

UNIVERSIDAD AUSTRAL DE CHILE  
FACULTAD DE CIENCIAS DE LA INGENIERÍA  
ESCUELA DE ELECTRICIDAD Y ELECTRÓNICA



**TELEFONÍA IP CON SEÑALIZACIÓN POR CANAL COMÚN**

Trabajo de Titulación para optar al Título de Ingeniero  
Electrónico

PROFESOR PATROCINANTE:  
Sr. José Mardones Fernández

**RAFAEL ÁNGEL MONTALBÁN ALVARADO**  
VALDIVIA 2005

COMISIÓN REVISORA

---

JOSÉ MARDONES F.

---

NÉSTOR FIERRO M.

---

LUIS VIDAL V.

Dedicada a quienes creyeron en mí.  
A mí: esposa, madre, tía Guille, padre y hermanos.  
Y al futuro, a mi hijo.

## **AGRADECIMIENTOS**

Agradezco a quienes me apoyaron, tanto en el principio como ahora al finalizar esta etapa de mi vida.

A mi esposa, que llegó en un importante momento en mi vida y me da fuerzas para salir adelante. Por intermedio de ella las gracias a mis suegros por el apoyo brindado en este tiempo.

A mi familia, es especial a mi tía y madrina Guille a mi mamá, por esmerarse en mi educación a mi papá y a Natalia por su ayuda y orientación, a mis hermanos por tolerarme.

A mis amigos, en especial a Marcelo, Nino y Gerardo, con quienes compartimos incontables horas de estudio esforzándonos para que todos nos saliera bien.

A los profesores, a todos los que durante mi permanencia en la Universidad, me brindaron su conocimiento. Un especial agradecimiento a quienes son parte de la revisión de esta tesis por aceptar ser parte de ella.

Mención especial dedico al profesor Wladimir Ríos por las facilidades prestadas, para la utilización de las dependencias del Edificio Multimedia con el fin de realizar pruebas que forman parte de este trabajo, extensivamente son también para el señor Carlos Trecaman alumno de Ingeniería Civil Informática por la desinteresada ayuda prestada.

A todos muchas gracias.

## ÍNDICE

<b>PORTADA</b> .....	i
<b>COMISIÓN REVISORA</b> .....	ii
<b>DEDICATORIA</b> .....	iii
<b>AGRADECIMIENTOS</b> .....	iv
<b>ÍNDICE</b> .....	v
<b>RESUMEN</b> .....	x
<b>SUMMARY</b> .....	xi
<b>1. CAPITULO I. INTRODUCCIÓN</b> .....	1
<b>2. CAPITULO II. INTRODUCCIÓN A REDES</b> .....	2
2.1. DEFINICIÓN DE RED. ....	2
2.2. ELEMENTOS DE UNA RED. ....	2
2.3. LAS REDES SEGÚN SU TECNOLOGÍA DE TRANSMISIÓN. ....	2
2.3.1. Redes de difusión. ....	3
2.3.2. Redes punto a punto. ....	3
2.4. LAS REDES SEGÚN SU CARÁCTER. ....	3
2.4.1. Redes públicas. ....	3
2.4.2. Redes privadas. ....	3
2.5. POR LAS SEÑALES QUE TRANSPORTAN. ....	4
2.5.1. Redes analógicas. ....	4
2.5.2. Redes digitales. ....	4
2.6. POR SU ÁREA DE COBERTURA. ....	5
2.6.1. Redes LAN. ....	5
2.6.2. Redes MAN. ....	6
2.6.3. Redes WAN. ....	6
2.7. SEGÚN SU TOPOLOGÍA. ....	7
2.7.1. Elementos constitutivos de las redes. ....	7
2.7.1.1. Nodo. ....	7
2.7.1.2. Enlace. ....	7
2.7.1.3. Por uso del enlace. ....	7
2.7.1.3.1. Troncales. ....	8
2.7.1.3.2. De usuario. ....	8
2.7.1.4. Por número de conexiones. ....	8
2.7.1.4.1. Enlaces punto a punto. ....	8
2.7.1.4.2. Enlaces multipunto. ....	8
2.7.1.4.3. Enlace difuso (en inglés, fuzzy link). ....	8
2.7.2. Por topología de conexión. ....	9
2.7.2.1. Redes tipo estrella. ....	9
2.7.2.2. Redes tipo anillo. ....	10
2.7.2.3. Redes tipo bus. ....	10
2.7.3. Redes en malla. ....	11
2.8. SEGÚN SU DISPONIBILIDAD. ....	11
2.8.1. Enlaces dedicados. ....	11
2.8.2. Redes conmutadas. ....	12

2.8.2.1.	Conmutación de circuitos.....	12
2.8.2.2.	Conmutación de paquetes.....	13
2.8.2.2.1.	Orientados a la conexión.....	14
2.8.2.2.2.	No orientados a la conexión.....	14
2.8.2.2.2.1.	Circuito Virtual Permanente.....	15
2.8.2.2.2.2.	Circuito Virtual Conmutado.....	15
2.8.2.3.	Conmutación de mensajes.....	15
<b>3.</b>	<b>CAPITULO III. TELEFONÍA.....</b>	<b>17</b>
3.1.	EL TELÉFONO. CARACTERÍSTICAS DE LA SEÑAL TELEFÓNICA.....	17
3.1.1.	Características de la voz humana.....	17
3.1.2.	El teléfono.....	17
3.2.	DIGITALIZACIÓN DE SEÑALES TELEFÓNICAS.....	18
3.2.1.	Digitalización de la señal vocal.....	18
3.3.	MULTIPLEXACIÓN DE SEÑALES DIGITALES.....	20
3.3.1.	Concepto de multiplexación.....	20
3.4.	REDES TELEFÓNICAS.....	20
3.4.1.	Funciones de la red telefónica.....	21
3.4.1.1.	Transmisión o transporte de datos en redes telefónicas.....	22
3.4.1.2.	Conmutación telefónica.....	22
3.4.1.2.1.	Centrales.....	22
3.4.1.2.2.	Funciones de los equipos de conmutación.....	24
3.4.1.2.3.	Clasificación de los sistemas de conmutación, según su tecnología.....	24
3.4.1.3.	Señalización telefónica.....	25
3.4.1.3.1.	Funciones de Señalización:.....	25
3.4.1.3.2.	La señalización telefónica se agrupan en forma general en:.....	26
3.4.2.	Pasos de establecimiento de una llamada.....	26
3.4.3.	Canal asociado.....	27
3.4.4.	Canal común.....	27
3.4.4.1.	Principales ventajas de la señalización por canal común.....	27
3.4.4.2.	Sistema de señalización por canal común R2.....	28
3.5.	SISTEMA DE SEÑALIZACIÓN POR CANAL COMÚN Nº 7.....	28
3.5.1.	Introducción.....	28
3.5.2.	Definición.....	29
3.5.3.	MODOS DE SEÑALIZACIÓN.....	29
3.5.4.	Arquitectura.....	30
3.5.5.	Capas del modelo S7.....	31
3.5.5.1.	Parte de transferencia de mensajes (MPT).....	31
3.5.5.2.	Funciones del enlace de datos de señalización datos de señalización.....	31
3.5.5.3.	Funciones de enlace de señalización (MTP 2), capa 2.....	34
3.5.5.3.1.	Unidad de señalización (SU).....	35
3.5.5.3.2.	Detección de errores.....	36
3.5.5.4.	Funciones de la red de señalización (NIVEL 3).....	37
3.5.5.5.	Tratamiento de mensajes de señalización.....	37
3.5.6.	Encaminamiento.....	38
3.5.7.	Comparición de carga.....	38
3.5.8.	Gestión de la red de señalización.....	38

3.5.8.1.	Gestión del tráfico de señalización.....	39
3.5.8.2.	Gestión de enlaces de señalización.....	39
3.5.8.3.	Gestión de la ruta de señalización.....	39
<b>4.</b>	<b>CAPITULO IV. PROTOCOLOS TCP/IP.....</b>	<b>40</b>
4.1.	INTRODUCCIÓN.....	40
4.2.	CAPA DE INTERFAZ DE RED.....	41
4.2.1.	CSMA/CD, IEEE 802.3.....	41
4.2.2.	Token Bus, IEEE 802.4.....	42
4.2.3.	Token Ring, IEEE 802.3.....	43
4.2.4.	FDDI.....	43
4.2.4.1.	Especificaciones.....	43
4.2.5.	IEEE 802.11x.....	43
4.3.	CAPA DE INTERNET.....	44
4.3.1.	Protocolo IP.....	44
4.3.1.1.	Estructura de la dirección IP.....	44
4.3.1.2.	Datagrama IP.....	45
4.3.1.3.	SOCKET.....	47
4.3.1.4.	Encaminamiento IP.....	47
4.3.2.	ICMP.....	48
4.3.3.	IGMP.....	50
4.3.4.	ARP (RARP).....	51
4.3.4.1.	Formato del mensaje ARP.....	51
4.3.4.2.	Tipo de Hardware.....	51
4.3.4.3.	Formato del Mensaje RARP.....	53
4.4.	CAPA DE TRANSPORTE.....	53
4.4.1.	UDP.....	53
4.4.1.1.	Formato.....	53
4.4.1.2.	Puertos.....	53
4.4.2.	TCP.....	54
4.4.2.1.	Formato datagrama TCP.....	55
4.5.	CAPA DE APLICACIÓN.....	56
4.5.1.	SMTP.....	56
4.5.1.1.	Funcionamiento.....	56
4.5.1.2.	Los comandos básicos de SMTP.....	57
4.5.1.3.	Formato del mensaje.....	57
4.5.2.	FTP.....	58
4.5.3.	TELNET.....	58
4.5.4.	HTTP.....	58
4.5.4.1.	Ejemplo de un dialogo HTTP.....	60
4.5.6.	DNS.....	61
4.5.6.1.	Nombres de Dominio.....	61
4.5.6.2.	Formato RRs.....	61
4.5.6.2.1.	Funcionamiento.....	62
4.5.6.2.2.	Formato de un mensaje DNS.....	62
4.5.6.2.3.	Formato de la cabecera.....	62
4.5.6.2.4.	Formato de la sección Preguntas.....	63

4.5.6.2.5. Formato de la sección Respuesta.....	63
4.5.6.2.6. Formato de la sección Autoridad.....	63
4.5.6.2.7. Formato de la sección Adicional.....	63
4.5.7. H.323.....	64
4.5.7.1. Arquitectura.....	64
4.5.7.1.1. Terminales.....	64
4.5.7.1.2. Gatekeepers.....	64
4.5.7.1.3. Gateways.....	65
4.5.7.1.4. MCU (Multipoint Control Unit).....	65
4.5.7.1.5. MC (Multipoint Control).....	66
4.5.7.1.6. MP (Multipoint Processor).....	66
4.5.7.1.7. Entidad.....	66
4.5.7.1.8. Extremo.....	66
4.5.7.2. Canal de registros, admisión y situación (RAS).....	66
4.5.7.2.1. Pila de protocolos.....	67
4.5.7.3. Descripción de sistemas H.323.....	68
4.5.7.3.1. Características de los terminales.....	69
4.5.7.3.1.1. Interfaz de red por paquetes.....	69
4.5.7.3.1.2. Códecs de audio y video.....	69
4.5.7.3.1.3. Canal de datos.....	69
4.5.7.3.1.4. Función de control H.245.....	70
4.5.7.3.1.5. Función de señalización RAS.....	71
4.5.7.3.1.6. Función de señalización de llamada.....	71
4.5.7.3.2. Capa H.225.0.....	72
<b>5. CAPÍTULO V. SEÑALIZACIÓN H.323.....</b>	<b>73</b>
5.1. INTRODUCCIÓN.....	73
5.2. SEÑALIZACIÓN.....	73
5.2.1. Direcciones (identificadores).....	73
5.2.1.1. Dirección de Red.....	73
5.2.1.2. Dirección de alias.....	73
5.2.2. Canal de registro, admisiones y situaciones (RAS).....	74
5.2.2.1. Descubrimiento del Gatekeeper (controlador de acceso).....	74
5.2.2.1.1. Registro de punto extremo.....	76
5.2.2.2. Empleo de mensajes RRQ ligeros.....	76
5.2.2.3. Canal de señalización de llamada.....	77
5.2.2.3.1. Encaminamiento del canal de señalización.....	78
5.2.2.3.2. Encaminamiento del canal de control.....	78
5.2.3. Identificador (ID) de llamada.....	79
5.2.4. Capacidad de llamada de un punto extremo.....	80
5.2.5. Servicio de presentación y restricción.....	82
5.2.5.1. Presentación de la dirección de la parte llamante.....	82
5.2.6. Mensajes y elementos de información.....	85
5.2.7. Acciones en el punto extremo de terminación.....	86
5.2.8. Acciones en un Gatekeeper.....	87
5.3. PROCEDIMIENTOS DE SEÑALIZACIÓN DE LA LLAMADA.....	87
5.3.1. Fase A – Establecimiento de la llamada.....	88

5.3.1.1.	Ningún punto extremo está registrado en un Gatekeeper.....	89
5.3.1.2.	Ambos puntos están registrados en el mismo Gatekeeper. ....	89
5.3.1.3.	Solamente un punto extremo posee Gatekeeper.....	91
5.3.1.3.1.	Punto extremo llamante cuenta con Gatekeeper.....	91
5.3.1.3.2.	punto extremo llamado cuenta con Gatekeeper.....	93
5.3.1.3.3.	Ambos puntos extremos están registrados pero en diferentes Gatekeeper.....	95
5.3.1.4.	Establecimiento de una comunicación a través de Gateways.....	101
5.3.1.4.1.	Establecimiento de comunicación entrante a través de Gateway.....	101
5.3.1.4.2.	Establecimiento de comunicación saliente a través de Gateway.....	102
5.3.1.5.	Reenvío de llamada. ....	102
5.3.2.	Fase B – Comunicación inicial e intercambio de capacidad. ....	102
5.3.3.	Fase C – Establecimiento de comunicación audiovisual.....	105
5.3.4.	Fase D – Servicios de la llamada.....	106
5.3.4.1.	Cambios de ancho de banda. ....	106
5.3.4.2.	Estado. ....	107
5.3.4.3.	Servicios suplementarios.....	107
5.3.5.	Fase E – Terminación de la llamada.....	107
5.3.5.1.	Liberación de la llamada sin un Gatekeeper.....	108
5.3.5.2.	Liberación de la llamada con un Gatekeeper.....	108
5.3.5.3.	Liberación de la llamada por el Gatekeeper. ....	109
5.3.6.	Tratamiento de fallo de protocolo. ....	111
<b>6.</b>	<b>CAPITULO VI. CONCLUSIONES.....</b>	<b>112</b>
	<b>BIBLIOGRAFÍA.....</b>	<b>114</b>
	<b>ANEXOS .....</b>	<b>115</b>

## **RESUMEN.**

En los últimos años se ha visto un crecimiento sostenido de las redes de conmutación de paquetes, producto cada vez mayor del tráfico de datos. Además es una necesidad constante la comunicación a tiempo real; ya sea esta voz, imágenes o audio; conjuntamente utilizamos las extendidas redes existentes de conmutación de circuito, redes digitales que en su mayoría utilizan sistemas de señalización por canal común, aparece como una necesidad integrar estas dos redes de comunicación.

El fin de este trabajo, se debe a que precisamente, las redes de voz sobre circuitos conmutados con redes de voz paquetizadas, generan una serie de situaciones que no han sido del todo resueltas. Entre ellas, se puede distinguir, y no con menor importancia, la señalización digital que es obligatoria entre conmutadores de voz sobre redes de circuitos y que debe ser generada por parte de redes de voz paquetizadas para que se produzca la correcta integración, sin que el usuario deba pagar costos de tiempo y recursos para que esto sea efectuado, sino que sea absolutamente transparente para él.

En la unión de estos dos medios, opera de forma fundamental un equipo llamado Gateway. Este es el encargado de adaptar los dos medios en forma bidireccional (eso incluye los protocolos que poseen ambas redes que operan en ambos sentidos). Pero aún existen problemas, algunos de ellos son: ¿Cuáles son los problemas en la compatibilidad de los dos sistemas?, ¿Cómo seguir paquetes de VoIp sobre una red conmutada de circuitos?, como también se tiene ventajas al utilizar señalización n° 7, ¿cuales son esas?, con el presente trabajo se pretenderá identificar y dar una respuesta a algunos de los inconvenientes que se presentan en el normal desempeño de este elemento, en forma teórica y en forma práctica.

## SUMMARY

In the last years a maintained growth of the networks of commutation of packages has been seen, product every greater time of the traffic of data. In addition the on time real communication is a constant necessity; whitchever it is voice, images or audio; jointly we used the existing networks of commutation of circuit, digital networks that in their majority use systems of signaling by common channel, it appears like a necessity to integrate these two communication networks.

The aim of this work, it must that indeed, the networks of voice on circuits commutated with packages voice networks, they generate a series of situations that absolutely have not been solved. Among them, it is possible to be distinguished, and not with smaller importance, signaling digital that is obligatory between voice commutators on networks of circuits and that must be generated on the part of paquetizadas networks of voice so that correct integration takes place, without the user must pay to costs of time and resources so that this is carried out, but that is absolutely transparent for him.

