidad de datos que es capaz el receptor de asumir. Esta ventana se comunica con el emisor. Respecto al segundo caso TCP utiliza una ventana deslizante para gestionar la cantidad de datos que se pueden enviar sin recibir una confirmación (ACK) del receptor. En el Anexo se puede ver un ejemplo.

El problema que aparece es que dado que TCP es orientado a conexión hace que cuando se pierde un paquete, el otro extremo debe retransmitirlo agravando las situaciones de congestión. Es necesario tomar las medidas adecuadas para evitar ocupar todo el ancho de banda de la red por el funcionamiento del protocolo TCP.

El otro problema que aparece es la sincronización global, es decir, si no se utilizan algoritmos de prevención de la congestión y se dé el caso de que las colas de los buffers están llenas, todos los paquetes entrantes serán descartados. Para los canales de ancho de banda reducido como puede ser un enlace WAN o una VPN, se produce un efecto de sincronización global entre las conexiones TCP tal que se generan y pierden paquetes. El resultado es que el tráfico TCP llega a los nodos de la red a modo de olas con gran cantidad de paquetes en las crestas que tienden a saturar las colas de los nodos de la red. Para evitar estos dos efectos no deseados se usan técnicas de prevención de la congestión.

A continuación, vamos a ver el segundo caso de los definidos, RED (*Random Early Detection*) [18], es decir, es una técnica que se implementa en los routers y funciona monitoreando la cola de espera de paquetes realizando un descarte aleatorio de paquetes antes de que las colas de los nodos de la red alcancen su valor máximo y haya sobrepasado un umbral de seguridad. ¿Qué implica la anterior? En el caso de que se produzca una disminución en la tasa de transmisión, las ventanas de control de flujo y de congestión del emisor disminuirá adaptándose al valor al que la red sea capaz de asumir. Esta técnica (RED) establecerá un límite superior o umbral máximo y un límite o umbral mínimos. Para aquellos casos donde la longitud de la cola es inferior al valor del umbral mínimo, los paquetes se aceptarán y se encolarán. Para el caso de que el valor de la cola esté por encima del umbral máximo, entonces se descartarán así evitando la congestión. Por tanto, a medida que los valores se aproximan al valor máximos, la probabilidad de descarte aumenta.

Para evitar que todos los datos se vean afectados a la vez, lo que hace RED es descartar algunos paquetes antes de que la cola se llene.

Es necesario aclarar que WRED (*Weighed Random Early Detection*) proviene de *Random Early Detection* (RED) incorporando medidas de calidad de servicio (QoS).

WRED permite tratar diferentes tipos de tráfico de manera distinta al gestionar la congestión en la red. Es necesario indicar que se introduce un cierto control en la aleatoriedad para el descarte de paquetes a través de un peso (IPP, *IP Precedence*), es decir, IPP es un campo de cabecera que indica la prioridad de un paquete. En el Anexo se puede ver un ejemplo de cómo se da el proceso de WRED.

La siguiente técnica es DBWRED (*DSCP-Based WRED*) que combina WRED (*Weighted Random Early Detection*) y DSCP (*Differentiated Services Code Point*) en la gestión de tráfico de redes. WRED es una técnica que acabamos de ver. Mientras que DSCP corresponde al campo situado en el encabezado IP que nos da la prioridad del paquete en términos de calidad de servicio (QoS) clasificando y gestionando el tráfico de red. El funcionamiento de DBWRED utiliza el valor DSCP de cada paquete para aplicar políticas de WRED. Los paquetes entrantes son clasificados según su valor

DSCP, es decir, indica la prioridad del tráfico. Además, se establecen diferentes umbrales de cola para cada clase de tráfico según el DSCP. Para aquellos tráficos con mayor valor de prioridad (DSCP) o umbrales más altos tendrán menor probabilidad de ser descartados y viceversa.

Para el caso de la Notificación explícita de la congestión o ECN⁷² que añade al paquete IP un aviso, en caso de haber congestión, entre los extremos de la conexión así evitando descartar paquetes. Este aviso vendrá definido en los dos últimos bits del campo ToS que se encuentra en la cabecera del paquete IP.

En los casos anteriores, al darse cuenta los routers de que había una congestión se descartaban paquetes reduciendo la velocidad de envío disminuyendo la congestión. Esto implica pérdida de datos y retransmisiones que implican que el rendimiento del sistema empeore. Como hemos indicado antes, ECN se basa en realizar notificaciones sin hacer descartes y es la continuidad de WRED salvo por el hecho de que WRED descartaba los paquetes directamente. Para implementar ECN en el campo ToS en la cabecera IP se muestra en el Anexo .

2.7.6 Adaptación del tráfico y funciones de policía

De inicio se puede afirmar que la adaptación del tráfico y las funciones de policía [4] en las redes IP son cruciales para garantizar que las llamadas VoIP se realicen con una calidad aceptable. Estas funciones aseguran que los paquetes de voz tengan prioridad, con latencia baja, etc.

Es necesario tener en cuenta que la red está siendo monitorizada continuamente por las *funciones de policía*. De esta manera, podrán comprobar si hay situaciones de incumplimientos por lo que tenga que tomar medidas de forma inmediata, es decir, en el momento que se dé esta situación podrá señalar si hubo un exceso en el tráfico, respecto a lo acordado, y señalarlo con menor prioridad o eliminarlo.

Durante la fase de diseño de una estrategia de calidad debe establecer de forma muy clara qué funciones policía. Para el caso de la señalización o el tráfico de voz la pérdida de paquetes debe ajustarse a un valor mínimo tolerable. De hecho, las aplicaciones en tiempo real (VoIP, videoconferencias, juegos en línea), presentan una criticidad muy elevada al retardo y las pérdidas de paquetes.

Las funciones de policía se pueden dividir en dos aspectos: Policing de entrada (*Ingress Policing*) y de Salida (*Egress Policing*) y *Shaping*. Para el primer caso, se controla el tráfico que entra y sale de la red. De tal manera que se garantice que los usuarios no envíen más tráfico del permitido por el SLA. De esta manera, se protege a la red de la congestión. En el caso de *shaping*, es una técnica que ajusta la tasa de tráfico retrasando los paquetes que exceden de un cierto umbral predeterminado, ayudando a suavizar el flujo de tráfico y reducir los picos de congestión.

Respecto a la adaptación del tráfico, en concreto para las llamadas VoIP, se deben recibir prioridad sobre otros tipos de tráficos. Las redes IP deben implementar políticas que garanticen la prioridad de paquetes, es decir, dar mayor prioridad a estos para minimizar la latencia o *jitter*.

Además, aparecen los adaptadores del tráfico que trabajan junto con los mecanismos de encolado (FIFO, PQ, WFQ, CBWFQ, RED) para adaptar el perfil del tráfico para cumplir con el contrato SLA. Con esto, se logra que en el caso de haber un tráfico en exceso éste será retrasado hasta que disminuya por debajo del umbral establecido.

Este tipo de técnicas ayudan a estabilizar los flujos de tráfico y favorecen que los efectos de las ráfagas de datos (grandes transferencias de archivos, actualizaciones de software, transmisiones de video, o picos en la actividad de los usuarios) no afecten demasiado al tráfico en tiempo real.

⁷² ECN: *Explicit Congestion Notification*

2.7.7 Control de admisión

Puede darse el caso que, en un momento determinado, se produzca una solicitud de tráfico. Entonces, el propio sistema dispone de un mecanismo denominado control de admisión (*Admission Control*) que decide si permitir o no este acceso. Esta decisión será tomada en función de una serie de recursos como son el ancho de banda, capacidad de procesamiento, etc., con el objetivo de no reducir el rendimiento del tráfico de la red y las políticas de seguridad (QoS). Es decir, que se asegure que la red no va a comprometer la estabilidad de la calidad por introducir una nueva solicitud de acceso. Además, se utilizan una serie de técnicas como *descarte de paquetes* y *de retransmisión* que son utilizadas por control de admisión para prevenir los problemas de congestión que se puedan dar y que las aplicaciones como VoIP y videoconferencia funcionen correctamente.

2.8 Infraestructura de comunicaciones

En este subapartado se muestran los equipos hardware que vienen definidos en telefonía tradicional y en la actual.

En este apartado, entramos en la parte que abarcan los centros actuales que ayudan físicamente a las comunicaciones, la red de ATM, entre las centrales telefónicas que conectan a los usuarios. Además, se muestran las nuevas tecnologías que ya se están implementando, MXONE, NGN (*Next Generation Network*), SBC, y están conviviendo con lo anterior a través de pasarelas. Todos estos elementos son imprescindibles a los cuales se les debe asegurar una seguridad a través de firewalls que garanticen que, en el caso de sufrir ataques, el impacto sufrido afecte al menor número posible de elementos hardware y software del sistema.

También se tratan la relación entre los PSTN y las redes privadas. Y como las redes telefónicas han ido evolucionando desde un punto de vista tradicional hasta el actual.

2.8.1 Backbones telefónicos tradicionales vs IP

Este apartado se va a dividir en tres partes; telefonía analógica, telefonía digital e IP.

2.8.1.1 Telefonía analógica

Cuando surgió la telefonía analógica el usuario se ponía en contacto marcando el número de teléfono deseado sin que la señal sufriese ningún tipo de digitalización, es decir, no existía ni la compresión ni la digitalización de la señal que surgió posteriormente. Por aquel entonces, las centrales telefónicas buscaban una ruta idónea, a través de un cable de cobre, que conectaba al usuario inicial que inició la llamada con su destinatario. Durante este proceso se establecía un circuito temporal cuya duración dependía de la conversación realizada y que era gestionado por una serie de conmutadores intermedios. En el momento que la conversación finalizaba, todos los recursos intervinientes y el propio circuito se liberaban para poder ofrecer otros servicios a otros usuarios. Cada llamada ocupaba un canal físico único. ¿Qué implicaba esto? Esto limitaba la cantidad de llamadas simultáneas que una infraestructura dada podía soportar. Las líneas de cobre solo podían transportar una llamada por petición.

2.8.1.2 Telefonía digital

Aquí aparece una evolución tecnológica que es PSTN. Es decir, surge una infraestructura de carácter global cuyos componentes son los que se exponen:

- Centrales Telefónicas: Son los nodos principales del PSTN donde se conmutan las llamadas. Dado que se particulariza por zonas geográficas, estos nodos pueden ser locales o regionales.
- Red de Acceso: Está formado por una serie de elementos que permiten a los usuarios conectarse a las centrales telefónicas. Estos componentes son las líneas contratadas por los

usuarios y los equipos físicos como son los modem y routers que son los equipos que ayudan a la conexión.

- Red de Transmisión: Es la línea de cobre que transporta la señal de voz que pasa a través de las centrales telefónicas y conectan a los usuarios.
- Centrales de Conmutación: Son aquellas centrales que dirigen las llamadas garantizando que los usuarios puedan conversar.

Gracias a la evolución tecnológica se pudo superar las limitaciones de la telefonía analógica. En este caso, se evolucionó hacia la *tecnología de multiplexación digital* (TDM). Esto fue una revolución porque permitía enviar varias llamadas dentro de un solo canal dividiendo el tiempo disponible en intervalos cortos, asignando cada intervalo a cada llamada. Esto significa que muchas llamadas pueden compartir el mismo medio físico. Por parte de la voz, las señales de voz analógicas se convierten en señales digitales mediante un proceso llamado PCM. Aquí aparece la digitalización y la multiplexación permitiendo mayor capacidad de envío, mayor calidad de las llamadas al degradarse menos la señal. Además, se mejor en el envío de datos, video y otros servicios en la misma red.

Las redes de voz de los operadores telefónicos están organizadas mediante centrales de conmutación interconectadas que unen servicios y llamadas telefónicas.

Utilizar un sistema de *backbones* telefónicos tradicionales implica reservar ancho de banda a circuitos de voz cuando se sabe que no se va a estar utilizando en todo momento.

En la actualidad, PSTN está siendo reemplazado por tecnologías como VoIP que ofrecen más flexibilidad, ancho de banda, servicios multimedia, etc.

2.8.1.3 Telefonía IP

Los *backbones telefónicos sobre IP* usan tecnología de protocolo de internet (IP) para enviar tráfico de voz y otros servicios multimedia a través de Internet. Además, se caracterizan por gran ancho de banda, integración de servicios, redundancia y fiabilidad.

Es capaz de soportar una gran cantidad de tráfico donde se asocia muchísimos datos garantizando las llamadas de voz sin interrupción.

Cuando se habla de redundancia quiere decir que habrá múltiples rutas por donde pueden transitar los servicios en caso de fallo. Para ayudar a este tránsito se crearon los protocolos de señalización y transporte como son SIP⁷³ y RTP (*Real-time Transport Protocol*).

El transporte de la voz se realiza digitalizando la voz e introduciendo en paquetes de datos enviándose posteriormente a través de la red apoyándose en los protocolos SIP y RTP.

La interconexión de redes ayuda a unir diferentes redes que pertenecen a diferentes proveedores de servicios.

El soporte para servicios multimedia facilita transmitir servicios multimedia como video conferencias y transmisión de datos en tiempo real. Se pueden utilizar los protocolos H.323 o WebRTC que realizan la codificación, transmisión y decodificación en tiempo real.

Finalmente, la *gestión de calidad de servicio* (QoS) introducen técnicas que aseguren el tráfico sensible al tiempo. Por ejemplo, se puede implementar políticas de QoS para priorizar los tráfico de llamadas VoIP y videoconferencias sobre el resto de los servicios minimizando la latencia y el *jitter*.

⁷³ SIP: *Session Initiation Protocol*

2.8.2 Redes corporativas de voz

Son redes internas que pertenecen a empresas y organismos que se conectan entre sí mediante PBX con la ayuda de enlaces troncales. Esto implica, no depender tanto de la red pública (PSTN) al ser llamadas internas.

Se debe incidir que PBX son las centrales telefónicas privadas que manejan el encaminamiento de llamadas internas y externas dentro de la organización. Mientras que los enlaces troncales disponen de conexiones dedicadas que interconectan múltiples PBX dentro de la organización, permitiendo la transmisión de llamadas y datos entre diferentes ubicaciones. Estas conexiones facilitan la comunicación entre sedes una misma organización. Es necesario indicar que las organizaciones tienen el control total sobre su sistema telefónico, configuración de servicios e introducción de políticas de seguridad.

Los enlaces troncales de la red pública, antes de la adopción generalizada de VoIP (*Voice over IP*), eran líneas dedicadas proporcionadas por los operadores tradicionales. Estos enlaces permitían la transmisión de llamadas a través de la infraestructura del operador, utilizando tecnologías como T1/E1, ISDN (RDSI en español). Es importante resaltar que esta arquitectura hereda los mismos inconvenientes de los backbones telefónicos convencionales de baja incidencia técnica y económica.

Con la evolución hacia la VoIP, se puede afirmar que la integración con la red pública a través de puertas de enlace (Gateway) VoIP-PSTN, que convierten las llamadas entre los formatos IP y PSTN. Esto permite a las organizaciones seguir comunicándose con usuarios en la red pública mientras aprovechan los beneficios de VoIP internamente.

La evolución técnica ha permitido crear centralitas que no sólo han incorporados la pasarela sino también que los teléfonos de distintas redes, antiguas y modernas se puedan conectar.

Las llamadas son gestionadas desde un servidor central, aunque también se ofrece la posibilidad de estar distribuida con varios servidores que lo soportan.

La voz sobre paquetes ofrece una gran gama de configuraciones. Estas configuraciones son la priorización del tráfico de voz respecto al resto de servicios, gestión del ancho de banda para las llamadas de voz, posibilidad de implementación en redes LAN, WAN, internet, etc., configurar rutas de llamadas, reenvío de comunicaciones, grabación, videollamadas, cifrado de voz, autenticación de usuarios, configuración de firewalls para VoIP, uso de protocolos (SIP, H.323, MGCP, etc), es compatible con una variedad de códec de audio y es escalable, es decir, se le puede agregar más recursos como servidores, Gateway, etc., sin que sea necesario reconfigurar la red.

2.8.3 Centros RCT

Es una red denominada Red de Telefonía Conmutada (RCT) o *Public Switched Telephone* (PSTN) que da servicios de voz y datos por conmutación de circuitos donde se designa un ancho de banda durante la conversación. Las conversaciones se producen por una conexión dedicada. En estos, pueden darse las conexiones entre circuitos analógicos y digitales.

En estos centros aparecen tres elementos importantes; central telefónica, línea de suscriptor y los troncales. Las centrales establecen y mantienen las comunicaciones entre los clientes. La línea de suscriptor son los cables por donde discurren las llamadas y pueden pasar por uno o varias centrales telefónicas. Por último, los troncales son las conexiones entre las centrales telefónicas.

RCT usa el protocolo de señalización SS7 para encaminar las llamadas.

Al inicio, las conversaciones telefónicas se mantenían por señales analógicas, pero con las mejoras tecnológicas se evolucionó a la modulación por impulsos codificados (PCM). Esta técnica permite la conversión de las señales analógicas a digitales. RCT está siendo reemplazado paulatinamente por las redes VoIP. Además, el coste y complejidad se reduce con esta evolución.

2.8.4 Centros ATM

Los ATM son los nodos de transmisión que conectan las centrales telefónicas de la red previa a la introducción a la I3D y que aún sigue funcionando. Además, “ATM es una tecnología de conmutación [19] que puede manejar tráfico de datos, voz y video”.

En el año 2006 la empresa Cingular Wireless LCC propuso la migración a IP con Alcatel. La solución que propuso fue la solución de servicio multiservicio de Alcatel *ofreciendo servicios móviles avanzados de tercera generación (3G) tales como comunicaciones de datos de alta velocidad y video bajo demanda* [20]. El inconveniente es que las grandes ventajas que ofrece en este servicio no se aprovechan al 100% por el Ministerio de Defensa. Estas ventajas hubiesen sido, por ejemplo, “*migrar redes ATM multiservicio de grandes dimensiones a implantaciones IP/MPLS*” [20]. Sin embargo, si se aprovecha con calidad de operador, sin comprometer la alta disponibilidad, la capacidad de gestión y la calidad de servicio, “*esta tecnología ofrece herramientas de operación, administración, mantenimiento y provisión que facilitan los costes de operación y del tiempo de puesta en servicio*” [20].

La gestión de la red se logra con los elementos del 5620NM y que se muestra en Figura 2-4.

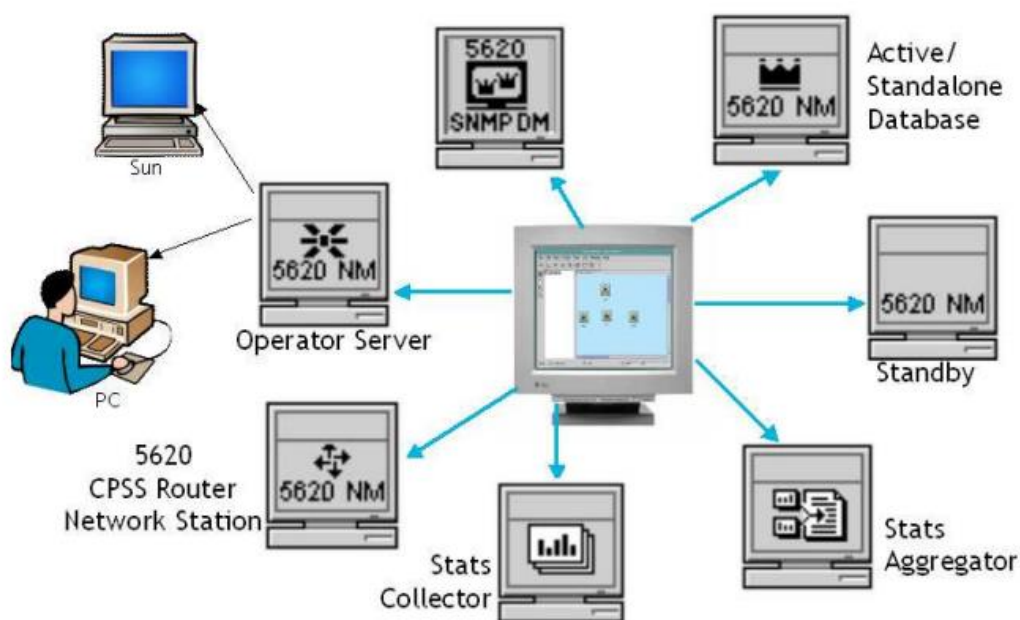


Figura 2-4 Elementos 5620 NM (Fuente: [20])

Los elementos que conforman el sistema son los que a continuación se relaciona:

- Estación Active / Standalone Database.
- Estación operador server
- Estación operador position
- CPSS router
- Statists collector/Aggregator

La estación Active es una estación que contiene la base de datos de todos los elementos que conforman la red. Existen dos tipos de estaciones database que son la estación standalone y las parejas de estaciones redundantes. Sin embargo, ambos tipos de estaciones no pueden funcionar al mismo tiempo. La estación standalone carece de una redundante mientras que la pareja de estaciones redundantes sí lo tiene. De tal manera que, tienen una base de datos sincronizada que se mantiene una de ellas en estado activo y la otra en reserva. La estación activa gestiona la red y mantiene la base de

datos actualizada. A su vez, la estación de reserva lo único que realiza es acceder a la base de datos de la estación activa para mantener actualizada su propia base de datos. En el caso de producirse un fallo de alimentación en la estación activa, la estación pasiva tomará el control pasando a ser la estación activa.

Las estaciones operator server ofrecen puntos de acceso de operación adicionales a la red y están conectados a la base de datos de la estación database.

Las estaciones operator position se conectan a las estaciones operator server para entrar en la base de datos de la estación database activa. El rango de funcionalidad de los usuarios dependerá de los privilegios que disponga cada usuario. En la Figura 2-5 se puede observar cómo se sitúa el operator position dentro de la estructura.

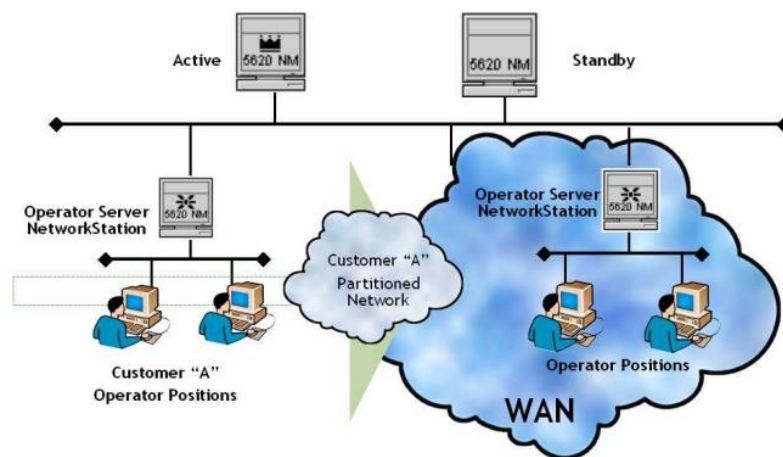


Figura 2-5 Operator position (Fuente:[20])

Los *integrated statistics collector* están instalados en las estaciones database y recogen datos que provienen de los mensajes. A cada elemento de la red se le asigna una única dirección. Mientras que a cada nodo necesita también una única dirección CPSS.

“ATM es una tecnología de conmutación y multiplexación de celdas de 53 bytes” [19], de longitud fija, para la transmisión de datos. Cada celda tiene 53 bytes, de los cuales 48 bytes son para datos y 5 bytes para la cabecera (información de control). ¿Qué permite la combinación entre conmutación y multiplexación? Aprovechar las ventajas de ambas.

ATM maneja diferentes tipos de tráfico (voz, video, datos) con diferentes requisitos de rendimiento y ofrece servicios como CBR, VBR⁷⁴, ABR y UBR. CBR calcula las rutas óptimas teniendo en cuenta las condiciones de retardo, *jitter*, pérdidas. ABR ofrece un uso eficiente del ancho de banda al permitir que las aplicaciones ajusten su tasa de transmisión, su ancho de banda y minimizando la congestión en la red. De hecho, pueden variar su tasa de transmisión. Es necesario aclarar que los nodos de la red ATM proporcionan información sobre la disponibilidad de ancho de banda y la congestión en la red. Aunque ABR no garantiza un ancho de banda fijo, suele proporcionar una tasa mínima garantizada. Finalmente, UBR se utiliza para la transmisión de datos sin calidad de servicio (QoS), ni tasa mínima de transmisión, retraso, o variabilidad del retraso (*jitter*). Es ideal para aplicaciones como la transferencia de archivos y correos electrónicos.

En redes backbone, ATM permite transportar grandes cantidades de tráfico logrando la integración de servicios de voz, video y datos en una única red.

ATM está siendo reemplazada por tecnologías más modernas como Ethernet y MPLS (Multiprotocol Label Switching) a costes más bajos.

⁷⁴ VBR: *Variable Bit Rate*

Los nodos ATM utiliza los mensajes CPSS, que sirven para intercambiar la información entre nodos y los usuarios de la red que fue realizado por Alactel-Lucent (*Control Packet Switching System*) basado en el protocolo X.25 FAST Select. Es decir, es un protocolo cuya información, que transporta CPSS, es de control, alarmas, ejecución, estado de la configuración, timing y mensaje de routing. Son transmitidos por vía PVCs (*Permanent Virtual Circuit*) (tecnología de redes de telecomunicaciones que permite establecer conexiones virtuales permanentes entre dos puntos de una red). De hecho, los PVCs garantizan la entrega de datos con una calidad de servicio (QoS) predefinida. PVC permite que las aplicaciones más comunes son la creación de redes privadas virtuales (VPN), interconexiones de LAN y servicios de transmisión de datos críticos.

2.8.5 Estándar E1

E1 es un sistema de 30 canales B y 1 canal D (delta o data) conocida como E1 en el sistema ISDN PRI⁷⁵. De tal manera que ISDN PR es un interfaz en redes digitales que logra enviar múltiples llamadas de voz y datos simultáneamente en una sola línea. De hecho, E1 utiliza el *sistema de multiplexación por división en el tiempo (TDM)* para multiplexar 32 canales.

Para el caso de los 30 canales B (Bearer) [21], son de 64 kbps cada uno de ellos para la transmisión de voz y datos. Mientras que el canal D, que transmite a 64 kbps, es utilizado para la señalización, gestión de configuración, control y liberación de las llamadas de los canales B. A parte de estos dos, existe otro canal denominado de sincronización. De esta forma, se logra que los canales B y D estén bien coordinados en el tiempo. Además, para lograr que sean transmitidos los canales B y D simultáneamente por la misma línea se utilizará la multiplexación a 2 Mbps.

Respecto a la telefonía digital, se puede afirmar que E1 logra enviar 30 llamadas a la vez por una única línea junto con el canal D para la señalización. De hecho, E1 es utilizado para interconectar sistemas PBX con la red pública de telefonía, logrando múltiples llamadas en una conexión.

2.8.6 Centrales I3D

El concepto es un núcleo central virtualizado que se encuentran en dos ubicaciones físicas distintas.

I3D está suponiendo la desaparición paulatina de los centros RCT donde los ATM permiten la comunicación entre las centrales telefónicas. Los elementos que van a sustituir a los RCT serán los nodos permanentes y los nodos desplegables.

Se puede afirmar que un nodo desplegable corresponde con aquellas unidades que se encuentran fuera de territorio nacional. Mientras que los nodos permanentes son aquellos situados en territorio nacional.

Los nodos desplegables, a diferencia de los nodos permanentes, se caracterizan por tener instalados los equipos call manager que, en caso de que se caiga la comunicación con TN u otras ZO, permiten mantener las comunicaciones internas dentro de la propia unidad. Existen excepciones donde hay despliegues sin call manager, es decir, los teléfonos se conectan directamente del switch. Todo esto se verá en apartados posteriores.