In the union of these two means, it to tap of fundamental form a called equipment Gateway. This he is the one in charge to adapt average both in bidirectional form (that includes the protocols that has both networks that operate in both senses). But still problems exist, some of them are: Which are the problems in the compatibility of both systems, How to follow packages of VoIp on a dial-up network of circuits?, as also signaling is had advantages when using n° 7, Which do you are? With the present work it will be tried to identify and to give an answer to some of the disadvantages that appear in the normal performance of this element, in theoretical form and practical form.

## 1. CAPÍTULO I. INTRODUCCIÓN.

Tradicionalmente durante muchos años prácticamente toda comunicación se realizaban vía conmutado, con el pasar de los años se crean nuevas tecnologías con el fin de optimizar la comunicación de la red de conmutación de circuitos; tales como el crecimiento de las plantas de conmutación con el consiguiente proceso de automatización, nuevos medios de transporte, digitalización de las señales transportadas, y la creación de nuevos protocolo de señalización. Dentro de los nuevos sistemas aparece el sistema señalización por canal común N° 7, que entre sus ventajas es su capacidad de implementar nuevos servicios.

Luego aparecen las redes de conmutación de paquetes, una revolución en el transporte de datos, en donde se van creando nuevos servicios y descubriendo nuevas aplicaciones, orientado al transporte de datos.

Un nuevo servicio es creado, para la red de conmutación de paquetes, Voz sobre Protocolo Internet, VoIP, que es la transmisión de voz digitalizada por medio del soporte IP, o sea paquetizada. Una herramienta netamente económica al transporte de voz pero limitados a las redes de conmutación de paquetes. Entonces lógicamente después como una evolución natural aparece la Telefonía IP, que es la integración de la Red de Conmutación de Circuitos con la Red de Conmutación de Paquetes.

La Telefonía IP une tanto la red de conmutación de circuitos como la red de conmutación de paquetes, asimismo ambas redes tienen su propio idioma de señalización, control y datos. Estas diferencias son el principal escollo para la integración plena de estas dos redes, en el punto encuentro, el lugar en donde ambas redes establecen una intercomunicación, debe existir un elemento capaz de reproducir la información que se genera en cada una de las redes en forma bidireccional; este elemento es el Gateway, o Pasarela, la que actúa como intermediaria transmitiendo señales de control y datos.

El presente trabajo está orientado a analizar la integración de ambas redes, además de la función y la importancia del Gateway.

## **2. CAPÍTULO II. INTRODUCCIÓN A REDES.**

### **2.1. DEFINICIÓN DE RED.**

Las redes en general están destinadas a compartir recursos y uno de sus objetivos es hacer que el conjunto de medios técnicos instalados, organizados, operados y administrados sean disponible para quien esté en la red lo requiera. En otras palabras, una red de computadoras, es una red de telecomunicaciones de datos que enlaza a dos o más Equipo Terminal de Datos.

Se definen, a su vez, basados e los estándares de la ITU-T. Como ETD a un Equipo Terminal de Datos, que es capaz de generar y/o procesar información y transmitirla y/o recibirla a través de los circuitos de control que cumplen el rol de controlador de comunicaciones y que podrán ser internos o externos a la unidad de procesamiento. Como ETCD a un Equipo de Terminación del Circuito de Datos, que tiene la función de actuar como interfaz entre el controlador de comunicaciones y el medio físico que actuará como enlace, se le denominaba también ECD -Equipo de Comunicaciones de Datos-.

### **2.2. ELEMENTOS DE UNA RED.**

Una red de computadores consta de hardware y software. En el primero se pueden mencionar a: estaciones de trabajo, servidores, tarjetas de interfaz de red (NIC). En el software se encuentra el sistema operativo de red (Network Operating System, NOS).

Las redes son independientes de la cantidad de enlaces que abarcan. Para analizar las redes, se pueden clasificar de diversas maneras, según las características que busquen, y cada una de éstas da lugar a uno o varios tipos de red específicos. En este caso, la estudiaremos de la siguiente manera:

- **Por tecnología de transmisión.**
- **Su carácter.**
- **La naturaleza de los datos que transportan.**
- **Su extensión o cobertura.**
- **Su topología.**
- **Su disponibilidad.**

### **2.3. LAS REDES SEGÚN SU TECNOLOGÍA DE TRANSMISIÓN.**

En términos generales, las redes tienen dos tecnologías de transmisión.

### **2.3.1. Redes de difusión.**

Las redes de difusión tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos (llamados también paquetes) que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir un paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a alguna otra máquina, lo ignora.

### **2.3.2. Redes punto a punto.**

Son redes con muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, esa es la razón por que los algoritmos de ruteo desempeñan un papel importante en las redes punto a punto.

## **2.4. LAS REDES SEGÚN SU CARÁCTER.**

Según el modo de ser utilizadas y compartidas, las redes son de carácter público o privado.

### **2.4.1. Redes públicas.**

Una red de comunicaciones es de este tipo cuando no tienen otra limitación que la disposición de medios técnicos. El acceso a este tipo de servicio puede ser o no gratuito.

Las redes públicas pueden ser de conmutación de paquetes o de conmutación de circuitos, y los servicios son suministrados por compañías que se dedican a transportar señales, llamadas carriers, las que dan cobertura tanto local como larga distancia.

### **2.4.2. Redes privadas.**

Una red de comunicaciones tiene carácter privado, cuando es operada con un fin determinado y sus usuarios pertenecen a una o varias corporaciones con intereses específicos en las mismas. En la práctica, una red privada puede ser una red con facilidades de una pública. En este caso, el cliente proporciona todo el equipamiento de conmutación y alquila enlaces entre distintos lugares. De este modo, el término privado se refiere al hecho de que la organización tiene el uso exclusivo de todo o una parte de ella, sin compartir los recursos de la red pública dentro de la cual funciona.

## **2.5. POR LAS SEÑALES QUE TRANSPORTAN.**

Según la naturaleza de las señales que transportan, las redes pueden ser analógicas o digitales. Es importante notar la diferencia que las características de analógica o digital deben asignarse a la señal de datos y no al enlace.

Generalmente los enlaces aptos para el transporte de señal digital tienen características físicas propias al material y cualidades distintas a los usados para transportar señales analógicas, pero bajo ciertas condiciones, pueden usarse para que un analógico transporte señal digital o viceversa.

Usualmente, se habla de un enlace digital en lugar de un enlace apto para el transporte de señal digital.

### **2.5.1. Redes analógicas.**

Son redes diseñadas y equipadas para el transporte de señales analógicas. Son el medio de transporte de señal más difundido, ya que en sus orígenes estas redes fueron ideadas para la transmisión de voz, y éste es un fenómeno que si bien es naturalmente analógico, en el momento de su mayor expansión no había tecnología para desarrollarlas en forma digital.

Son las más usadas actualmente, ya que trabajan sobre la base de las redes de telefonía públicas y se encuentran disponibles con una cobertura mundial y con grandes inversiones de capital. Son más económicas frente a las redes digitales. Sus servicios están normalizados internacionalmente por el ITU-T que es el Comité de Telecomunicaciones de la Unión Internacional de Telefonía, y esta normalización hace que existan las interfaces estándares con equipos ETD.

### **2.5.2. Redes digitales.**

Son redes diseñadas y equipadas para el transporte de señales digitales, y aparecieron ante la necesidad de transmitir digitalmente mensajes codificados de forma digital. Ahora, es cada vez más común la digitalización de transmisión y conmutación en las redes, debido a:

- diseños cada vez más simples;
- facilidad de construcción de circuitos integrados;
- regenerar las señales sin necesidad de amplificación;

- minimización del ruido y la interferencia;
- capacidad para transportar voz, imagen y texto; al mismo tiempo.
- Las exigencias de las comunicaciones actuales, junto a las nuevas tecnologías, han hecho que sea posible la existencia de Redes Digitales de Servicios Integrados (RDSI) o integrated switched data network (ISDN).
- Podemos encontrar aplicaciones como: la telefonía digital (voz, sonido, video), el fax, el transporte de datos, correo electrónico, televisión, alarmas, telemedición y control. Las centrales de conmutación están controladas por computadoras. Esto permite que estas redes marquen presencia en el mercado, al bajar sus costos y aumentar su confiabilidad, mejorando sus prestaciones.

## **2.6. POR SU ÁREA DE COBERTURA.**

Uno de los aspectos más estudiados de las redes, son sus características dependiendo de la cobertura geográfica que tengan. Encontraremos redes de distintas magnitudes, que en cada caso, se llaman:

- Redes de área local (LAN, por Local Area Network): la definición más general es la de una red de comunicaciones utilizada por una sola organización dentro de un área limitada (generalmente un edificio o campus), la cual permite compartir información y recursos.
- Redes de área urbana (MAN, por Metropolitan Area Network): abarca el área geográfica de una ciudad y generalmente interconectan redes LAN. Funcionan de la misma forma, pero a diferencia de las primeras tienen elementos de conmutación, los cuales encaminan los paquetes por una de varias líneas de salida potenciales.
- Redes de área amplia (WAN, por Wide Area Network): nacen al ampliar una LAN pero llega un momento en que es poco práctico fruto de limitaciones físicas o económicas. Tienen una cobertura más amplia que una ciudad, por ello también se las llama interurbanas, aunque la mejor definición es decir que son ilimitadas.

### **2.6.1. Redes LAN.**

Es una red privada de comunicaciones cuya área de cobertura geográfica se contiene en un edificio. En una red de este tipo, los ETD son generalmente, pero no necesariamente, computadoras, ya sea personales, del tipo rango medio o grandes computadoras trabajando en

modo estación de trabajo o servidor. También se encuentra terminales no inteligentes trabajando con sus correspondientes computadoras.

Las LAN se distinguen de otros tipos de redes por tres factores: (1) tamaño, que está restringido lo que significa que el tiempo de transmisión está limitado y se conoce de antemano. (2) tecnología de transmisión como pueden ser par trenzado (UTP), coaxial, FO o enlaces no tangibles; desarrollan velocidades de transmisión del orden de 101 y 102 Mbps (por ejemplo, 10 Mbps Ethernet, 16 Mbps Token Ring, 100 Mbps Fast Ethernet). Y (3) su topología, pueden ser diversas entre ellas están: Bus Ethernet, las computadoras pueden transmitir cuando quieran, si dos o más chocan, esperan un tiempo al azar y retransmiten; otro tipo es por difusión en anillo también el más popular es Token Ring.

Las LAN tradicionales pueden operar a velocidades de transmisión que están entre 10 y 100 Mbps, tienen bajo retardo y experimentan pocos errores.

### **2.6.2. Redes MAN.**

Son redes con cobertura urbana, básicamente una LAN de mayor tamaño. Al decir cobertura urbana, se entiende que su extensión (el tamaño del cable que las enlaza) se mide en metros, en kilómetros, puede llegar en ciudades grandes a segmentos de 50 kilómetros. Transportan señales a velocidades de 100 Mbps (por ejemplo, 100 Mbps FDDI y 155 Mbps DQDB), utilizando para ello fibra óptica, 100 Mbps (por ejemplo, en Trama de 2 Mbps) usando fibra óptica, coaxial y par no trenzado y 10 Mbps (por ejemplo, conexiones en 64 Kbps y 128 Kbps) usando recursos generalmente telefónicos.

La principal razón que distinguen a la MAN, para estar en una categoría especial es que se ha adoptado un estándar para ellas, ya está implementado y se llama DQDB (distributed queue dual bus, o bus dual de cola distribuida) o IEEE 802.6.

Prestan servicios de transporte para interconexión de redes, telefonía con PBX, etc. Pueden ser de conmutación de circuitos o de paquetes con servicios orientados o no a la conexión

### **2.6.3. Redes WAN.**

Estas redes también son llamadas de área extendida o área amplia, y prácticamente son de cobertura ilimitada, ya que unen diferentes redes de menor cobertura. En muchas redes WAN, las

subredes tienen 2 componentes diferentes; las líneas de transmisión -llamados circuitos, canales o troncales donde se mueve la información- y los elementos de conmutación -computadores especializados que conectan dos o más líneas de transmisión y son encargados de decidir que camino, que línea de salida toma la información que llega por la línea de entrada-.

Generalmente usan redes públicas y/o privadas y hacen uso de diferentes tipos de topologías de transmisión.

## **2.7. SEGÚN SU TOPOLOGÍA.**

Se analizan las redes según sus elementos constitutivos principales, que son los nodos y los enlaces, éstos dan lugar a distintos tipos de redes, según el grafo resultante. La topología, puede determinar desde el protocolo de capa de las capas bajas (física, enlace, red) hasta las capacidades y prestaciones mismas de las redes.

### **2.7.1. Elementos constitutivos de las redes.**

Una red está básicamente constituida por nodos y enlaces.

#### **2.7.1.1. Nodo.**

Es el equipo de la red que interconecta a enlaces, con capacidad de computación y que está diseñado para transferir información desde un enlace a otro, en función de sus parámetros de diseño.

#### **2.7.1.2. Enlace.**

Es el conjunto de medios de comunicación que no incluye los ETD, permite establecer uno o más canales de transmisión entre dos o más puntos de la red.

Este concepto incluye a; los ETCD, los vínculos físicos tangible e intangibles, y los equipos que, entre los puntos origen y destino, son atravesados por la conexión, actuando o no como nodo.

#### **2.7.1.3. Por uso del enlace.**

Dependiendo de qué tipos de dispositivos, para qué fines y con qué rutas se esté enlazando, los enlaces podrán ser:

#### **2.7.1.3.1. Troncales.**

Cuando enlazan dos nodos abarcando varios canales y transportando señales de varias comunicaciones de forma simultanea.

#### **2.7.1.3.2. De usuario.**

Cuando enlazan un nodo y un sitio de usuario, transportando señal sólo para el ETD del usuario.

#### **2.7.1.4. Por número de conexiones.**

Se puede clasificar a los enlaces según cuántos ETD enlazan concurrentemente. De este modo, encontraremos:

##### **2.7.1.4.1. Enlaces punto a punto.**

Es la configuración en que un enlace trabaja con un ETD en cada extremo. Estos ETD están definidos como estáticos, fijos e invariables. La comunicación punto a punto trabaja con ETD que son pares, es decir, el hardware propio del ETD o el ETCB relacionado, no contempla relaciones distintas que entre ETD iguales. Circunstancialmente, también los protocolos que los unen en una WAN, bajo ciertas condiciones, si establecen diferencias entre extremo primario (o maestro) y secundario.

##### **2.7.1.4.2. Enlaces multipunto.**

Es la configuración en la cual un ETD, al que se llama siempre primario (o maestro) está conectado a varios ETD secundarios (o esclavos), mediante un enlace que tiene un extremo para el primario y varios extremos secundarios conectados en paralelo. Este tipo de enlaces son comunes para transmisiones sincrónicas de datos. Las colisiones que aparecieran si varios secundarios transmitieran al mismo tiempo, se resuelven por medio de los protocolos de comunicación de datos correspondientes.

##### **2.7.1.4.3. Enlace difuso (en inglés, fuzzy link).**

Es la configuración en la cual varios ETD se conectan entre sí, no existe una jerarquía para los extremos de los enlaces ni para los ETD. En este enlace todos los ETD acceden mediante un medio de comunicación que lo dejará conectado en modo llamado broadcasting. Las

colisiones que aparecerán si más de un ETD transmitieran en forma simultánea, se soluciona por los protocolos de comunicación de datos correspondientes.

Estos tipos de enlaces se usan para distintos tipos de redes. Esto está determinado por el protocolo.

Enlace	LAN	MAN	WAN
PaP	Si	Si	Si
MP	No	No	Si
D	Si	Si	No

### **2.7.2. Por topología de conexión.**

Por otro lado, la forma en que los nodos se unen por medio de enlaces, resulta en distintos diagramas que dan lugar a las redes de tipo estrella, anillo, bus y malla.

#### **2.7.2.1.Redes tipo estrella.**

Están basadas en un nodo central que actúa como concentrador del tráfico, que tiene un conjunto de enlaces punto a punto para unir las estaciones remotas con el nodo principal. Una ventaja de usar este tipo de red es, de ocurrir una falla solo se ve la parte afectada por dicha falla y no inhabilita alguna parte de la red; y el problema es si la falla es en el nodo central la red queda inhabilitada en forma total. Esta configuración se utiliza en redes WAN, donde este nodo central o host es habitualmente una computadora de gran tamaño, llamado generalmente un mainframe o de mediano tamaño, un midrange, que actúa como una ETD con una gran cantidad de interfaces para la conexión de DCE. Suelen utilizarse en estos casos cuando existe dispersión de los sitios de usuarios. Se usan para enlace redes públicas o privadas, tanto dedicadas o conmutadas.

También se utiliza en redes LAN, donde el nodo central es un hub o un switch, que conecta en estrella a las estaciones de trabajo para redes Ethernet, o una Mau o una Cau que conecta en estrella estaciones de trabajo para redes Token Ring.

En las redes de telefonía por su parte, se observa que el nodo central es, por ejemplo, una central telefónica zonal, mientras que cada extremo es un usuario que utiliza, por ejemplo, un teléfono. Además, la red es conmutada.

### **2.7.2.2.Redes tipo anillo.**

En este tipo de red, el enlace une a cada ETD consecutivamente, cerrando el círculo uniendo el último con el primero. Los ETD se interponen en el camino del enlace. Esto significa que interrumpen el enlace, siendo que éste entra y sale del ETD o del ECD, si hubiera.