La primera unidad en la que se instaló la I3D, como nodo permanente, fue en la residencia militar Sancho Ramiro (Huesca). A partir de esta, se fueron incorporando como San Javier, ciertas unidades en Madrid, etc.

La asignación de la numeración de los teléfonos de estas unidades ya no depende de sus CECOM (Centro de Comunicaciones) respectivos, es decir, el personal responsable de la telefonía enviará un listado de números de teléfonos para que lo puedan asignar estos CECOM a sus usuarios.

⁷⁵ PRI: *Primary Rate Interface*

2.8.7 MXONE

La plataforma de virtualización del proveedor VMware es utilizada para la gestión y administración de los servicios virtualizados de telefonía MXONE. Además, forma parte de los sistemas de gestión de la I3D.

En la parte de telefonía, el diseño de la plataforma de virtualización consta de una serie de servidores y cabinas de almacenamiento ubicados físicamente en Madrid de forma redundada.

Los servidores tienen instalado un sistema operativo VMware. Con ello, se logra monitorizar y configurar los servidores gracias a la instancia de vCenter.

Cada servidor cuenta con más de 200 GB de capacidad RAM, decenas de cores para procesamiento y almacenamiento interno de más de 200 GB más una docena de TB de almacenamiento usado por el protocolo ISCSI (*Internet Small Computer Systems Interface*) manejado por las máquinas virtuales. En telefonía puede utilizarse para el registro de llamadas, registros de voz, datos de usuarios, etc.

Con todo esto, se logra la prestación del servicio de telefonía MXONE. Además, se realiza la configuración en el clúster de DRS⁷⁶ para balancear la utilización de los recursos que necesitan las máquinas virtuales. Con ello, se permite la optimización de recursos. Mientras que en las cabinas de almacenamiento se configura el almacenamiento *inter-clúster* en modo “activo-pasivo” donde una de las ubicaciones físicas toma el rol de nodo activo y la otra ubicación física ostenta el modo pasivo. De tal manera que, el nodo pasivo realiza *backups* periódicos de datos almacenados en el nodo máster. Esta supervisión es realizada por la instancia denominada *NetApp Mediation* que monitoriza el estado de los nodos. Y, en caso de que el nodo activo tenga un fallo, se notifica al nodo pasivo para que tome el rol de activo y mantenga el servicio.

Se puede afirmar que la gestión centralizada permite una implementación más rápida y coordinada de la actualización software de los teléfonos.

2.8.8 Gateway

Es un equipo informático configurado para traducir los datos de un protocolo empleado en una red al protocolo utilizado en la red de destino, es decir, es un tipo de enrutador para los datos en su camino hacia otras redes. En telefonía garantiza la liberación de llamadas y conversión de los formatos de información entre diferentes tipos de redes. Además, determina la ruta adecuada para las llamadas entrantes y salientes basándose en las políticas de encaminamiento que se hayan establecido. También es conocido que el *Gateway* convierte los flujos de audio y video de los formatos utilizados en la red PSTN, como por ejemplo G.711, a los formatos utilizados en la red IP.

Si un dispositivo dentro de una red desea comunicarse con otro fuera de ella, requiere la funcionalidad de un *Gateway*. De tal manera que los *Gateway* pueden adoptar varias formas con el propósito de cumplir ciertas tareas. Por ejemplo [22]:

- Gateway de red: proporcionan una interfaz entre dos redes distintas que funcionan con varios protocolos.
- Firewall de aplicaciones web: filtran el tráfico hacia y desde un servidor web, analizando los datos de la capa de aplicación.
- Gateway de almacenamiento en la nube: es un servidor de red que descifra las solicitudes de almacenamiento en la nube. Además, permite almacenar la información en una sola red privada.
- Gateway API: supervisan el flujo de tráfico dentro y fuera de un servicio.
- Gateway VoIP: facilitan el uso de datos con los servicios de telefonía antiguo.

⁷⁶ DRS: *Distruted Resource Scheduler*

- Gateway de seguridad de email: evitan la entrada de correos electrónicos que no cumplan con la política de la empresa.
- Gateway IoT: permiten agregar y transmitir datos a los sensores en un entorno IoT (Internet de las cosas) funcionan como intermediarios para la comunicación remota, permitiendo el uso de sensores, actuadores y otros dispositivos para la supervisión y control de distintos procesos de producción. De esta forma, las puertas de enlace actúan como un traductor universal que permite la comunicación y operatividad de estos dispositivos.

Centrándonos en la telefonía, los tipos de Gateway son Media Gateway, *Signaling Gateway* (traduce la señalización entre SS7 utilizado en PSTN y protocolos de señalización utilizados en VoIP, como SIP o H.323), VoIP Gateway (conecta teléfonos analógicos y sistemas PBX tradicionales a redes VoIP).

2.8.9 Media Gateway

Es un dispositivo que permite las comunicaciones entre diferentes tipos de redes como puede ser el modo de transferencia asíncrono (ATM) y el protocolo de internet (IP).

Los media Gateway [23] de voz sobre protocolo VoIP permiten la conversión entre la voz desde la multiplexación por división del tiempo (TDM) a un protocolo de transporte en tiempo real (RTP), o bien a un protocolo de señalización utilizado en VoIP.

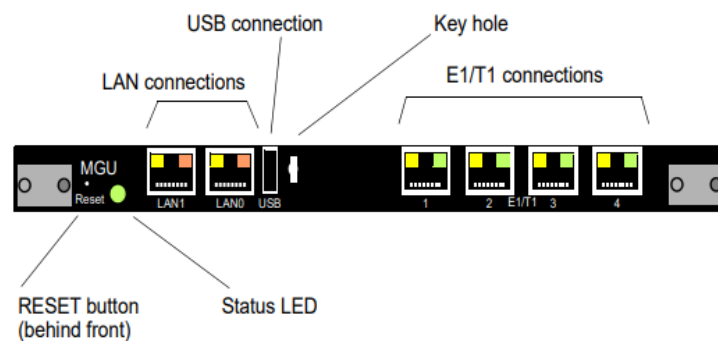


Figura 2-6 Media Gateway Unit, MGU2 (Fuente: [23])

A continuación, se muestra Media Gateway en una red IP.

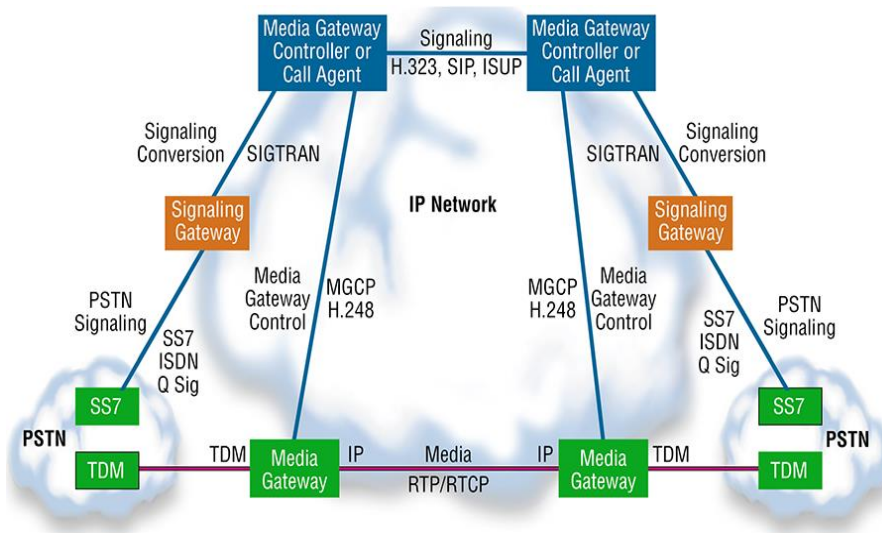


Figura 2-7 Gateway en la red IP (Fuente: [24])

En definitiva, la función de un Gateway [24] es traducir protocolos para permitir la comunicación entre redes distintas. Mientras que la función de una Media Gateway es convertir y manejar flujos como la voz y el video entre diferentes tecnologías, es decir, convertir las señales de voz de una red telefónica convencional a un formato en una red IP.

2.8.10 NGN

Integra servicios como son la voz, datos y multimedia sobre una red basada en paquetes usando el protocolo IP. Además, permite la conexión entre los usuarios finales y la red central garantizando que puedan utilizarse varios servicios con el intercambio seguro de datos entre los distintos intervinientes.

Utiliza tecnologías como MPLS y Ethernet pudiendo incluir servidores de aplicaciones, bases de datos, firewalls, sistemas de detección y prevención de intrusiones y encriptación.

NGN dispone de prioridades para aquellas situaciones críticas, en voz y video, donde sea necesario tener una prioridad mayor en ciertas comunicaciones sobre los tráficos menos prioritarios.

Otra característica importante es que NGN permite a los usuarios acceder a cualquiera de sus servicios desde cualquier ubicación independientemente del dispositivo físico con el que desee acceder fuera de la red de su organización. Con ello, se garantiza a los usuarios movilidad.

NGN se divide en tres capas; capa de transporte, capa de control y capa de servicios y aplicaciones. La capa de transporte es el responsable de la transmisión de datos en la red. La capa de control se encarga del control de conexiones y llamadas. Finalmente, la capa de servicios y aplicaciones ofrece las aplicaciones a los usuarios.

En telefonía, NGN la gestión de los números y marcación se realiza de forma centralizada en servidores y bases de datos. Esto permite la conversión de números de teléfono de siete a nueve cifras de forma eficiente. Estos servidores pueden programarse en función de las necesidades del cliente antes de encaminar las llamadas. Además, los servidores (denominados los *Softswitches* o los *Call Agents*) utilizarán tablas de traducción con reglas que garanticen el correcto funcionamiento del sistema. Es conocido que también utilizarán bases de datos centralizadas con los planes de marcación para que el usuario pueda aunar toda la información. Es decir, el plan de marcación consiste en un conjunto de reglas que dicta cómo se marcan los números de teléfono para realizar llamadas nacionales e internacionales y cómo se encaminan esas conexiones dentro de la red. En estos planes de marcación se definirán la longitud de los números de teléfonos y los prefijos a marcar, en función de si se encuentra el destinatario en el mismo país o en otro. Además, el servicio ENUM (E.164 *Number Mapping*) se puede utilizar para gestionar la conversión de números de siete a nueve cifras.

Durante los procesos de migración de un sistema antiguo a otro, NGN permite que ambos coexistan, aunque la longitud de la numeración sea distinta y garantiza el paso desde gradual sistema antiguo al nuevo.

Se puede afirmar que la gestión centralizada permite una implementación más rápida y coordinada de la conversión de números.

Finalmente, se puede afirmar que NGN posee una arquitectura flexible, con una gestión centralizada y la capacidad de implementar reglas de traducción y normalización de números en tiempo real.

2.8.11 Call Manager

Es un servidor que se encarga de dar de alta o de baja a los usuarios. Aquellos que se dan de alta se le asigna una numeración y gestionará las llamadas telefónicas que se produzcan. Todo esto dentro del contexto de una red VoIP usando los protocolos SIP o H.323. Además, se caracteriza por lo siguiente:

- Se encarga de la señalización, establecimiento y terminación de las llamadas.

- Ofrece posibilidades como la transferencia de llamadas, conferencias, buzón de voz, grabación de llamadas, reenvío de llamada, entre otros.
- Puede dar servicio a empresas de pequeño o gran tamaño.
- Implementan medida de protección en las comunicaciones y cifrado en las llamadas.
- Proporciona la convergencia de datos, voz y video en una única red.

2.8.12 Teléfonos software o *softphone*

Es una aplicación software que ofrece funcionalidades telefónicas a un dispositivo que no es un teléfono, como puede ser una tableta o un pc. Se puede decir que las aplicaciones Skype, Google Video, etc., son un tipo concreto de *softphone*. De hecho, alguna de ellas cuenta con su licencia pudiendo presentar problemas de compatibilidad con VoIP.

Relativo a los teléfonos software o *softphone* se puede afirmar los siguientes puntos:

- Funcionalidades:
 - Se pueden hacer y recibir llamadas de voz y video.
 - Llamadas de Voz sobre IP (VoIP) que se transforman en datos digitales y son enviados a través de redes IP.
 - Videollamadas.
- Interfaz de usuario:
 - Pantalla de marcado que simula de un teléfono tradicional
 - Agenda de contactos.
- Otras funciones:
 - Se puede enviar y recibir mensajes de texto.
 - Se puede comunicar mensajes de voz.
 - Posibilidad de conferencia de voz y video.
 - Se puede transferir llamadas a otros usuarios.
 - Grabación de llamadas.
- Compatibilidad:
 - Está disponible para sistema operativos como Windows, macOS, Linux, Android e IOS.
 - Puede unirse a sistemas de comunicaciones unificadas, CRM y otras.
- Las ventajas son:
 - Permite al usuario realizar llamadas siempre que tenga conexión a internet.
 - Las llamadas VoIP suponen un menor coste que las llamadas basadas en tecnologías anteriores. Sobre todo, las llamadas internacionales.
 - Se puede adaptar y escalar a las necesidades de las empresas interesadas.
 - Logra una mejor eficiencia al poderse integrar con otros sistemas de comunicación.
- Laboralmente se pueden adaptar a:
 - Las organizaciones mejorarán su comunicación no sólo a nivel interno sino también con sus clientes.
 - Facilita el teletrabajo de los trabajadores de las empresas.

2.8.13 PBX

Es una red telefónica privada utilizada dentro de una organización. Los usuarios pueden comunicarse internamente, dentro de la empresa, y externa, fuera de la organización, usando diferentes

canales de comunicación. Dos ventajas que ofrece PBX [25] sobre PSTN es que puede ofrecer a sus usuarios más líneas telefónicas y gratuitas.

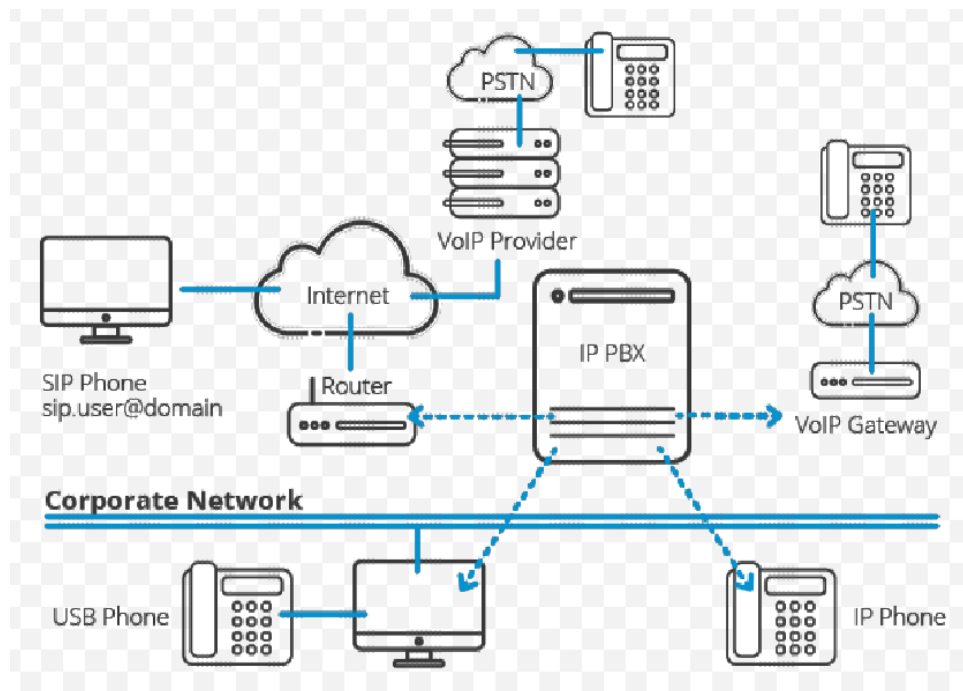


Figura 2-8 Central PBX (Fuente: [25])

2.8.1 PSTN

Es un conjunto de redes interconectadas entre sí, que prestan servicios de voz e infraestructura física necesaria para hacer y recibir llamadas (y transportar el tráfico de datos) entre los usuarios.

Las compañías telefónicas que operan a nivel internacional, nacional o regional crearon una red de cables interconectados cuyas interconexiones se les denominan *nodos*. Cuando un usuario levanta un teléfono y marca los dígitos para hablar con su interlocutor, envía una señal DTMF atravesando los nodos para que sepan el destino de la llamada telefónica.

Originalmente, la red de PSTN fue construida utilizando cables de cobre, pero ahora es casi completamente digital en su núcleo de red al utilizar cables de fibra óptica, enlaces de satélite, y centros de cambio de alta tecnología. Esta red presenta una topología muy compleja, pero puede simplificarse en una configuración jerárquica. Cada línea de los usuarios se conecta a una central local que, a su vez, se conecta a centrales troncales y así sucesivamente.

La arquitectura PSTN [26] se puede mostrar de la siguiente manera:

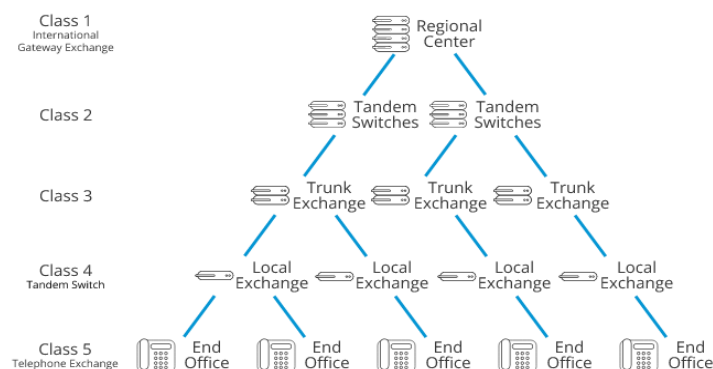


Figura 2-9 PSTN (Fuente: [26])

2.8.2 SBC

Es un dispositivo situado [27] en los límites de una red de tipo VoIP que gestionan las conexiones con otras redes en tiempo real.

Desde el punto de vista de la seguridad e independientemente del trabajo que realizan los firewalls, SBC también filtra el tráfico no deseado para evitar ataques como DoS (*Denial of Service*), y otras amenazas. Respecto a la encriptación, pueden cifrar el tráfico de señalización y medios (por ejemplo, usando SRTP y TLS) para proteger la privacidad de las comunicaciones.

Para el caso del control de Calidad (QoS) se centran en dos puntos. La priorización del tráfico y la gestión del ancho de banda. SBC puede priorizar el tráfico de voz sobre otros servicios y ayuda en la gestión del ancho de banda pudiendo evitar la congestión en la red en tiempo real.

Los SBC permite la interacción entre diferentes sistemas y protocolo como SIP, H.323 y MGCP. Mientras que *transcoding* realiza la conversión de códec de audio y video para asegurar la compatibilidad entre dispositivos que utilizan diferentes códec.

Cuando se inician las llamadas telefónicas, se controlan mediante una gestión de sesiones donde los SBC pueden encaminar las conexiones de manera eficiente y asegurarse de que se dirijan al destino correcto. Además, ofrece una política de control que implementan políticas de control sobre quién puede iniciar llamadas, a quién se puede llamar y qué recursos se pueden utilizar.

Finalmente, la monitorización y registro se divide en supervisión de llamadas y registro de llamadas. Para el primero, permiten la supervisión en tiempo real de las sesiones de comunicación para detectar y resolver problemas rápidamente. Mientras que, para el segundo, mantienen registros detallados de todas las sesiones de comunicación para auditoría, facturación y análisis de rendimiento.

El SBC se debe ubicar en el *borde de la red interna*, es decir, en la zona interna de una organización y su proveedor de servicios VoIP. O bien, *entre diferentes redes VoIP* ayudando la interconexión entre diferentes operadores de servicios VoIP.

2.9 Mecanismos de seguridad

2.9.1 Intrusion Detection Systems (IDS)

Es un software [28] que monitorea el tráfico de red y las actividades del sistema en busca de actos sospechosos o maliciosos y genera alertas cuando detecta posibles intrusiones. De tal manera que, analiza el tráfico de red en busca de patrones que coincidan con firmas de ataques conocidos. Además, notifica a los administradores de red sobre actividades sospechosas o anómalas.

Dentro de la telefonía [28], en concreto VoIP, se realiza la inspección de mensajes SIP para detectar anomalías, como intentos de registrar dispositivos falsos o ataques de *flooding*. Además, se supervisa los flujos RTP para detectar interrupciones o inyecciones de paquetes maliciosos e identificación de comportamientos que puedan indicar fraude en llamadas, como el uso de servicios sin autorización.

2.9.2 Intrusion Prevention Systems (IPS)

Se encarga de realizar el seguimiento de todas las actividades que se dan en una red. Es un software cuyo objetivo es detectar eventos que puedan afectar a la seguridad de la red en tiempo real. Es similar a IDS, pero a diferencia de esta toma acciones o medidas para mitigar las amenazas. Por ejemplo, puede bloquear direcciones IP que traten de inundar el servidor SIP, filtrar tráfico malicioso para evitar la sobrecarga del servidor de VoIP, etc. También se pueden implementar políticas de seguridad que eviten la explotación de vulnerabilidades.

2.9.3 Firewall

Tanto para telefonía como para otros servicios, es una barrera de seguridad entre redes de distinta naturaleza. Su principal objetivo es controlar el tráfico teniendo en cuenta unas reglas de seguridad predefinidas tal que únicamente pase el tráfico autorizado.

A continuación, se determinan las funciones y reglas de seguridad que se asocian a un firewall:

- Control de Acceso: En este caso, sólo pueden acceder esta dirección IP.
- Protección contra Ataques:
 - DDoS (*Distributed Denial of Service*): Es un método que trata de bloquear los ataques que tienen como objetivo sobrecargar la red y a los servidores de VoIP.
 - SIP *Flooding*: Trata de evitar que el sistema sufra ataques que lo inunden con solicitudes SIP falsas. Si no se detiene habrá una interrupción en el servicio.
 - *Malware y Phishing*: Protege contra la entrada de software malicioso y tentativas de phishing a través del tráfico de VoIP.
- NAT transversal (*Network Address Translation*): Se logra que dos dispositivos que se encuentran en redes distintas puedan comunicarse. Lo que hace es que la dirección IP interna de una organización se transforme en una única dirección IP externa.
- Encriptación/seguridad: Con la ayuda de los protocolos TLS y SRTP se puede asegurar la confidencialidad e integridad.
- Prevención de fraude: Detecta y bloquea aquellos accesos que no han sido autorizados en la red. Estas amenazas pueden utilizar números falsificados o interceptar llamadas.
- Calidad de Servicio (QoS): Asigna prioridades al tráfico de paquetes.

Los tipos de firewall para la telefonía son:

- Firewalls integrados: Son aquellos que se encuentran dentro de routers y otros dispositivos de red, ofreciendo seguridad para el tráfico VoIP.
- Firewalls especializados: Son aquellos dispositivos hardware o software dedicados exclusivamente a la protección del tráfico de VoIP.

3 DESARROLLO DEL TFM

3.1 Situación actual

En este apartado se van a describir la situación actual de la telefonía y cómo se relacionan el mundo de los ATM con la I3D, las arquitecturas de telecomunicaciones de los nodos tanto permanentes como desplegables. En éstos se incluirán gráficas y tablas donde se explican con detalle los elementos que los forman.

Durante los últimos veinte años, el funcionamiento de la telefonía en las fuerzas armadas se ha basado en una red de ATM. Sin embargo, en los últimos años se está implementando la telefonía basada en la I3D, incluidos otros servicios. Ha sido necesario realizar una serie de adaptaciones técnicas para lograr que ambas tecnologías funcionen de forma coordinada y correcta. Por un lado, los ATM son los nodos de transmisión que conectan las centrales telefónicas. Mientras que en la I3D el concepto de centrales telefónicas distribuidas desaparece y los teléfonos, que se conectan a los switches y éstos últimos a los firewalls a través de la red MPLS, dependen de la MXONE como elemento centralizador que gestiona las altas, bajas, etc., de los usuarios telefónicos.

Ambos mundos, ATM e I3D, pueden compararse a las redes corporativas de voz donde se autogestionan las comunicaciones telefónicas. Esto implica, no depender de la red pública (PSTN) dado que la mayoría de las llamadas que se realizan son a nivel interno. De hecho, la red de ATM sobre los que se conectan las centrales telefónicas se le puede comparar con los PBX que, al ser una red telefónica privada, permite a los usuarios más líneas telefónicas a menor coste.

En la Figura 3-1 aparece cómo está desplegado actualmente la I3D y la red de ATM.

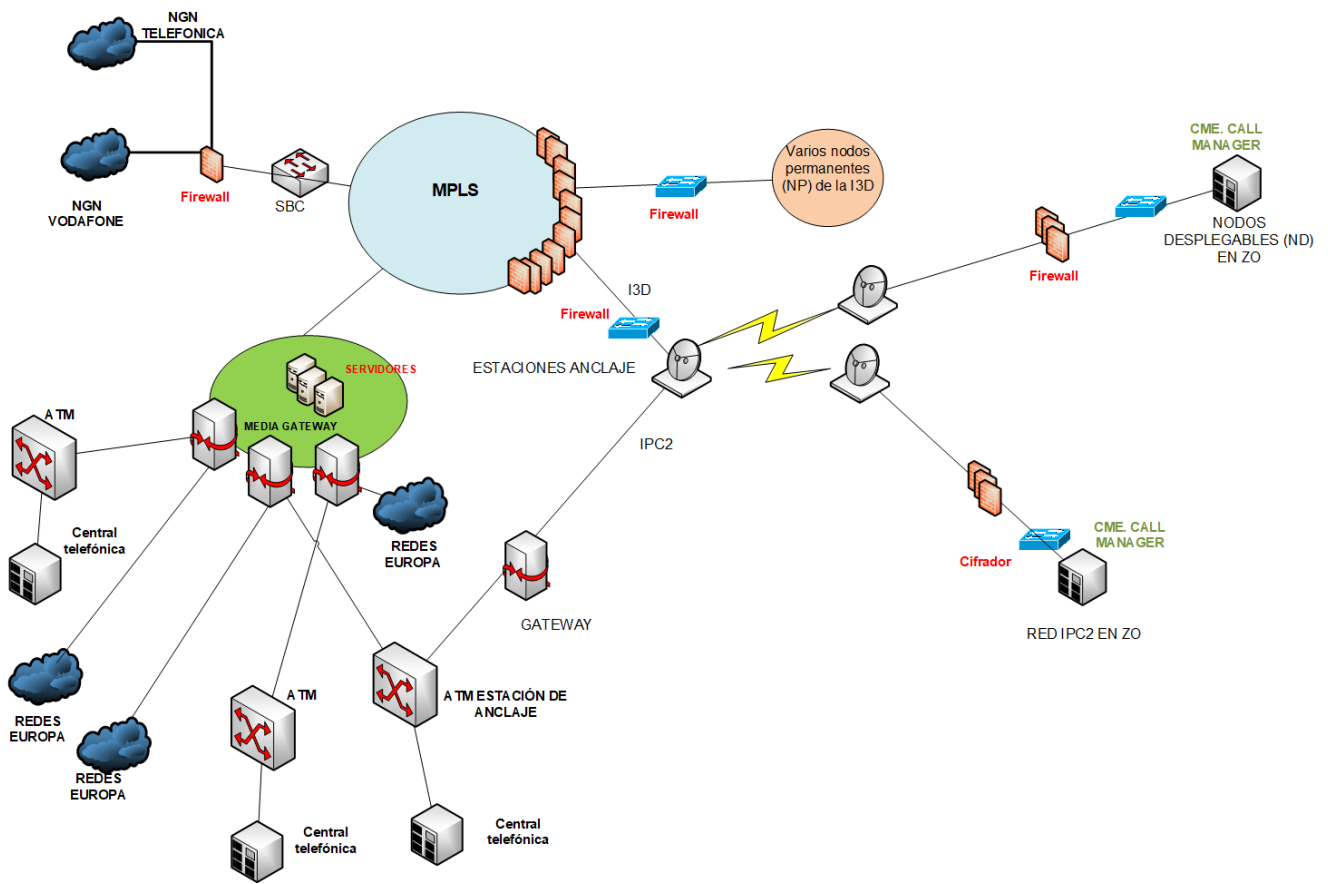


Figura 3-1 Red de telefonía (imagen propia)

En la Figura 3-2 se muestra cómo conviven el mundo de la red de ATMs con la nueva I3D que se está implantando.