La información, circula en una única dirección, entrando al ETD, siendo procesado y continuando. Como se podrá ver, la información se pone en el enlace y todos la van a recibir, pero sólo el que corresponde la va a procesar.

La desventaja de este tipo de topología radica en que si un EDT falla la red completa puede fallar, otro el inconveniente es que el mensaje tiene que dar una vuelta casi completa al anillo en la situación más desfavorable. Pero por otro lado, son previsibles en cuanto al tiempo que demorará el mensaje en llegar a destino, lo que permite armar redes de tiempo real.

En aplicaciones prácticas, los anillos suelen ser lógicos. Tomemos, por ejemplo, las redes de área local con protocolo Token Ring. En ellas, cada estación está conectada en estrella a un dispositivo central, que se llama Mau o Cau. Pero éste tiene como función únicamente recibir una trama de una estación y redireccionarla a la siguiente estación, controlando que ella esté presente, para saber si la tiene que direccionar o saltar. Así la red es físicamente una estrella, pero lógicamente un anillo, porque nunca se invierte el orden establecido.

### **2.7.2.3.Redes tipo bus.**

Es un red de diseño simple tipo de redes, que utiliza un sólo cable para enlazar a todas las ETD mediante un enlace difuso.

Se puede encontrar también bajo la forma de un enlace que se conecta secuencialmente de estación en estación, pero esto es, formalmente, un anillo abierto. Esta topología es la que utilizan las redes tipo LAN con protocolo Ethernet, aún aquellas que se construyen con el dispositivo llamado hub que conecta las estaciones en estrella, porque en la práctica, para ellas la estrella es también sólo aparente. En realidad, en el hub internamente está construida el bus y cada conector que soporta un enlace en estrella hacia una estación, es una T.

A diferencia de las redes en estrella, donde la caída de un enlace directo a una estación no afecta sino a esa sola estación, en las redes en bus la rotura de la bus deja inhabilitada toda la red. Como contrapartida son redes de fácil configuración y se pueden implementar de manera barata.

### **2.7.3. Redes en malla.**

Son aquellas formadas por enlaces punto a punto entre los nodos, en una configuración del tipo todos con todos. Al tener caminos redundantes, se aumenta la disponibilidad de enlaces entre los nodos.

La utilización más usual de estas redes es en conmutación de paquetes y de conmutación de mensajes para las aplicaciones de transporte de datos. Sin embargo, si analizamos las redes de transporte de voz, que suelen ser de conmutación de circuitos, encontraremos que también son redes del tipo malla. Los nodos trabajan de dos modos: con un enlace activo a un tiempo, o varios (o todos) activos al mismo tiempo. Los nodos que satisfacen este último criterio, suele tener capacidad de control no sólo sobre el vínculo sino que, mediante los protocolos adecuados, suelen manejar la comunicación para poder secuenciar los paquetes o administrar los mensajes puestos en cada vínculo. Como consecuencia de su configuración, las redes en malla terminan teniendo nodos terminales o finales (end node) y nodos de paso o intermediarios (intermediate node).

Estas redes son más complejas y por lo tanto son de mayor costo implementarlas, pero son de una alta fiabilidad.

## **2.8. SEGÚN SU DISPONIBILIDAD.**

Según sea la disponibilidad que el usuario tiene para acceder a un enlace y la posibilidad que tenga de establecer la misma ruta para los datos, las redes se clasifican en redes de circuitos dedicados y redes de conmutación.

En las primeras, dos ETD disponen de un enlace permanente, el que a su vez tiene un trayecto fijo y conocido. En las otras redes, son los ETD los que deben procurarse para disponer del enlace. En otras palabras un servicio de líneas conmutadas, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a la de la transmisión de estos.

### **2.8.1. Enlaces dedicados.**

Es un camino de comunicación –trayecto- fijo entre dos puntos de comunicación por un enlace físico determinado o también por un camino lógicamente definido dentro de un sistema de comunicaciones. Este sistema puede, además, ser multiplexado y/o conmutado.

Estos circuitos pueden ser fijos cuando se arriendan líneas que mantienen una conexión permanente entre dos lugares fijos, nombre que se le da a redes punto a punto. Se utilizan por lo general en la construcción de redes privada.

Un circuito también puede ser del tipo lógico, como lo son redes X.25 o Frame Relay que son protocolos de transmisión de datos en redes de conmutación de paquetes. Estos circuitos no son punto a punto, es un enlace que se establece en forma virtual preparando el camino para la transmisión, se le llama Circuito Virtual Permanente.

### **2.8.2. Redes conmutadas.**

Cuando las redes no requiere conexiones permanentes entre dos puntos y otros, se le dice que son redes conmutadas porque debe establecerse la ruta de datos –o trayecto- antes de comenzar la comunicación entre dos puntos. Son rutas temporales entre diversos puntos, una vez establecida podría incluso ser dinámicamente alterada sin que se altere la comunicación entre los ETD, dependiendo del tipo de red.

De acuerdo a cuál sea la tecnología empleada y la técnica para conmutar, encontramos redes de conmutación:

- de circuitos (circuit switching),
- de paquetes (packet switching) y
- de mensajes (messages switching).

Independientemente de cuál analicemos, las características principales de ellas son:

- La transmisión no puede ser preestablecida o preacondicionada, por cuanto los circuitos que se establecen y las rutas de los datos empleadas podrán cambiar de sesión en sesión.
- Cuando la comunicación se corta, se libera el enlace.
- El costo es generalmente una función del tiempo de conexión o una función de la cantidad de datos transmitidos.

#### **2.8.2.1. Conmutación de circuitos.**

En la conmutación de circuitos es el proceso de definir un canal dedicado y permanente que una a dos o varios DTE, el tiempo en que dura la conexión.

El estado natural de un ETCD, en este sistema, es desconectado. Cuando desea establecer una comunicación, existen acciones concretas que se realizan antes de comenzar la transmisión, lo que se denomina acciones en tiempo de conexión. Estas acciones hacen que la red establezca el circuito de datos, el que no podrá ser cambiado durante la comunicación. Dentro de estas acciones están los parámetros de velocidad de transmisión, protocolo, etc. La sesión de comunicación, o sea el tiempo que dura una comunicación completa entre dos ETCD, suele llamarse una llamada.

### **2.8.2.2. Conmutación de paquetes.**

Paquete de datos se denomina como el conjunto de datos que conforman una información, que en longitud y forma dependen del protocolo al que pertenezca. También se le suele llamar trama. Este paquete representa un bloque reducido de datos que precede al destino y la extensión de la información. La conmutación de paquetes es el proceso de transmisión de datos en donde la entidad controlada son los paquetes (paquete se define como Unidad de Datos del Protocolo de Red, en términos del modelo OSI) que provistos de direcciones, hacen que el canal esté ocupado solamente durante la transmisión del paquete, con esto queda libre, antes o después, el canal de comunicación para la transmisión de otro paquete.

La red de conmutación de paquetes es red de malla que soporta múltiples usuarios al mismo tiempo enviando cada uno paquetes con distintos destinos. Siempre se representa como una nube que simboliza a esta red. Esta representación se debe a la existencia de una gran cantidad de conexiones y rutas por donde el paquete puede alcanzar su destino, y por ello se dice que es una red de cualquiera contra cualquiera, a diferencia de la red de conmutación de circuitos, que ofrece una conexión temporalmente dedicada entre dos ETCD.

En este tipo de redes los nodos son quienes se encargan de encaminar los paquetes. Se le llama nodo al lugar de la red que interconecta a varios enlaces, capaces de procesar información y diseñados para transferir paquetes a diferentes líneas, de acuerdo a parámetros establecidos. El nodo deberá elegir entonces lo que asegure el arribo con éxito del paquete dados los siguientes criterios de diseño, ya que dos criterios básicos determinan al nodo, según qué se quiera optimizar, se emplea:

- el tiempo de respuesta: mínimo tiempo en la red por la ruta más corta, o

- el menor tráfico: tránsito por la ruta más descongestionada.

Los nodos también sirven para controlar errores, mediante la verificación de los paquetes transmitidos y recibidos.

Las redes de conmutación de paquetes son redes de prestación de servicios de comunicaciones y, acá se pueden clasificar a su vez en:

#### **2.8.2.2.1. Orientados a la conexión.**

También llamados de prestación de circuitos virtuales, los ETCD correspondientes mantienen la información del estatus acerca del diálogo que están manteniendo. Esta información del estado de la conexión soporta control de error, secuencia y control de flujo entre las correspondientes entidades. Es decir, La entidad receptora le avisa a la entidad transmisora si la información útil llegó correctamente, si no es así también le avisa que vuelva a retransmitir. Nótese que los datos deben ser entregados en el orden emitido no importa la ruta en que en forma individual sigan.

Los protocolos orientados a conexión operan en tres fases. La primera fase es la Fase de la Configuración de la Conexión, durante la cual los ETCD correspondientes establecen la conexión y negocian los parámetros que definen la conexión. La segunda fase es la fase de transferencia de datos, durante la cual se intercambian información útil durante la conexión. Finalmente, la última fase, fase de liberación de la conexión, en la cual ambas entidades se ponen de acuerdo para terminar la conexión.

Su uso es necesario en aplicaciones donde se requiera mucha precisión [transacciones electrónicas bancarias, archivos de datos, comercio electrónico, etc.].

#### **2.8.2.2.2. No orientados a la conexión.**

Los protocolos orientados a la no-conexión no proveen capacidad de control de error, secuencia y control de flujo. Están siempre en la fase de transferencia de datos, y no les interesan las fases restantes de configuración y liberación de una conexión. Este tipo de negociación se encuentra ausente dado que cada paquete es una entidad en sí misma.

Los protocolos orientados a no-conexión se emplean en aplicaciones donde no se requiera mucha precisión. Tal es el caso de la voz, música o el video.

El concepto principal de las redes de conmutación de paquetes, es el de circuito virtual. Un CV es un camino a través de una red de conmutación de paquetes, creado para garantizar la comunicación confiable entre dos dispositivos de red, se comporta como si fuera un enlace dedicado, proporcionando para los ETCD una sesión orientada a la conexión.

La característica distintiva es que tiene un trayecto predefinido a través de una red que tiene muchos trayectos. No obstante, los trayectos pueden variar a lo largo de la sesión para evitar una congestión, o una indisponibilidad de enlaces.

Un circuito virtual puede ser:

#### **2.8.2.2.1.Circuito Virtual Permanente (PVC, por permanent virtual circuit).**

Conexión entre dos ETCD que se define por adelantado -en tiempos anteriores a la conexión-, es decir cuando se negocia la contratación y por lo tanto tiene un tiempo de establecimiento muy pequeño -insignificante frente a otros tiempos-. Cuando dos ETCD están enlazados por este tipo de circuitos, la única actividad necesaria para comenzar la sesión entre ellos es que se enciendan.

#### **2.8.2.2.2.Circuito Virtual Conmutado (SVC, por switched virtual circuit).**

Es la conexión temporal establecida por la red para dos ETCD, que durará sólo el tiempo necesario para el desarrollo de la sesión. Se establecerá a pedido de uno de los ETCD y ante la aceptación del otro. Esta negociación se lleva a cabo durante el tiempo de conexión. Para que el enlace se establezca, el ETCD además de encenderse debe tomar acciones de establecimiento del circuito. Estas acciones son el envío de un paquete -o trama- de control que se llama paquete de llamada, que es el que negocia el establecimiento del enlace.

#### **2.8.2.3.Conmutación de mensajes.**

El concepto de mensaje usado aquí, no corresponde al de la UDP de capa 7 OSI, sino al de una unidad de intercambio independiente que no necesita ser secuenciada. Las redes de conmutación de mensajes son, en la práctica, un caso especial de la conmutación de paquetes,

pero en las cuales lo que transita son mensajes, también llamados celdas, con las siguientes características:

- La información está contenida en paquetes unitarios y no se admite secuenciamiento.
- La longitud de los mensajes es, intrínsecamente, variable.
- Los nodos se limitan al control de destino.

Por lo demás, se puede aplicar a ésta los conceptos generales de conmutación de paquetes.

### 3. CAPÍTULO III. TELEFONÍA.

#### 3.1. EL TELÉFONO. CARACTERÍSTICAS DE LA SEÑAL TELEFÓNICA.

##### 3.1.1. Características de la voz humana.

La voz se produce de la vibración de las cuerdas vocales. Estas están situadas en el conducto que lleva el aire de la respiración desde los pulmones a la boca y la nariz. La generación de sonidos se logra mediante las cuerdas vocales. Rango de frecuencias de la voz humana es de 20 Hz - 32 Khz. y el rango de frecuencias del oído humano: 20 Hz - 20 Khz.

La señal de telefonía debe ser señal de voz con la mínima calidad suficiente: 0.3 - 3.4 Khz.

##### 3.1.2. El teléfono.

El fundamento del actual teléfono está basado en el ideado por Antonio Meucci en 1855<sup>\*</sup>. Este aparato se compone de una membrana de hierro dulce muy flexible situada delante de un imán, en el cual está enrolla un hilo conductor aislado; al hablar delante de la membrana, se producen cambios de presión en el aire produciendo una vibración de la membrana que a su vez produce una corriente variable. Por otro lado, un conductor eléctrico une este aparato con otro de iguales características, en el que la corriente eléctrica origina fenómenos inversos, logrando reproducir la voz humana.

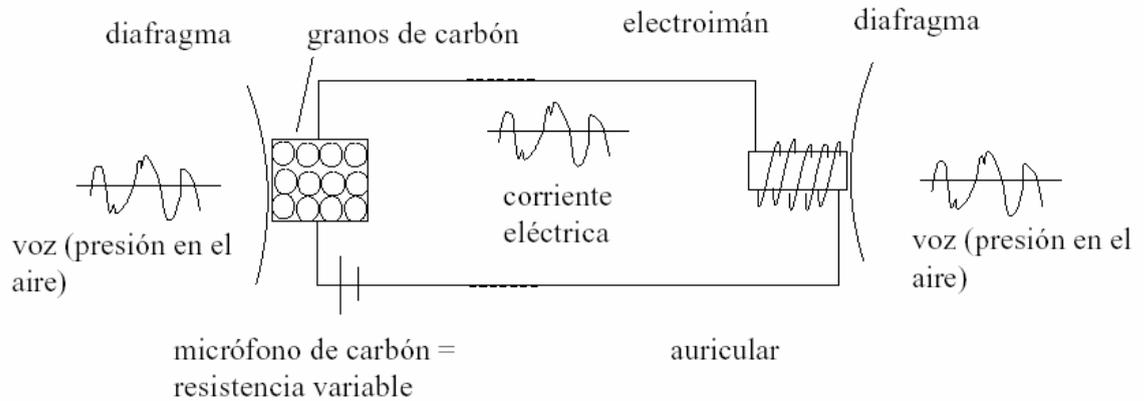
Diagrama eléctrico de una telefónica.




---

\* El 11 de junio de 2002 el Congreso de los Estados Unidos lo reconoce en forma oficial como el inventor del teléfono, falsamente atribuido a Graham Bell.

Diagrama esquemático de un aparato telefónico.



El aparato telefónico, entonces, estaría compuesto por dos transductores. Un transductor acústico-eléctrico, (micrófono) será el encargado de traducir la voz en una señal eléctrica capaz de viajar por el medio de transmisión, en nuestro caso un cable; y el otro, el que hace el proceso inverso es el auricular, se encarga de traducir la señal eléctrica enviada por el otro comunicante en una señal audible.

Los elementos que componen un teléfono necesitan algún tipo de alimentación para su funcionamiento, igual que la corriente que hace funcionar el timbre, la energía es proporcionada por la central a través de la línea telefónica, este voltaje es aproximadamente de 60 Volt de corriente continua. Otros parámetros de la línea de abonado son corriente de lazo aproximadamente 25 mA y de 600  $\Omega$  la impedancia de la línea.

## 3.2. DIGITALIZACIÓN DE SEÑALES TELEFÓNICAS.

### 3.2.1. Digitalización de la señal vocal.

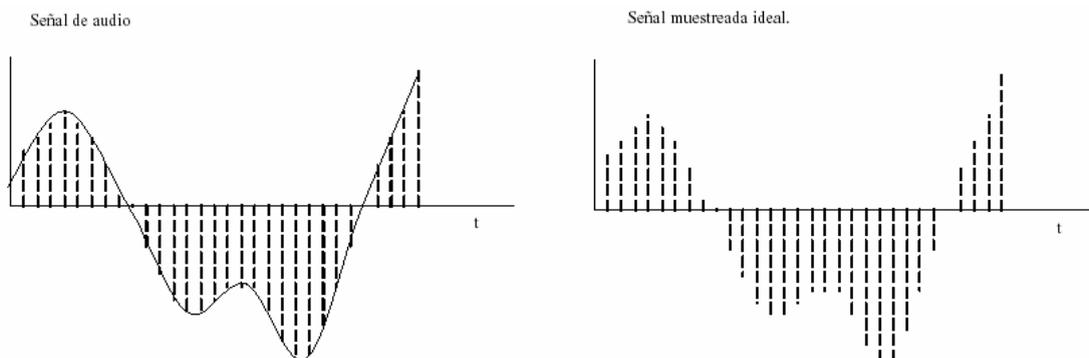
A pesar de que en un principio la transmisión de la señal telefónica era totalmente analógica, es decir, del emisor al receptor, en la actualidad esta se reduce al último tramo, el comprendido desde la central local al abonado; el recorrido restante es transmitido en forma digital. Las ventajas de la transmisión digital: es posible recuperar la señal original perfectamente, en la transmisión analógica se va añadiendo ruido que es imposible eliminar.