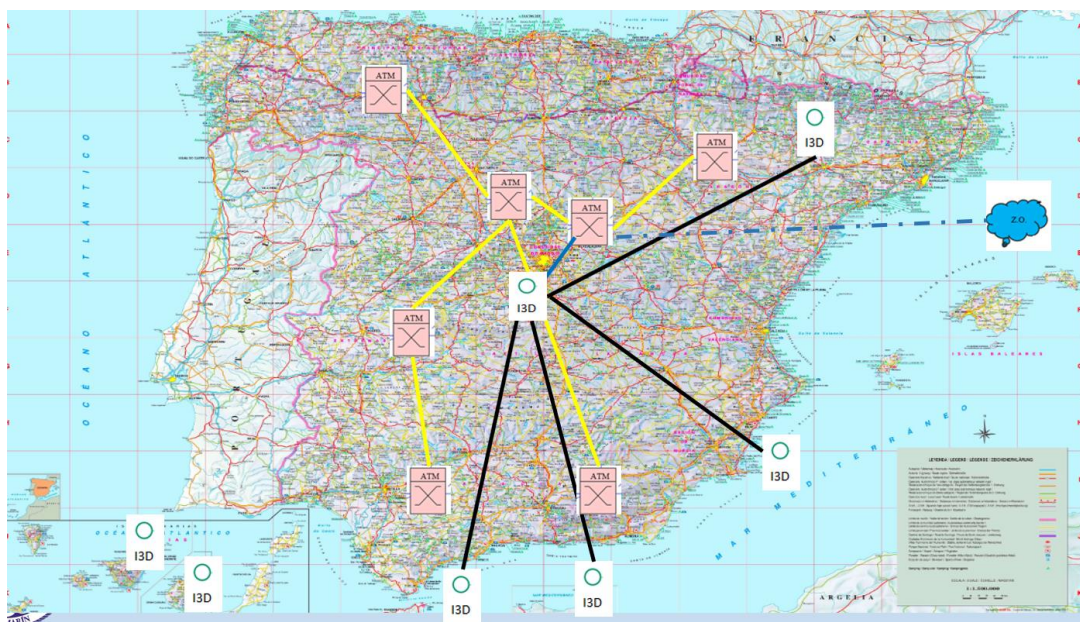


Figura 3-2 Red ATM e I3D (imagen propia)

El nexo entre la telefonía que está dando paso a la I3D y ésta última se da a través de los nodos ATM con los números 100 y 121. Esto permite comunicar los centros que ya están adaptados a la I3D con el mundo ATM. Además, se puede ver la conexión entre Zona de Operaciones y los ATM que se describirán con más detalle en apartados posteriores. Los círculos de la Figura 3-2 en color verde representan a las unidades donde ya se han implantado la I3D, siendo un ejemplo de cómo se comunican ambos mundos.

En relación con la I3D, los números de teléfonos de los usuarios se alojan en la nube de la MXONE pudiendo utilizar tantos números como queramos contratar y del lugar geográfico donde que queramos ubicarlos.

Es necesario comentar que cada teléfono de la I3D está conectado a cualquier conexión de Ethernet. Actualmente, los teléfonos se configuran como extensiones, teniéndose en cuenta su MAC, y no importa a qué puerto RJ-45 los conectemos porque mantendrán su numeración. Además, estos teléfonos tienen numeración para comunicarse interiormente de siete cifras (vxxxxxx) y un número de la red pública de nueve cifras (por ejemplo, 91xxxx).

Los ATM permiten envían grandes cantidades de datos permitiendo la integración de servicios de voz, video y datos en una única. ATM está siendo reemplazada por tecnologías más modernas como Ethernet y MPLS a costes más bajos e integración más sencilla con las redes IP. Desafortunadamente, la tecnología ATM no ha sido aprovechada al 100% de sus capacidades.

3.2 Arquitecturas

3.2.1 Arquitectura de telecomunicaciones de un nodo permanente de la I3D

Dentro de la infraestructura de baja clasificación se puede determinar: una serie de switches, firewalls y teléfonos.

Las fronteras (firewall, FWFRT) que se están instalando se conectan a través de la MPLS del operador. La red MPLS es una red protegida que se conecta a la MXONE virtualizado en dos sedes distintas. Es decir, desaparece el concepto pasado de los teléfonos que se conectaban a la central de su unidad. De tal manera que los teléfonos se dan de alta y conectan a un servidor central denominado MXONE.

Dentro de cada unidad, los switches desplegados manejan la información de los dominios de seguridad. Seguidamente, se producirá una separación lógica en VLAN, aunque físicamente estén conectados, de tal manera que se implementará diferentes dominios. Esto permite la creación de VLAN funcionales como puede ser para ordenadores, teléfonos IP, servidores, impresoras, etc., que estarán dentro de cada dominio de seguridad. Cada VLAN gestionará su parte de la infraestructura de baja clasificación. En este caso, al disponer de dos Firewall habrá dos enlaces troncales, cada uno a cada Firewall de Frontera, y que irán hacia las VLAN definidas. En el caso de que hubiese un Firewall sería necesario únicamente un enlace troncal.

Los elementos hardware que van a formar parte de esta arquitectura, en nodo permanente, son firewall/ frontera, switch de core, switches de acceso, VoIP Media Gateway y teléfonos.

Existen varias funciones de las que se encarga los firewalls como filtrar el tráfico VoIP para permitir solo las conexiones autorizadas, protege al sistema frente a ataques de tipo DDoS, *malware* o *phishing*.

Los switches de core son responsables de controlar el tráfico de datos entre los diferentes switches que a él se conectan, así como los equipos que a éstos últimos se unen. La función que tienen asignada es enrutar de forma rápida y eficiente entre los distintos switches de acceso y hacia el exterior. Además, se caracterizan por una gran capacidad de procesamiento, ancho de banda, alta disponibilidad y redundancia que garantice su operatividad.

La función del switch de gestión es agrupar y controlar el tráfico de varios conmutadores de acceso y encaminarlos hacia el núcleo de la red o hacia otros segmentos de la red. Además, posee la capacidad de segmentar la red en VLANs y gestionar las políticas de la red como la calidad de servicio (QoS). Se conecta directamente al switch de core. Es necesario matizar que los teléfonos que utilizan los usuarios se conectan a los switches de acceso.

El VoIP Media Gateway, como se ha visto en la teoría los Media Gateway, son utilizados en las redes de telefonía IP para conectar la red de telefonía tradicional (PSTN) con la red IP (voz sobre paquetes). Con la ayuda de estos equipos se logra que se puedan transformar las llamadas telefónicas desde el mundo IP al mundo de la telefonía tradicional y viceversa. Es decir, se puedan realizar llamadas desde números de teléfonos analógicos siguiendo un camino de dos hilos hasta el media Gateway que realiza el cambio al mundo IP y viceversa.

Los teléfonos que actualmente se están desplegando en los nodos permanentes corresponden a las marcas Grandstream y MITEL [29]. Además, a parte del número que le corresponda y que se conectan a los switches de acceso, tendrá asignada una dirección IP que será monitorizado desde la MXONE. Es necesario aclarar que las antiguas centrales telefónicas que estaban ubicadas en las unidades están siendo retiradas y sustituidas por esta nueva arquitectura donde el servidor MXONE es el elemento central de los teléfonos.



Figura 3-3 Fuente: mitel teléfono serie 6900 [29]

Es necesario tener en cuenta que, si el switch de core pierde la conexión con la red MPLS, todos los teléfonos pertenecientes a esa unidad no podrán comunicarse ni entre ellos ni con el exterior. Sin embargo, para los nodos desplegables no ocurrirá así dado que se ha instalado un equipo denominado call manager que permitirá la conexión entre los teléfonos perteneciente a esa unidad, aunque se hayan quedado aislado con el exterior. Ciertamente existe otra excepción como son determinados centros donde se instalarán unos servidores de supervivencia de telefonía denominados EX (Exchange) que permitirá la comunicación interna en el caso de pérdida de conexión con la MXONE. En el momento que se recupera la conexión con la MXONE, el servidor EX entrega el control y sincroniza los registros y las llamadas.

Cuando las unidades pasan a la telefonía de I3D, se asigna una numeración acotada a los CECOM para que éstos puedan decidir los números a los nuevos usuarios en su unidad.

Otro aspecto para tener en cuenta es que en los nodos permanentes no implementan en su arquitectura el equipo call manager.

En esta tabla 3-3 se describe los segmentos de red donde aparecen las VLAN y los nombres con las funciones correspondientes (la gestión de red, central VoIP de la central, servidores, impresoras, media Gateway, etc.) y se le asignan distintas VLAN. Se quiere mostrar una idea de cómo funciona en baja clasificación y cómo se divide la red donde forma parte la telefonía junto con otros servicios que se ofrecen.

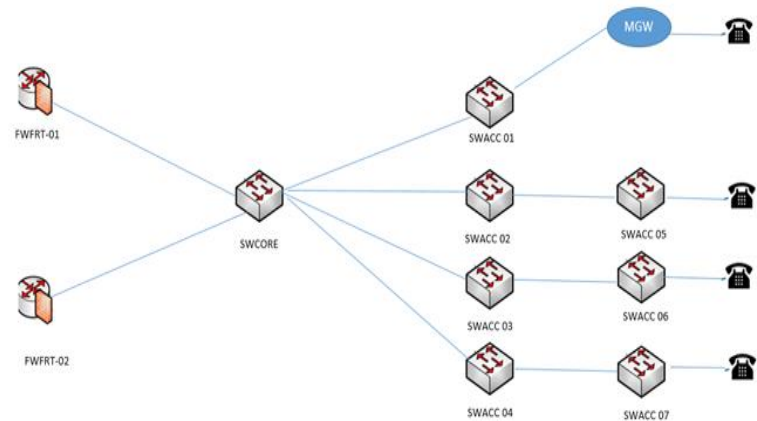


Figura 3-4 Nodo permanente (imagen propia)

En la Figura 3-4, se muestra la imagen de la arquitectura de equipos en el nodo permanente. Mientras que en la tabla 3-1 se puede ver el listado de los equipos que componen el nodo permanente. Es importante añadir que el media *Gateway* se encargará de integrar a los teléfonos analógicos en la red I3D.

Equipo	Observaciones
FWFRT	Es la frontera
SWCORE	Es el switch de core
SWACC	Es el switch de acceso
MGW	Conecta a los teléfonos analógicos a la red I3D

Tabla 3-1 Equipos nodo permanente

En la tabla 3-2, se muestra el inventario de equipamiento de red de este nodo. En esta, aparecen los switches de core (SWCORE), de acceso (SWACC) con el modelo del equipo.

Equipo	Características básicas
SWCORE	Switch de 24 puertos SFP 1Gb/10Gb, 3 puertos QSFP
SWACC01	Switch 48 puertos 10/100/1000BASE-T, 2 puertos QSFP
SWACC02	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP
SWACC03	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP
SWACC04	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP
SWACC05	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps
SWACC06	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps
SWACC07	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps

Tabla 3-2 Inventarios equipos de red nodo permanente

A continuación, se muestra la tabla 3-3:

VLAN	Observaciones	IP
70	Asignación direccionamientos IP a los ordenadores	192.43.194.128/23
120	Gestión de la red	192.78.68.40/25
170	Gestión de los servidores	192.43.197.64/27
270	Gestión de las impresoras	192.43.197.128/25
250	Gestión de otros dispositivos	192.78.69.24/25
380	Telefonía VoIP. Teléfonos registrados en la MXONE	192.76.214.43/22
421	Teléfonos analógicos a la VoIP con un Media Gateway	192.76.250.8/29

Tabla 3-3 VLAN asignadas

Conectaremos los teléfonos a los switches de acceso con los valores 05, 06 y 07. Y éstos, colgarán de otros tres switches en cascada con la numeración 02, 03 y 04 respectivamente, tal y como aparece en la Figura 3-4.

Los teléfonos se conectarán a los switches de acceso que serán gestionados por VLAN asignadas en la tabla 3-3. VLAN 380 corresponde con los terminales telefónicos que se conectan a la central local MXONE. Mientras que VLAN 120 se encarga de gestionar los dispositivos de red (como routers, switches, firewalls, etc., en sus configuraciones de dispositivos, monitoreo y administración) usando la misma red que transporta el tráfico regular de datos como navegación web o datos.

La VLAN, con denominación 421, adaptará los teléfonos analógicos a la VoIP con un media Gateway. Como ya se indicó el media *Gateway* se encargará de integrar a los teléfonos analógicos en la red I3D.

Para la configuración, administración y configuración de los switches y sus puertos se utilizarán las direcciones IP descritas en las tablas 3-3 y 3-4. Además, para realizar la configuración se pueden utilizar SSH⁷⁷, Telnet, etc.

En la Tabla 3-4 se describe los switches con sus modelos e IP que se les han asignado.

⁷⁷ SSH: Secure Shell

Equipo	Características básicas	IP
SWCORE01	Switch de 24 puertos SFP 1Gb/10Gb, 3 puertos QSFP	192.78.212.1/23
SWACC01	Switch 48 puertos 10/100/1000BASE-T, 2 puertos QSFP	192.78.212.2/23
SWACC02	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	192.78.212.3/23
SWACC03	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	192.78.212.4/23
SWACC04	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	192.78.212.5/23
SWACC05	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps (x3)	192.78.212.6/23
SWACC06	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps (x3)	192.78.212.7/23
SWACC07	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps (x3)	192.78.212.8/23

Tabla 3-4 Relación switches nodo permanente

En la Tabla 3-5 se muestra la relación entre los switches y las VLAN configuradas.

Equipo	Características básicas	VLAN
SWCORE01	Switch de 24 puertos SFP 1Gb/10Gb, 3 puertos QSFP	70,120,170,270,250,380,421
SWACC01	Switch 48 puertos 10/100/1000BASE-T, 2 puertos QSFP	70,120,170,270,250,380,421
SWACC02	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	70,120,170,270,250,380,421
SWACC03	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	70,120,170,270,250,380,421
SWACC04	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	70,120,170,270,250,380,421
SWACC05	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps	70,120,170,270,250,380,421
SWACC06	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps	70,120,170,270,250,380,421
SWACC07	Switch 48 puertos 10/100/1000BASE-T y 4 puertos SFP 1Gbps	70,120,170,270,250,380,421
VOIP_MGW (Media Gateway)		120, 380

Tabla 3-5 Relación de switches y VLAN asignados

La tabla 3-6 muestra los puertos del switch de core. En las observaciones se puede ver la palabra “Troncal”, ésta corresponde con la conexión entre dos switches. En caso de ser “acceso” corresponde con la conexión entre el switch de acceso y por un teléfono u otro dispositivo físico como puede ser un pc. Se dejan los puertos 1 al 18 del SWCORE para posibles conexiones de teléfonos, pc, etc., para

cubrir posibles eventualidades. Para realizar las conexiones con los firewalls, se van a usar los puertos 19 y 20.

Hay que tener en cuenta que para conectar el switch de core y el switch de acceso número 01, la velocidad será de 1Gbps por el puerto número 21 del switch de core que será suficiente. Mientras que, en el caso de desear mayor velocidad, en este caso 10 Gbps, se podrá conectar uno de los puertos denominados 1q o 2c del switch de core con el puerto denominado 4p perteneciente al switch de acceso 01.

Tomando como referencia la Figura 3-4, el switch de core se conecta con los switches de acceso 02, 03 y 04. Para ello, usaremos los puertos 22, 23 y 24 del switch de core. Se puede indicar que los puertos del switch de core comprendidos entre el 1 y el 24 ofrecen una velocidad de 1 Gbps. Mientras que los puertos 1p y 2q ofrecen una velocidad de 10 Gbps. Es importante que el usuario decida a qué velocidades debe conectar el switch de core con los switches de acceso.

Puerto	Conectado a	VLAN	Observaciones
1..18			Acceso
19	FWFRT-01	70,120,170,270,250,380,421	Troncal
20	FWFRT-02	70,120,170,270,250,380,421	Troncal
21	Puerto 1 SWACC-01	70,120,170,270,250,380,421	Troncal
22	Puerto 24 SWACC-02	70,120,170,270,250,380,421	Troncal
23	Puerto 24 SWACC-03	70,120,170,270,250,380,421	Troncal
24	Puerto 24 SWACC-04	70,120,170,270,250,380,421	Troncal
1q		70,120,170,270,250,380,421	Troncal
2c		70,120,170,270,250,380,421	Troncal

Tabla 3-6 Designación de puertos del switch de core

La tabla 3-7 corresponde a la designación de puertos del switch de acceso 01. En este caso, se conecta su puerto número 1 con el puerto 21 del switch de core.

Se puede indicar que los puertos del switch de acceso 01 comprendidos entre el 1 y el 24 ofrecen una velocidad de 1 Gbps. Mientras que el puerto 4p ofrece una velocidad de 10 Gbps.

Puerto	Conectado a	VLAN	Observaciones
1	Puerto 21 SWCORE	70,120,160,260,320,370,411	Acceso (Voz y datos) y Troncal
2--24		70,120,160,260,320,370,411	Acceso
4p		70,120,160,260,320,370,411	Troncal
Ethernet 0/0	Puerto 2 de MGW	411	Acceso (Voz y datos) y Troncal

Tabla 3-7 Designación de puertos del switch de acceso 01

La tabla 3-8 corresponde con el Media Gateway. En el puerto 0/0 conectamos el Media Gateway con el puerto número 2 del switch de acceso 01 para manejar el tráfico de voz sobre IP, mientras que se dejan para los teléfonos analógicos los puertos comprendidos entre el 2 y el 24.

Puerto	Conectado a	VLAN	Observaciones
Ethernet 0/0 2--24	Puerto 2 de SWACC01	411	Acceso (Voz y datos) y Troncal Acceso

Tabla 3-8 Designación de puertos el Media Gateway

Los puertos de los switches de acceso 02, 03 y 04, que corresponde con el número 23, se conectan a los switches con numeración 05, 06 y 07 respectivamente en el puerto 23 y que se muestra en la tabla 3-9.

Puerto	Conectado a	VLAN	Observaciones
23	SWACC 05, 06 y 07	70,120,160,260,320,370,411	Acceso (Voz y datos) y Troncal
24	SWCORE	70,120,160,260,320,370,411	Acceso y troncal
4p		70,120,160,260,320,370,411	Troncal

Tabla 3-9 Designación de puertos de los switches de acceso 02, 03 y 04

Finalmente, los teléfonos colgarán de los switches de acceso 05, 06 y 07 que se muestra en la tabla 3-10 y que se conectan con los switches con numeración 02, 03 y 04 respectivamente en el puerto número 23.

Puerto	Conectado a	VLAN	Observaciones
23	Puerto 1 SWACC-02, SWACC-03 y SWACC-04	70,120,160,260,320,370,411	Voz, datos y troncal

Tabla 3-10 Designación de puertos de los switches de acceso 05, 06 y 07

3.2.2. Arquitectura de telecomunicaciones de un nodo desplegable de la I3D

Es necesario indicar que este tipo de arquitectura puede utilizarse en posiciones estáticas (edificios) como en posiciones dinámicas (vehículos o buques). Es importante aclarar que, aunque un vehículo o posición estático se encontrase en Territorio Nacional realizando maniobras, se le considera como nodo desplegable.

A parte de lo anterior, hay que añadirle otra posibilidad que es decidir si se incluye en la arquitectura call manager o no. Por ello, vamos a ver las dos posibilidades.

Con call manager

Los elementos hardware que van a formar parte de la arquitectura, que se va a presentar en este caso, en un nodo desplegable, son los que a continuación se relacionan: firewall, switch de core, call manager y tres switches de acceso que se muestra en la Figura 3-8. Es necesario aclarar que el hecho de que se habilite o no un switch de gestión dependerá de si se desea ocupar un número de puertos para realizar las funciones gestión en el switch de core o se prefiere instalar un switch de gestión.

La frontera (firewall), que se encuentra en el nodo desplegable, se conectan por vía satélite a las estaciones de anclaje que se encuentran situadas en España. Además, las llamadas realizadas por los teléfonos, que se encuentran en la estación, se encaminarán a través de su firewall [30] y están dados de alta a la MXONE situada en Territorio Nacional.



Figura 3-5 Firewall (Fuente: Tonitrus [30])

El *switch [31] de core* se encuentra en el núcleo de la red y es responsable de controlar el tráfico de datos entre las diferentes partes. La función que tiene asignada es enrutar de forma rápida y eficiente entre los distintos switches de acceso y hacia el exterior. Además, se caracterizan por una gran capacidad de procesamiento y ancho de banda. Y se le asigna una alta disponibilidad y redundancia que garantice su operatividad.



Figura 3-6 Switch (Fuente: instaladores de telecom hoy [31])

La función del *switch de gestión* (es opcional y en este caso no está) es agrupar y controlar el tráfico de varios conmutadores de acceso y encaminarlos hacia el núcleo o hacia otros segmentos de la red. Además, posee la capacidad de segmentar la red en VLANs, gestionar las políticas de la red como la calidad de servicio (QoS). Para el caso de la telefonía, al conectarse directamente al switch de core, puede transmitir el flujo de llamadas hacia los usuarios de la red o hacia la MXONE.

Los teléfonos que se están utilizando en los nodos desplegables corresponden a las empresas CISCO, *Grandstream* [32] y *MITEL*. Aparte del número que le corresponda y que se conectan a los switches de acceso, tendrá asignada una dirección IP y son registrados y monitorizados desde la MXONE situada en Madrid. Además, en el equipo MXONE se realiza la asignación de la numeración, así como las altas y bajas de los teléfonos que se despliegan.



Figura 3-7 Teléfono GXP1610 GRANDSTREAM (Fuente: grandstream[32])

Es necesario tener en cuenta que, si el switch de core pierde la conexión con la MXONE a través de su conexión satélite, el call manager express (CME) permitirá la conexión entre los teléfonos perteneciente a esa unidad.

Para integrarse el call manager en la I3D debe realizar previamente una configuración y despliegue de medios hardware y software que a continuación se mostrará mediante imágenes. Esta arquitectura establece donde se ubicarán los teléfonos, switch, etc., así como las VLAN necesarias para proteger las distintas partes del sistema con la ayuda de los firewalls/fronteras definidas previamente.

Cuando se conecta un teléfono a la red lo primero que se espera es que el DHCP del call manager le dé una dirección IP. A continuación, existen ciertos teléfonos que se tienen que dirigir a la MXONE para solicitar la configuración. Una vez recibido, se reinician pudiéndose utilizar posteriormente. Sin embargo, existen otros teléfonos que al estar asociados a la marca del equipo call manager no se tiene que dirigir a la MXONE sino al call manager donde reside el archivo de configuración para que, una vez descargado en el teléfono, se reinicie y pueda utilizarse.

Se propone una arquitectura, figura 3-8, donde se observa dos equipos firewall (FWFRT-01), un call manager CME-01 y un switch de core y tres switches de acceso. En el call manager, CME-01, se configuran los teléfonos que van a conectar a los switches de acceso SWACC-01, SWACC-02 y SWACC-03. Éstos tres últimos, se van a conectar en el switch SWCORE-01. En todos estos switches se van a configurar los puertos para la gestión de y otros puertos para los servicios. Por ejemplo, se configuran las VLAN para los distintos servicios como telefonía, etc. Por ello, es necesario remarcar que, si no se hace así, no puede acceder ni al CME ni a los switches de acceso para su configuración posterior.

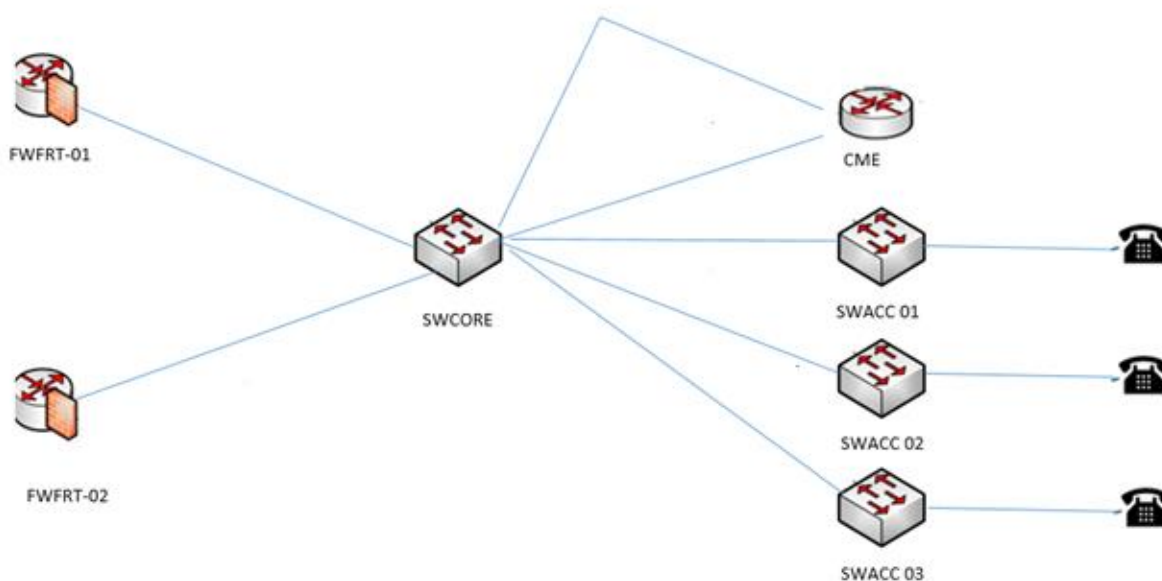


Figura 3-8 Nodo desplegable con call manager (imagen propia)

La arquitectura de equipos en el nodo desplegable está formada por la frontera (FWFRT), los switches de core (SWCORE), de acceso (SWACC) y el call manager (CME). En esta arquitectura se contemplan dos firewalls, switches de core y el call manager que se encargará de la gestión de los teléfonos que se van a integrar en los diferentes switches de acceso. Es necesario aclarar que existe la opción de añadir teléfonos directamente al switch de core que, aunque se haya instalado un call manager como se da en este caso, tiene conexión directa con la MXONE. El inconveniente es que, si se cae la conexión por satélite, los teléfonos que dependen del call manager podrán comunicarse internamente pero el que depende directamente de la MXONE se quedará sin funcionar. Un problema

que puede haber es tener una versión software del call manager no sea renovada o una versión software de tipo TRIAL de 90 días caduque. Para estos casos, no se podrá gestionar, ni hacer configuraciones ni dar altas o bajas, es decir, funcionará de forma muy limitada.

En la siguiente tabla, se muestra el inventario de equipamiento de red de este nodo. En esta, aparecen los switches de core (SWCORE), de acceso (SWACC), el call manager y los equipos frontera. Además, se añade el modelo del equipo y la dirección IP y VLAN que se le asigna.