La digitalización de la señal vocal debe pasar por tres procesos, a saber, muestreo, cuantificación y codificación

- Muestreo: Consiste en tomar muestras (medidas) del valor de la señal  $n$  veces por segundo con lo que tendrán  $n$  niveles de tensión en un segundo.

Para un canal telefónico de voz es suficiente tomar 8000 muestras por segundo o lo que es lo mismo una muestra cada 125  $\mu$ seg. Esto es así porque, de acuerdo con el teorema de muestreo, si se toman muestras de una señal eléctrica continua a intervalos regulares y con una frecuencia doble a la frecuencia más elevada de la señal, dichas muestras contendrán toda la información necesaria para reconstruir la señal original.

Como en este caso tenemos una frecuencia de muestreo de 8 KHz. (periodo 125  $\mu$ seg), sería posible transmitir hasta 4 KHz., suficiente por tanto para el canal telefónico de voz, donde la frecuencia más alta transmitida es de 3,4 KHz.



- Cuantificación: En la cuantificación se asigna un determinado valor cuántico a cada uno de los niveles de tensión obtenidos en el muestreo. Como las muestras pueden tener un infinito número de valores en la gama de intensidad de la voz, gama que en un canal telefónico es de aproximadamente 60 dB, o lo que es lo mismo una relación de tensión de 1000:1, con el fin de simplificar el proceso, lo que se hace es aproximar al valor más cercano de una serie de valores predeterminados.
- Codificación: En la codificación, a cada nivel de cuantificación se le asigna un código binario distinto, con lo cual ya tenemos la señal codificada y lista para ser transmitida.

### **3.3. MULTIPLEXACIÓN DE SEÑALES DIGITALES.**

#### **3.3.1. Concepto de multiplexación**

Es la transmisión simultánea de varios canales de información separados en el mismo circuito de comunicación (también medio de transmisión) sin interferirse entre sí. Para la comunicación de voz, esto significa dos o más canales de voz en una sola portadora. Para los sistemas telefónicos, significa muchos canales en un sólo par de cables o en una sola línea de transmisión coaxial. Existen varios tipos de multiplexación, entre los más conocidos está por división de tiempo, por división de frecuencia.

#### **– Multiplexación por División en el Tiempo (TDM)**

Es la más utilizada en la actualidad, especialmente en los sistemas de transmisión digitales. En ella, el ancho de banda total del medio de transmisión es asignada a cada canal durante una fracción del tiempo total (intervalo de tiempo).

#### **– Multiplexación por División de Frecuencia (MDF o FDM).**

Del inglés Frequency Division Multiplexing, es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos. Mediante este procedimiento, el ancho de banda total del medio de transmisión es dividido en porciones, asignando cada una de estas fracciones a un canal.

### **3.4. REDES TELEFÓNICAS.**

Una red telefónica es la interconexión de medios de conmutación, con el fin de conectarse con otro usuario en la red. Por consiguiente una Red telefónica Local, está formada por un Centro de Conmutación (Central Local) y una Red de Cables (Planta Externa); esta última permite el enlace entre cada abonado y la central. Las líneas telefónicas que conectan al abonado con la central se les denomina Circuito de Abonado (Loop de Abonado), las que permiten la conexión entre centrales de las conoce como Troncales o Enlaces.

Los requerimientos que se exigen de la red es que debe proporcionar los medios y recursos para conectar y desconectar las comunicaciones entre abonados.

Dentro del sistema telefónico se puede encontrar con las siguientes partes que lo componen:

Línea de Abonado	: Línea que conecta al abonado con la central Local a la cual pertenece y es asignada permanentemente a un abonado específico.
Troncal	: Conexión entre centrales y cuyo uso es compartido en el tiempo, siendo su número función del tráfico efectivo.
Troncal Urbana	: Es la que conecta Centrales Locales entre sí.
Troncal Tándem	: Es la que conecta Centrales Locales con Centrales Tándem.
Troncal Urbana de Larga Distancia	: Es la que conecta una Central Local con el Primer Centro de Larga Distancia.
Troncal Interurbana	: Es la que conecta Centros de Conmutación de ciudades diferentes.
Red Local	: Es el conjunto de Líneas de Abonados conectadas a una misma Central Local y la Central Local a la cual pertenecen, (pueden haber varias redes locales en una misma ciudad; Área Multicentral).
Red Urbana	: Es el conjunto de Redes Locales y Troncales Urbanas perteneciente a una misma ciudad.
Red Interurbana	: Es la conexión entre centros de Conmutación que pertenecen a ciudades diferentes y Troncales Interurbanas que se emplean para comunicaciones de Larga Distancia (L.D.).
Concentrador	: Sistema conectado a una central Local para suministrar servicio telefónico a varios abonados, mediante un porcentaje de vías de conexión.

### **3.4.1. Funciones de la red telefónica.**

Dentro de la red se pueden distinguir 3 funciones principales:

- **Transmisión:** Se refiere específicamente a la transmisión del mensaje del abonado y de las señales de control. (Mensaje: cualquier información que un abonado desee enviar de un lugar a otro, Ej.: voz, datos, fax, TV, etc.).

- **Conmutación:** Comprende la identificación y conexión de los abonados a una trayectoria conmutación adecuada.
- **Señalización:** Se encarga del suministro e interpretación de señales de Control y de Supervisión, que se necesitan para realizar la operación de conmutación.

#### **3.4.1.1. Transmisión o transporte de datos en redes telefónicas.**

Los enlaces entre abonados y los centros locales son generalmente de cables de cobre, pero las centrales entre si se pueden comunicar de diversas formas, entre ellas cable coaxial, F.O. o microondas, e incluso cuando las distancias lo ameritan se utiliza enlaces satelitales. A medida de que aumenta el nivel jerárquico de las centrales los volúmenes de tráfico también se incrementan, por lo tanto las capacidades deben aumentar de la misma forma, caso contrario aunque el usuario tenga acceso a la red no podrá realizar la llamada por no establecer un enlace completo.

Esta función se resume, en la conversión de las señales acústicas en señales eléctricas, su transporte a través de los medios de comunicación, y la conversión de señales eléctricas nuevamente en acústicas para ser entregadas al destinatario.

#### **3.4.1.2. Conmutación telefónica.**

La red de conmutación es la encargada de estructurar una red que sea capaz de satisfacer las necesidades del servicio telefónico. La red estará constituida de centros de conmutación y enlaces troncales adecuados que permitan el establecimiento rápido y preciso; permitiendo el empleo eficiente de los recursos del sistema telefónico.

##### **3.4.1.2.1. Centrales.**

El centro de conmutación se puede clasificar en centro local (CL) el cual posee la conexión entre el usuario y la red (utiliza señalización DSS1); al conjunto de los elementos necesarios para unir una central local con sus abonados, se denomina “red de abonados” o “red local” de la central. Las restantes son llamadas centrales de tránsito se están.

El centro primario (o nacional primario CP) cuya función principal consiste en interconectar centrales locales, el área comprendida por las centrales locales que se enlazan recibe el nombre de área primaria, esta conexión se conoce como sección primaria y consta de un

grupo de circuitos individuales llamados enlaces, estos enlaces deben ser capaces de ser soporte de una comunicación. El centro primario debe también ser capaz de establecer llamadas ente diferentes centros locales, pueden tener abonados propios. Y por último, el centro primario debe comunicarse con un centro de su misma categoría y además puede conectarse con un centro secundario (CS).

El centro secundario (CS), en forma análoga a la anterior, conecta entre si centrales primarias, el conjunto que abarcan las centrales primarias se le denomina área secundaria, su función es la de cursar llamadas de tránsito, no tienen abonados propios.

Y por último el centro terciario (CT) o nodal, área terciaria es la abarcada por todas las áreas secundarias emplazadas con un centro terciario en común. La función de la central terciaria es unir centros secundarios cursando llamadas de tránsito entre estos, el centro terciario no tiene abonados propios.

La unión de entre centrales terciarias se le llama área cuaternaria.

Dentro de la red existen dos aspectos fundamentales estos son la disciplina del Encaminamiento Jerárquico y el principio del Encaminamiento Alternativo Automático.

La estratificación de las centrales se conoce como Encaminamiento Jerárquico y se encarga de agrupar y distribuir el tráfico mediante la interconexión, en forma jerárquica, de todos los centros de conmutación presentes en una conmutación interurbana. Cada una de ellas depende de una y de sólo una de categoría inmediatamente superior, estando las centrales de máxima categoría unidas entre sí. Es decir, a un Centro Primario se conectan Centros Locales, Centros Primario a Centros Secundarios y Centros Secundario se conecta a Centros Terciarios, etc. Además existen enlaces para cada nivel de conexión. Este es uno de los aspectos fundamentales que caracterizan a una red interurbana.

El segundo aspecto se conoce como Principio del Encaminamiento Alternativo Automático se encarga de enrutar el tráfico por las rutas directas, de no ser posible se disponen de otras rutas, alternas o secundarias, previamente establecidas. Cuando las rutas directas se encuentran copadas el tráfico de desborde o de sobrecarga, se le llama a todas las comunicaciones que no son cursadas por la ruta directa por estar estas ocupadas, utiliza rutas secundarias o finales.

El componente principal de una central de conmutación es el equipo conmutador, este se divide en dos partes:

**-Red de conexión:** incorpora al conjunto de órganos y circuitos, que componen el soporte físico de la comunicación. En otras palabras, es la red de conexión de la central en donde se conectan las líneas de abonado y los enlaces. Para finalmente entablar una llamada se sigue un llamado camino de conversación que es por donde pasará la conversación entre los abonados, este camino estará definido por una cantidad de puntos de cruce de la red de conexión. Cada punto de cruce es una conexión individual.

**-Unidad de control:** es quien determina los puntos de cruce, se basa en la información que recibe desde fuera de la central, básicamente la numeración, y la información que emane desde dentro de la central, disponibilidad de puntos de cruce.

#### **3.4.1.2.2. Funciones de los equipos de conmutación.**

**Interconexión,** es la capacidad de establecer la comunicación del abonado a través de la red de conexión, tanto en otras centrales como en la misma central.

**Control,** es almacenar y procesar la información para controlar la red de conexión

**Supervisión,** se realiza en la red de conexión para cursar la llamada en caso de presentarse la ocasión y en las llamadas ya establecidas.

**Señalización,** con el abonado con el fin de gestionar tanto una llamada saliente como una entrante y el término de la llamada. Con otros centros para realizar o recibir llamadas y realizar las acciones adecuada para lograr la conexión.

**Interfase,** proporcionar las señales de acuerdo al medio de transmisión saliente sin importar el formato de llegada.

**Sincronización,** consiste en conseguir que todas las centrales trabajen con una misma señal de reloj básica.

**Temporización,** generación de varias señales de tiempo de referencia, a partir de la señal de reloj básica, para que el sistema de conmutación funcione en forma armónica.

**Conmutación de paquetes,** esto es necesario cuando son redes digitales de servicios integrados, para ello debe admitir la conexión de terminales de datos.

### 3.4.1.2.3. Clasificación de los sistemas de conmutación, según su tecnología.

**Sistemas electromecánicos** Red de conexión y unidad de control electromecánicas

**Sistemas semielectrónicos,** Red de conexión electromecánica y unidad de control electrónica)

**Sistemas electrónicos,** Red de conexión y unidad de control electrónicas

### 3.4.1.3. Señalización telefónica

Señalización se define como: “el conjunto de informaciones que deberán intercambiar los diferentes elementos de una red de telecomunicación para establecer, supervisar, mantener y liberar una conexión”. Es decir, es la forma que la central y el abonado pueden ponerse de acuerdo para establecer la comunicación y la compañía puede rarificar.

#### 3.4.1.3.1. Funciones de Señalización:

Supervisión

Control (Forward)

Tomar

Retener

Liberar

Estado (Backward)

Desocupado

Ocupado

Desconectar

Dirección

Estación

Decádica

DTMF

Digital

Enrutamiento

Canal

Troncal

Auditiva/Visual

Alerta

Timbrado

Aviso descolgado

Progreso

Tono de marcar

Tono de ocupado

#### **3.4.1.3.2. La señalización telefónica se agrupar en forma general en:**

- Señalización de línea: La que se da entre centrales, se utiliza para monitorear la línea antes durante y después de establecerse una llamada.
- Señalización de usuario: La que se da entre el usuario y la central, se le conoce también como “Señalización de Abonado”
- Señalización de registro: La que se da dentro de la central, conocida como “Señalización Interna”. Para transmitir señales numéricas, esta se almacena en los registros por ser transmitida una sola vez.

Y en cada una de estas existen señales de supervisión, estas señales son las encargadas de controlar el proceso de conmutación. En ella se incluyen señales hacia delante, que son las que se dirigen hacia donde progresa el proceso de conmutación, se les conoce como señales de control. Y las señales hacia atrás, conocidas como señales pilotos, progresan en sentido inverso progresan en sentido inverso, por ejemplo las señales de respuesta.

#### **3.4.2. Pasos de establecimiento de una llamada.**

Un ejemplo cotidiano, en el cual es posible apreciar la utilización de la señalización es en el establecimiento de la llamada, también es distinguible el sentido.

1. Cuando un abonado levanta el auricular de su aparato telefónico, la central lo identifica y le envía una "invitación a marcar".
2. La central espera a recibir el número seleccionado, para, a su vez, escoger una ruta del usuario fuente al destino.
3. Si la línea de abonado del usuario destino está ocupada, la central lo detecta y le envía al usuario fuente una señal ("tono de ocupado").

4. Si la línea del usuario destino no está ocupada, la central a la cual está conectado genera una señal para indicarle al destino la presencia de una llamada.
5. Al contestar la llamada el usuario destino, se suspende la generación de dichas señales.
6. Al concluir la conversación, las centrales deben desconectar la llamada y poner los canales a la disposición de otro usuario, a partir de ese momento.
7. Al concluir la llamada se debe contabilizar su costo para su facturación, para ser cobrado al usuario que la inició.

Existen dos métodos de señalización por canal asociado, o por canal común.

### **3.4.3. Canal asociado.**

Por canal asociado, la información se transmite por el mismo canal por el que se está llevando a cabo la comunicación (por ejemplo ISDN).

En los sistemas digitales, la señalización asociada al canal se utiliza el intervalo de tiempo (o Time Slot) 16 para transmitir la información de señalización para dos canales específicos en cada trama, son necesarios 15 intervalos para completar la señalización de los 30 canales.

### **3.4.4. Canal común.**

Por canal común, la información de señalización es transportada por un canal único y colectivo (por ejemplo R2, SS7).

#### **3.4.4.1. Principales ventajas de la señalización por canal común.**

Las ventajas principales de la señalización por canal común han sido reconocidas desde su proyecto el origen de son:

Se ahorra al suprimirse los terminales de señalización, parcialmente contrarrestado por el sobre costo del software de gestión. Una estructura centralizada no es rentable en rutas de bajo tráfico, caso contrario ocurre con rutas de alto tráfico en donde se justifica plenamente. Para combatir la mala rentabilidad se opta por una red de señalización híbrida o modo cuasi-asociado.

Se aumenta el vocabulario de señalización lo que permite una mayor cantidad de servicios y aplicaciones.

Ganancia de velocidad de establecimiento de llamadas

Aumento de la fiabilidad mediante el empleo de métodos más eficaces de detección y corrección de errores.

La eliminación de los enlaces de señalización por canal asociado, hace que desaparezca la orientación de los circuitos (entre el circuito de salida y el de llegada).

Las ventajas solamente para el sistema N° 7:

- Permite un canal digital de 64 Kbps.
- Flexibilidad de la composición de los mensajes, debido al uso de DIC con mensajes de longitud variable.
- Accesibilidad total, el etiquetado de los mensajes permite un intercambio fluido sin restricción entre dos puntos de señalización en cualquier red.
- La SS7 fue concebida para constituir una red de señalización de multiservicio.

#### **3.4.4.2. Sistema de señalización por canal común R2.**

La versión digital del sistema de señalización de línea R2, requiere de cuatro canales de señalización (Intervalo de tiempo 16 de una trama de 32), para lo cual se utilizan cuatro bits por circuito telefónico en cada sentido de transmisión.

El sistema de señalización de línea R2, se emplea en los siguientes casos:

- a) En combinación con la señalización entre registradores multifrecuencia R2, o
- b) En la explotación de circuitos unidireccionales o bidireccionales, o
- c) En circuitos con sistemas de transmisión PCM de 30+2 canales a la velocidad de 2048 Kbit/s, de acuerdo a las recomendaciones G. 732 y G.734 del CCITT.

El sistema se efectúa de extremo a extremo, por método de secuencia de obligado (MFC), con superposición de marcación.

### **3.5. SISTEMA DE SEÑALIZACIÓN POR CANAL COMÚN N° 7.**

#### **3.5.1. Introducción.**

El sistema de señalización por canal común N° 7 proporciona una normalización a nivel mundial útil para cualquier aplicación.

Sin embargo, debe cumplir ciertos objetivos. Estas eran funcionar en redes digitales que funcionen con Centrales SPC; que sean flexibles para afrontar requerimientos de transmisión de información presente y futuros, en control, señalización, gestión y mantenimiento; y ofrezca

medidas de seguridad aceptables para la transferencia de información correlativa, sin pérdidas y que no se dupliquen.

Este sistema también cubre las exigencias de señalización de control de llamadas para servicios, de telecomunicaciones y de transmisión de datos. Está optimizado para enlaces digitales de 64 Kbps, sin embargo también lo puede hacer en canales analógicos de menor velocidad.

La característica fundamental de SS7 es que se trata de una señalización por canal común, en este método se transfieren un canal, mediante mensajes identificables, la información relativa a varios circuitos y otros tipos información relativa a la red telefónica.

### **3.5.2. Definición.**

El SS7 está dividido en dos partes funcionales. La primera, la parte de transferencia de mensajes (MPT), realizara todas la funciones requeridas para el transporte de los datos de señalización, y en partes de usuario (UP) o partes de aplicación (AP), que son diferentes según la aplicación que se le asigne.

### **3.5.3. MODOS DE SEÑALIZACIÓN.**

Es la relación o la asociación entre el trayecto seguido por un mensaje de señalización y la relación a la que se refiere el mensaje.

Se puede clasificar de acuerdo a la relación entre la ruta de señalización y la ruta de datos en tres.

**MODO ASOCIADO:** los mensajes de señalización o hacen el mismo recorrido que el canal de comunicaciones que los datos, asociado al canal de datos uniendo los puntos de origen-destino.

**MODO NO-ASOCIADO:** o disociándolos mensajes de señalización transferido por rutas de señalización que no son el origen y el destino.

**MODO CUASI-ASOCIADO:** cuando el modo no asociado está predeterminado y fijo para diferentes relaciones de señalización. El SS7 es el único sistema especificado para trabajar en forma asociado y cuasi-asociada.

La función de punto de transferencia de señalización en algunos nodos aparece producto del Modo Cuasi asociado que se resume en lo siguiente :

1.- Una central telefónica que posee diferentes vías de interconexión con diferentes centrales, sus relaciones de señalización se harán con un menor número de rutas de señalización. Así es como, una misma ruta concentrara el tráfico de varias relaciones de señalización esto permite una economía, en enlaces de señalización, así como también una mayor flexibilidad en el encaminamiento de los mensajes de señalización.

2.- Al tener unos pocos enlaces de señalización se concentra en ellos una gran cantidad de circuitos de conversación, por ello en rutas de alto tráfico es necesario la disposición de rutas alternativas para una misma relación de señalización.

3.- Debido a su estructura y objetivos de multiservicios del SS7, un mismo punto de señalización con diferentes "UPs" tendrá diferentes relaciones de señalización con otros puntos de señalización, para esto es necesario que puntos intermedios funcionen como puntos de transferencias de mensaje, para permitir todas las relaciones posibles con otras UPs.

#### **3.5.4. Arquitectura.**

Con el objeto de independizar el transporte de la información de señalización del tratamiento, por software, de la misma se divide en dos:

La parte de transferencia de mensaje (MTP): la cual garantiza el transporte fiable de la información de señalización.

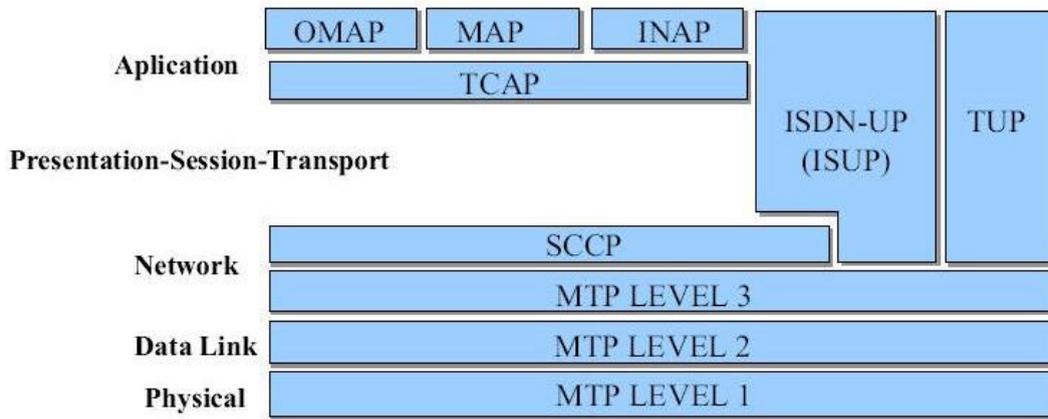
Las diferentes partes de usuario (UP) y/o aplicaciones (AP): específica de usuario-aplicación y encargada de la comunicación y tratamiento de los mensajes de señalización.

Cada usuario/aplicación, del SS7, se asimila como un software que se usa para comunicarse con otro semejante utiliza las facilidades de transferencia de mensajes.

Inicialmente la SS7 se basa en requisitos necesarios para el control de telefonía relacionados con circuitos. Con estos objetivos como premisa se especifico los niveles funcionales que son cuatro. La MTP en donde se contienen los tres primeros niveles y los UPs que incluye el nivel 4.

Con las nuevas evoluciones en el área de la comunicación también han aparecidos nuevos circuitos, por ello fue necesario que el SS7 también evolucionara. Se necesito adaptar el SS7 del CCITT a algunos elementos del modelo OSI (Open Sistem Connection). Esto se refleja en la conexión de los niveles funcionales y las capas del modelo OSI, por ejemplo, la SCCP es una

parte de usuario de nivel 4 en MTP, pero también, proporciona un servicio de capa 3 en la red OSI.



Torre de protocolos SS7

### 3.5.5. Capas del modelo S7.

#### 3.5.5.1. Parte de transferencia de mensajes (MPT).

MTP representa un sistema de transferencia de mensajes, que permite transmitir información de señalización a través de la red hacia el punto de destino. MTP se compone de tres niveles:

- Nivel 1: enlace de datos de señalización;
- Nivel 2: enlace de señalización;
- Nivel 3: red de señalización.

#### 3.5.5.2. Funciones del enlace de datos de señalización datos de señalización (nivel 1)

Esta capa está definida en la ITU-T Q.702, en el cual se define las características físicas y eléctricas de los enlaces y de las señales transmitidas.

Su descripción sería la de un trayecto de transmisión bidireccional compuesta de dos canales de datos para transmisión full dúplex. La velocidad típica es  $N \times 64$  Kbps pero puede adaptarse a velocidades inferiores como 64 Kbps para el acceso al usuario ISDN. La velocidad mínima aceptada para la transferencia de señalización relacionada con el control de llamadas es de 4800 Kbps.

Se puede poner de ejemplo, el canal de 64 puede derivarse de una red de canales digitales a 2 Mbps con estructuras de trama según la ITU-T G.704. De esta forma se puede tener una interfaz de entrada-salida del tipo analógica ITU-T V.11 o del tipo digital ITU-T G.703 codireccional o contradireccional. En tales casos se respeta los códigos, niveles e impedancias de dichas interfaces. En un sistema de 2 Mbps el canal de señalización de 64 Kbps es un canal de datos y por ello puede ocupar el intervalo de tiempo TS:16 o cualquiera otro. Es más, como un solo canal de señalización de 64 Kbps es un canal de datos, y por ello puede ocupar el intervalo de tiempo TS:16 o cualquier otro. Es mas, con un solo canal de 64 Kbps puede llenar el dialogo de señalización de cerca de 1300 canales telefónicos. Muchos sistemas de 2 Mbps tendrán disponibles el canal 16 para información útil pasando a ser un sistema de 31 canales. Lo objetivos de calidad y disponibilidad de deslizamiento y fluctuaciones de fase para este canal están de acuerdo con el ITU-T G.821, G.811 y G.823.

<b>Modelo de capas para el Sistema de Señalización SS7.</b>	
<b>MTP-1</b>	<b>Capa 1.</b> Tiene las funciones de conexión física entre módulos a interconectar.
<b>MTP-2</b>	<b>Capa 2.</b> Se ocupa del alineamiento de paquete mediante banderas ( <i>Flag</i> ) al inicio y final. Permite la detección de errores mediante un código CRC-16. Realiza el proceso de numeración secuencial de mensajes e indicación de retransmisión. Efectúa la confirmación o rechazo del mensaje para la retransmisión automática en mensajes con errores. Los paquetes son numerados en forma secuencial con módulo-7. Indica la longitud total del mensaje transmitido.
<b>MTP-3</b>	<b>Capa 3.</b> Posee una dirección de punto de acceso al servicio <b>SAP</b> en la información de servicio <b>SIO</b> . SAP permite identificar a la capa superior SCCP sobre el protocolo MTP3. En la red PSTN se dispone de las direcciones de procesador CPU de origen y destino (14 bits de dirección). Por otro lado identifica el enlace de señalización utilizado cuando existe más de uno. Realiza las funciones de Routing dentro de la red de señalización SS7.
<b>UP</b>	<b>Capa 7.</b> Parte de usuario. Asegura la generación y tratamiento del mensaje de señalización. Contiene: <ul style="list-style-type: none"> <li>-Usuario de telefonía <b>TUP</b>.</li> <li>-Usuario de datos <b>DUP</b>.</li> <li>-Usuario de red ISDN <b>ISUP</b>. Esta es la capa utilizada para enlaces internacionales de telefonía o de datos.</li> </ul>
<b>ISUP</b>	<b>Capa 7.</b> Este protocolo sirve para los mensajes de señalización de usuario ISDN. Algunos tipos de mensajes son: <b>IAM</b> . Contiene la

	<p>información inicial de llamada para el encaminamiento. <b>SAM.</b> Transporta las cifras no enviadas en el mensaje IAM. <b>ACM.</b> Indica que se ha obtenido en acceso al destino. <b>ANM.</b> Indica que el usuario llamado ha respondido. <b>BLO.</b> Permite el bloqueo del canal útil. <b>UBL.</b> Desbloquea el canal útil. <b>REL</b> (<i>Release Message</i>). Permite iniciar la liberación del canal. <b>RLC.</b> Informa que la liberación ha sido completada.</p>
<b>SCCP</b>	<p><b>Capa 3.</b> Efectúa funciones de direccionamiento adicionales a MTP3, especial para sistemas celulares. La combinación de SCCP y el MTP3 se denomina parte de servicio de red <b>NSP</b>. SCCP puede brindar servicios con y sin conexión. En telefonía celular se trata de un servicio sin conexión y la capa superior es TCAP. En el caso de servicio con conexión la capa superior es ISUP. El caso con conexión se aplica para consulta de base de datos (ejemplo, tarjeta de crédito).</p> <p>SCCP entrega una dirección (adicional a 14 bits de MTP3) que se denominada <b>SSN</b> (<i>SubSystem Number</i>). Permite direccionar al usuario del protocolo SCCP en el nodo. Se trata de 4 direcciones: al registro de localización VLR y HLR, la red de conmutación MSC, el centro de autenticación EIR. El campo de direcciones de SCCP posee la dirección de origen y destino y la selección de ruta de señalización. Dispone de 16 tipos de mensajes: requerimiento de conexión, confirmación de conexión, conexión negada, formato de datos, control de flujo, datos urgentes (puentea el control de flujo), requerimiento de reset y confirmación de reset, etc.</p>
<b>TCAP</b>	<p><b>Capa 7.</b> Facilita la transferencia de mensajes en tiempo real entre MSC, HLR y VLR. Se aplica también para enlaces con O&amp;M. En tarjetas de crédito permite verificar la autenticidad y movimientos de cuenta. Realiza el control de diálogo con el terminal remoto. Es un servicio de transporte. La información contiene: tipo de mensaje (unidireccional, inicio, final, intermedio, aborto); longitud del mensaje (número de bytes total); identificador de origen y destino de transacción; tipo de componente (retorno de resultado, reporte de error y de reject) y contenido de información (código de operación, de error, de problema, parámetros, etc.).</p>
<b>MAP</b>	<p><b>Capa 7.</b> ETSI ha especificado MAP para transferencia de información que no es de circuitos de usuario. Se utiliza para interconectar los siguientes elementos entre sí: HLR (<i>Home Location Register</i>), VLR (<i>Visitor LR</i>), MSC (<i>Mobile Switching Center</i>), EIR (<i>Equipment ID Register</i>), además permite conectar a varios MSC de distinto proveedor de servicio SP (<i>Service Provider</i>). Permite las operaciones de: Actualización de localización; Roaming; Handover; autenticación; información de llamada entrante; información de servicio de subscriber; identificación de equipos móviles; carga de información a los registros; etc.</p>

Las características más importantes de este nivel son entonces los que se refiere al tipo de soporte. Los intervalos de tipo PCM de 2048 Kbps conectados directamente a las red de conexión del conmutador, todo los canales incluido el 16. Para el soporte analógico se utiliza adaptadores en donde se inyecta las señales digitales en intervalos PCM de 64 Kbps.

### 3.5.5.3. Funciones de enlace de señalización (MTP 2), capa 2.

Esta capa proporciona las funciones para disponer de un enlace de señalización fiable para la transferencia de Sus entre nodos adyacentes (conectados directamente). A esta capa se le conoce también como Campo de Información de Señalización desde la capa 3 y arma una trama denominada Unidad de Mensaje de Señalización. Estas unidades son de longitud variable y contienen información de señalización, información de control, información de control de transferencia, para asegurar el funcionamiento adecuado del enlace de señalización. En el modelo OSI se define en esta capa los procedimientos para establecer, mantener y liberar la conexión.

Las funciones básicas de esta capa son:

- Alineamiento del enlace.
- Delimitación y alineamiento de Sus
- Detección y corrección de errores.
- Monitoreo de errores
- Control de flujo.
- Indicación de congestión al nivel 3
- Indicación de interrupción del procesador y del enlace fuera de servicio.

El procedimiento de intercambio de mensaje en el enlace que se utiliza es el procedimiento DIC, al igual que en el modelo OSI.

El DIC es un protocolo de nivel enlace full-duplex. Su estructura es única y los campos de información son los siguientes:

**Flag** (bandera): 8 bit, indica inicio y final de trama su secuencia es 01111110.

**Dirección:** 8 bit, señala la estación de origen.

**Control:** 8 bit, identifica el tipo y la función de la trama.

**Sin enumerar:** se utiliza para enviar comandos y sus respuestas.

**De información:** datos.

**De supervisión:** confirmación o inhibición de la transmisión.

**Información:** longitud variable, datos.

**Secuencia de verificación de trama:** 16 bit, detecta errores de transmisión.

### 3.5.5.3.1. Unidad de señalización (SU)

La señalización y otra información que vienen de una UP se transfieren por lo SU. Existen 3 tipos que se distinguen por medio del indicador de longitud, estos son:

Unidades de señalización de mensaje.

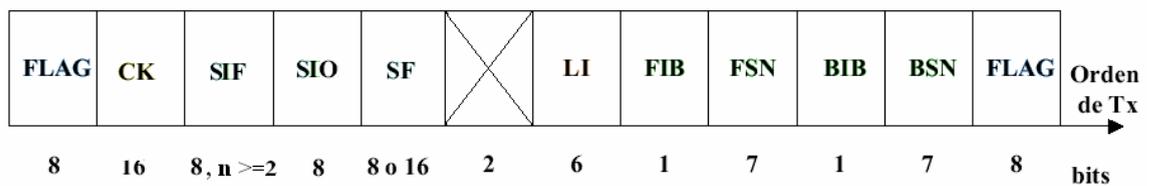
Unidades de señalización de estado de enlace (LSSUs).

Unidades de señalización de relleno (FISUs).

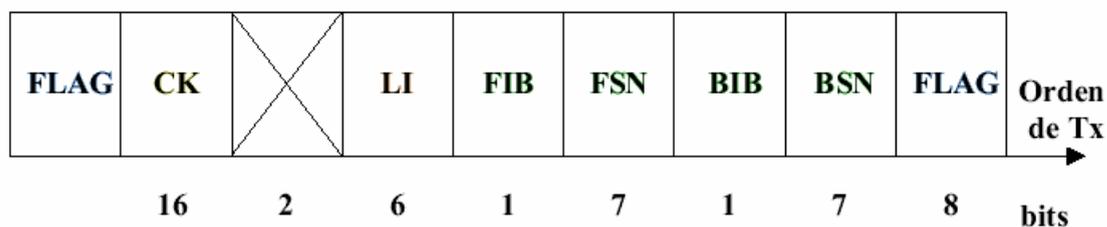
En caso de error solo la primera es retransmitida.

**FISUs** (Fill-In SUs) o unidad de relleno, se transmite en el SDL (Signaling Data Link, enlace de datos de señalización), siempre que no hay otra información para transmitir. Lleva información de alineación, control de flujos y de corrección de errores.

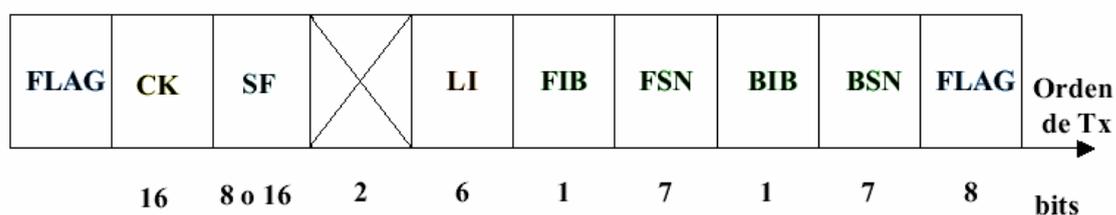
**LSSUs** (Link Status SUs) o unidad de estado, su unidad de estado de enlace de señalización se utiliza para señalar, el estado actual y los cambios de estado del enlace, lleva información de las FISU para alineación control de flujo y control y corrección de errores de enlace.