Equipo	Características básicas	IP	VLAN
SWCORE	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos 1/10Gb SFP	192.77.72.1/29	70,71,110,3200,370,409
SWACC01	Switch de 24 puertos 10/100TX y 4 puertos SFP	192.77.72.2/29	70,71,110,3200,370,409
SWACC02	Switch de 24 puertos 10/100TX y 4 puertos SFP	192.77.72.3/29	70,71,110,3200,370,409
SWACC03	Switch de 24 puertos 10/100TX y 4 puertos SFP	192.77.72.4/29	70,71,110,3200,370,409
CME	4 puertos	192.77.72.5/29	70,71,110,3200,370,409

Tabla 3-11 Relación de equipos con sus direcciones IP y VLAN

A partir de aquí, se van a determinar las distintas VLAN. que van a estar presentes con sus direcciones IP. Sin embargo, solamente nos vamos a centrar en las ip de telefonía. Es necesario recordar que la VLAN deben estar en subredes distintas para segmentar el tráfico de red para mejorar la seguridad, mejorar la eficiencia y aplicar políticas de seguridad más concretas.

VLAN	Observaciones	IP
70	Asignación direccionamientos IP a los ordenadores	192.77.70.1/29
120	Gestión de la red	192.77.70.9/29
320	Gestión de otros dispositivos	192.77.70.17/29
370	Telefonía VoIP. Teléfonos registrados en el call manager	192.166.74.4/24
409	Conexión central local MXONE	192.166.75.5/30

Tabla 3-12 Relación de VLAN con sus direcciones IP y observaciones

Los teléfonos se conectarán a los switches de acceso que serán gestionados desde el call manager a través de las diferentes VLAN definidas. Una de las VLAN servirá para la conexión con los terminales telefónicos que se conectan a la central local, otros con la conexión con la central MXONE local a través de un TRUNK SIP. En otro caso, VLAN para la gestión de los dispositivos de red (como routers, switches, firewalls, etc., en sus configuraciones de dispositivos, monitoreo y administración) usando la misma red que transporta el tráfico regular de datos como navegación web o datos.

La IP de gestión es la dirección que se utiliza para acceder a la interfaz de administración del switch. Con esta interfaz se puede configurar y gestionar el switch incluyendo ajustes de puertos, VLAN, QoS, etc. Además, se puede acceder a esta IP con la ayuda de una consola web, SSH, Telnet o cualquier otro método. Es importante, no confundir con la IP del switch que es el que usa la red para

enrutarlo, comunicándolo con otros dispositivos. Por tanto, la IP de gestión permite administrar el switch, como configurar los puertos, etc.

En la tabla 3-13 se muestra los puertos del switch de core. En las observaciones se puede ver la palabra “Troncal”, ésta corresponde con la conexión entre dos switches. En caso de ser “acceso” corresponde con la conexión entre el switch de acceso y por un teléfono u otro dispositivo físico como puede ser un pc. Se dejan los puertos 1 al 18 del SWCORE para posibles conexiones de teléfonos, pc, etc., para cubrir posibles eventualidades. Se utilizan los puertos 19 y 20 para conexiones con los firewalls.

Puerto	Conectado a	VLAN	Observaciones
1..18		70,71,110,310,370,409	Acceso (Voz y datos)
19	FWFRT-01	70,71,110,310,370,409	Troncal
20	FWFRT-02	70,71,110,310,370,409	Troncal
21	Puerto 25 de SWACC-01	70,71,110,310,370,409	Troncal
22	Puerto 26 de SWACC-02	70,71,110,310,370,409	Troncal
23	Puerto 27 de SWACC-03	70,71,110,310,370,409	Troncal
24	CME	70,71,110,310,370,409	Troncal
26-28		70,71,110,310,370,409	Troncal

Tabla 3-13 Designación de puertos del switch de core

En la tabla 3-14 se muestra los puertos de los switches de acceso 01, 02 y 03. Para aquellos puertos con la numeración entre el 1 y el 22 se asignan a las tomas a los teléfonos de los usuarios o para ordenadores. Mientras que los puertos 25, 26 y 27 se conectan, por troncal, a los puertos 21, 22 y 23 del switch de core respectivamente. Finalmente, el puerto 24, ver también tabla 3-15, se conecta al call manager. Todos ellos tendrán una velocidad de conexión de 1Gbps.

Puerto	Conectado a	VLAN	Observaciones
1..22	Tomas de usuario	70,71,110,310,370,409	Acceso (Voz y datos)
25	Puerto 21 de SWCORE	70,71,110,310,370,409	Troncal
26	Puerto 22 de SWCORE	70,71,110,310,370,409	Troncal
27	Puerto 23 de SWCORE	70,71,110,310,370,409	Troncal
28			Troncal

Tabla 3-14 Designación de puertos de los switches de acceso 01, 02 y 03

Puerto	Conectado a	VLAN	Observaciones
Puerto GE1/1 o GE1/2	Puerto 24 de SWCORE	110,370,409	Troncal

Tabla 3-15 Designación de puertos del call manager

Finalmente, se muestra la configuración de los troncales, terminales telefónicos con los códecs correspondientes. Es necesario aclarar que los códec G722, G729A, G723 son de audio y se utilizan para comprimir y descomprimir datos de audio. De tal manera que son esenciales para convertir la voz en datos digitales para transmitirse por la red.

El códec G729A es una versión de G729 es un algoritmo de compresión tanto de voz como de datos. De hecho, la versión A de G.729 es una variante con una calidad de voz inferior. Mientras que la versión G.729 AB consiste en supresión de silencios VAD que detecta periodos de silencio en la conversación y reduce el uso de ancho de banda al no transmitir datos de voz durante estos periodos.

En relación con G.722 transmite el audio en el rango de frecuencia comprendido entre 50Hz y 7kHz lo que implica una calidad mejor que los códec de banda estrecha como G.729 y G.723. G.722 se utiliza para videoconferencias donde la calidad de la voz es esencial.

Se debe indicar que el códec G.723 opera en 5,3 kbps o 6,3 kbps cuyo ancho de banda es limitado y es utilizado en enlaces de baja velocidad.

Los códec G.729 A y G.729 AB se pueden utilizar en los sistemas de comunicación unificados tales como Telefonía IP, mensajería instantánea, correo electrónico, conferencias de audio y video, etc. Mientras que los códec G.729 y G.722 permiten utilizar las aplicaciones Skype y Microsoft Teams para el primero y Zoom para el segundo. En el caso de que la conexión sea con un nodo desplegable, donde se asume que la conexión será por vía satélite, al enviarse los datos puede haber problemas de latencia.

Concepto	Códec	Observaciones
Troncal SIP	G729AB, G722, G729A, G723	4 canales simultáneos hacia la MX-ONE
Terminales telefónicos	G729AB	

Tabla 3-16 Códec

En la siguiente tabla se exponen los modelos de teléfonos utilizando la MAC, el número de teléfono interior y el número asociado con la red pública que se le asociada como si estuviese en la zona donde se encuentre (puede ser Madrid, Ceuta, Melilla, Murcia, etc). Sin embargo, se toman las medidas software necesarias para que, en el caso necesario de llamar al 112, se conecte a la red de la zona. Sin embargo, no es aplicable a Zona de Operaciones.

Modelo	MAC	Extensión	DDI
zzzz	7C95XXXX09B6	YY0XXXX	+349145XXXX
Zzzz	DCA5XXXX18C6	YY0XXXX	+3491454 XXXX
zzzz	DCAXXXX719FA	YY0XXXX	+349145 XXXX
ATA		YY0XXXX	+349145 XXXX

Tabla 3-17 Modelo de teléfono con asignación de extensión telefónica y DDI

Puede ocurrir que los teléfonos desplegados en ZO no tengan asignado un número de teléfono, o DDI, para que se les pueda llamar desde otra red exterior. Para solucionarlo, se entra en la NGN de la I3D y se le asigna un número DDI con numeración 91xxxx. De esta manera, no solo podrán llamar al

exterior sino también podrán recibir llamadas desde el exterior. Este caso, es asimilable para aquellos despliegues donde no hay instalado un call manager.

Sin call manager

Se puede decir que la arquitectura es exactamente igual que el caso de call manager pero con la diferencia de que en caso de que produzca una caída de conexión a través del satélite, los teléfonos no se podrán comunicar entre sí ni con otros que se encuentren en otras ZO o en Territorio Nacional.

Todos los teléfonos, antes de ser enviados a zona de operaciones, se tienen que programar, conectar a la MXONE y probar que funcionen correctamente. Una vez que sean enviados, se podrán conectar tanto a los switches de acceso como de core.

En la Figura 3-9 se muestra la arquitectura sin call manager.

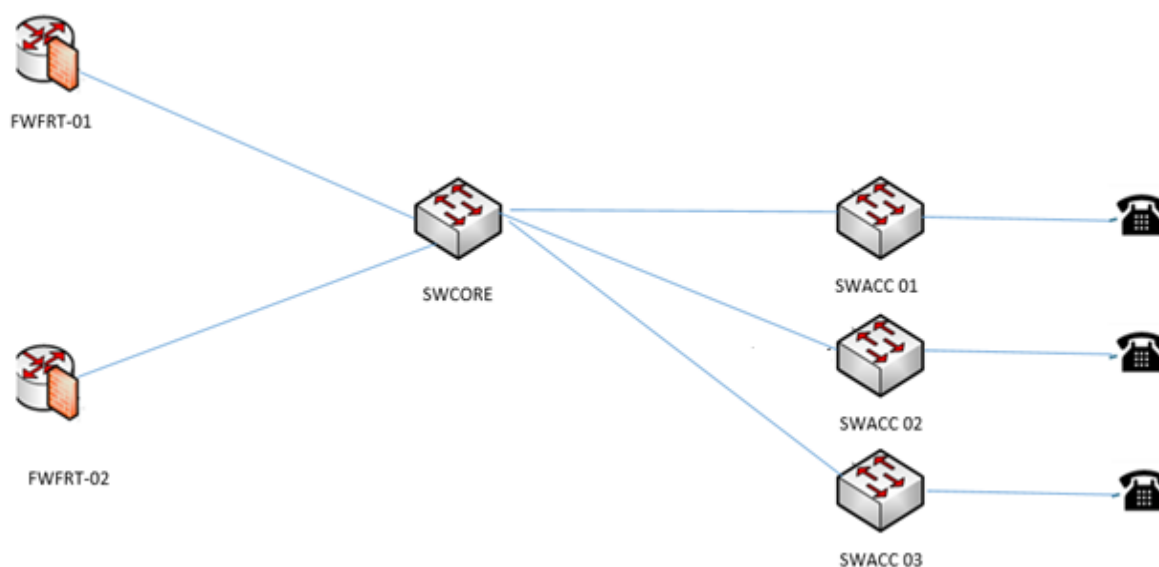


Figura 9-9 Nodo desplegable sin call manager (imagen propia)

En la siguiente tabla, se muestra el inventario de equipamiento de red de este nodo. En esta, aparecen los switches de core (SWCORE), de acceso (SWACC) y los equipos frontera. Además, se añade el modelo del equipo y la dirección IP que se le asigna.

Equipo	Características básicas
SWCORE	Switch de 24 puertos 10/100/1000BASE-T y 4 puertos SFP
SWACC01	Switch de 28 puertos 10/100 y 4 puertos 100/1000X SFP
SWACC02	Switch de 28 puertos 10/100 y 4 puertos 100/1000X SFP
SWACC03	Switch de 28 puertos 10/100 y 4 puertos 100/1000X SFP

Tabla 3-18 Inventario equipamiento de red en nodo desplegable

A partir de aquí, se van a determinar las distintas VLAN. que van a estar presentes con sus direcciones IP. Sin embargo, solamente nos vamos a centrar en las IP de telefonía. Es necesario recordar que las VLANs deben estar en subredes distintas para segmentar el tráfico de red para mejorar

la seguridad, mejorar la eficiencia y aplicar políticas de seguridad más concretas. Respecto al caso anterior, se elimina la VLAN 370 que hace referencia a los teléfonos registrados en el call manager.

VLAN	Observaciones	IP
70	Asignación direccionamientos IP a los ordenadores	192.77.70.1/29
110	Gestión de la red	192.77.70.9/29
320	Gestión de otros dispositivos	192.77.70.17/29
409	Conexión central local Trunk SIP MXONE	192.166.92.17/30

Tabla 3-19 Relación de VLAN con sus direcciones IP y observaciones

3.2.3. Arquitectura servidor MXONE virtualizado

En esta arquitectura, que se muestra en la figura 3-10, existen dos ubicaciones físicas. En estas puede haber cuatro, cinco, etc., servidores físicos en cada uno de ellos. Todo dependerá de la necesidad del usuario. Todos ellos constituyen un único clúster, a pesar de estar separados. Estos servidores llevan instalados un sistema operativo que centraliza la monitorización y configuración de estos servidores. Además, se emplea vCenter para monitorizar y configurar estos servidores.

Por otro lado, existen dos cabinas de almacenamiento NetApp, o de otro tipo de marca, de una cierta capacidad en TB utilizado para el despliegue de máquinas virtuales, que se comunican por el protocolo iSCSI. Además, es apropiado que el número de cabinas sea cuatro. Es necesario aclarar que tanto los servidores y las cabinas ubicadas en los dos emplazamientos, estén comunicados entre sí y comparten sus recursos.

El objetivo es disponer de una plataforma para desplegar las máquinas virtuales para prestar el servicio de telefonía. En el caso de que sea necesaria la migración de las máquinas virtuales entre los dos servidores, se configurará en el clúster el Distributed Resource Scheduler (DRS). De hecho, éste último tiene como misión analizar los recursos de cada servidor, siendo una funcionalidad de vMware Sphere.

Una de las ubicaciones se encontrará en modo activo y el otro en modo pasivo. De tal manera que, el que se encuentre en modo pasivo realizará los backups periódicos de los datos almacenados en el nodo activo.

Dentro de cada servidor habrá los siguientes servicios:

- vCenter: Gestiona las máquinas virtuales. Además, se encarga del balanceo entre los servidores cuando sea preciso.
- NetApp Mediation: Gestiona la distribución de datos en las cabinas.
- MICAM CallServer: Controla las llamadas telefónicas desde su inicio hasta su finalización.
- Provisioning Manager: Configura nuevas extensiones telefónicas.
- Media Processing Application: Convierte los formatos de audio y video. Gestiona las videollamadas.
- Data Base: Almacena información como configuración de usuario e historial de llamadas.
- Media Server: Reproduce música o grabación de audio cuando una llamada está en espera.
- Service node: Verifica que cuando un usuario quiere hacer una llamada, comprueba que está disponible. O en el caso de que un usuario quiera hacer una llamada al exterior de su red privada, le permitirá o no realizarla si tiene ciertos privilegios.

- Servicios de red: Utiliza los servicios como DHCP, para asignar direcciones IP, DNS y NAT.
- SBC: Protege las comunicaciones de voz y video.

Cada uno de ellos, ofrecerán distintas capacidades de almacenamiento RAM, HDD y CPU todas ellas virtualizadas

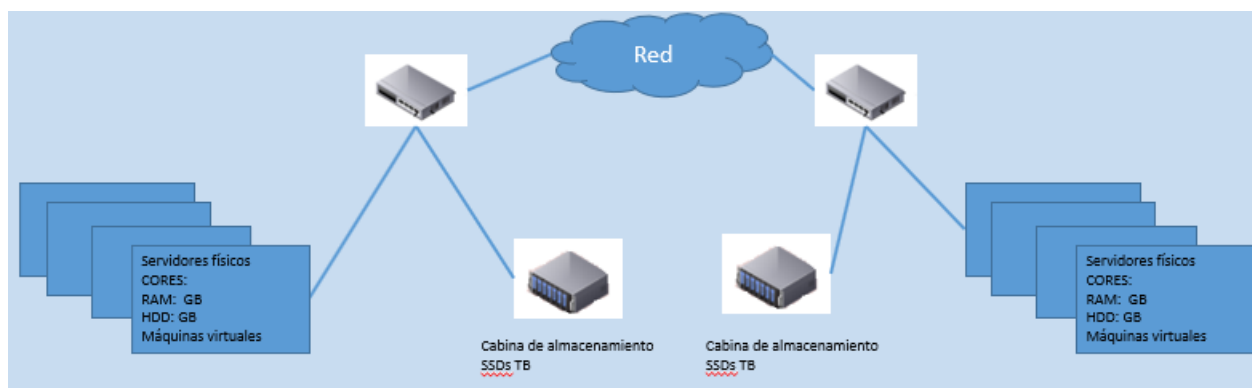


Figura 3-10 Distribución equipos de la MXONE (imagen propia)

3.3 Implantación de los nodos permanentes en la I3D

3.3.1 Proceso de implantación en la I3D

En todo proceso de implementación, en ingeniería, es necesario cumplir una serie de hitos que garanticen el cumplimiento de los objetivos deseados. Una vez que todos los requisitos de la implantación de la I3D ya están establecidos y la documentación generada, nos encontramos en los inicios del trabajo de implementación.

3.3.2 Planificación y documentación previa

En este hito se debe realizar una o varias reuniones donde se revisen los requisitos establecidos. Viéndose el inventario de equipos necesarios, compatibilidad entre ellos y las versiones software que se deben implementar. A partir de ahí, es necesario crear un calendario de recepción de equipos e instalaciones anuales por unidades, teniendo en cuenta las particularidades de cada una de ellas, diseñando la red de diagramas que muestren la tipología donde se incluyan la conexión entre los dispositivos, para nuestro caso los switches, firewall, teléfonos, etc. Además, los materiales que se instalen no sólo ser contabilizados, sino también deben cumplir con la legislación relativa a la catalogación para garantizar que el proceso de mantenimiento y abastecimiento queden garantizados en todo el ciclo de vida del sistema.

Debido a la gran cantidad de documentación que se va a generar, es importante reseñar que estos servirán de guía para las instalaciones.

Hay que tener en cuenta que no es comparable adaptar a la I3D una unidad pequeña o un nodo desplegable, que para este último se realiza y se envía desde TN⁷⁸ a ZO⁷⁹, que un nodo permanente que debido a su complejidad y tamaño precisa de más tiempo para llevarlo a cabo.

Un aspecto muy importante, es la coordinación entre las distintas áreas involucradas dado que sin el apoyo de éstas el objetivo no se podría lograr. Desde la configuración de las VLAN, puertos de los switches hasta la configuración final de los teléfonos conforman una cadena que van de la mano para ofrecer un servicio al usuario final.

⁷⁸ TN: Territorio Nacional

⁷⁹ ZO: Zona de Operaciones

Se establecerá un plan de pruebas donde se definan los objetivos de las pruebas, asignar responsabilidades y recursos para las pruebas.

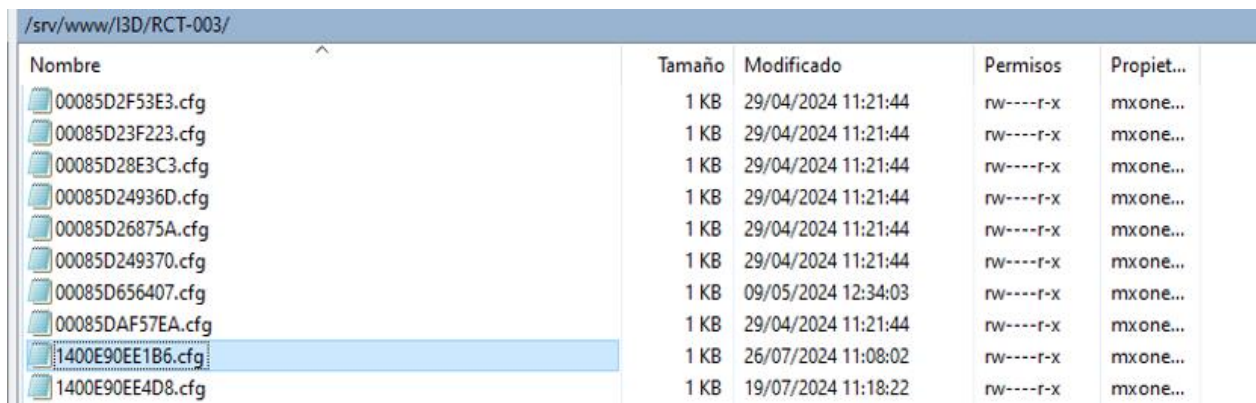
3.3.3 Instalación física y configuración inicial

En este punto, se realiza un trabajo concreto por cada unidad. Se contabiliza las unidades necesarias de los equipos que deben instalarse. A partir de ahí, se procede a la instalación de firewalls y switches y teléfonos en la ubicación designada. Se conectarán a los switches adecuados y a las fuentes de alimentación. A continuación, se procede a la configuración básica de equipos: En los firewalls se configurarán interfaces, políticas básicas de seguridad y reglas de acceso. La configuración de las VLAN, puertos y protocolos de red se realizará en los switches. La configuración de los interfaces de red y parámetros básicos de VoIP en los Media Gateway. Finalmente, en los teléfonos VoIP se configurarán los parámetros de red y perfiles de usuario.

A continuación, se muestra de forma más concreta cómo se realizaría en la parte de voz.

En este punto, nos encontramos en el momento en el que la instalación física ya se ha realizado. A partir de aquí, el personal de las unidades implicadas en la instalación tomará el documento donde viene reflejado la arquitectura. Determinará las VLAN para la arquitectura de baja clasificación. Una vez definida se determinará las direcciones IP para cada uno de los equipos que han sido instalados. Mientras que la sección de IP determinará las VLAN y el PATH a través de una aplicación software para que la sección de conmutación pueda conectar los teléfonos a la MXONE. Desde la sección de conmutación, antes de recibir el PATH de conexión dará de alta los teléfonos en la MXONE. Para ello, necesita varios parámetros, pero los más importantes son la MAC del teléfono y el número de extensión. Es importante añadir que una vez que estos teléfonos se conecten por primera vez a la roseta con conexión RJ-45, se descargarán los ficheros de configuración y será reconocido por la MXONE.

Cuando se conecta un teléfono a la red lo primero que se espera es que el DHCP de los servidores de la MXONE y le dé una dirección IP. A continuación, existen ciertos teléfonos que se tienen que dirigir a la MXONE tiene que solicitar la configuración. Una vez recibido, se reinician pudiéndose utilizar posteriormente. Ver figuras 3-11 y 3-12.



Nombre	Tamaño	Modificado	Permisos	Propiet...
00085D2F53E3.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D23F223.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D28E3C3.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D24936D.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D26875A.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D249370.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
00085D656407.cfg	1 KB	09/05/2024 12:34:03	rw----r-x	mxone...
00085DAF57EA.cfg	1 KB	29/04/2024 11:21:44	rw----r-x	mxone...
1400E90EE1B6.cfg	1 KB	26/07/2024 11:08:02	rw----r-x	mxone...
1400E90EE4D8.cfg	1 KB	19/07/2024 11:18:22	rw----r-x	mxone...

Figura 3-11 Alta número de teléfono 1 (imagen propia)

```
MDSH> extension -p -d 8112534
MDSH> extension -i -d 8112534 -l 2 --csp 2 --feature-level basic
MDSH> ip_extension -i -d 8112534 --protocol SIP
MDSH>
```

Figura 3-12 Alta número de teléfono 2 (imagen propia)

La ventaja de estos teléfonos es que se pueden conectar en cualquier ubicación sin perder el número de teléfono. No es como en el pasado que el puesto/roseta iba asociada al número de teléfono. Esto permite una flexibilidad importante.

3.3.4 Configuración avanzada

En este caso, es preciso realizar la configuración de los firewalls donde se implementarán las reglas de seguridad, NAT, etc. Además, se establecerán procedimientos para la inspección de paquetes y prevención de intrusiones. Se implementará la seguridad en los puertos de los switches. Respecto a los Media Gateway y VoIP se configurarán los protocolos de señalización (como son H.323, SIP) y configurar los códec de audio. Se procederá a la integración con MPLS estableciendo las políticas de enrutamiento para el tráfico VoIP y datos. Además, se configurarán los dispositivos para conectar ambas redes. Seguidamente, se procederá a la integración con la MXONE configurando éste para gestionar y controlar todos los equipos. Asegurarse que la conexión y comunicación con todos los dispositivos es correcta.

3.3.5 Plan de verificación y pruebas detallado.

Se establecen una serie de pruebas, tanto hardware como software, que verifiquen el correcto funcionamiento de la instalación realizada. En relación con las pruebas hardware se verificará que todas las conexiones son correctas y que los LED⁸⁰ de enlace entre los equipos funcionen adecuadamente. Además, pruebas de diagnóstico que aseguren que no hay defectos de hardware. Mientras que en las pruebas software, para el caso de los firewalls se verificarán las reglas de acceso y políticas de seguridad. Respecto a los switches, se debe validar la configuración de las VLAN y verificar la priorización del tráfico VoIP. En los Media Gateway se comprobará la configuración de los protocolos de señalización y la funcionalidad de las llamadas.

Una vez comprobados los componentes hardware y software se llevarán a cabo una serie de pruebas que son de conectividad y rendimiento, donde se testee las conexiones internas (*ping* y *traceroute*) y que la priorización es correcta. Probar la conexión a través de la MPLS con otras redes privadas. Verificar la latencia, jitter y pérdida de paquetes. Comprobar el rendimiento de la red usando herramientas de monitoreo para comprobar el tráfico de la red.

Respecto a las pruebas de seguridad se utilizarán ciertas herramientas para identificar vulnerabilidades en todos los dispositivos de la red. Además, se realizarán prueba de penetración para evaluar la efectividad de las políticas de seguridad. Seguidamente, se procederá a realizar inspecciones de los firewalls comprobando que las reglas cumplen con lo establecido.

Para las pruebas de funcionalidad se harán llamadas de prueba para evaluar la claridad, latencia y ausencia de eco o ruido. Se realizarán múltiples llamadas simultáneas para asegurar que el sistema puede soportarlo. Además, se comprobará que las llamadas y datos son gestionados correctamente con la MXONE.

Mientras que para las pruebas de integración con la MXONE se verificará que éste monitorea el estado de todos los dispositivos en tiempo real. Se debe comprobar que este sistema envía alertas en caso de fallos, intrusiones o degradación del servicio. Además, se debe confirmar que se pueden aplicar configuraciones y actualizaciones de forma remota y eficiente.

Finalmente, se van a realizar pruebas de redundancia y recuperación donde se desconectan los dispositivos temporalmente como pueden ser firewalls, switches, media Gateway para verificar que la red manejar adecuadamente los fallos y existe mecanismos de redundancia. Para el caso de recuperación ante desastres lo que se hará es evaluar el tiempo de recuperación de la red y asegurar que los procedimientos establecidos son efectivos.

⁸⁰ LED: Light Emitting Diode

A continuación, se muestra de forma más concreta cómo se realizaría en la parte de voz.

No sólo hay que realizar la conexión sino también una serie de comprobaciones, es decir, realizar llamadas tanto a teléfonos de la I3D como a teléfonos de la red de ATM, móviles, fijos de la red pública y contactar con Zona de Operaciones. Todas estas pruebas deben establecerse y realizarse, aparte del resto de pruebas que afecten a otros servicios tanto de baja como de alta clasificación, donde pueda comprobar que cumple con los requisitos de establecimiento/recepción de llamadas en la unidad donde se realizó la instalación.