Formato básico de una unidad de señalización de mensaje (MSU)



Formato de señalización de relleno (FISUs)



Formato de señalización del estado de enlace (LSSUs)

En donde:

**FLAG:** Bandera, indica el comienzo/final de la unidad de señalización. El código es 01111110.

**CK:** Bit de Chequeo, o bit de control para la detección de errores.

**SF:** Campo de Estado, el identificador de longitud determina la longitud del campo de estado, si es 1 el campo de estado se compone de un byte y si es 2 de 2 bytes

**LI:** indicador de longitud, 0 FISU, 1 ó 2 LSSU, 3 ó más MSU

**FIB:** Bit indicador directo, se utiliza en el método básico de corrección de errores.

**FSN:** Número secuencial directo (hacia adelante),

**BSN:** Número secuencial inverso, indica un acuse de recibo.

**BIB:** Bit indicador hacia atrás, se utiliza en el método básico de corrección de errores.

**n:** Número de bytes en el SIF,

**SIF:** Campo de información de señalización, comprende los valores de 2 y 272 bytes que permiten a una unidad de señalización alojar un bloque de 256 bytes de información más una etiqueta e información adicional.

**SIO:** Byte de información de servicios, está dividido en Indicador de Servicio y Campo de subservicio. El primero asocia la información con la UP

### 3.5.5.3.2. Detección de errores.

Los bits contenidos al final de cada unidad de señalización son los encargados de la función de detección de errores. Se utilizan dos métodos de detección y corrección de errores.

El método básico, es un método de secuencia no obligada en el que la corrección se realiza por retransmisión.

Y el método de corrección de errores por retransmisión cíclica preventiva, es un método de corrección de errores hacia delante de secuencia no obligada, en el que se necesita acuses de recibo positivos para apoyar la corrección de errores acalla adelante.

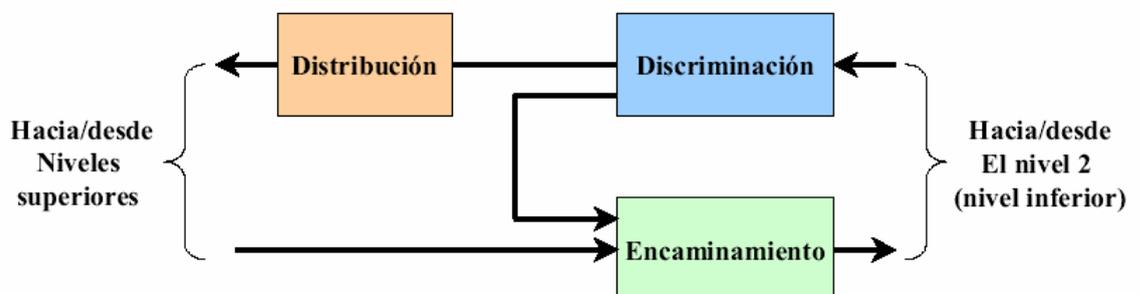
### 3.5.5.4. Funciones de la red de señalización (NIVEL 3).

En el nivel 3 se define las funciones de transferencia y los procedimientos de operación de los distintos enlaces de comunicación. Permite que nodos (STP) no adyacentes se puedan enviar MSUs incorporando información de encaminamiento (routing). Incorpora la gestión de red, necesaria para enfrentar fallos y proporciona además la fiabilidad del SS7.

### 3.5.5.5. Tratamiento de mensajes de señalización

Comprende las funciones de encaminamiento, discriminación y distribución, que se efectúa en cada punto de la red de señalización.

El encaminamiento se refiere los mensajes, que se van a enviar. La discriminar de los mensajes recibidos. La distribución a la funciones de dirigir a UP que corresponde.



El tratamiento del mensaje de señalización garantiza que los mensajes lleguen a su destino. Para ello se utiliza una etiqueta que identifica explícitamente los puntos origen-destino.

La parte de la etiqueta utilizada para el tratamiento de mensaje de señalización, por la parte de transferencia de mensaje se le denomina etiqueta de encaminamiento.

La etiqueta normalizada (Q.704) tiene una longitud de 32 bits y se coloca al comienzo del campo de información de señalización.

Se utiliza un plan de numeración para la codificación de los puntos de señalización  
El campo SLS se utiliza para compartir carga.

### **3.5.6. Encaminamiento.**

Es el proceso en el cual se selecciona al enlace de señalización por donde ha de enviar cada mensaje. Por esto se analiza la etiqueta de encaminamiento.

El encaminamiento depende del destino pero puede ser modificado por el campo de comparación de carga que permite distribuirlo por otro enlace.

Ruta de mensaje: es el conjunto sucesivos de trayectos de los enlaces de señalización que puede utilizarse para la transmitir el mensaje desde el punto de origen al punto de destino.

Ruta de señalización: es el conjunto de enlaces y puntos de señalización origen-destino posibles de utilizar.

El mensaje de señalización sigue una ruta predeterminada y fija, pero cuando existen fallas en los enlaces de la ruta esta es modificada por la función de gestión de tráfico de la capa 3.

### **3.5.7. Comparación de carga.**

Cada punto de señalización tendrá la información de encaminamiento que le permita elegir el enlace por el cual enviara el mensaje, para esto debe ponderar entre el código de destino, el campo de selección de enlace y si es necesario el indicador de servicio o indicador nacional. Esto podría indicar a más de un enlace, por eso que finalmente quedara en manos del campo de selección del enlace de señalización la elección de la ruta a seguir.

Existen dos casos de comparación de carga:

1.- Entre enlaces que pertenecen a un mismo conjunto de enlaces, en este caso será compartido entre los enlaces que pertenezcan al conjunto.

2.- Entre enlaces que no pertenecen a un mismo conjunto de enlaces, el tráfico será compartido bajo el criterio del campo de selección en el conjunto de enlaces de señalización que no pertenezcan al mismo conjunto de enlaces de señalización.

El resultado es que todos los mensajes que tengan la misma etiqueta de encaminamiento tomarán las mismas rutas y puntos de transferencia.

### **3.5.8. Gestión de la red de señalización.**

La función de gestión de red es proporcionar los procedimientos para mantener y reestablecer el servicio de señalización y estas funciones se dividen en

#### **3.5.8.1. Gestión del tráfico de señalización.**

El cual controla el encaminamiento de los mensajes, controla la transferencia del tráfico de señalización junto con modificar los encaminamientos, y por último el control de flujo.

#### **3.5.8.2. Gestión de enlaces de señalización**

Controla los enlaces conectados localmente, además da información sobre la disponibilidad de enlaces a la función de tráfico de señalización. Recibe el estado de los enlaces de señalización (nivel 2) y puede realizar acciones al nivel 2, como alineación inicial de un enlace fuera de servicio.

#### **3.5.8.3. Gestión de la ruta de señalización**

Es usada solamente en el modo cuasi-asociado de señalización y su función es transmitir información sobre los cambios de disponibilidad de las rutas de señalización en esta red, para que otros puntos de red sean el estado del enlace.

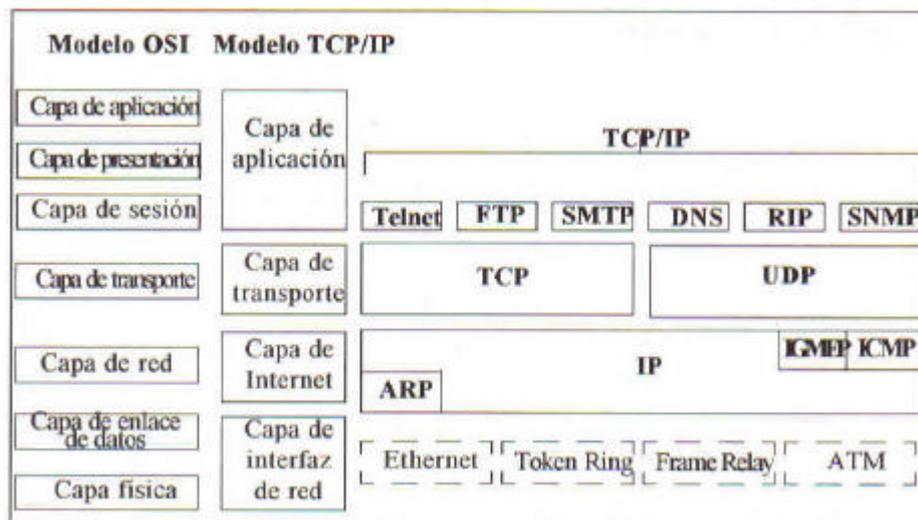
## 4. CAPÍTULO IV. PROTOCOLOS TCP/IP.

### 4.1. INTRODUCCIÓN.

Por todos conocidos TCP/IP se le asocia comúnmente a un solo protocolo, la verdad es que son varios; TCP/IP ya dos protocolos TCP (Protocolo de control de transmisión, en inglés) e IP (Protocolo de Internet, por sus siglas en inglés) este último el más difundido tanto en Internet como en redes Unix.

Todo comenzó gracias a las investigaciones del gobierno de los Estados Unidos, relacionadas con tecnologías de comunicación. Una de esas líneas investigativas fue llamada ARPANET en la cual se desarrollaron un gran número de protocolos que fueron agrupadas y pasaron a llamarse TCP/IP. En 1983 nace INTERNET y con ello llega la masificación de estos protocolos. Detrás de la masificación existían razones por la cual se prefirió, entre ellas están: independencia del fabricante, soporta múltiples tecnologías, puede funcionar en máquinas de cualquier tamaño.

El modelo de referencia OSI es representado por siete capas, en cambio la arquitectura TCP/IP solo figura cuatro capas.



A continuación se entrega una breve descripción de las capas del modelo TCP/IP.

En la Capa de Aplicación, se definen los protocolos de aplicación TCP/IP, además proporciona interfaces entre los programas de aplicación y los servicios de la capa de transporte.

Algunos de los protocolos y servicios son HTTP, Telnet, FTP, TFPT, SNMP, DNS, SMTP, VoIP, etc.

En la Capa de Transporte se proporciona sesiones de comunicación entre maquinas host. Define el nivel de servicio (primera capa o capas inferiores) y el estado de la conexión (con o sin conexión) utilizados al transferir datos. Entre los protocolos que se utilizan en este nivel se cuentan UDP y TCP.

En la Capa de Internet los datos se empaquetan en datagramas IP. Estos contienen la información de origen y de destino utilizada para transmitir datos entre los host a través de la red. Esta capa aplica el enrutamiento IP. Los protocolos que se emplea acá se incluyen IP, ICMP, IGMP y ARP (RARP).

Capa de Interfaz de red es la capa destinada a los detalles físicos relacionados con la transmisión de datos por la red. Define tanto el medio de transmisión entre los hardware conectados; a saber: FO, UTP, STP, coaxial, etc. También define los estándares tales como Ethernet, Token Ring, FDDI, X.25, Frame Relay, IEEE 802.2, etc., que corresponde los protocolos de acceso al medio.

## **4.2. CAPA DE INTERFAZ DE RED**

### **PROCOLOS Y TOPOLOGÍAS DE ACCESO AL MEDIO.**

En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Entre los más comunes se cuentan CSMA/CD, Token Bus, Token Ring y FDDI.

#### **4.2.1. CSMA/CD, IEEE 802.3.**

Esta norma está diseñada para funcionar sobre una topología de bus con acceso aleatorio. CSMA, significa Carrier Sense Media Access, o Acceso al Medio por Detección de Portadora, es un algoritmo que permite colocar las trama s en la señal física de la portadora. CD, significa Collision Detection (Detección de Colisión), permite percibir cuando existió colisión con otra trama colocada en la red en el mismo instante por otra estación. Optar tratar de evitar una nueva colisión se activa un algoritmo de retardo aleatorio en la colocación de la trama.

La implementación comercial de este protocolo se conoce como Ethernet.

La velocidad de transmisión de esta implementación es de 10 Mbps. La frecuencia de portadora es de 25 Mhz

Existen 3 sub-estándares de Ethernet. El primero llamado también llamada 10 Base X, en donde X puede ser:

- 2 Ethernet con coaxial delgado.
- 5 Ethernet con coaxial grueso.
- T Ethernet con par trenzado de cuatro hilos.
- F Ethernet con Fibra Óptica.
- S Ethernet con Fibra Óptica.

Y también 100 Base X, en donde X representa a:

- T Ethernet con par trenzado ocho hilos.
- F Ethernet con Fibra Óptica.
- S Ethernet con Fibra Óptica.

Y el tercero 1000 Base X, donde X corresponde:

- F Ethernet con Fibra Óptica.
- S Ethernet con Fibra Óptica.

#### **4.2.2. Token Bus, IEEE 802.4.**

Conocida comercialmente como ARC NET, corresponde a un protocolo de acceso al medio compartido, basado en la posesión del Token, símbolo de autoridad o derecho al acceso transferido entre las estaciones.

La transferencia del Tokenes determinística o preestablecida.

Sus características más relevantes son:

- No existen colisiones.
- Es más lento (20 Mbps).
- Es más confiable y más eficiente.
- No es full duplex.
- Existen prioridades.
- Es de fácil reconfiguración.
- Es complicada la implementación del controlador.

### **4.2.3. Token Ring, IEEE 802.3.**

Protocolo de acceso al medio con paso de testigo que funciona sobre una topología de anillo. Es totalmente determinística, es síncrona, y el Token se desplaza en sentido anti-horario.

### **4.2.4. FDDI.**

Fiber Distributed Data Interface, este estándar pertenece a la ANSI. Dentro de sus cualidades de conectar ETC D mediante FO están:

Los computadores funcionan a velocidades muy altas.

Ayuda a resolver los problemas de rapidez de computador con las unidades de disco.

Proporciona un mayor ancho de banda, ideal para voz digitalizada, video conferencia, etc., a tiempo real.

Es síncrona y asíncrona a la vez.

#### **4.2.4.1. Especificaciones.**

Cada canal de FO funciona a 100 Mb/s.

Cada anillo puede soportar hasta 1000 nodos y estos nodos pueden estar separados por no más de 2 Km. y la circunferencia máxima del anillo es de hasta 200 Km.

FDDI consta de 2 anillos concéntricos en donde los datos viajan en forma opuesta. La tasa de transmisión es 200 Mb/s, con 100 Mb/s por cada canal.

Dentro de esta norma existe una clasificación de acuerdo a la cantidad de anillos a que sean conectados los dispositivos. Los dispositivos denominados A, se clasifican como los más críticos dentro del sistema estos son conectados tanto al anillo interior como al exterior. En cambio los dispositivos B se conectan solamente a un anillo. Esto permite dar prioridad a una estación de trabajo de acuerdo a su importancia y a costos.

Existe un dispositivo llamado concentrador de cableado; este dispositivo se utiliza para conectar estaciones, realizar reconfiguraciones, ayuda a localizar y aislar problemas y permite adaptar a otros medio de conexión (coaxial, par de cobre).

### **4.2.5. IEEE 802.11x**

Protocolos de acceso al medio para redes locales con soporte físico inalámbrico.

Existen subespecificaciones.

11a Blue Tooth (5 GHz) spread spectrum 50 mW.

11b Wi Fi (2,4 GHz) spread spectrum 100 mW.

Ambas están basadas en el protocolo CMDA/CD, aun cuando se está utilizando el protocolo CDMA/AC (AC, Avoidance Collitions).

Las velocidades de transmisión alcanzadas son entre los 1 a 54 Mbps.

Ambos protocolo son adaptativos, es decir, se acomodan a condiciones adversas de funcionamiento bajando su velocidad de transmisión.

### 4.3. CAPA DE INTERNET.

#### 4.3.1. Protocolo IP.

El protocolo IP forma parte del modelo OSI y es fundamental en el modelo TCP/IP, el debe velar por el direccionamiento del datagrama de transmisión y administración de esos datagramas fragmentados.

Sus características son las siguientes:

No orientado a la conexión; permite, sin establecer una llamada previa, el intercambio de datos entre dos computadores.

Es un protocolo tipo datagrama, unidades de transmisión, no proporciona elementos de corrección de errores ni mecanismos de control de flujo.

Utiliza fragmentación, es la operación en donde una PDU es dividida en segmentos más pequeños.

##### 4.3.1.1. Estructura de la dirección IP.

Las redes TCP/IP identifican a los computadores y a las redes que se conectan mediante direcciones de 32 bits. Su formato es **DIRECCIÓN IP = DIRECCIÓN DE RED + DIRECCIÓN DEL PC**

La dirección IP no individualiza a un PC sino que identifica la conexión de dicho aparato a una red. Por eso cuando un computador se cambia de red se debe reasignar su identificación IP.

Las direcciones IP se clasifican por sus formatos en:

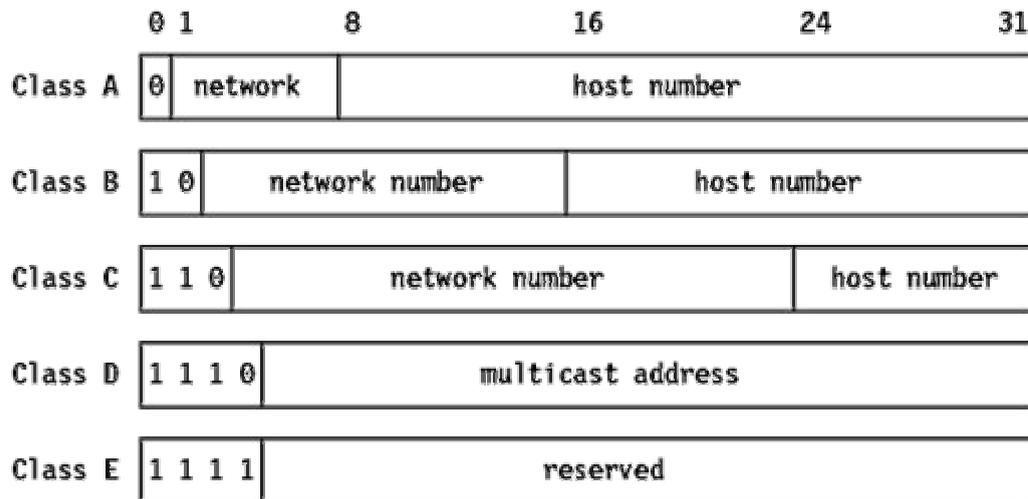
**Clase A:** grandes redes, identificador de redes de 7 bits (127 redes) y el identificador de computador 24 bits ( $2^{24}$  computadores).

**Clase B:** redes de tamaño mediano, identificador de red 14 bits ( $2^{14}$  redes) y el identificador de computador 16 bits ( $2^{16}$ ).

**Clase C:** redes pequeñas, identificador de red 8 bits (256) y el identificador de computador 21 bits.

**Clase D:** multidifusión, dirección de multidifusión 28 bits.

**Clase E:** reservado uso futuro.



#### 4.3.1.2. Datagrama IP.

Consta de los siguientes campos:

VERS	HLEN	Tipo de servicio	Longitud total	
Identificación			Flag	Desplaz de fragmento
TTL		Protocolo	CRC cabecera	
Dirección IP origen				
Dirección IP destino				
Opciones IP (si las hay)				Relleno
Datos				
...				

**Versión:** 4 bits, identifica la versión del protocolo en uso, se utiliza ya que algunos nodos pueden no soportar la última versión.

**Longitud de cabecera (HLEN):** 4 bits, mide la cabecera del datagrama.

**Tipo de servicio (TOS):** 4 bits, identifica funciones QOS de Internet.

**Longitud total:** 16 bits, mide el tamaño total del datagrama IP, expresadas en bytes, se incluyen tanto la cabecera como los datos.

**Identificación:** 16 bits, número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.

**Banderas o indicadores:** 3 bits, sólo 2 bits de los 3 bits disponibles están actualmente utilizados.

**El bit de *Más fragmentos* (MF),** indica que no es el último datagrama.

**No fragmentar (NF),** prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste se descartará.

**Desplazamiento de fragmentación** 13 bits, indica el lugar relativo de un fragmento de datos esto da la posición en la cual se insertará el fragmento dentro del datagrama completo, está medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.

**Tiempo de vida o TTL:** 8 bits, número máximo de segundos que puede estar un datagrama en la red de redes. Este contador se decrementa cada vez que pasa por un router hasta llegar a cero. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" al origen.

**Protocolo:** 8 bits, indica el que protocolo de nivel superior reciben los paquetes después del procesamiento IP este completado.

- |    |  |
|----|--|
| 0  | Reservado.                                   |
| 1  | ICMP ("Internet Control Message Protocol").  |
| 2  | IGMP ("Internet Group Management Protocol"). |
| 3  | GGP ("Gateway-to-Gateway Protocol").         |
| 4  | IP (IP encapsulation).                       |
| 5  | Flujo ("Stream").                            |
| 6  | TCP ("Transmission Control").                |
| 8  | EGP ("Exterior Gateway Protocol").           |
| 9  | PIRP ("Private Interior Routing Protocol").  |
| 17 | UDP ("User Datagram").                       |
| 89 | OSPF ("Open Shortest Path First").           |

**CRC cabecera:** 16 bits, comprueba la integridad del paquete IP. La verificación de errores de los datos corresponde a las capas superiores.

**Dirección origen:** 32 bits, contiene la dirección IP del origen.

**Dirección destino:** 32 bits, contiene la dirección IP del destino.

**Opciones IP:** No obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red, seguridad, etc.).

**Relleno:** Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

**Data:** Contiene la información del nivel superior (TCP, UDP).

#### **4.3.1.3.SOCKET.**

Cuando se utiliza el protocolo TCP/IP la aplicación debe identificarse con un número de puerto. Este puerto sirve para identificar la aplicación que recibirá el tráfico.

Los puertos también se pueden utilizar, solo los protocolos basados en TCP/IP, con un identificador llamado **socket**. El socket está extraído de las redes Unix de las operaciones I/O.

En general un socket, participa en el proceso de comunicación entre dos puntos terminales; en TCP/IP esta se logra mediante una concatenación del número de puerto y la dirección IP del computador que da el soporte al servicio de puertos.

#### **4.3.1.4.Encaminamiento IP.**

Una función importante de la capa IP es el encaminamiento IP es el encaminamiento, pues proporciona los mecanismos para interconectar diferentes redes físicas. Esto significa que un host puede actuar simultáneamente como host normal y como "router".

Un "router" básico de este tipo se conoce como "router" con información parcial de encaminamiento, ya que sólo contiene información acerca de cuatro tipos de destino:

- Los hosts conectados directamente a una de las redes físicas a las que está conectado el "router".
- Los host o redes para las se le han dado al "router" definiciones específicas.
- Los hosts o redes para las que el host ha recibido un mensaje ICMP redirect.
- Un destino por defecto para todo lo demás.

Los dos últimos casos permiten a un "router" básico comenzar con una cantidad muy limitada de información para ir aumentando debido a que un "router" más avanzado lance un mensaje ICMP redirect cuando reciba un datagrama y conozca un "router" mejor en la misma red al que dirigir el datagrama. Este proceso se repite cada vez que un "router" básico se reinicia.

#### 4.3.2. ICMP.

Internet Control Message Protocol, Internet es un sistema continuo sin control central: pero de todas formas es necesario para saber de la fuente original eventuales problemas, con el objetivo de ser susceptibles de repararse o evitarlos.

Para esto existe el protocolo ICMP, proporciona el medio para enviar los mensajes de error y control entre los elementos de la red (host, Gateway, routers, etc.). Este protocolo permite generar mensajes de error a nivel IP, sin intervención del usuario. Su implementación es obligatoria como subconjunto lógico del protocolo IP.

Cuando un datagrama causa un error, el protocolo ICMP solo puede reportar la condición del error a la fuente original del paquete de datos; la fuente debe relacionar el error con un programa de aplicación individual o tomar otra acción para corregir el problema. El formato de cada mensaje ICMP es diferente, pero todos tienen en común tres campos. En el comienzo del mensaje el campo TYPE (tipo) de mensaje, 8 bits, identifica el tipo de mensaje; campo CODE (código), 8 bits, da más información acerca del mensaje; y un campo de CHECKSUM (cheque de error), de 16 bits.

Byte +0								Byte +1								Byte +2								Byte +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Type								Code																							
Optional Data																															

**Datagrama ICMP**

Tipo	Mensaje ICMP
0	Respuesta al eco
3	Destino Inalcanzable
4	Fuente saturada
5	Redirección de ruta
8	Solicitud de Eco
11	Tiempo del datagrama excedido
12	Parámetro problema en datagrama
13	Requerimiento de hora y fecha
14	Respuesta de host y fecha
17	Requerimiento de mascara de dirección
18	Respuesta de mascara de dirección

**Tabla tipos de mensajes ICMP**

La siguiente es la descripción según el campo TYPE de mensaje ICMP.

**Tipo 0 y 8** El ECO o PING es de la forma más conocida y cotidiana que se tiene, del uso del protocolo ICMP, se utiliza para comprobar si otro host está operativo.

**Tipo 3** Informe de destino inalcanzable, si un Gateway no puede enviar un paquetes de datos a la dirección de destino, este envía de vuelta a la dirección de origen un mensaje de error. El cual el valor del campo tipo es 3, y el tipo de error viene dado por el campo CODE.

Code	Descripción
0	Red no alcanzable
1	Host no alcanzable
2	Protocolo no alcanzable
3	Puerto no alcanzable
4	Necesaria fragmentación con la opción DF
5	Fallo de la ruta de origen
6	Red de Destino desconocida
7	Host de Destino desconocido
8	Fallo del Host de Origen
9	Red prohibida administrativamente
10	Host prohibido administrativamente
11	Tipo de servicio de Red no alcanzable
12	Tipo de servicio de Host no alcanzable

**Tabla del campo CODE para informe de destino inalcanzable.**

**Tipo 4** Para que un Gateway pueda contener los paquetes de datos necesita de un buffer. La cantidad de datagramas es muy grande esta memoria temporal se llena, es decir el buffer se satura. Cuando se llega a este extremo el buffer comienza a descartar todos los datagramas que le llegan, hasta obtener un nivel de memoria libre aceptable. Todos los paquetes descartados hacen que el Gateway envíe un paquete ICMP de control de flujo al origen, indicando que el mensaje fue descartado. El código es cero.

**Tipo 5** Los Gateway contienen tablas de redireccionamiento, cuando la ruta no es la mejor el Gateway puede enviar un mensaje al host que existe una ruta correcta. El código varía de acuerdo a la siguiente tabla.

Código	Razón para la redirección
1	Por el Host
2	Por el tipo de servicio y red
3	Por el tipo de servicio y Host

**Tipo 11** Para prevenir bucles de redirección indefinidos los paquetes IP tienen un tiempo de vida definido por el origen, a medida que un Gateway procesa un datagrama el tiempo de vida comienza a disminuir. Cuando la cuenta llega a cero el Gateway envía un mensaje de error ICMP al host de origen y desecha el datagrama.

**Tipo 12** Cuando un paquete está mal construido en el origen, y un Gateway lo detecta este envía un mensaje ICMP de errores de parámetro y descarta el datagrama.

**Tipo 13 y 14** El mensaje de fecha y hora ICMP se utiliza para diagnóstico de problemas de redes con el objetivo de evaluar su rendimiento. Su formato además de los campos habituales tienen un identificador y un número de secuencia (16 bits c/u) utilizado para identificar la respuesta; también lleva fecha y hora original, es cuando se inicia la transmisión, fecha y hora del receptor es el tiempo inicial de cuando el receptor recibe el mensaje; y la fecha y hora de transmisión cuando el receptor transmite de vuelta el mensaje.

**Tipo 17 y 18** La máscara de subred de una LAN física se puede conocer enviando una solicitud ICMP de máscara de subred.

### 4.3.3. IGMP.

Internet Group Management Protocol, es un protocolo que funciona como una extensión del protocolo IP. Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento.

Un Gateways multicast manda mensajes una vez por minuto como máximo. Un host receptor responde con un mensaje IGMP, que marca al Host como miembro activo. Un host que no responde al mensaje se marca como inactivo en las tablas de direccionamiento de la red multicast.

### 4.3.4. ARP (RARP).

El Protocolo de Resolución de Direcciones (ARP) está encargado de traducir las direcciones IP en direcciones Ethernet. Cuenta para ello con una tabla con la dirección IP y asociada a esta la dirección Ethernet.

La tabla ARP se crea formulando una pregunta ARP y al ser respondida, se inserta una nueva entrada en su tabla, no solo la estación que formula la pregunta inserta la entrada a la tabla si no que todas las que escuchan la pregunta ARP lo hacen pues representan una probable comunicación futura, es útil para optimizar la red y reducir la congestión. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla

#### 4.3.4.1.Formato del mensaje ARP.

El mensaje ARP está formado por 28 octetos. En los campos que se describen a continuación se supone un Interfaz Ethernet.

Byte + 0								Byte +1								Byte +2								Byte +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
<i>Hardware</i>																<i>Protocol</i>															
<i>Length HW Address</i>								<i>Protocol Length</i>								<i>Operation</i>															
<i>Source Hardware Address</i>																															
<i>Source Hardware Address</i>																<i>Source IP Address</i>															
<i>Source IP Address</i>																<i>Destination Hardware Address</i>															
<i>Destination Hardware Address</i>																															
<i>Destination IP Address</i>																															

#### 4.3.4.2.Tipo de Hardware.

El campo Hardware indica el tipo de interfaz de Hardware. A continuación se detalla.

Tipo de Interfaz de Hardware	
Tipo	Descripción
1	Ethernet (10mb)
2	Experimental Ethernet (3 mb)
3	Amateur Radio X.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Network
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet

**Números de Protocolo:** el campo protocolo identifica el protocolo Ether usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

**Longitud de la dirección Hardware:** El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 sem.-octetos).

**Longitud del Protocolo:** Este campo se usa para definir la longitud de la dirección de red. Para una red IP es 4.

**Operación:** Especifica el código de la operación. La solicitud ARP tiene valor 1, y la respuesta ARP tiene valor 2.

**Dirección Hardware del Origen:** Los campos dirección Hardware del Origen, dirección IP del Origen, y dirección IP del Destino los completa el emisor (si los conoce). El receptor añade la dirección Hardware del Destino y devuelve el mensaje al emisor con el código de operación 2. (El código de la Respuesta ARP).

La dirección Hardware de Origen (para Ethernet) está formada por octetos que representan una dirección Ethernet de 48 bits, o un número.

**Dirección IP de Origen:** la dirección IP de Origen puede ser una dirección de clase A, B o C. (Ver Direcciones IP para obtener una definición de estas clases).

**Dirección Hardware de Destino:** Este campo está formado igual que el campo dirección Hardware de Origen.

**Dirección IP de Destino:** Este campo es igual que el campo dirección IP de Origen

El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.

#### 4.3.4.3. Formato del Mensaje RARP.

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud es 3, y el valor para una respuesta es 4.

### 4.4. CAPA DE TRANSPORTE.

#### 4.4.1. UDP.

El User Datagram Protocol, es un servicio no orientado a la conexión. Es un servicio simple y eficiente. Se utiliza en aplicaciones TFTP y DNS.

Es un servicio similar al protocolo IP. Una dirección IP dirige el datagrama hacia una máquina, el número de puerto de destino va en la cabecera UDP. Se utiliza para enviar el paquete de datos UDP a un proceso específico localizado en la cabecera IP. En la cabecera UDP también tiene el puerto de origen con el fin de que puede ser respondido el paquete de datos.

##### 4.4.1.1. Formato.

Son cuatro los campos.

Byte +0								Byte +1								Byte +2								Byte +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Puerto UDP origen																Puerto UDP destino															
Longitud mensaje UDP																Suma verificación UDP															
Datos																															

**Número de puerto de origen y destino**, 16 bits, cada uno, junto con una dirección IP definen el punto final y el de partida de una comunicación.

**Longitud de mensaje**, 16 bits, contiene el número total de bytes que forman el paquete de datos, incluida la cabecera.

**Checksum**, 16 bits, su uso es opcional, cuando no se utiliza es cero. Está formado por la suma de los campos UDP y algunos campos IP. Estos campos IP conforman una pseudo cabecera UDP, su longitud es de 12 bytes, y su único uso es el de calcular la suma.

#### 4.4.1.2. Puertos.

Las aplicaciones que envían datagramas necesitan identificar un objetivo más específico que la dirección IP, necesitan apuntar a un proceso específico, esto se hace a través de puertos.

TCP también usa puertos con los mismos valores. Estos puertos son totalmente independientes de los de UDP. Normalmente, un servidor usará TCP o UDP, aunque hay excepciones. Como por ejemplo DNS que ocupa el puerto 53 tanto TCP como UDP.

Un puerto es un número de 16 bits que identifica en un host que proceso está asociado a un datagrama. Se dividen en bien-conocidos ("well-known"), los puertos bien-conocidos pertenecen a servidores estándar y están destinados para evitarse las operaciones de configuración y efímeros los clientes no necesitan puertos bien-conocidos porque inician la comunicación con los servidores y los datagramas UDP enviados al servidor contienen su número de puerto.

#### 4.4.2. TCP.

Transmission Control Protocol, es un protocolo de uso general ampliamente utilizado en la transmisión fiable de información y sus funciones principales son 5:

**Servicio orientado a la conexión.** Es decir, la información que es enviada es recibida en forma íntegra.

**Conexión de circuito virtual** Se establece entre el host de origen y el de destino una comunicación continua, monitoreada para asegurar que los datos sean recibidos sean correctos.

**Transferencia con memoria intermedia.** No siempre las aplicaciones de la capa 7 proporcionan datagramas iguales o exactos, que sean de un tamaño adecuado para, que mediante el protocolo de transmisión, se envíe al host de destino. Cuando son muy pequeños los paquetes la información es almacenada hasta que la información alcanza un tamaño razonablemente largo como para ser enviado. Si el tamaño es muy grande este protocolo se encarga de seccionarlo con el mismo fin.

Si una aplicación en que los datos deben ser entregados aunque no se llene la memoria intermedia, existe la opción de utilizar un servicio conocido como push para forzar la transferencia.