A continuación, se plantea una serie de pruebas de validación y verificación. Es necesario aclarar qué son exactamente. La verificación es el proceso de comprobar si el producto cumple con los requisitos técnicos y funcionales. Es decir, nos preguntamos si hicimos el trabajo correctamente. Para ello, se realiza una revisión si el producto se ha construido conforme a las especificaciones dadas. Las pruebas consisten en la inspección, pruebas, revisión de documentos y análisis. La inspección es hacer una visual de los componentes. Mientras que las pruebas son test funcionales. Otro aspecto importante es la revisión de documentos que consiste en comprobar la documentación técnica realizada. Mientras que el análisis son teóricas basadas en cálculos. Todo esto implica un tiempo que se debe dedicar para comprobar si las pruebas de verificación son correctas. De hecho, se tendrá que realizar un documento que indique si los resultados son correctos o no. Para la verificación, en este caso, se pueden centrar en la creación de los diagramas de red, configuración de los equipos, que se ha seguido el plan de instalación comprobando los componentes hardware (teléfonos, switches, routers, servidores) en los lugares correctos, verificar conexiones de cables y la infraestructura de red (cable estructurado y tomas de red).

Las pruebas, que como hemos indicado son funcionales, consistirán en llamadas entre teléfonos de la I3D, de la I3D a la red IPC2, teléfonos en la red pública civil y con Zona de Operaciones. También se añadirán transferencias de llamadas, buzón de voz, etc.

Mientras que las *pruebas de validación* consisten en el sistema cumple con las necesidades de los usuarios finales. Estas pruebas se realizarán en sesiones de prueba en condiciones reales con llamadas, uso del buzón de voz, etc. Son pruebas de aceptación de usuario en escenarios reales. Se realiza la revisión de los requisitos y confirma que todos los objetivos se cumplen. Además, se tiene que prever que los usuarios finales reciben una formación adecuada y determinada en el pliego de prescripciones técnicas, donde se tengan que resolver las dudas de los usuarios.

Por tanto, para la verificación y validación se debe garantizar que la instalación sea la correcta cumpliendo con las especificaciones técnicas y aporta el valor a los usuarios finales. Las pruebas que se plantean no dejan de ser algo sencillo sin llegar a grandes complejidades.

Para este caso, se va a suponer que el originador de la llamada pertenece a la I3D en Territorio Nacional que enviará y recibirá varias comunicaciones con destinos como; teléfono perteneciente a la I3D, teléfono IPC2, teléfono nodo desplegable estación estática, teléfonos que se encuentran en otros destinos y teléfono nodo desplegable vehicular.

A continuación, se enviará y recibirá llamadas desde un teléfono que pertenece a la I3D en un nodo permanente con la numeración v xxxxxx, o desde un nodo desplegable con la numeración m xxxxxx.

Teléfono origen	Teléfono destino	Observaciones
	v xxxxxx	Teléfonos fijos de las unidades
	0t xxxxxx	Teléfonos unidades fuera de España
	0w xxxxxx	Teléfonos otros destinos
vxxxxxx/m xxxxxx	m xxxxxx	Teléfono nodo desplegable I3D
	0s xxxx xxxx	Teléfono nodo desplegable
	t xxxxxx /z xxxxxx	Teléfonos red pública fijos y móviles con prefijo 1
	v(s/t) xxxxx	Teléfonos móviles corporativos

Tabla 3-20 Destinatarios a los que puede llamar teléfonos I3D

En estos dos casos, se podrá comprobar si la instalación y configuración, en la parte de voz, se hizo correctamente.

Este proyecto se va a describir con la herramienta *Project libre* donde se va a visualizar, en la figura 3-13, con el diagrama de Gantt los plazos del proyecto de la primera instalación y, en una tabla, los plazos de duración de cada uno de los proyectos.

		Nombre	Duración	Inicio	Terminado	Predecesores
1		Inicio	0 days	29/07/24 8:00	29/07/24 8:00	
2		Recepción material UCO	30 days	29/07/24 8:00	6/09/24 17:00	
3		Planificación instalación UCO	15 days	6/09/24 17:00	27/09/24 17:00	
4		Instalación	30 days	27/09/24 17:00	8/11/24 17:00	
5		Pruebas de V&V	30 days	8/11/24 17:00	20/12/24 17:00	

Figura 3-13 Diagrama de plazos proyecto 1 (imagen propia)

Inicialmente, se va a realizar la entrega, instalación, pruebas de integración, conexión con la MXONE y puesta en marcha de los equipos en la I3D.

Inicialmente, se dispone de 30 días para la entrega del material. Durante estos días, se tendrá 15 días para ir al lugar para planificar cómo va a realizar la instalación. Esto es necesario para comprobar la situación in situ, mientras tanto se va redactando el documento donde se plasme la arquitectura y las direcciones IP que se asignarán.

A continuación, se llevará a cabo la instalación a la que se dará un periodo de 30 días. Esta duración estará sujeta a la cantidad de elementos a instalar, pudiéndose darse en otros casos un mayor o menor número de días. Tras la instalación habrá que realizar la configuración de los equipos. Una vez finalizada se pasará a la siguiente fase, verificación y validación.

En la fase de verificación y validación se llevarán a cabo las pruebas que garanticen no sólo que los equipos están configurados correctamente sino también que, el sistema completo, funciona correctamente. Una vez se garantice esta fase, se podrá determinar que el sistema es apto para la recepción oficial.

En las Figuras 3-14, 3-15 y 3-16 se muestra el diagrama de Gantt que muestra cómo se da el proceso.

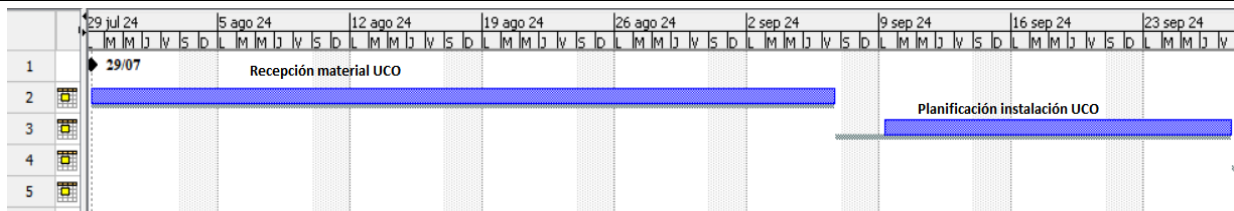


Figura 3-14 Diagrama de plazos proyecto 2 (imagen propia)

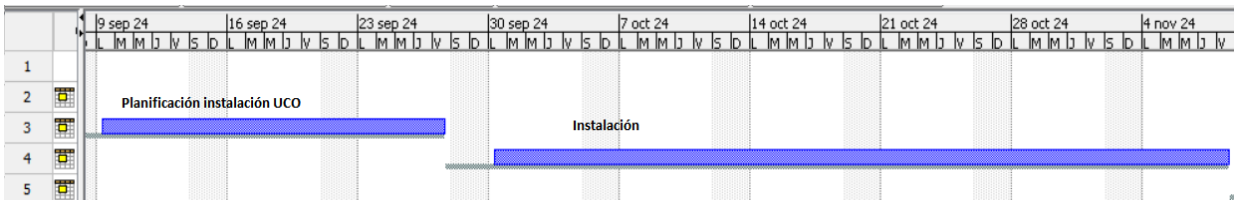


Figura 3-15 Diagrama de plazos proyecto 3 (imagen propia)

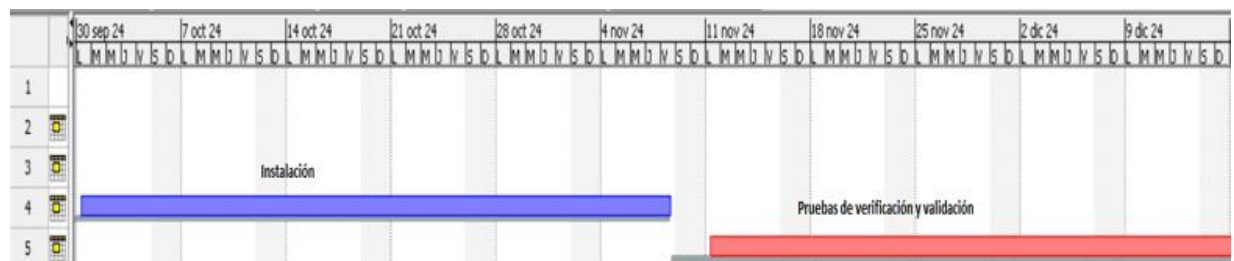


Figura 3-16 Diagrama de plazos proyecto 4 (imagen propia)

Una vez se han superado las pruebas de verificación/validación, aceptación y se ha aprobado la instalación con toda la documentación asociada, se procede a dar de alta a todos los usuarios de voz de la I3D que la unidad precisa.

Es muy importante insistir en que, para iniciar los trabajos, es necesario disponer de toda la documentación de arquitectura donde vienen reflejados todos switches y direccionamientos IP para garantizar que el trabajo se realice de forma adecuada.

De inicio, se reservará numeración a siete cifras a los que se solicitará, por el conducto ya establecido, la asignación de numeración pública de nueve cifras, por ejemplo, el número 811xxxx se le asigna el número 9154xxxxx. De tal forma que, se crean módulos en la NGN del operador de telefonía fija que identifique esa numeración con la zona geográfica con el objeto de que cuando se tenga que llamar a los servicios de emergencias, como el 112, se establezca comunicación con este servicio en su zona geográfica. Además, se incluirá una categorización para poder realizar llamadas telefónicas. Es necesario aclarar que estas categorizaciones son para realizar llamadas como pueden ser a redes públicas ya sean fijas o móviles. Esto último, es distinto a la categorización que se hacen desde esta instancia, es decir, para I3D determina a qué lugares se pueden realizar las llamadas telefónicas. En este sentido, los usuarios podrán realizar llamadas dentro de la red militar (I3D y red de ATM), llamadas a usuarios a la red pública (incluyendo lo anterior) y llamadas que pueden hacer a zona de operaciones (incluyendo red pública).

Una vez que se recibe la documentación que hace referencia a los direccionamientos IP, números de red pública asociados, categorización, se le asigna numeración telefónica interna de siete cifras. Además, la unidad logística proporciona los equipos telefónicos a las unidades. Estos teléfonos disponen de una MAC que se tendrá que asociar a esa numeración asignada. De tal forma que independientemente donde se instale ese teléfono, se podrá utilizar con esa numeración. Todo esto se realizará utilizando las herramientas como MANAGER PROVISIONING y PUTTY (a través de

comandos) para dar de alta a los usuarios en la MXONE. A continuación, se procederá a conectar los teléfonos a los puertos RJ-45 que se registrarán en la MXONE descargando las configuraciones para que los usuarios puedan realizar las llamadas telefónicas. Es necesario indicar que todas las actualizaciones software de las configuraciones de los teléfonos se realizarán de forma automática sin que se tenga que intervenir un componente humano y no afectando al uso de los usuarios.

Independientemente de las pruebas de verificación, validación y aceptación que se realizaron en su momento, comprobándose que la instalación era correcta, se harán una batería de pruebas sobre los teléfonos dados de alta para garantizar que el usuario no tenga ningún inconveniente para comunicarse. Además, se ayuda al usuario que lo desee a implementar alguna de las funcionalidades como desvíos, grupos de salto, grupo de captura, supervisión de línea de jefe, etc.

Es bueno añadir que, conforme pase el tiempo y se desee realizar altas de usuarios, bajas, incidencia, cambio de categorías, etc., el personal responsable de cada unidad (CISPOC⁸¹), según los procedimientos establecidos, enviará solicitud al centro de atención de usuarios para solventar estos casos.

Es necesario tener en cuenta que en I3D no sólo transita el servicio de voz por los switches, firewalls, etc., sino también otro tipo de servicios. Esto último, no ocurre con la red de ATM dado que lo único que viaja es la voz.

3.3.6 Documentación de resultados.

Se creará un registro de pruebas realizadas con los pasos seguidos, resultados obtenidos y cualquier incidencia encontrada. Se analizarán los resultados para identificar las áreas a mejorar. Finalmente, se elaborará un informe con los resultados obtenidos, acciones correctivas y la aprobación para pasar a la fase de producción.

La documentación generada debe indicar, de inicio, cuál es el objetivo que se trata de alcanzar. Con una breve descripción sobre la motivación de las pruebas. Además, se indicará quienes participarán, qué equipos serán necesarios y una serie de tablas y pasos a seguir. Las tablas estarán inicialmente vacías y que se irán rellenando conforme se vaya realizando las pruebas. La documentación será entregada a todos los intervinientes y habrá un recuadro de observaciones donde se rellenará tanto si hay o no comentarios a añadir. Una vez finalizadas las pruebas, será firmada por todos los intervinientes previamente acordado.

3.3.7 Aprobación y despliegue.

Se realizará una revisión al informe de las pruebas y aprobación. Una vez superado lo anterior se procederá a la aprobación del despliegue de la infraestructura.

3.3.8 Seguimiento del sistema una vez implementado.

Se realizará un monitoreo permanente de la red con unas actualizaciones periódicas y un mantenimiento preventivo de los dispositivos. Y se programarán revisiones periódicas del estado de la red y se ajustarán las configuraciones.

Lo usual es realizar contratos de mantenimiento que se aplique durante todo el ciclo de vida del sistema. Para ello, se puede aplicar un calendario de mantenimiento con inspecciones periódicas para comprobar el estado y rendimiento de los equipos que forman el sistema. Otro aspecto muy importante, son las actualizaciones software en los equipos que garanticen la seguridad. Además, se pueden hacer auditorías para comprobar el estado del sistema respecto a las políticas de seguridad existentes. Además, se podrán recomendar cambios y/o actualizaciones, siendo todo ello documentado.

⁸¹ CISPOC: Communication and Information System Point of Contact.

En el caso de aplicar mantenimiento predictivo, es necesario recopilar información sobre los parámetros como pueden ser latencia, pérdida de paquetes, tiempo de uso de los equipos, etc., para identificar aquellas situaciones que no sean normales. Con ello, se tenderá a predecir fallos antes de que éstos ocurran.

Si se utiliza el mantenimiento correctivo, se podrá solucionar aquellos problemas que ya han ocurrido previamente y que están documentados. Para estos casos, ya existen procedimientos de recuperación antes fallos, planes de contingencia, etc.

Una opción muy buena es controlar el sistema de forma continua, es decir, se configura una serie de alertas que avisen sobre problemas de tráfico, caídas de conexión, etc. Esta información se almacenará en logs para identificar patrones y posibles errores. Esta información se utilizará para posteriores auditorías.

Toda esta información se almacenará en todo el ciclo de vida del sistema junto con los costes asociados y los recursos que han sido empleados durante todo el proceso. Guardar esta información permitirá controlar la trazabilidad sobre los sistemas y eventos y, sobre todo, cada cuanto tiempo se están reemplazando los equipos, entre otras opciones. Además, permitirá tomar decisiones más acertadas posteriormente.

3.3.9 Capacitación del personal.

Se debe asegurar que el personal que trabaje a diario con este sistema esté capacitado para gestionar y mantener la infraestructura. Para ello, se debe exigir que este personal disponga de las certificaciones para poder utilizar estos sistemas. Además, conocer equipos, arquitectura y configuraciones de los sistemas con los que tenga que trabajar. Esta formación debe venir incluida en los contratos de mantenimiento y que deben ser cumplidos por las empresas adjudicatarias de los contratos, ya sea de adquisición o de mantenimiento.

Esta formación debe asegurar que cada persona pueda responder correctamente a cada evento imprevisto que se produzca.

Esta formación no sólo debe cubrir aspectos técnicos sino también legales y normativas aplicables. También es interesante una formación continua que evite que se queden obsoletos sus conocimientos impidiendo adaptarse a las nuevas evoluciones que tengan que implementarse.

Es muy importante que el personal que oferte los cursos disponga de la formación y experiencia previa para solventar todas las dudas de los alumnos que puedan darse durante los cursos.

3.3.10 Seguridad física.

Verificar que los equipos hardware estén protegidos físicamente contra accesos no autorizados. Se debe informar de que habrá un personal definido al que tengan acceso a ciertas áreas restringidas. Los accesos realizados serán documentados, es decir, se incluirá la fecha, hora y motivo para que posteriores auditorías puedan comprobar que se está cumpliendo con la normativa establecida.

Para acceder a estos lugares, como un centro de proceso de datos, el personal habilitado tendrá que llevar consigo tarjetas de acceso, pulsar claves para evitar el acceso no autorizado. En estos lugares, se instalarán cámaras de vigilancia para controlar quién entra en cada momento en el caso de que se precise. Además, habrá sistema de extinción de incendios, detectores de humos que sean compatibles con los sistemas instalados. Se instalarán sistemas que protejan a los equipos de sobretensiones.

3.3.11 Cumplimiento legal.

Durante toda la vida del sistema, se debe asegurar que la red y sus equipos cumplan con las normativas estándar.

Es preciso formar al personal en normas de seguridad sobre eventos que puedan ocurrir en lugares como los centros de proceso de datos. Con ello, se pretende evitar, en la medida de lo posible, accidentes en la manipulación de los equipos que sean sensibles.

3.3.12 Plan de contingencia.

Tener documentado un plan de contingencia en caso de fallos críticos, con copias de seguridad con configuraciones y datos importantes.

Otro aspecto importante es el plan de recuperación ante desastres que consiste en cómo reestablecer al sistema tras un desastre natural como puede ser una inundación, terremoto o incendios. Esto último, viene recogido en el Real Decreto 346/2011, de 11 de marzo, por el que se aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para accesos a los servicios de telecomunicación en el interior de las edificaciones en el Anexo V, punto 4.

Hay que considerar que el almacenamiento de los equipos de repuesto es muy importante. Es decir, es necesario disponer de lugares seguros y protegidos. Estos equipos deben estar inventariados junto con la documentación técnica con unos documentos actualizados. Se debe garantizar quiénes deben acceder a esta documentación y deben estar respaldados para evitar su pérdida.

Es muy importante que los equipos y el personal se encuentren ubicados en lugares adecuados que garanticen un funcionamiento adecuado al servicio que están proporcionando.

3.4 Despliegue de nodos desplegables

Existen circunstancias en las cuales se requiere que la instalación, ya sea en vehículos o en baúles en posiciones estáticas, de equipos cumplan con la arquitectura I3D que van a ser desplegados en Zona de Operaciones. Dentro de esta instalación, nuestro trabajo se centra en baja clasificación y, en concreto, telefonía.

En la Figura 3-17 se muestra el diagrama de Gantt, como en el caso anterior, con la herramienta Project Libre con los plazos de duración de un proyecto concreto. Para este caso, se establecerá un plazo de dos semanas para el acopio de material, configuración de los equipos y pruebas que garanticen el funcionamiento correcto del sistema para que pueda ser posteriormente desplegado.



Figura 3-17 Diagrama de Gantt 5 (imagen propia)

Esta instalación se realiza en varias etapas. Inicialmente, se recibe una comunicación oficial de instalar un nodo, ya sea en un vehículo o estático, en I3D antes de ser enviado a una zona determinada. A continuación, se recibe el material y el vehículo, en caso necesario, donde se debe realizar la instalación. En este ejemplo, se precisa de tres días para que sea enviado al lugar que se indique para iniciar los trabajos. Una vez que ya se tenga todo el material en un mismo lugar, se divide la configuración en dos partes. La primera de ellas, para los equipos de alta clasificación que serán configurados por el personal ya determinado y que dispondrá de tres días para realizarlo. Una vez finalizado, se procederá a la configuración de los equipos de baja clasificación, también por personal de la administración, donde se incluye los servicios de la telefonía. Una vez finalizado las configuraciones se realizan las pruebas de funcionamiento que garanticen que el sistema funciona correctamente. Es necesario aclarar que en el mismo mensaje oficial de comunicación de instalación se debe añadir documentación donde venga reflejada la arquitectura que se tiene que desplegar. Durante

la configuración e instalación se determinan las direcciones IP definitivas, los números de teléfono a usar, etc.

Es necesario aclarar que no es comparable con la instalación de un nodo permanente dada la premura de tiempo para estos casos. Además, la instalación de los nodos permanentes requiere de un trabajo más complejo, por el tamaño de la unidad, la cantidad de recursos a instalar y todo el trabajo de ingeniería que lleva aparejado.

En la Figura 3-18 se muestra un ejemplo de arquitectura de nodo desplegable sin call manager de baja clasificación:

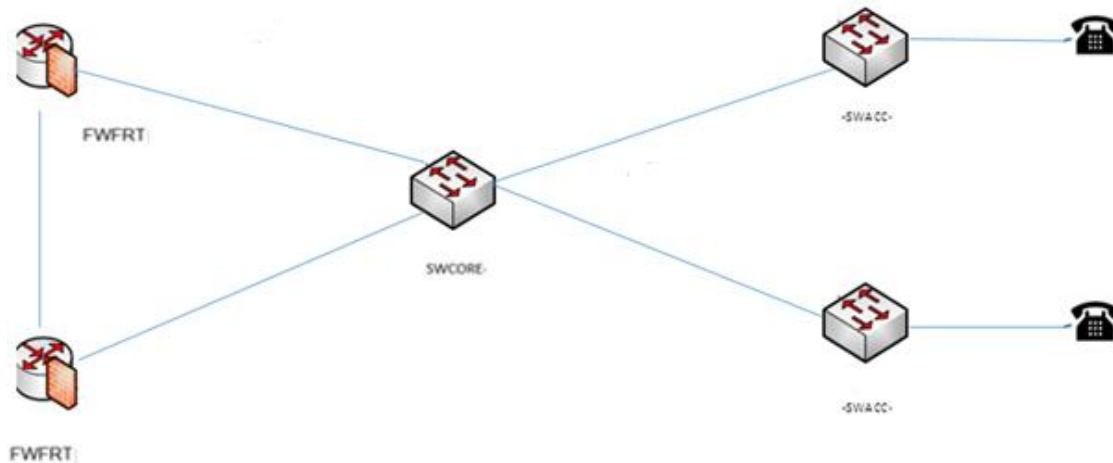


Figura 3-18 Arquitectura nodo desplegable (imagen propia)

3.5 Procedimiento de llamadas

La I3D se basa en un núcleo central virtualizado donde se darán de alta a todos los usuarios de telefonía en una máquina denominada MXONE. Esta MXONE está duplicada en dos centros en localizaciones físicas distintas.

En este apartado se describe cómo transitan las llamadas desde el momento en que se inicia hasta el destinatario. Las llamadas pueden originarse desde España o desde zona de operaciones siendo importante entender cómo se encaminan.

Es necesario distinguir entre *nodos permanentes* y los *nodos desplegables*. Los primeros son los que se encuentran en España. Mientras que los segundos son las unidades que se encuentran desplegados en diferentes países y en otras ubicaciones en nuestro país. Es importante aclarar que los *nodos desplegables* no solo están instalados en vehículos sino también en posiciones estáticas dentro de edificios.

3.5.1 Procedimiento de llamada del nodo permanente de la I3D

Las llamadas generadas dentro de la I3D pueden dirigirse hacia teléfonos de la I3D o a telefonía basada en la red de ATM o en una red IPC2. En ambos casos, los destinatarios de las llamadas pueden estar ubicados en nodos permanentes o en nodos desplegables.

3.5.1.1 Llamada teléfono I3D a I3D

Este es el caso de llamadas entre usuarios que se encuentran dentro de la I3D, ambos en España y registrados en la MXONE. Este proceso se puede ver en la Figura 3-19 siguiendo la numeración desde el número 1 hasta el 4.

El teléfono en I3D, utilizando SIP, envía una señalización al MX-ONE, es decir, un mensaje INVITE indicando que quiere iniciar una llamada a otro teléfono. Con la señalización SIP, los dos

teléfonos negocian el códec a utilizar para la llamada. Se suelen utilizar los códec G.711 y G.729. Sin embargo, si queremos que la señal de la voz sea de calidad superior a los dos citados anteriormente, se utilizará el códec G.722. Este códec trabaja en el rango de frecuencia comprendido entre 50 Hz y 7 KHz.

La MXONE enruta la llamada a través de la red MPLS y la señal de voz va encapsulada en RTP que es común en redes VoIP. Además, MPLS encamina los paquetes de voz, maneja y dirige todos los tipos de datos, en nuestro caso la voz, con un sistema de etiquetas.

Para el caso del Firewall, puede bloquear o permitir tráfico basado en reglas predefinidas, por lo que podría inspeccionar los paquetes de VoIP y permitir o denegar el tráfico en función de políticas de seguridad.

Una vez que los paquetes de voz de la llamada se encuentran dentro de la MPLS, éstos van etiquetados e indican el camino por donde circulan. De esta manera, se evita las congestiones. A continuación, llegará al firewall, la voz irá en paquetes RTP y la señalización SIP se reencaminará hacia el teléfono de destino. El teléfono de destino recibe la llamada decodificando en G.711 o G.729 logrando la comunicación.

En el caso que se desee realizar el proceso inverso, solamente hay que fijarse desde el valor 4 hasta el 1 de la Figura 3-19.

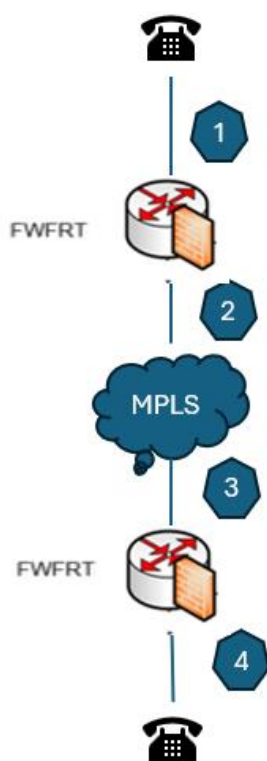


Figura 3-19 Llamada desde teléfono en nodo permanente (imagen propia)

3.5.1.2 Llamada teléfono I3D a la red de ATM

Para el segundo caso, es decir, llamadas desde la I3D hacia un teléfono que se encuentra en la red de ATM. Este proceso, la Figura 3-20, se puede observar la numeración desde el número 1 hasta el 6.

El teléfono en I3D, utilizando SIP, envía una señalización al MX-ONE, es decir, un mensaje INVITE indicando que quiere iniciar una llamada. Ambos negocian el códec que se usará en la llamada. Los códecs que pueden utilizarse en VoIP son G.711, G.729 y G.722 (alta definición). A continuación, MX-ONE decide que la llamada se dirija a la red de ATM, que usa celdas en lugar de

paquetes, paso previo por el Media Gateway. En éste se producen dos procesos. El primero de ellos es la transcodificación, es decir, el Media Gateway convierte el audio comprimido por el códec en formato (RTP) en un formato de ATM. Mientras que el segundo es la conversión de protocolos, es decir, el Media Gateway convierte la señal SIP usada en la red VoIP a un protocolo compatible con la red ATM como ISUP que pertenece a SS7. De hecho, ISUP realiza la señalización para el establecimiento, gestión y liberación de llamadas en la conmutación de circuitos.

Un proceso importante es el transporte en la red ATM. Por ello, el Media Gateway se encarga de convertir los paquetes en celdas a un tamaño fijo de 53 bytes. Es decir, encapsula los paquetes en celdas y los envía a la central telefónica posteriormente. A continuación, la central telefónica recibe la señal y los datos. Finalmente, la central encamina la llamada al destinatario y se inicia la llamada.

Respecto a los códec, ATM es un protocolo de transporte que encapsula datos, voz y video, es decir, no utiliza códec propio para el audio. Es decir, Media Gateway encapsula el audio en G.711, G.729 o G.722 y ATM los transporta en celdas. Y es el destinatario quien debe entender ese códec que ha sido transmitido por el ATM.

En el caso que se desee realizar el proceso inverso, solamente hay que fijarse desde el valor 6 hasta el 1 de la Figura 3-20.

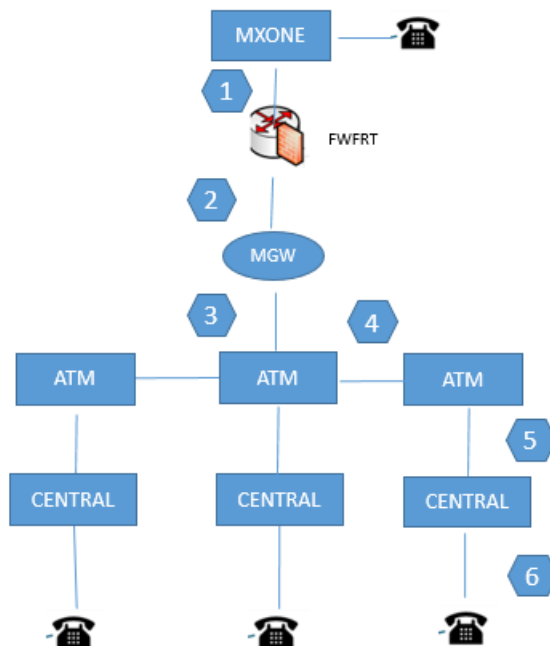


Figura 3-20 Llamada desde teléfono en nodo permanente a red ATM (imagen propia)

3.5.1.3 Llamada teléfono I3D a red pública

Por último, se propone el caso de una llamada desde un teléfono de la I3D a un teléfono de la red pública. Para poder realizar este tipo de llamadas, se tiene que dar, a este teléfono particular, una categorización. Estas categorías de voz para llamadas telefónicas en I3D, se dividen en tres casos. La primera categoría corresponde para aquellos usuarios que pueden llamar a extensiones corporativas fijas y móviles, es decir, teléfonos con la numeración vxx xx xx. La segunda categoría, corresponde con aquellos usuarios que cumplen con la primera categoría y pueden llamar a teléfonos públicos y móviles civiles marcando, desde su teléfono, el valor 1 y el teléfono al que desea llamar. Finalmente, el tercer caso, corresponde con aquellos usuarios que cumplen con los anteriores y pueden llamar por teléfono a través de satélite, marcando el valor s, y a unidades militares fuera de España marcando los valores w o z antes de marcar el número completo. Además, se muestra en la Figura 3-21 el encaminamiento de la llamada que se debe realizar.

El teléfono en I3D, utilizando SIP, envía una señalización al MX-ONE, es decir, un mensaje INVITE indicando que quiere iniciar una llamada con una marcación externa NGN (ya sea fijos o móviles). Una vez que el servidor MX-ONE recibe la señal INVITE lo analiza y reenvía esta petición SIP al SBC, que es el encargado de gestionarlo, utilizando el códec G.729. El SBC recibe el INVITE, lo analiza y reenvía a la NGN pasando a través del firewall. Para cumplir con los criterios de seguridad, se enmascara y oculta el direccionamiento interno configurado en el firewall. Es necesario aclarar que el firewall se sitúa entre NGN y el SBC.

Dado que la red exterior a la que se dirige la llamada ya no es de conmutación sino IP, ya no sería necesario que hubiese en el exterior un media Gateway que realice las funciones de transcodificación y conversión de protocolos con la conversión de la señal SIP al protocolo compatible con esa red como es ISUP que pertenece a SS7. Esta transcodificación tendrá que hacerla el SBC en caso de que los teléfonos utilicen distintos códec.

Para matizar, en la frontera entre NGN y la red exterior existe el SBC que se encargará de controlar la seguridad, la calidad de servicio y la adaptación de direcciones IP (NAT transversal). NAT no deja de ser un cambio de dirección IP privada a IP pública. De hecho, NAT se hace para que los equipos, que se van a comunicar, se puedan ver, y otro NAT para gestionar los mensajes RTP. Normalmente, SBC asigna los dos la misma dirección pública. Sin embargo, existen ciertos casos que no coinciden cuando la señalización y la voz y/o video están en servidores distintos. Además, los SBC se ubicarán en el *borde de la red interna*, es decir, en la zona interna de una organización y la red exterior ayudando la interconexión entre diferentes operadores de servicios. Además, permite la conversión de números de teléfono de siete a nueve cifras de forma eficiente. Hay que tener en cuenta que durante la llamada se dan dos procesos; establecimiento de llamada y la conversación. Durante el proceso de establecimiento, llamada y al terminar la conversación se cifra con TLS, mientras que el contenido (audio y/o video) se protege con SRTP.

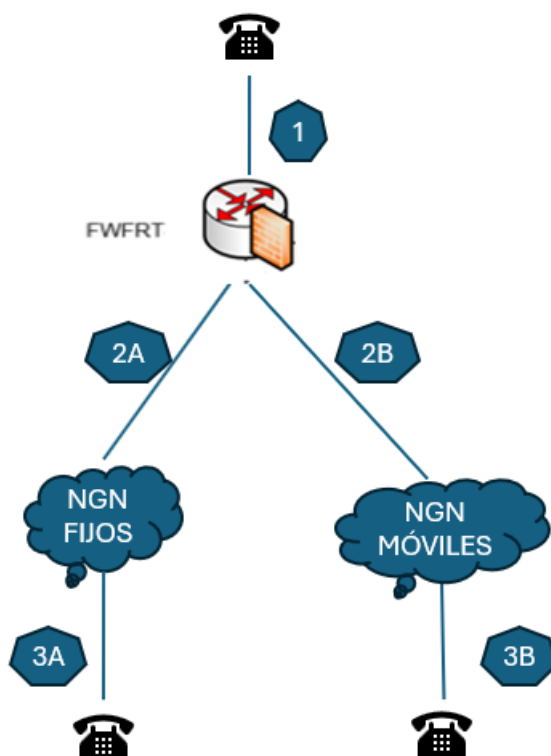


Figura 3-21 Llamada desde teléfono en nodo permanente a red pública (imagen propia)

En el caso que se desee realizar el proceso inverso, solamente hay que fijarse en el proceso desde el valor 3 A/B hasta el 1 de la Figura 3-21.

3.5.1 Procedimiento de llamada del nodo desplegable de la I3D

En este apartado se va a explicar cómo realizar una llamada telefónica desde un nodo desplegable que pertenece a la I3D a un teléfono que pertenezca a la I3D o a la telefonía basada en ATM o bien a un destino que está en una red pública civil (teléfono móvil o fijo).

3.5.1.1 Llamada teléfono I3D (ZO) a I3D

Primero, vamos a ver el caso una llamada realizada desde un puesto desplegado a otro usuario que se encuentra en un nodo permanente de la I3D situado en territorio nacional. Este proceso se puede ver en la Figura 3-22 siguiendo la numeración desde el número 1 hasta el 10.

El usuario descuelga el teléfono y marcará el número de teléfono del destinatario. La señal pasará a través del switch de acceso al que el teléfono está conectado y por el equipo frontera (firewall, FWFRT) situado en ZO. La llamada se propaga a través de la estación satélite local viajando hasta las estaciones de anclaje ubicadas en España. A continuación, se envía la llamada al firewall que se une a la MPLS que va hacia el firewall antes de llegar a la MXONE. Es necesario indicar que el Firewall puede bloquear o permitir tráfico basado en reglas predefinidas, por lo que podría inspeccionar los paquetes de VoIP y permitir o denegar el tráfico en función de políticas de seguridad. Una vez que llega a la MXONE, ésta encamina la llamada en dirección a la red MPLS y la señal de voz va encapsulada en RTP que es común en redes VoIP. Además, MPLS encamina los paquetes de voz, maneja y dirige todos los tipos de datos, en nuestro caso la voz, con un sistema de etiquetas que indican el camino por donde circulan evitando, en lo posible, congestiones. éstos van etiquetados e indican el camino por donde circulan. Es importante señalar que, el teléfono de origen envía una señalización al MX-ONE, es decir, un mensaje INVITE indicando que quiere iniciar una llamada a otro teléfono. Con la señalización SIP, los dos teléfonos negocian el códec a utilizar para la llamada. Se suelen utilizar los códec G.711 y G.729. Sin embargo, si queremos que la señal de la voz sea de calidad superior a los dos citados anteriormente, se utilizará el códec G.722. Este códec trabaja en el rango de frecuencia comprendido entre 50 Hz y 7 KHz.

En el caso que se desee realizar el proceso inverso, solamente hay que fijarse desde el valor 10 hasta el 1 de esta la Figura 3-22.

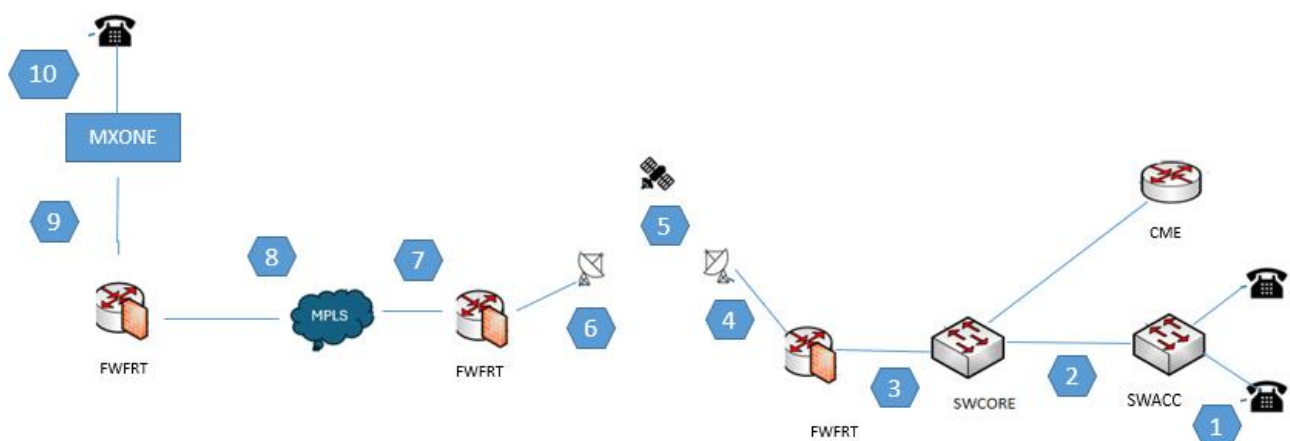


Figura 3-22 Llamada desde teléfono en nodo desplegable a otro en nodo permanente (imagen propia)

3.5.1.2 Llamada teléfono I3D (ZO) a red ATM

Para el segundo caso, el destinatario pertenece a la red ATM. De tal forma que, el usuario que se encuentra en zona de operaciones y su única forma de llamar telefónicamente es a través de enlace

satélite. A continuación, descuelga el teléfono marcando el número del destinatario. La señal pasará a través del switch de acceso al que el teléfono está conectado y por el equipo frontera (firewall, FWFRT). Se propaga a través de la estación satélite local viajando hasta las estaciones satelitales ubicadas en España.

En este momento el Media Gateway comprueba que el destinatario pertenece a la red ATM. Es aquí cuando en el Media Gateway, que usa celdas en lugar de paquetes, se producen dos procesos. El primero de ellos es la transcodificación, es decir, el Media Gateway convierte el audio (RTP) en un formato de ATM. Mientras que el segundo es la conversión de protocolos, es decir, el Media Gateway convierte la señal SIP usada en la red VoIP a un protocolo compatible con la red ATM como ISUP que pertenece a SS7. De hecho, ISUP realiza la señalización para el establecimiento, gestión y liberación de llamadas en la conmutación de circuitos. Un proceso importante es el transporte en la red ATM. Por ello, el Media Gateway se encarga de convertir los paquetes en celdas a un tamaño fijo de 53 bytes. Es decir, encapsula los paquetes en celdas y los envía a la central telefónica posteriormente. Respecto a los códec, ATM es un protocolo de transporte que encapsula datos, voz y video, es decir, no utiliza códec propio para el audio. De hecho, Media Gateway encapsula el audio en G.711, G.729 o G.722 y ATM los transporta en celdas.

Regresando al Media Gateway, éste envía la solicitud a su ATM y si no le pertenece consulta al resto de ATM. El ATM aludido enviará la solicitud a la central y éste al teléfono destinatario. Finalmente, la central telefónica encamina la llamada al destinatario y se inicia la llamada.

Este proceso se puede ver en la Figura 3-23 siguiendo la numeración desde el número 1 hasta el 14. En el caso que se desee realizar el proceso inverso, solamente hay que fijarse desde el valor 14 hasta el 1.

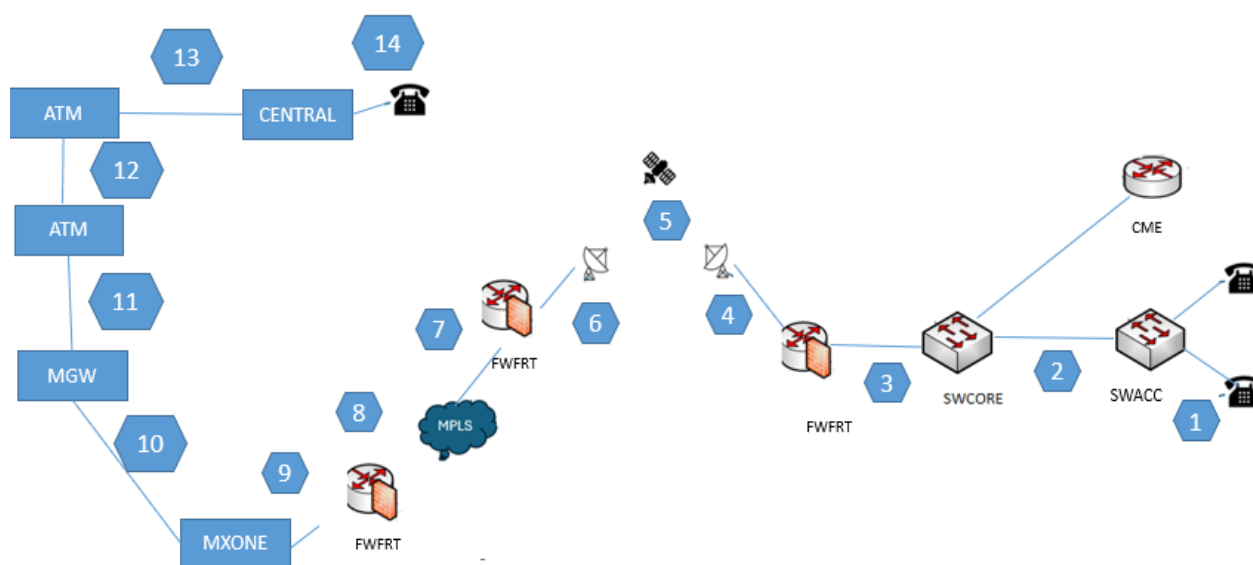


Figura 3-23 Llamada desde teléfono en nodo desplegable a otro en red ATM (imagen propia)

3.5.1.3 Llamada teléfono I3D (ZO) a red pública

En este caso, el usuario que está ubicado en zona de operaciones quiere enviar o recibir llamadas de la red pública civil, ya sea por teléfono fijo o móvil. Previamente, éste debe estar dado de alta en las NGN que se encuentran en España. En la Figura 3-24, se puede ver el camino desde el número 1 hasta el 8 A/B por donde discurre la llamada.

En el momento de iniciar la llamada, el usuario descuelga el teléfono y marcará el número del destinatario. La señal pasará a través del switch de acceso al que el teléfono está conectado y por el

equipo frontera (firewall, FWFRT). Se propaga a través de la estación satélite local viajando hasta las estaciones satélites ubicadas en Madrid.

El teléfono en I3D, utilizando SIP, envía una señalización al MX-ONE, es decir, un mensaje INVITE indicando que quiere iniciar una llamada con una marcación externa NGN (ya sea fijos o móviles). Una vez que el servidor MX-ONE recibe la señal INVITE lo analiza y reenvía esta petición SIP a la ruta establecida para las llamadas salientes (fijos o móviles) que ya están definidas en la central. Estas rutas SIP que se dirigen hacia el SBC utiliza el códec G 729. El SBC recibe el INVITE, lo analiza y reenvía a la NGN pasando a través del firewall. Para cumplir con los criterios de seguridad, se enmascara y oculta el direccionamiento interno configurado en el firewall. Es necesario aclarar que el firewall se sitúa entre NGN y el SBC.

Dado que la red exterior a la que se dirige la llamada ya no es de conmutación sino IP, ya no sería necesario que hubiese en el exterior un media Gateway que realice las funciones de transcodificación y conversión de protocolos con la conversión de la señal SIP al protocolo compatible con esa red como es ISUP que pertenece a SS7. Esta transcodificación tendrá que hacerla el SBC en caso de que los teléfonos utilicen distintos códec.

Para matizar, en la frontera entre NGN y la red exterior existe el SBC que se encargará de controlar la seguridad, la calidad de servicio y la adaptación de direcciones IP (NAT transversal). NAT no deja de ser un cambio de dirección IP privada a IP pública. De hecho, NAT se hace para que los equipos, que se van a comunicar, se puedan ver, y otro NAT para gestionar los mensajes RTP. Normalmente, SBC asigna los dos la misma dirección pública. Sin embargo, existen ciertos casos que no coinciden cuando la señalización y la voz y/o video están en servidores distintos. Además, los SBC se ubicarán en el *borde de la red interna*, es decir, en la zona interna de una organización y la red exterior ayudando la interconexión entre diferentes operadores de servicios. Además, permite la conversión de números de teléfono de siete a nueve cifras de forma eficiente. Durante el proceso de establecimiento, llamada y al terminar la conversación se cifra con TLS, mientras que el contenido (audio y/o video) se protege con SRTP.

En el caso que se desee realizar el proceso inverso, solamente hay que fijarse en el proceso desde el valor 8 A (teléfonos fijos) o 8 B (teléfonos móviles) hasta el 1 de la Figura 3-24.

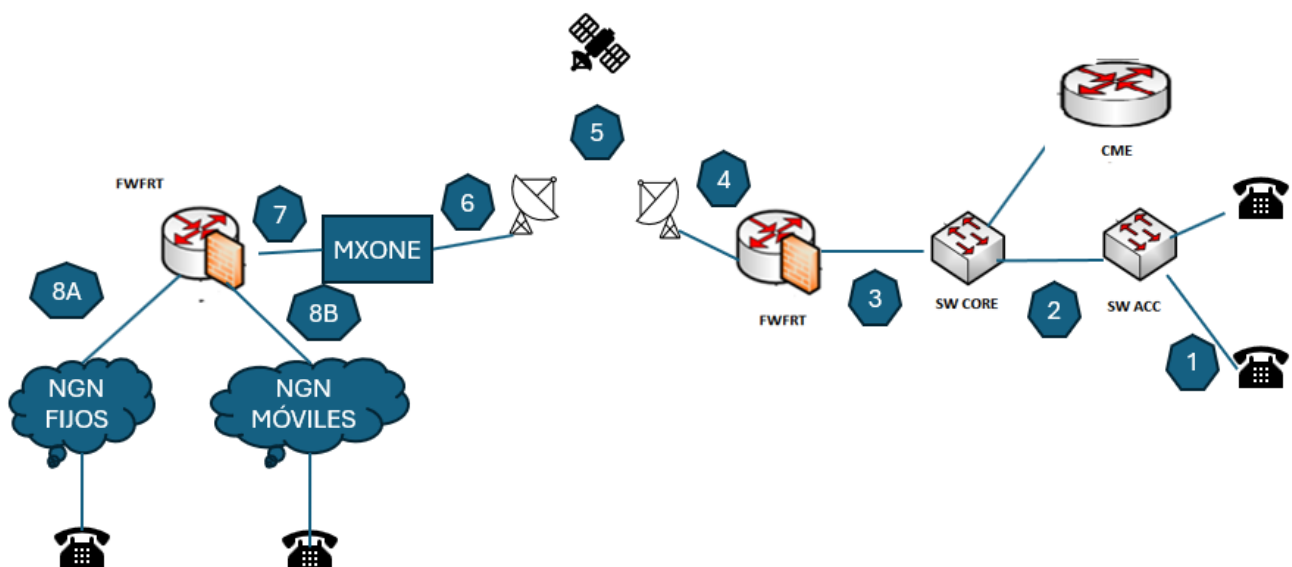


Figura 3-24 Llamada desde teléfono en nodo desplegable a otro en red pública (imagen propia)

4 RESULTADOS

A continuación, se matizará que distingue la instalación de un nodo permanente y un nodo desplegable. Además, se va a determinar con un ejemplo, basado en un análisis, porqué se tiende a ir a una solución basada en un nodo MXONE virtualizado, junto con los elementos que lo acompañan durante su funcionamiento como son SBC, NGN y firewalls. De esta manera, se quiere demostrar con datos porqué se ha adoptado esta decisión.

4.1 Proceso para la implementación de la I3D

Con lo visto en los apartados anteriores, se puede distinguir claramente lo que supone implementar un nodo permanente a un nodo desplegable. El nodo permanente está sujeto a un proceso de ingeniería mucho más profundo que para un nodo desplegable, cuyo caso no es necesario.

Cada unidad tiene unas peculiaridades que los hacen distintos por lo que el tiempo de instalación será diferente. Aparte de la cantidad de equipos a instalar y todas las pruebas y documentación que se tendrá que generar. Mientras que para un nodo desplegable no precisará de tanto nivel de detalle al estar formado por equipos que se instalarán en sus baúles cuyo trabajo será más breve y sistemático.

4.2 Ejemplo análisis de costes implementación nodo permanente, nodo MXONE virtualizado y sin virtualizar

A continuación, se va a realizar una valoración económica para la instalación de un nodo permanente, servidor MXONE virtualizado y otro servidor MXONE sin virtualizar. En ésta, se va a incluir los costes asociados a la parte de instalación/mano de obra, equipos adquiridos y el mantenimiento para un periodo estimado de diez años. Todo esto, considerando que es un entorno aislado sin otro tipo de servicios que discurran por la red I3D.

De inicio, se va a determinar que el número de usuarios del nodo permanente, que van a recibir este servicio, es de cien teléfonos IP. Este nodo no estará virtualizado ni será de alta disponibilidad. Al ser una pequeña unidad, se instalarán 3 switches de acceso gestionables para soportar VLAN y tráfico de calidad. Además, se añadirá un switch de core que se encargará de controlar el tráfico de datos entre los diferentes switches que a él se conectan, y dos firewalls que garanticen la seguridad y que se conectarán a la red MPLS. A su vez, los firewalls se conectarán al firewall de la MXONE que permita la conexión entre el nodo permanente y el nodo donde se encuentra el servidor de telefonía.

Es necesario indicar que el servidor MXONE, en ambas versiones, se conectará con los equipos NGN, SBC y firewalls.

A continuación, se va a particularizar los costes asociados para cada uno de ellos.

4.2.1 Costes asociados a la instalación del nodo permanente

En la instalación del nodo permanente, se tiene previsto dos firewalls, cuatro switches y cien teléfonos. Para realizar esta implementación, se van a necesitar dos ingenieros que trabajarán durante 22 días, con una tarifa de 60 euros/hora. Cada jornada tendrá una duración de 8 horas.

Ahora se va a hacer la valoración económica de los equipos. Los firewalls están valorados en 3.500 €/unidad, switch de core en 5.000 €, switch de acceso en 2.500 €/unidad, los ordenadores en 800 €/unidad y los teléfonos por 190 €/unidad. Además, se va a incluir cursos de formación para dos personas valorados en 3.000 € por persona. Se va a considerar que las licencias vienen incluidas en la adquisición. Los valores de los equipos son variables y dependen del fabricante, por lo que se ha decidido tomar valores aproximados.

A continuación, se desglosa los costes asociados a la adquisición e instalación.

Concepto	Cantidad	Precio/unidad (€)	Coste (€)
Mano de obra	22 días, 8 horas, 2 ingenieros	60	21.120
Firewall	2	3.500	7.000
Switch de core	1	5.000	5.000
Switch acceso	3	2.500	7.500
Teléfonos	100	190	19.000
Ordenadores	2	800	1.600
Formación	2	3.000	6.000
Coste total			67.220

Tabla 4-1 Precio adquisición, instalación y mano de obra nodo permanente

El coste total asociado para la instalación y mano de obra para el nodo permanente es de 67.220 €.

En el caso de que queramos hacer un mantenimiento para diez años, se tendrá que añadir los siguientes costes. Los firewalls tendrán un coste anual por suscripción de 852 €/unidad. Esto supondrá que con dos unidades durante diez años el coste asociado sea de 17.040 €. En el caso de los switches, tiene un coste del 10% del costo del equipo anual, es decir, 5.000 € para el switch de core y 7.500 € para los switches de acceso. Para el caso de los teléfonos, no se introducirá ningún valor dado que se desconoce cuántos se van a dar de baja durante diez años. Además, todo equipo telefónico que no funcione se descartará, sin reparación, y será sustituido por otro. Finalmente, el coste total por el mantenimiento es de 29.540 €.

Concepto	Cantidad	Precio/año (€)	Años	Coste(€)
Firewall	2	852	10	17.040
Switch de core	1	500	10	5.000
Switch acceso	3	250	10	7.500
Coste total				29.540

Tabla 4-2 Inventarios equipos de red nodo permanente

Por tanto, para la instalación del nodo permanente, incluyendo los diez años de mantenimiento, ascenderá a 96.760 €.

4.2.2 Costes asociados para el servidor MXONE virtualizados

A continuación, se van a definir los costes asociados a la adquisición e instalación de los equipos físicos, sistemas virtualizados, almacenamiento compartido, ordenadores, licencias y formación. Es necesario indicar que el almacenamiento compartido sirve para que cuando ocurra un fallo en una de las máquinas virtuales, ésta pueda ser migrada de un servidor al otro para mantener la operatividad del sistema.

Para la instalación se van a necesitar dos ingenieros que trabajarán por un periodo de 30 días, con una tarifa de 60 euros/hora, cuya jornada tendrá una duración de 8 horas.

Para este nodo van a ser necesarios dos servidores MXONE, para cien usuarios telefónicos del nodo permanente, SBC, firewalls y NGN (para telefonía fija y móvil). Todo esto permitirá que ofrezca alta disponibilidad. NGN soportarán llamadas a teléfonos fijos y móviles.

El servidor MXONE está valorado en 20.000 €, los firewalls están valorados en 3.000 €/unidad, SBC en 6.000 €/unidad, NGN en 10.000 €/unidad, licencias en 20.000 € incluyendo a todas las virtualizaciones y cuatro ordenadores en 1.200 €/unidad. Además, se va a incluir cursos de formación para cuatro personas valorados en 3.000 € por persona. Los valores de los equipos son variables y dependen del fabricante, por lo que se ha decidido tomar valores aproximados.

Concepto	Cantidad	Precio/unidad (€)	Coste (€)
Mano de obra	30 días, 8 horas, 2 ingenieros	60	28.800
Servidores físicos (para la virtualización)	2	15.000	30.000
Servidor MXONE	2	20.000	40.000
Licencias de virtualización	2	10.000	20.000
Licencias SBC	100 usuarios	50/usuario	5.000
Licencias NGN	100 usuarios	100/usuario	10.000
SBC virtual	1	6.000	6.000
Firewall virtual	1	3.000	3.000
NGN virtual	1	12.000	12.000
Ordenadores	4	1.200	4.800
Almacenamiento compartido 2TB	1	15.000	15.000
Ordenadores	4	800	3.200
Formación	4 personas	3.000	12.000
Coste total			194.800

Tabla 4-3 Precio adquisición, instalación y mano de obra nodo virtualizado

El coste total asociado para la instalación para el nodo virtualizado es de 194.800 €.

En el caso de que queramos hacer un mantenimiento para diez años se tendrá que añadir los siguientes costes anuales.

Concepto	Cantidad	Precio/año (€)	Años	Coste (€)
Servidor MXONE	2	3.000	10	60.000
Almacenamiento compartido	2	1.500	10	15.000
SBC virtual	1	1.000	10	10.000
Firewall virtual	1	900	10	9.000
NGN virtual	1	1.500	10	15.000
Licencias de virtualización	2	1.200	10	24.000
Coste total				133.000

Tabla 4-4 Coste mantenimiento nodo virtualizado durante un periodo de 10 años

Finalmente, el coste total por el mantenimiento es de 133.000 €.

Por tanto, para la instalación del nodo virtualizado más los equipos que le acompañan más diez años de mantenimiento, se tendrá que aprovisionar un montante de 327.800 €.

4.2.3 Costes asociados para el servidor MXONE sin virtualizar

A continuación, se van a definir los costes asociados a la adquisición e instalación de los equipos físicos, sistemas sin virtualizar, almacenamiento compartido, ordenadores, licencias y formación. Es necesario indicar que el almacenamiento compartido sirve para que cuando ocurra un fallo en una de las máquinas virtuales, ésta pueda ser migrada de un servidor al otro para mantener la operatividad del sistema.

Para la instalación se van a necesitar dos ingenieros que trabajarán por un periodo de 30 días, con una tarifa de 60 euros/hora, cuya jornada tendrá una duración de 8 horas.

Para este nodo van a ser necesarios dos servidores MXONE, para cien usuarios del nodo permanente, SBC, firewalls y NGN (para telefonía fija y móvil). Todo esto permitirá que ofrezca alta disponibilidad. Los equipos NGN soportarán llamadas a teléfonos fijos y móviles.

El servidor MXONE está valorado en 20.000 €, los firewalls están valorados en 4.000 €/unidad, SBC en 8.000 €/unidad, NGN en 12.000 €/unidad, licencias en SBC en 5.000 €, licencias en NGN en 10.000€ y cuatro ordenadores en 800 €/unidad. Además, se va a incluir cursos de formación para cuatro personas valorados en 3.000 € por persona. Los valores de los equipos son variables y dependen del fabricante, por lo que se ha decidido tomar valores aproximados.

Concepto	Cantidad	Precio/unidad (€)	Coste (€)
Mano de obra	30 días, 8 horas, 2 ingenieros	60	28.8000
Servidor MXONE(HA)	2	20.000	40.000
Licencias SBC	100 usuarios	50/usuario	5.000
Licencias NGN	100 usuarios	100/usuario	10.000
SBC físico (HA)	2	8.000	16.000
Firewall físico (HA)	2	4.000	8.000
NGN físico (HA)	2	12.000	24.000
Ordenadores	4	800	3.200
Almacenamiento compartido 2TB (físico)	1	15.000	15.000
Formación	4 personas	3.000	12.000
Coste total			162.000

Tabla 4-5 Precio adquisición, instalación y mano de obra nodo no virtualizado

El coste total asociado para la instalación para el nodo no virtualizado es de 162.000 €.

En el caso de que queramos hacer un mantenimiento para diez años se tendrá que añadir los siguientes costes anuales.

Concepto	Cantidad	Precio/año (€)	Años	Coste (€)
Servidor MXONE (HA)	2	2.000	10	40.000
Almacenamiento compartido 2TB (físico)	2	1.000	10	20.000
SBC físico (HA)	2	1.500	10	15.000
Firewall físico (HA)	2	500	10	10.000
NGN físico (HA)	2	1.000	10	20.000
Licencias SBC	100 usuarios	100	10	50.000
Licencias NGN	100 usuarios	100	10	100.000
Coste total				255.000

Tabla 4-6 Coste mantenimiento nodo no virtualizado durante un periodo de 10 años

Finalmente, el coste total por el mantenimiento es de 255.000 €.

Por tanto, para la instalación del nodo no virtualizado más los equipos que le acompañan más diez años de mantenimiento se tendrán que aprovisionar un montante de 417.000 €.

4.2.4 Comparativa costes instalación nodo virtualizado vs nodo no virtualizado

Este análisis se puede desglosar en varios apartados; instalación, mantenimiento y coste total.

En el apartado de la instalación, dentro del apartado económico, la inversión que se puede hacer en el nodo virtualizado asciende a 194.800 €, mientras que para el nodo no virtualizado es de 162.000 €. Se puede concretar que la inversión inicial para el nodo virtualizado es un 20,25% superior al nodo no virtualizado. Esto está justificado debido a que la centralización de recursos, es decir, el uso menos máquinas físicas y más licencias software incrementa el coste.

Relativo al mantenimiento, dentro del apartado económico, la inversión en mantenimiento que se puede hacer en el nodo virtualizado asciende a 133.000€, mientras que para el nodo no virtualizado es de 255. 000 €. Con estos valores, se deduce que el nodo virtualizado es más eficiente a largo plazo con un ahorro del 47,84%. En el caso del nodo no virtualizado, el mantenimiento de varios equipos físicos eleva los costes durante los 10 años.

Finalmente, el coste total de instalación y mantenimiento para el nodo virtualizado es de 327.000 €, mientras que el nodo no virtualizado asciende a 417.000 €. Esto supone un ahorro del 21,39% para la opción de nodo virtualizado.

Al realizar la comparativa se puede deducir que, aunque el coste inicial de la instalación del nodo virtualizado sea más elevado, debido a su eficiencia compensa el gasto inicial. Además, a largo plazo se ve recompensada al reducirse el coste económico al compararlo con el nodo no virtualizado.

Todos estos costes, vienen incluidos IVA, generación de documentación y trámites administrativos como la catalogación de los equipos. Es necesario recordar que, el nodo permanente está formado por equipos físicos, mientras que el nodo formado por MXONE, SBC, NGN y firewall están virtualizados en dos servidores.

Otro aspecto por tener en cuenta es el siguiente. Supongamos que se necesitase añadir más usuarios, es decir, elevar a más de cien usuarios telefónicos. Esto afectaría más al mundo no virtual. debido a que, en el mundo no virtual precisaría de más recursos económicos, al tener que adquirir más equipos y aumentar el gasto en mantenimiento. Además, el consumo energético aumentaría. Si lo comparamos con el mundo virtual, éste ofrece una escalabilidad superior, es decir, sus servidores permiten añadir más usuarios sufriendo un impacto económico menor, al no tener que adquirir más equipamiento, a pesar de que se tengan que adquirir más licencias.

Por tanto, si se decide aumentar a más de cien usuarios, la mejor opción es la virtualización debido a la disminución en costes que se producirán a largo plazo.

4.3 Ejemplo análisis consumos energéticos y huella de carbono nodo MXONE virtualizado y sin virtualizar

4.3.1 Consumos energéticos nodo MXONE virtualizado y sin virtualizar

En este apartado, se pretende demostrar cómo afecta implementar la virtualización en los equipos MXONE, SBC, NGN y firewall en los consumos energéticos y los costes económicos, comparándolos con un sistema no virtualizado. Todo esto, considerando que es un entorno aislado sin otro tipo de servicios que discurran por la red I3D.

Vamos a tomar como opción emplear dos servidores físicos que van a virtualizar a 4 firewalls, 2 NGN, 2 SBC y 2 MXONE en cada uno de ellos. Además, se configuran para ofrecer alta disponibilidad, es decir, en caso de que deje de funcionar uno de los equipos, su homólogo tomará el control sin que se pierda la operatividad completa del sistema.

A continuación, se muestra el cálculo de los valores obtenidos con el consumo energético sin virtualización y con virtualización, tomando como referencia la información de los equipos.

4.3.1.1 Sin virtualización

En esta tabla, se observan los valores de los consumos en un año con los equipos físicos sin virtualizar.

Equipo	Cantidad	Consumo (W)	Consumo total/hora(W)	Consumo anual. Consumo total/hora * 24*365 horas(W)
Firewall	2	100	200	1.752
NGN	2	300	600	5.256
SBC	2	200	400	3.504
MXONE	2	500	1.000	8.760
Coste total anual				19.272 KWh/año

Tabla 4-7 Consumo de energía en un año sin virtualización

En esta tabla, se observan los valores de los consumos en un año de dos equipos físicos con firewall, NGN, SBC y MXONE virtualizados.

Equipo	Cantidad	Consumo (W)	Consumo total/hora(W)	Consumo anual. Consumo total/hora * 24*365 horas(W)
Servidor físico	2	600	1200	10.512
Coste total anual				10.512 KWh/año

Tabla 4-8 Consumo de energía en un año con virtualización

La diferencia de coste es de 10,512 kWh/año. Esto supone que existe un porcentaje de ahorro de:

$$\text{Porcentaje de ahorro} = \frac{10.512}{19.272} \times 100 = 54,54\%$$

Para este caso, con dos servidores, se obtiene un porcentaje de ahorro del 54,54%, si los comparamos con la opción de no virtualizar. Si se considera que el coste energético constante de 0,15 €/kWh, vamos a valorar el ahorro económico en un año.

Equipo	Consumo anual (kWh/año)	Precio €/kWh	Consumo (€)
Sin virtualización	19.272	0,15	2.890
Con virtualización	10.512	0,15	1.576,8
Coste total anual	8.760		1.313,2

Tabla 4-9 Variación de consumo de energía en un año virtualización/sin virtualización

Finalmente, se deduce que la mejor opción, por ahorro energético y económico, es virtualizar dado que habrá un ahorro anual de 1.313,2 €. Lo que supondrá un ahorro en 10 años de 13.132 €.

Como conclusión, se puede afirmar que la mejor opción es utilizar dos servidores virtualizados para obtener un ahorro de costes. Ambos casos, al ofrecer alta disponibilidad garantizarán continuidad en el servicio, es decir, en caso de que uno de los equipos falle, el otro podrá sustituirle.

4.3.2 Cálculo de la huella de carbono nodo MXONE virtualizado y sin virtualizar

El objetivo de este apartado es comprobar cuál es el valor de la huella de carbono para sistemas no virtualizados y los virtualizados con los mismos equipos. Para ello, se va a utilizar la siguiente ecuación [33]:

$$\text{Emisiones Co2(kg)} = \text{Consumo energía(kWh)} \cdot \text{Factor de emisión} \left(\frac{\text{kg CO2}}{\text{kWh}} \right)$$

Para aquellos casos en los que hemos estado trabajando anteriormente, se puede obtener el valor de las emisiones de CO₂ tanto para la virtualización como la no virtualización. Es necesario indicar que el valor de factor promedio en Europa es de 0,233 kg CO₂/kWh. En la siguiente tabla se desglosan los valores.

Equipo	Consumo anual (kWh/año)	Factor emisión (kg CO2/kWh)	Emisiones CO ₂ (kg)
Sin virtualización	19.272	0,233	4.490,37
Con virtualización	10.512	0,233	2.449,3
Variación			2.041,07

Tabla 4-10 Variación de la emisión de CO₂ en un año virtualización/sin virtualización

En este caso, se comprueba que el sistema con virtualización obtiene un resultado con menor cantidad de emisiones de CO₂ en 2.449,3 kg. Esto supone un ahorro en emisiones de:

$$\text{Porcentaje de ahorro} = \frac{\text{Reducción de CO}_2(\text{kg})}{\text{Emisiones sin virtualización (kg)}} \times 100 = \frac{2.449,3}{4.490,37} = 54,54\%$$

Se puede comprobar que, al comparar el nodo virtualizado con el no virtualizado, y en concreto al pasar de diez a dos equipos físicos, provoca un ahorro energético con una disminución en las emisiones de CO₂ en un 54,54%, equivalente a 2.041,07kg al año, si se opta por el nodo virtualizado. Esto supondrá que en un periodo de diez años habrá una disminución de CO₂ en torno a 20.410,7kg.

Una vez visto todos los resultados de este apartado, se debe considerar que la mejor opción es la virtualización, y que actualmente se está dando en múltiples empresas y organizaciones.

Otro aspecto por tener en cuenta es el siguiente. Supongamos que se necesitase añadir más usuarios, es decir, elevar a más de cien usuarios telefónicos.

Esto afectaría más al mundo no virtual. debido a que el adquirir más equipos físicos implicará un aumento tanto en el consumo energético como en la huella de carbono. Si se compara con el mundo virtual, éste aumentará su huella de carbono, pero sin llegar al nivel del mundo no virtual.

Por tanto, si se decide aumentar a más de cien usuarios, la mejor opción es la virtualización debido a la disminución energética y de huella de carbono que se producirán a largo plazo.

4.4 Implicaciones de la I3D

Implementar la telefonía I3D supone no sólo una gran inversión económica sino también un reto técnico importante. Todo esto, se puede ver desde tres puntos de vista. Un primer punto de vista son los costes de implantación. Dado que, en cada una de las anualidades se debe plantear una serie de unidades que van a pasar de la red de comunicación de nodos ATM, donde se conectan las centrales telefónicas de estas unidades, a la MXONE donde todos los teléfonos se conectan directamente a esta última. Se debe desplegar una infraestructura tecnológica con una red y un hardware concreto que van a soportar físicamente las comunicaciones. Se debe determinar un ancho de banda que permita las comunicaciones dado que no solo se deben tener en cuenta la voz sino también los datos de todos los servicios que tienen que convivir. Un coste muy importante son las licencias software de todos los equipos (teléfonos, MXONE, etc.) sin las cuales éstos no podrían operar. Estas licencias software requieren un añadido económico y unas actualizaciones que implican un trabajo de seguimiento continuo que implica que exista un personal dedicado a estas labores. Otro coste asociado es el mantenimiento y soporte técnico, es decir, es necesario contratar a personal de forma permanente que estén comprobando que el sistema funciona correctamente y, recuperándolo cuando sea necesario. Existen diferentes estrategias para contratar personal para realizar estas tareas de mantenimiento. Sin embargo, siempre estarán asociados a contratos de mantenimiento donde se contrate a personal que garantice durante una serie de años las redes de comunicaciones. Este personal precisará una formación básica y permanente dado que las tecnologías evolucionan constantemente y las mejoras que pueden introducir son muy interesantes. De tal manera, que en ciertos momentos no se pueden introducir mejoras, pero conforme pasa el tiempo se puede observar que se han podido introducir mejoras virtualizadas, es decir, por ejemplo, sustituir equipos físicos por software provocando que no se tenga que invertir económicamente, con la reducción de coste que supone. De hecho, una gran inversión en virtualización demuestra que a largo plazo provoca una disminución en emisiones de CO₂, ahorro energético y disminución de costes en mantenimiento de equipos.

El segundo punto de vista es la protección de las comunicaciones, tanto internas como externas, mediante un seguimiento diario de todos los eventos registrados. Además, se debe evaluar qué nuevas tecnologías se pueden implementar para la mejora de la protección del sistema. Además, es necesario tener en cuenta que, aunque existan distintas sedes, todas ellas deben tener un equipamiento hardware y software actualizado y que tengan las mismas versiones. Es decir, se debe realizar una trazabilidad de no solo de todos los eventos sino de que las configuraciones software son las mismas y que están actualizadas siguiendo las recomendaciones del fabricante. El hecho de no tenerlo puede provocar

debilidades o agujeros de seguridad de imprevisibles consecuencias. Por ello, es necesario controlar lo anterior y tomar medidas de seguridad importantes, tanto físicas como lógicas (ciberseguridad).

El último punto de vista es que las organizaciones deben ser conscientes de la gran cantidad de datos que se generan, se propagan y que la red debe ser capaz de soportar. Por ello, es importante dimensionar la red de forma idónea para que el usuario reciba los servicios demandados de forma correcta. Además, se debe cumplir con la normativa y las leyes que regulan las telecomunicaciones.

Para nuestro ámbito el retorno de inversión no es como una organización privada, cuyas prioridades se centran en otros aspectos, sino que el objetivo es el cumplimiento de la misión y que los servicios estén garantizados 24/7. Además, hay que poner de manifiesto que la implementación de la I3D es un proceso complejo con una gran inversión económica que abarca una importante infraestructura, capacitación, cumplimiento de aspectos legales, creación de nuevas normas de mantenimiento y funcionamiento, desarrollo de políticas de seguridad, etc.

Todavía quedan varios años para completar la implementación de la I3D. Sin embargo, es difícil determinar cuándo finalizará dado que un proyecto de esta envergadura siempre viene acompañado de problemas que suelen aparecer a lo largo del camino, ya sean propios o ajenos.

4.5 Retos futuros

Tal y como se define en el documento *Instrucción Técnica 07/23 Organización de la estructura de apoyo a la gestión de los servicios de la infraestructura de telecomunicaciones de la I3D “facilita la transición de la estructura de apoyo para la gestión existente en el Sistema de Telecomunicaciones Militares (STM), a la nueva estructura necesaria para la IT I3D...”*. Es decir, se va hacia un modelo que abarque a todos los sistemas, incluido a la telefonía.

Según el Documento guía del “Puesto de Trabajo Digital” del Ministerio de Defensa de 13 de noviembre de 2020 el equipamiento que hay en el puesto de trabajo digital dispone de un terminal que está compuesto por un ordenador de sobremesa o portátil, telefonía fija IP que actualmente se está implantando en la I3D, teléfono móvil corporativo integrado en la plataforma de gestión corporativa de dispositivos móviles EMM⁸² de la I3D con aplicaciones instaladas para acceder al correo electrónico corporativo y sistema de mensajería instantánea y VTC⁸³. Una vez que se logre la implantación completa de la I3D se avanzará hacia la denominada “comunicaciones unificadas” [25]. Para ello, se compartirá el mismo número de teléfono entre los dispositivos (teléfono fijo, móvil y ordenador portátil) con una APP⁸⁴ de tipo *softphone*. Esto permite realizar llamadas desde cualquiera de los dispositivos. Además, existirá la posibilidad de utilizar un terminal particular para integrar a la telefonía y datos de la I3D, una vez afiliado a EMM, en un dispositivo bajo la responsabilidad del usuario.

Es importante aclarar que EMM son herramientas que son utilizadas por dispositivos móviles, ya sean tabletas, Smartphone, etc., que se utilizan para acceder a los datos que pertenecen a las empresas. Es importante que estos equipos cumplan con las políticas establecidas de seguridad por el importante valor que suponen los datos para cualquier organización. Se pueden hablar de distintas aplicaciones como puede ser el MDM⁸⁵ que nos ayuda a la configuración de los equipos a distancia o bien eliminar los datos de ese dispositivo en cuanto el usuario se dé cuenta que lo ha perdido. Además, hará que los usuarios introduzcan contraseñas adecuadas y que no puedan descargar o acceder a sitios web no permitidos por criterios de seguridad.

Implementar EMM puede garantizar que los usuarios accedan a datos confidenciales al estar cifrados y cumplan con las políticas de seguridad establecidas. Esta herramienta permite la gestión de

⁸² EMM: Enterprise Mobile Management

⁸³ VTC: Video TeleConference

⁸⁴ APP: Aplication

⁸⁵ MDM: Mobile Device Management

la identidad y acceso de los usuarios a los datos y aplicaciones con un criterio de autenticación multifactor (MFA⁸⁶) [34], es decir, un primer factor puede ser nombre de usuario y contraseña. Un segundo factor consiste en que el usuario recibe en su dispositivo un código de verificación y que él debe ingresar. Y, el tercer factor es el reconocimiento facial que se haría con la ayuda de la cámara del equipo.

Las comunicaciones unificadas describen cómo accede el personal de la empresa a la información y trabaja con ella en tiempo real. Puede darse en pequeñas y grandes empresas donde el usuario puede acceder desde su propio dispositivo, ya sea un ordenador, tableta o teléfono móvil.

El mundo de la telefonía convive con el resto de los servicios con un único dispositivo físico como puede ser un ordenador portátil, tableta o smartphone.

Si queremos hacer llamadas telefónicas, sin usar un teléfono, utilizando un ordenador portátil lo que se utiliza son las aplicaciones Skype, Microsoft Team, Zoom o Google Meet. En el caso de utilizar una tableta se puede usar las aplicaciones de VoIP como WhatsApp, Telegram, Google Voice o Zoom. Incluso se pueden utilizar los relojes inteligentes, como Apple Watch entre otros, que pueden realizar llamada que no precisan estar vinculados a teléfonos inteligentes.

La telefonía está evolucionando hacia las nuevas tecnologías como 5G e IoT⁸⁷. La primera de las dos citadas, proporciona una conexión más rápida y estable tanto en las llamadas como en las videollamadas. Para el segundo caso, se afirma que los dispositivos físicos podrán comunicarse usando las redes 5G.

Respecto a la realidad aumentada, realidad virtual o telefonía 3D la tendencia es ir hacia que los usuarios podrían interactuar mediante avatares o entornos tridimensionales en sus conversaciones. Incluso se podrán realizar reuniones en entornos virtuales.

Si nos enfocamos en IA⁸⁸ los asistentes pueden manejar consultas de usuarios y gestionarlas sin intervención humana.

Para el caso de la ciberseguridad, las llamadas necesitarán mecanismos más fuertes para proteger los datos de usuario como la citada anteriormente autenticación multifactor.

Y, si nos centramos en la telefonía ecológica ya no existirá el equipo hardware dado que la telefonía se encontrará en la nube.

Uno de los problemas relativos a la telefonía, que antes no existían, es el coste asociado a las licencias software. Es decir, antaño se instalaba un teléfono al cuál el coste iba asociado a su adquisición y a la línea telefónica que se contrataba. Sin embargo, en la actualidad a parte del coste anteriormente citado ahora se le une un software que controla el funcionamiento del sistema y sin el que no existirá la comunicación. Afortunadamente, no es necesario renovar las licencias de estos teléfonos dado que sería un coste tan elevado que podría ser inviable su mantenimiento para las organizaciones que lo precisasen. Otro aspecto para tener en cuenta es que, para otros equipos como MXONE y call manager sí se le debe renovar las licencias software con el coste asociado.

Hace tiempo, se podría haber pensado que la telefonía quedaría relegada a ser un mero medio de transmisión entre dos personas. Sin embargo, con la evolución tecnológica se ha comprobado que ha servido como un trampolín para otras tecnologías. Las evoluciones desde 1G y sucesivas han mostrado que conforme mejora la tecnología se están dando más servicios a los usuarios tanto en lo laboral como en ocio. Esto ha permitido que no sólo dos personas puedan comunicarse, sino que además puedan compartir un medio común para realizar reuniones y tomar decisiones en tiempo real.

⁸⁶ MFA: Autenticación Multifactor

⁸⁷ IoT: Internet of Things

⁸⁸ IA: Inteligencia Artificial

Finalmente, la línea futura y que afecta a este trabajo dependerá de los objetivos establecidos y, que vendrán también definidos, en gran parte, por las evoluciones tecnológicas que se den en la sociedad. Todo ello, que fuere de provecho para nuestra organización. Se puede hablar de muchas tecnologías incipientes, pero se debe tener una visión clara para que se tenga que adoptar e implementarla en el sistema.

5 CONCLUSIONES Y LÍNEAS FUTURAS

Una vez visto todos los puntos, se puede observar cómo se está dando la transición de la telefonía de la red de ATM a la I3D. En este sentido, se muestra que todavía no se han implantado todos los nodos, pero en un futuro no muy lejano, terminarán de instalarse haciendo que la red de ATM deje paso a la I3D. En su momento se tuvo que realizar un gran esfuerzo para que hubiese comunicación entre ellos. Se ha mostrado cómo es la conexión entre ambas redes. En este modelo, donde conviven ambos mundos, es necesario realizar un mantenimiento continuo de ambos sistemas independientemente de que se estén añadiendo nuevas unidades en la I3D. Esto último, no sólo afecta a la telefonía sino también a otros servicios que se ofrecen tanto en aplicaciones que trabajan a nivel clasificado como no clasificado.

Actualmente, la tecnología ya no se puede ver como elementos únicos que realizan funciones únicas. Es decir, el teléfono, tableta, televisión, ordenador portátil, etc., son capaces de hacer varias funciones y ofrecer varios servicios. En el caso de la telefonía, ya se puede utilizar los teléfonos fijos, no sólo para comunicarse por voz sino también para hacer video llamadas, establecer reuniones online y, quién sabe si en un futuro para realizar funciones que ahora no somos capaces de imaginar. Además, estas tecnologías permiten movilidad para aquellas personas que se encuentren fuera de su lugar de trabajo, pudiendo mantener reuniones en el caso de estar realizando un viaje o trabajando de forma remota. Lo importante, es que los equipos telefónicos sean capaces de evolucionar de acuerdo con las necesidades de los usuarios y estén a la altura de los avances tecnológicos. El inconveniente que veo es que la telefonía anterior no precisaba de un software al que actualmente viene asociado con el coste que los usuarios deben soportar.

Para ayudar al usuario en su día a día, se están elaborando una serie de normas e instrucciones para que los usuarios de telefonía de nuestra organización puedan comunicar las distintas incidencias que ocurran. Estos procedimientos indicarán quiénes se encargarán de solventar todos estos problemas y qué medios telemáticos deben utilizar para comunicar los eventos acaecidos.

Se muestra casos prácticos e incluso las numeraciones y categorización de los usuarios para realizar las llamadas telefónicas.

Se aborda la validación y verificación de pruebas como elemento clave en la ingeniería que garantice que los requisitos se cumplen satisfactoriamente. Otro aspecto muy importante, es el trabajo que se realiza antes, durante y tras la implementación de un nodo, ya sea permanente o desplegable. Una vez que ya se superado las pruebas de verificación/validación, aceptación y se ha aprobado la instalación con toda la documentación, se pasa a la fase de dar de alta a un buen número de usuarios en la MXONE. Siendo este servidor el corazón de telefonía de baja clasificación. A partir de aquí, se reserva numeración interna y se asigna éstos un número de teléfono que será la referencia para que los usuarios que se encuentran fuera de la red oficial, les pueda reconocer como, por ejemplo, 9154xxxxx.

Con la documentación relativa a la arquitectura, que hace referencia a la IP, categorización, etc., se pueden ir dando de alta a los usuarios en el servidor MXONE. Para ello, se emplean herramientas muy útiles como MANAGER PROVISIONING y PUTTY. Es necesario remarcar el cambio que supone que un teléfono de la red de I3D pueda conectarse en cualquier ubicación manteniendo la numeración. Además, los teléfonos recibirán las configuraciones actualizadas sin intervención humana de tal forma que se haga fuera del horario laboral. No acaba todo aquí, dado que es necesario comprobar que funciona correctamente y que, a lo largo del ciclo de vida de este sistema, se garantice un mantenimiento idóneo donde ya no se cambiarán tarjetas como ocurre con la red de ATM, sino que la tendencia es ir hacia productos donde la solución sea la sustitución de otro equipo en caso de fallo.

Una vez finalice la implantación de la red de I3D, desaparecerán los procesos de transcodificación de audio y la conversión de protocolos de señalización, es decir, el audio en formato RPT de los paquetes IP ya no se convertirán en formato ATM. Y la señalización SIP usada en la red IP ya no tendrá que convertirse en ISUP que es parte de SS7 que es el protocolo usado en la señalización en la red de ATM.

Se definen técnicas que nos ayudan a evitar problemas en la congestión en la red, así como protocolos que se implementan para un buen funcionamiento de la red. Además, se hace referencia a los mecanismos de seguridad como son los IDS, IPS y firewall que nos ayudan a implementar barreras de seguridad para prevenir de ataques a la red.

En este trabajo, se muestra cómo serían los costes asociados a la instalación y mantenimiento de un servidor MXONE, firewalls, NGN y SBC, en un entorno virtualizado y sin virtualizar, junto con un nodo permanente. A partir de los datos obtenidos, se demuestra porque ahorro energético y la disminución de la huella de carbono es mejor ir a la opción para la virtualización.

Finalmente, se informa cómo se pretende que sea el futuro en el uso de la telefonía con las nuevas tecnologías y cómo afectará las nuevas tecnologías en el trabajo diario. Actualmente, se piensa que el futuro de la telefonía puede darse hacia las comunicaciones tridimensionales. En este caso, los participantes aparecerían en tres dimensiones sin tener que desplazarse físicamente. A esto se le denomina holografía. Otro avance es la denominada realidad aumentada. Esta consiste en añadir elementos virtuales en un entorno real. Para estos dos casos y aplicando las tecnologías como 5G ayudaría a tener conversaciones en tres dimensiones con un gran ancho de banda y muy baja latencia. Aparte de lo anterior, existe las comunicaciones multidimensionales que suponen sensaciones táctiles, vibraciones, sonidos en tres dimensiones denominada tecnología háptica. Por todo lo anterior, las comunicaciones ya no sólo serían por voz sino también por imágenes en tres dimensiones, vibraciones, etc, con las ventajas que ofrece 5G en velocidad en la transmisión de la información.

Con este trabajo, se trata de ofrecer un punto de vista más cercano, dentro de una variedad de servicios, de cómo funciona la telefonía actual y dar una visión de cómo un sistema complejo evoluciona gracias a la evolución tecnológica.

6 BIBLIOGRAFÍA

- [1] «Web de server VoIP». [En línea]. Available: [https:// www. servervoip.com/blog/antecedentes-historicos-de-telefonía-ip/](https://www.servervoip.com/blog/antecedentes-historicos-de-telefonía-ip/) [Último acceso: 13 noviembre 2024]
- [2] «Web de server VoIP». [En línea]. Available: [https:// www. servervoip.com/blog/tag/telefonía-analógica/](https://www.servervoip.com/blog/tag/telefonía-analógica/) [Último acceso: 13 noviembre 2024]
- [3] Proyecto fin de carrera “Diseño de la infraestructura de telefonía corporativa de una gran empresa”. Autor: Juan Carlos Ramiro Mas.
- [4] J.M. Huidubru Moya y D. Roldán Martínez.Tecnología VoIP y telefonía IP. La telefonía por Internet, Editorial Creaciones Copyright. 2016.
- [5] «Web de blogspot.com». [En línea]. Available: [https:// redesycomunicaciones01.blogspot.com/2010/09/](https://redesycomunicaciones01.blogspot.com/2010/09/) Último acceso: 13 noviembre 2024]
- [6] Seminario titulación “Las tecnologías aplicadas a las redes de computadoras”. Autor: Jorge Luis Miguel Estrada
- [7] M. Moro Vallina. Infraestructuras de redes de datos y sistemas de telefonía, Editorial Paraninfo. 2013.
- [8] «Web de cyberzaintza». [En línea]. Available: <https://www.ciberseguridad.eus/ciberglosario/tls-transport-layer-security> [Último acceso: 27 de octubre de 2024]
- [9] «Web de IBM». [En línea]. Available: [https:// www.ibm.com/docs/es/i/7.5?topic=authentication-remote-dial-in-user-service-overview](https://www.ibm.com/docs/es/i/7.5?topic=authentication-remote-dial-in-user-service-overview). [Último acceso: 27 de octubre de 2024]
- [10] «Web de f5». [En línea]. Available: https://www.f5.com/es_es/glossary/diameter-protocol [Último acceso: 27 de octubre de 2024]
- [11] «Web de amazon». [En línea]. Available: <https://aws.amazon.com/es/what-is/ipsec/> [Último acceso: 27 de octubre de 2024]
- [12] «Web de Internet Engineering Task Force (IETF)». [En línea]. Available: [https:// datatracker.ietf.org/doc/html/rfc6189](https://datatracker.ietf.org/doc/html/rfc6189). [Último acceso: 27 de octubre de 2024]
- [13] ITU-T Recommendation G.144
- [14] «Web de todo ingenierías.com». [En línea]. Available: <https://todoingenierias.com/estandares-de-calidad-de-servicio-en-redes-lo-que-debes-saber/>
- [15] Shigeru Kashiara. VoIP Technologies. Editorial IntechOpen. 2011.

- [16] ITU-T Recommendation P.861 (PSQM)
- [17] ITU-T Recommendation G.107 (E-model)
- [18] «Web de ietf»[En línea]. Available: [https:// datatracker.ietf.org/doc/html/rfc2309](https://datatracker.ietf.org/doc/html/rfc2309). RFC 2309: "Recommendations on Queue Management and Congestion Avoidance in the Internet" por Sally Floyd y Van Jacobson. [Último acceso: 14 de noviembre de 2024]
- [19] «Web de monografías de voz sobre VoIP». [En línea]. Available: [https:// www.monografias.com/trabajos23/voz-sobre-ip/voz-sobre-ip](https://www.monografias.com/trabajos23/voz-sobre-ip/voz-sobre-ip) [Último acceso: 14 noviembre 2024]
- [20] «Web de ITespresso». [En línea]. Available:<https://www.itespresso.es/cingular-wireless-migra-a-ip-con-alcatel-27309.html> [Último acceso: 14 noviembre 2024]
- [21] «Web de theipv6company». [En línea]. Available:<https://www.theipv6company.com/html/Tutoriales/Articulos/rdsi.html> [Último acceso: 14 noviembre 2024]
- [22] «Web de Alaisecure». [En línea]. Available: <https://alaisecure.co/glosario/gateway-que-es-y-para-que-sirve/>[Último acceso: 14 noviembre 2024]
- [23] «Web de purestorage». [En línea]. Available: <https://www.purestorage.com/la/knowledge/what-is-vmware.html>[Último acceso: 11 septiembre 2024]
- [24] «Web de patton». [En línea]. Available: <https://www.patton.com/media-gateway>. [Último acceso: 11 septiembre 2024]
- [25] «Web de 3CX». [En línea]. Available: [https:// www.3cx.es/voip-sip/comunicaciones-unificadas/](https://www.3cx.es/voip-sip/comunicaciones-unificadas/) [Último acceso: 26 de octubre de 2024]
- [26] «Web centrale nexo». [En línea]. Available: <https://www.centralesnexo.com.arg/soporte/voip/site> [Último acceso: 12 de noviembre de 2024]
- [27] «Web de loopup». [En línea]. Available: <https://loopup.com/es/resource-center/blog/what-is-a-session-border-controller-sbc-how-does-it-work>. [Último acceso: 27 de octubre de 2024]
- [28] «Web de incibe». [En línea]. Available: <https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips> [Último acceso: 27 de octubre de 2024]
- [29] «Web de mitel». [En línea]. Available: <https://www.mitel.com/products/6900-voip-business-phones> [Último acceso: 12 de noviembre de 2024]
- [30] «Web de tonitrus». [En línea]. Available: [https:// www.tonitrus.com/es/redes/accessories/others/10238632-003-palo-alto-pa-200-firewall-system/](https://www.tonitrus.com/es/redes/accessories/others/10238632-003-palo-alto-pa-200-firewall-system/) [Último acceso: 12 de noviembre de 2024]
- [31] «Web de instalad». [En línea]. Available:<https://www.instaladoresdetelecomhoy.com/switches-universales-serie-4000-con-gestion-cloud> [Último acceso: 12 de diciembre de 2024]
- [32] «Web de grandstream». [En línea]. Available: [https:// www.grandstream.com/hubfs/Product_Documentation/datasheet_gxp1610_1615_spanish.pdf](https://www.grandstream.com/hubfs/Product_Documentation/datasheet_gxp1610_1615_spanish.pdf) [Último acceso: 12 de noviembre de 2024]
- [33] «Web de esginnova». [En línea]. Available: <https://www.esginnova.com/sostenibilidad/como->

calcular-la-huella-de-carbono/ [Último acceso: 25 de diciembre de 2024]

- [34] «Web de cisco». [En línea]. Available: <https://duo.com/producto/multi-factor-authentication-mfa> [Último acceso: 12 de noviembre de 2024]
- [35] J. T. Kendall, VoIP vs traditional telephony, explore the clash between tradition and innovation in communication, Editorial, Jerry Kendall. 2023.

ANEXO I: SUBNETTING

Se va a mostrar un ejemplo de cómo obtener cuatro subredes a partir de una red principal. Para ello, vamos a definir la red principal con una dirección IP y una máscara de subred. La dirección IP de la red es 192.168.1.0/24 y para la máscara será 255.255.255.0. Como necesitamos 4 subredes por ello, subiremos a “barra 26”. Con ello, se podrá crear 4 subredes con 62 usuarios telefónicos o direcciones IP, es decir, $2^6 - 2 = 62$. Entonces, la nueva submáscara de la subred es 255.255.255.192 (/26)

- Red Principal:
 - Dirección IP: 192.168.1.0
 - Máscara de Subred: 255.255.255.0 (/24)
- Nueva Máscara de Subred:
 - 255.255.255.192 (/26)
- Calcular Rangos de Subredes:
 - Subred número 1: Desde 192.168.1.0 – hasta 192.168.1.63
 - Subred número 2: Desde 192.168.1.64 – hasta 192.168.1.127
 - Subred número 3: Desde 192.168.1.128 – hasta 192.168.1.191
 - Subred número 4: Desde 192.168.1.192 – hasta 192.168.1.255

Dirección IP y máscara de subred:

```
Dirección IP: 192.168.1.0
Máscara de Subred: 255.255.255.0
```

Figura A1-1 Dirección IP y máscara de subred

Nueva máscara de subred

```
Nueva Máscara de Subred: 255.255.255.192 (/26)
```

Figura A1-2 Nueva máscara de subred

Subredes resultantes

```
Subred 1: 192.168.1.0 - 192.168.1.63
Subred 2: 192.168.1.64 - 192.168.1.127
Subred 3: 192.168.1.128 - 192.168.1.191
Subred 4: 192.168.1.192 - 192.168.1.255
```

Figura A1-3 Subredes resultantes

ANEXO II: EJEMPLO CREACIÓN SUBREDES

A continuación, se expone el ejemplo donde se necesitan cuatro subredes. La primera de ellas se precisan 50 líneas telefónicas, en la segunda 20, en la tercera 10 usuarios y en la última 5 usuarios. Vamos a suponer que tenemos una red la dirección 192.168.1.0/24 y necesitamos crear las cuatro subredes antes citadas. Para ello, vamos a determinar primero la primera subred. Ésta precisará de 50 direcciones IP distintas por lo que necesitaremos $2^6 = 64$ direcciones. Por tanto, se necesita una máscara de subred de /26. En el segundo caso, se necesitan 20 usuario con teléfono por tanto $2^5 = 32$ direcciones con una máscara de subred de valor /27. Para el tercer caso, con 10 usuarios será suficiente con $2^4 = 16$ direcciones con una máscara subred de /28. Y, finalmente una pequeña subred para 5 usuarios, necesitarán $2^3 = 8$ direcciones con una máscara de subred de /29.

En la Tabla 0-1 Anexo II, se va a asignar los valores de los rangos, las direcciones de red, de broadcast y los hosts que van a ser asignados a cada una de las subredes.

Subred	Rango	Dir. Red	Dir. Broadcast	Host
A. 192.168.1.0/26	192.168.1.0-192.168.1.63	192.168.1.0	192.168.1.63	192.168.1.1-192.168.1.62
B. 192.168.1.64/27	192.168.1.64-192.168.1.95	192.168.1.64	192.168.1.95	192.168.1.65-192.168.1.94
C. 192.168.1.96/28	192.168.1.96-192.168.1.111	192.168.1.96	192.168.1.111	192.168.1.97-192.168.1.110

Tabla 0-1 Anexo II ejemplo de creación de subredes

En las Figuras II-1 y II-2, se muestran los valores de la red principal, así como las subredes A, B, C y D.

```

Red Principal: 192.168.1.0/24

Subred A: 192.168.1.0/26
- Dirección de Red: 192.168.1.0
- Dirección de Broadcast: 192.168.1.63
- Rango de Hosts: 192.168.1.1 - 192.168.1.62

Subred B: 192.168.1.64/27
- Dirección de Red: 192.168.1.64
- Dirección de Broadcast: 192.168.1.95
- Rango de Hosts: 192.168.1.65 - 192.168.1.94
  
```

Figura A2-1 Subredes A y B

Subred C: 192.168.1.96/28

- Dirección de Red: 192.168.1.96
- Dirección de Broadcast: 192.168.1.111
- Rango de Hosts: 192.168.1.97 - 192.168.1.110

Subred D: 192.168.1.112/29

- Dirección de Red: 192.168.1.112
- Dirección de Broadcast: 192.168.1.119
- Rango de Hosts: 192.168.1.113 - 192.168.1.118

Figura A2-2 Subredes C y D

ANEXO III: EJEMPLO DIVISIÓN RED PRINCIPAL EN SUBREDES

Supongamos que tenemos una red principal con una dirección IP de 192.168.0.0/24 y queremos dividirla en subredes más pequeñas usando *FLSM*. Esta técnica requiere seguir una serie de pasos. Primero, se debe determinar el número de subredes que se van a necesitar. Pongamos por caso que son 4 subredes. El siguiente paso será calcular la nueva submáscara de subred, es decir, $2^2 = 4$ subredes, es decir, 24 bits originales de la red + 2 bits = /26. Como paso final, se divide la red principal en cuatro subredes con una máscara de /26. En la siguiente tabla se puede ver el resultado obtenido.

Subred	Dir. Red	Dir. Broadcast
A. 192.168.1.0/26	192.168.1.0	192.168.1.63
B.192.168.1.64/27	192.168.1.64	192.168.1.95
C.192.168.1.96/28	192.168.1.96	192.168.0.127
D.192.168.1.112/29	192.168.1.112	192.168.0.255

Tabla 0-1 Anexo III ejemplo división red principal en subredes

ANEXO IV: STREAMING; CÓMO VE EL USUARIO EL CONTENIDO MULTIMEDIA

- El cliente se conecta mediante una conexión RTSP al servidor.
- A continuación, envía un comando denominado *SETUP* al servidor donde se configura la sesión. Ahí se define si es UDP o TCP y los puertos utilizados.
- El cliente envía un comando denominado *PLAY* para iniciar la transmisión del flujo de medios.
- El servidor inicia el envío de datos en paquetes RTP que están encapsulados.
- Durante la comunicación, se pueden enviar comandos como *PAUSE* para detener la reproducción.
- En el momento de finalizar la comunicación se envía el comando *TEARDOWN*.

ANEXO V: SECUENCIA EN UN ESTABLECIMIENTO DE LLAMADA

Antes del establecimiento de la llamada entre dos terminales es la resolución de la dirección IP del destinatario de la llamada. El terminal que realiza la llamada invoca a *H.225 RAS* al *gatekeeper* para conocer la IP del destinatario. Si el destinatario está bien registrado en el *gatekeeper* se le entregará al que inicia la llamada para que se inicie la comunicación. Sin embargo, aunque este dado de alta, el *gatekeeper* tiene la potestad de denegar una llamada. Es necesario aclarar que el terminal que realiza el inicio de llamada, a través del *canal RAS*, solicita al *gatekeeper* permiso para iniciar el proceso. Una vez concedido, el terminal abre una conexión TCP con el destino y envía un mensaje de tipo *Q.931* de establecimiento de conexión, *SETUP*. El destino, al recibir la solicitud, realiza una petición de permiso al *gatekeeper* al igual que hizo el solicitante de inicio de llamada. Cuando el receptor de la llamada reciba la autorización del *gatekeeper*, envía al que realizó la llamada un mensaje *Q.931* notificando que ha aceptado la petición de llamada, que será de tipo *H.225 RAS* que se transporta por UDP. Se entra en la *fase de negociación*, es decir, con la ayuda de los mensajes intercambiados de tipo *H.245* sobre datagramas de tipo TCP se decidirá el tipo de *códec* que se empleará en la conversación. A continuación, la comunicación queda establecida cuando ambos extremos se informan mutuamente de los puertos UDP de los *canales RTP* por donde se transmitirán los datos de cada extremo. *H.323* utiliza *UDP* como nivel de transporte de la voz y videos. Dentro de *H.323*, con la ayuda de *UDP*, se encuentran RTP y RTCP que son los responsables de introducir *marcas de tiempo* en cada datagrama de información para una correcta secuenciación y posterior reconstrucción de voz o video.

ANEXO VI: FUNCIONES QUE REALIZAN XML, CGI, TCL, C++

- XML. SIP archivos en formato XML para definir parámetros como de red, políticas de control de llamadas, y entre otros. Además, facilita la *interoperabilidad entre diferentes sistemas* y con un formato común para el intercambio de datos.
- CGI (*Common Gateway Interface*) en Perl. Se puede utilizar para crear interfaces web que interactúan con *servidores SIP*.
- TCL (*Tool Command Language*). Puede utilizarse para escribir *scripts* que controlan el comportamiento de las llamadas en sistemas VoIP, como encaminamiento, filtrado y manipulación de señales.
- C++. Se utiliza para *desarrollar servidores SIP* robustos y eficientes que pueden manejar grandes volúmenes de llamadas. Muchos componentes de red, como *gateways* y *routers*, están desarrollados en C++ debido a su rendimiento y capacidad de manejo de bajo nivel.

ANEXO VII: COMUNICACIÓN MGC Y MG

La comunicación entre los *MGC* y los *MG* se basa en los siguientes comandos:

- *AuditEndpoint*: Permite al *MGC* descubrir y obtener información sobre los endpoints disponibles en el Media Gateway, como los puertos y sus capacidades.

```
AuditEndpoint {  
    RequestIdentifier: 1234  
}
```

Figura A7-1 Comando AuditEndpoint

- *EndpointConfiguration*: Se utiliza para configurar los parámetros específicos en el *Media Gateway* que incluye el *codec* a utilizar, la dirección IP de destino, los puertos de entrada y salida, entre otros.

```
EndpointConfiguration {  
    RequestIdentifier: 5678  
    EndpointIdentifier: 1  
    DesiredAction: Modify  
    ConfigurationData: Codec=G.729, IP=192.168.1.200, Port=6000  
}
```

Figura A7-2 Comando EndpointConfiguration

- *AuditConnection*: Permite al *MGC* obtener información detallada sobre una conexión de medios existente en el *Media Gateway* y proporciona detalles como el estado de la conexión, los parámetros de medios utilizados (codec, ancho de banda).
- *ModifyConnection*: Se utiliza para cambiar los parámetros de una conexión de medios existente en el *Media Gateway*. Permite al *MGC* ajustar dinámicamente los parámetros de medios, como el codec utilizado o la dirección IP de destino. En el siguiente ejemplo se realiza un cambio de code.

```
ModifyConnection {  
    RequestIdentifier: 2468  
    ConnectionIdentifier: 1234  
    EndpointIdentifier: 1  
    ConfigurationData: Codec=G.711  
}
```

Figura A7-3 Comando ModifyConnection

- *DeleteConnection*: Es utilizado por el MGC para solicitar la terminación y liberación de recursos de una conexión de medios en el *Media Gateway*. En el ejemplo se ve la liberación del recurso utilizado en la conexión.

```
DeleteConnection {  
    RequestIdentifier: 1357  
    ConnectionIdentifier: 1234  
}
```

Figura A7-4 Comando DeleteConnection

- *Notification*: Es un comando utilizado por el *Media Gateway* para informar al MGC sobre eventos y cambios que ocurren en el estado de las conexiones de medios. Por ejemplo, puede notificar al MGC sobre la detección de tonos DTMF, cambios en la calidad de la señal, o la desconexión de una línea.
- *CreateConnection*: MGC envía un comando para establecer una conexión de llamada utilizando el endpoint ya configurado.

```
CreateConnection {  
    RequestIdentifier: 9876  
    ConnectionIdentifier: 1234  
    EndpointIdentifier: 1  
    // Otros parámetros de la conexión  
}
```

Figura A7-5 Comando CreateConnection

ANEXO VIII: LLAMADA TELEFONÍA TRADICIONAL RED IP

Este ejemplo consiste en el inicio de la llamada en la red *telefónica tradicional* se realiza por un usuario en la red telefónica tradicional (PSTN) levanta el teléfono y marca un número. La señalización SS7 en la red *PSTN* se utiliza para establecer la llamada. De tal manera que, SG recibe la señalización SS7 y ésta convierte la señalización SS7 en un formato que pueda ser comprendido por la red IP, típicamente utilizando el protocolo SIGTRAN. A continuación, SG envía la señalización convertida al *Media Gateway Controller* (MGC) a través de la red IP. MGC recibe la señalización convertida y determina cómo debe gestionarse la llamada traduciendo la señalización SS7 a señalización SIP (o H.323) que se utiliza en la red IP. Además, MGC consultará su *base de datos* para obtener la dirección IP asociada al número de teléfono marcado por la persona que inició la llamada que serán enviados a SG y MG. El MG recibe las instrucciones del MGC sobre cómo manejar los medios (audio) de la llamada y convierte el flujo de medios de la red telefónica tradicional al formato utilizado en la red IP (como puede ser G.711, G.729). Seguidamente, MG establece una conexión de medios RTP (*Real-time Transport Protocol*) con el destino en la red IP. De tal forma que, la señalización SIP, que contiene la información sobre la llamada, se envía desde el MGC al destinatario en la red IP y el flujo de medios (voz) convertido se transmite a través de la red IP utilizando RTP. Finalmente, el destinatario en la red IP recibe la señalización SIP y el flujo de medios RTP estableciéndose la llamada y el usuario puede comunicarse con el usuario en la red telefónica tradicional.

ANEXO IX: COMPARACIÓN SEÑAL ORIGINAL Y DEGRADADA

- Preparación de las Señales de Entrada: Las *señales de referencia* y *señal degradada* son las señales original y degradada que se usarán para la comparación.
- Alineación Temporal: Se alinean las señales para realizar las comparaciones.
- Preprocesamiento: Con la ayuda de un filtro se acentúa las frecuencias más altas.
- Ventanas de *Hanning*: Las señales se dividen en segmentos para minimizar los *efectos de discontinuidades*.
- Transformación en el Dominio de Frecuencia: Se obtiene el valor de la señal en el dominio de la frecuencia.
- Análisis Perceptual: Se evalúa la calidad de la voz introduciendo un ruido simulado.
- Procesado Asimétrico: Ocurre cuando el oído humano es más tolerante a ciertas distorsiones que deben ser evaluadas.
- Cálculo de la Distorsión: Se hace una comparación entre las señales de referencia y la degradada para obtener la distorsión.
- Ponderación de Periodos de Silencio: Se tiene en cuenta los periodos de silencio para que no afecte a la puntuación de calidad.
- Agregación de los Resultados: Se comparan las puntuaciones de calidad de los diferentes segmentos de la señal.
- Generación del PSQM Score: El resultado final es una puntuación PSQM, que indica la calidad de la voz.

ANEXO X: EJEMPLO TRÁFICO VOZ IP, VIDEO Y DATOS

Se puede utilizar WFQ asignando al tráfico de voz (VoIP) con un 70% del ancho de banda con 70 Mbps, para el tráfico de video de un 30% con 30 Mbps y para el tráfico de datos un 10% con 10 Mbps.

ANEXO XI: EJEMPLO DISTRIBUCIÓN ANCHO DE BANDA EN FUNCIÓN DEL PESO

Se puede asignar al tráfico de voz (VoIP) con un peso de 5 y un ancho de banda de 40%, para el tráfico de video un peso de 3 y un ancho de banda de 30% y tráfico de datos con un peso de 1 con un ancho de banda del 10%.

ANEXO XII: MECANISMO CONTROL DE FLUJO REDES IP A NIVEL TRANSPORTE

- Se produce el inicio de la conexión: Al establecerse una conexión TCP, el receptor envía su tamaño de ventana de recepción al emisor, y en el caso de que el emisor no sepa cuánta cantidad de red está disponible entre él y el receptor y, evitar sobrecarga de la red, TCP utiliza la técnica *slow start* para comenzar con una tasa de envío baja y aumentarla gradualmente. Por ejemplo, “puedo recibir hasta 10KB de datos”.
- Envío de datos: El emisor envía datos hasta llenar la ventana de recepción sin esperar confirmaciones. Es necesario indicar que existen dos tipos de ventanas; ventana de congestión (*Congestion Window, cwnd*) y la ventana de recepción. La ventana de congestión indica la cantidad de datos máxima de datos que el emisor puede enviar y que de inicio será un valor pequeño.
- Recepción y confirmaciones: A medida que el receptor recibe datos, envía confirmaciones (ACK) de los datos recibidos y actualiza la ventana de recepción y TCP incrementa la ventana de congestión (*cwnd*) Esto demuestra que la tasa de envío crezca rápidamente al principio mientras se evita la congestión inicial. Por ejemplo, después de recibir 5KB de datos, puede enviar un ACK y anunciar que aún puede recibir 5KB más.
- Deslizando la ventana: El emisor ajusta su ventana deslizante según las confirmaciones recibidas. Este método garantiza que el emisor no envíe más datos de los necesarios.
- Ajuste dinámico: La ventana de recepción puede cambiar dinámicamente en función de la capacidad de procesar datos del receptor.

ANEXO XIII: FUNCIONAMIENTO WRED EN CASO DE CONGESTIÓN

El funcionamiento de WRED consiste en:

- Clasifica el tráfico en diferentes clases o prioridades. Por ejemplo, tráfico de voz, video, y datos pueden tener diferentes niveles de prioridad.
- Se diferencian los umbrales entre mínimos y máximos y determinan cuándo y con qué probabilidad se descartarán los paquetes. Existe un umbral mínimo para un IPP dado por encima del cual los paquetes con ese peso empiezan a ser descartados aleatoriamente.
- Para el tráfico de mayor prioridad se aplica la probabilidad de Descarte Basada en Prioridad (PBDP, *Probability-Based Drop Priority*) y para el tráfico con menor prioridad (como algunos datos) tiene umbrales más bajos y mayor probabilidad de descarte. Hay que aclarar que los umbrales son configurables.

ANEXO XIV: CÓMO IMPLEMENTAR ECN EN EL CAMPO ToS

Para implementar ECN en el campo *ToS* en la cabecera IP se renombra como *Campo DS* (*Differentiated Services*), y los dos últimos bits de este campo se utilizan para ECN y que se muestra a continuación:

- *ECN-Capable Transport* (ECT): Indica si un paquete puede ser marcado con ECN. Los valores son; ECT (0): 10 en binario y ECT (1): 01 en binario
- *Congestion Experienced* (CE): Indica si el paquete ha experimentado congestión. El valor es CE: 11 en binario

Los valores combinados de los dos bits de ECN se interpretan de la siguiente manera:

ECN Field	Significado
00	No ECN-Capable
01	ECN-Capable Transport (1)
10	ECN-Capable Transport (0)
11	Congestion Experienced (CE)

Tabla 0-1 Anexo XIV implementar ECN en el campo ToS

El funcionamiento de ECN consiste en los siguientes pasos tomando como referencia la tabla anterior:

- **Inicio de la Comunicación:** Los dos extremos (emisor y receptor) deben soportar y estar de acuerdo en usar ECN. Esto se negocia durante el establecimiento de la conexión TCP.
- **Marcado de Paquetes:** Los emisores marcan sus paquetes como ECT (0) o ECT (1) para indicar que son capaces de manejar notificaciones de congestión sin descartes.
- **Detección de Congestión por Routers:** Si un router detecta congestión, en lugar de descartar un paquete, lo marca con CE (11). Esto se hace cambiando los bits de ECN en el encabezado IP del paquete.
- **Notificación al Emisor:** Cuando el receptor recibe un paquete marcado con CE, envía una notificación de congestión al emisor utilizando una bandera en el encabezado TCP llamada ECN-Echo (ECE). El emisor, al recibir esta notificación, reduce su tasa de envío para aliviar la congestión.