**Flujo no estructurado.** Se puede enviar la información de control junto con los datos.

**Conexión full duplex** Transmisión simultánea en ambos sentidos.

#### 4.4.2.1. Formato datagrama TCP.

Byte + 0								Byte +1								Byte +2								Byte +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Puerto TCP origen																Puerto TCP destino															
Número de secuencia																															
Número de acuse de recibo																															
Data offset				Reservado				Bits código												Ventana											
Suma de verificación																Puntero de urgencia															
Opciones (si las hay)																Relleno															
Datos																															

**Puerto TCP origen:** 16 bits. Dirección de puerto del emisor, que el receptor usa para responder.

**Puerto TCP destino:** 16 bits, número de puerto del receptor.

**Número de secuencia:** 32 bits, el número de secuencia del primer byte de datos del segmento. Si el byte de control SYN está a 1, el número de secuencia es el inicial(n) y el primer byte de datos será el n+1.

**Número de acuse de recibo:** Si el bit de control ACK está a 1, este campo contiene el valor del siguiente número de secuencia que se espera recibir.

**Data Offset:** 32 bits, número de palabras de de la cabecera TCP. Indica dónde empiezan los datos.

**Reservado:** 6 bits, reservado para su uso futuro; deben ser cero.

**Bits código:** 6 bits reservados para funciones especiales.

**URG:** Indica que el campo "urgent pointer" es significativo en el segmento.

**ACK:** Indica que el campo de reconocimiento es significativo en el segmento.

**PSH:** Función "Push".

**RST:** Resetea la conexión.

**SYN:** Sincroniza los números de secuencia.

**FIN:** No hay más datos del emisor.

**Ventana:** Usado en segmentos ACK. Especifica el número de bytes de datos que comienzan con el byte indicado en el campo número de reconocimiento que el receptor está dispuesto a aceptar.

**Checksum:** El complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la pseudocabecera, la cabecera TCP y los datos TCP.

La pseudocabecera es la misma que utiliza UDP para calcular el checksum. Es una pseudocabecera IP, usada sólo para calcular el checksum.

Byte + 0								Byte +1								Byte +2								Byte +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
<i>Source IP Address</i>																															
<i>Destination IP Address</i>																															
<i>Zero</i>								<i>Protocol Number</i>								<i>Number of octets in header and data</i>															

**Puntero de Urgencia:** Apunta al primer octeto de datos que sigue a los datos importantes. Sólo es significativo cuando el bit de control URG está a uno.

**Opciones:** Este campo permite que una aplicación negocie durante la configuración de la conexión características como el tamaño máximo del segmento TCP. Si este campo tiene el primer byte a cero, esto indica que no hay opciones.

**Relleno:** Bytes todos a cero para rellenar la cabecera TCP a una longitud total que sea un múltiplo de 32 bits.

## 4.5. CAPA DE APLICACIÓN.

### 4.5.1. SMTP.

Simple Mail Transfer Protocol, protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras y/o distintos dispositivos (PDA's, Celulares, etc.).

En 1982 se diseñó el primer sistema para intercambiar correos electrónicos para ARPANET, definido en las RFC 821 (protocolo) y RFC 822 (formato). La primera de ellas define el protocolo y la segunda el formato del mensaje.

#### 4.5.1.1. Funcionamiento.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. Este protocolo va sobre de TCP, usa el puerto 25 en el servidor para establecer la conexión.

En una comunicación SMTP, se ha de establecer una conexión entre el emisor (cliente) y el receptor (servidor). Esto puede hacerse automáticamente con un programa cliente de correo o mediante un cliente telnet.

En el siguiente ejemplo se muestra una conexión típica. Se nombre con la letra C al cliente y con S al servidor.

```
S: 220 Servidor ESMTP
C: HELO
S: 250 Hello, please meet you
C: MAIL FROM: yo@midominio.com
S: 250 Ok
C: RCPT TO: destinatario@sudominio.com
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Campo de asunto
C: From: yo@midominio.com
C: To: destinatario@sudominio.com
C:
C: Hola,
C: Esto es una prueba.
C: Adios.
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye
```

#### **4.5.1.2. Los comandos básicos de SMTP:**

- HELO, para abrir una sesión con el servidor
- MAIL FROM, para indicar quien envía el mensaje
- RCPT TO, para indicar el destinatario del mensaje
- DATA, para indicar el comienzo del mensaje, éste finalizará cuando haya una línea únicamente con un punto.
- QUIT, para cerrar la sesión
- Las respuestas que da el servidor pueden ser de varias clases:
- 2XX, para una respuesta afirmativa
- 3XX, para una respuesta temporal afirmativa
- 4XX, para una respuesta de error, pero se espera a que se repita la instrucción
- 5XX, para una respuesta de error

Cuando recibe el mensaje el servidor, que finaliza con un punto, este es almacenado o retransmitido según corresponda, si el destinatario pertenece o no al dominio.

#### **4.5.1.3.Formato del mensaje.**

El mensaje está compuesto por dos partes:

Cabecera: estos ayudan al ordenar y organizar los mensajes.  
subject (asunto),  
from (emisor) y  
to (receptor).

Estos dos últimos campos no hay que confundirlos con los comandos MAIL FROM y RCPT TO, que pertenecen al protocolo, pero no al formato del mensaje.

Cuerpo del mensaje: es el mensaje propiamente dicho. En el SMTP básico está compuesto únicamente por texto, y finalizado con una línea en la que el único carácter es un punto.

#### **4.5.2. FTP.**

File Transfer Protocol (Protocolo de Transferencia de Archivos) y es usado para transferir datos por la red.

Es necesario un Servidor de FTP y un cliente de FTP, ocasionalmente los servidores son de libre acceso estos son de login anónimo o FTP anónimo.

Gran parte de las páginas Web son subidas mediante este protocolo a sus servidores de alojamiento.

#### **4.5.3. TELNET.**

Telnet es un protocolo y un programa cliente que permite acceder a otro host mediante una red, la maquina se puede manejar como si se estuviera delante de ella.

El acceso a host es mediante modo terminal. Esta herramienta fue muy útil para arreglar fallas en host remotos sin al necesidad de estar físicamente. También se utilizó en consulta de datos a distancias.

A pesar de ser una herramienta útil el problema mayor es la seguridad, ya que los datos viajan sin cifrar. Por eso, se ha ido dejando de lado su utilización. Siendo reemplazado por una versión cifrada de Telnet el SSH.

#### 4.5.4. HTTP.

Hyper Text Transfer Protocol, es decir, protocolo de transferencia de hipertexto. El hipertexto es el contenido de las páginas Web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones para acceder a una página Web, y la respuesta de esa Web, devolviendo la información que se desplegará en pantalla. También, el protocolo se utiliza, para enviar información adicional en ambos sentidos, como formularios con mensajes y otros.

Este es un protocolo que no guarda ninguna información sobre conexiones anteriores (sin estado). Al finalizar la transacción todos los datos se pierden. Por eso la aparición de las cookies es masiva, estas son pequeños archivos guardado en el computador, esto son leídos por el sitio Web con el cual se establece la conexión, contienen información relacionada con conexiones anteriores y puede identificar al cliente. Con ello puede almacenar gran cantidad de información relacionadas con sus visitantes

La versión actual de HTTP es la 1.1, y su especificación está en el documento RFC-2616 (<http://www.ietf.org/rfc/rfc2616.txt>).

HTTP dispone de medidas de seguridad en una variante, que es cifrada mediante SSL llamada HTTPS.

Está basado en el modelo cliente-servidor: Un cliente HTTP abre una conexión y realiza su solicitud al servidor, el cual responde generalmente el recurso solicitado y la conexión se cierra.

El formato tanto del mensaje como de la respuesta es como sigue:

```
<Línea inicial>  
Header-1: value-1  
...  
Header-n: value-n
```

```
<Cuerpo del mensaje (Opcional)>
```

La línea inicial es diferente en las solicitudes y en las respuestas. En las solicitudes van tres campos separados por un espacio en blanco: "Método recurso versiónDelProtocolo". Por ejemplo: "GET /path/to/file/index.html HTTP/1.0". La línea inicial de una respuesta tiene tres campos separados por un espacio: "versiónDelProtocolo códigoRespuesta Mensaje". Por ejemplo: "HTTP/1.0 200 OK" o bien "HTTP/1.0 404 Not Found".

Los encabezados están normados en el protocolo, e incluyen, en el caso de una solicitud, información del navegador y eventualmente del usuario cliente; En el caso de una respuesta, información sobre el servidor y sobre el recurso.

El cuerpo del mensaje contiene el recurso a transferir o el texto de un error en el caso de una respuesta. En el caso de una solicitud, puede contener parámetros de la llamada archivos enviados al servidor.

#### 4.5.4.1. Ejemplo de un dialogo HTTP.

Para obtener un recurso con el URL `http://www.tuhost.com/index.html`

1. Se abre un socket con el host `www.tuHost.com`, puerto 80 que ese el puerto por defecto para HTTP.
2. Se envía un mensaje en el estilo siguiente :

```
GET /index.html HTTP/1.0
From: yo@miHost.com
User-Agent: HTTPTool/1.0
[Línea en blanco]
```

3. La respuesta del servidor está formada por encabezados seguidos del recurso solicitado, en el caso de una página Web:

```
HTTP/1.0 200 OK
Date: Fri, 31 Dec 2003 23:59:59 GMT
Content-Type: text/html
Content-Length: 1221
```

```
<html>
<body>
<h1>Página principal de tuHost</h1>
(Contentido)
.
.
.
</body>
</html>
```

4. Al recibirse la respuesta, el servidor cierra la comunicación.

#### 4.5.5. URL.

Los recursos se identifican con un URL o "Universal Resource Locator" que es un identificador único en el mundo que se asocia con el recurso dado.

Códigos de respuesta

Son códigos de tres dígitos:

- 1xx Mensajes de información
- 2xx Operación exitosa
- 3xx Redirección hacia otro URL
- 4xx Error por parte del cliente
- 5xx Error por parte del servidor

#### 4.5.6. DNS.

Las direcciones IP proporcionan un medio para la identificación de host sean fuentes o destinos de los enlaces de comunicación, aunque sea efectivo la mayor parte de las personas prefieren memorizar un nombre que una secuencia de números.

Para que esto se logre un servidor debe transformar el nombre en la dirección correcta.

##### 4.5.6.1. Nombres de Dominio.

El programa del usuario proporciona el **nombre de dominio** como una secuencia de palabras. Están listadas de izquierda a derecha.

Estos programas DNS cambia el nombre de dominio proporcionado por el usuario para que sea mejor interpretado por otros software. Para estos el nombre de dominio es una secuencia de etiquetas y cada uno están formadas por un byte mas una cadena de caracteres (alfanuméricos y el signo menos).

Un nodo DNS se representa por una etiqueta en el interior del nombre de dominio, y todos los nodos tienen unos archivos de recursos (recourse records (RRs)) que contienen información que habilitan al programa para encontrar el nombre del dominio solicitado

##### 4.5.6.2. Formato RRs.

**Nombre del propietario** (*Owner Name*) o (SNAME): es el nombre del nodo al cual pertenece el RR. Este nombre que será comparado con el nombre proporcionado por el programa de usuario

**Tipo** (*Type*): 16 bits, describe el tipo de Resource Record.

**Clase** (*Class*): 16 bits, que define la clase del Resource Record. Un RR de Internet tiene el campo igual a 1.

**Tiempo de vida** (*Time-to-live*): 32 bits, que especifica el intervalo de tiempo en el cual el RR debe ser almacenado en la memoria caché, antes de ser actualizado con la información del

origen. El valor cero significa que el RR debe ser utilizado solo en la transacción en progreso, y no tiene que ser almacenado. El valor cero también se utiliza para datos muy volátiles.

**Longitud RD** (*RDLenght*): 16 bits, especifica la longitud en octetos del campo RDATA.

**RData**: variable, el formato de esta información varía según el tipo y clase del RR. Para el tipo A RR (Internet), el campo RData contiene una dirección IP de 32 bits.

#### 4.5.6.2.1. Funcionamiento.

Un cliente envía una solicitud de nombre, que se desea resolver, una de aclaración de clase de nombre, el tipo de respuesta deseada y un código que especifica si el servidor de nombres debe traducir el nombre completamente. Existen tres respuestas:

Dirección duplicada, si el nombre hace referencia a un alias este devuelve el dominio de ese alias.

Error de nombre, no existe el nombre.

Error de dato no encontrado, el nombre existe pero no es una dirección IP.

#### 4.5.6.2.2. Formato de un mensaje DNS.

Utiliza UDP para solicitudes y respuestas entre servidores de nombres. TCP se usa en la transferencia de zonas completas.

El formato de un mensaje DNS tienen 5 partes.

**Cabecera**, define el formato del mensaje.

**Pregunta**, objeto a resolver.

**Respuestas**, resolución.

**Autoridad**, referencia a 1 servidor autorizado.

**Adicional**, otra información no relacionada con la respuesta.

#### 4.5.6.2.3. Formato de la cabecera.

La cabecera contiene los siguientes campos:

7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
ID								QR	Opcode				A	T	RQ	RA	Z	Rcode					
QDCOUNT								ANCOUNT															
NSCOUNT								ARCOUNT															

**ID**: 16 bits, se utiliza para relacionar solicitudes y respuestas.

**QR:** 1 bit, identifica el mensaje como una solicitud (0) o una respuesta (1).

**OPcode:** 4 bits, describe el tipo de mensaje. 0 Solicitud normal (nombre a dirección), 1 Solicitud Inversa (dirección a nombre) y 2 Solicitud del estado del servidor.

**A:** 1 bit, el valor 1 indica que la respuesta la ha hecho un servidor autorizado

**T:** 1 bit, el valor 1 indica que el mensaje ha sido truncado

**RQ:** 1 bit, el valor 1, indica la solicitud de un servicio recursivo por parte del servidor de nombres. Este servicio normalmente no está disponible.

**RA:** 1 bit, que indica la disponibilidad del servicio recursivo.

**Z:** 3 bits, reservado para un uso futuro, y su valor debe ser 0.

**RCode:** 4 bits, que lo rellena el servidor de nombres, y sirve para indicar el estado de la búsqueda. 0 Sin errores, 1 Error de Imposible interpretar el formato de la búsqueda, 2 Error de Imposible procesar el servidor, 3 Error de nombre inexistente, 4 Tipo de búsqueda no soportado, 5 Solicitud rechazada.

**QDCount:** 16 bits, indica el número de entradas en la sección de Preguntas.

**ANCCount:** 16 bits, indica el número de Resource Records en la sección de Respuesta.

**NSCount:** 16 bits, define el número de Resource Records en la sección de Autoridad.

**ARCount:** 16 bits, que define el número de Resource Records en la sección de Archivos Adicionales.

#### **4.5.6.2.4. Formato de la sección Preguntas.**

Esta sección la construye el cliente, y siempre está presente. Contiene el nombre de dominio objetivo, seguido por los campos Qtype y Qclass. Esta sección es idéntica en longitud y formato que la definida para los campos Clame, tipo y clase de un Resource Record.

#### **4.5.6.2.5. Formato de la sección Respuesta.**

Esta sección contiene uno o más RRs.

#### **4.5.6.2.6. Formato de la sección Autoridad.**

La sección autoridad contiene uno o más RRs que apuntan hacia los orígenes de la información autorizada.

#### **4.5.6.2.7. Formato de la sección Adicional.**

Esta sección contiene uno o más RRs que proporcionan fuentes adicionales de información

#### **4.5.7. H.323.**

Es una recomendación sobre un método de establecer un enlace no orientado a la conexión para comunicaciones multimediales (voz, video, datos) a través de redes que no proporcionan calidad de servicio (QOS), como lo son las redes basadas en IP; permite aclarar una gran cantidad de conceptos. Se encarga del control de llamadas, administración de multimedia, administración del ancho de banda para conferencias de punto a punto y de puntos múltiples. H.323 también administra los códecs de audio y video. H.323 es independiente de la plataforma, de la red y aplicación, de forma que si un dispositivo cumple con este estándar se puede comunicar con otro que igualmente lo cumpla.

##### **4.5.7.1.Arquitectura.**

La recomendación H.323 define la integración de cuatro elementos que conforman parte de la comunicación, a saber: Terminales, Gatekeepers y Gateways, MCU (Multipoint Control Units).

##### **4.5.7.1.1. Terminales.**

Un terminal H.323 es un punto extremo de la red que facilita las comunicaciones en tiempo real y en los dos sentidos con otro terminal, pasarela o unidad de control multipunto H.323, en otras palabras debemos entender el equivalente a los teléfonos actuales. Esta comunicación consta de control, indicaciones, audio, imágenes de vídeo en color y en movimiento y/o datos entre los dos terminales. Un terminal puede proporcionar sólo señales vocales, señales vocales y datos, señales vocales y vídeo o señales vocales, datos y vídeo.

##### **4.5.7.1.2. Gatekeepers.**

Dentro del esquema de Voz IP, la funcionalidad principal que debe ofrecer todo Gatekeeper se basa en el control de llamadas y gestión del sistema de direccionamiento, pero el conjunto de tareas puede ser el más importante de todo el sistema.

Aunque los terminales pueden conectarse directamente sin intervención del Gatekeeper, limita su funcionalidad. Todo terminal antes de realizar una llamada, debe consultar con el Gatekeeper si esta es posible. Una vez obtenido el permiso, el Gatekeeper es quien realiza la transferencia entre el identificador de usuario destino y la dirección IP equivalente.

Establecida la comunicación entre los terminales, el Gatekeeper no necesita intervenir, con lo que la carga del sistema se reparte entre los terminales.

Es la responsabilidad principal del Gatekeeper mantener un control de todo el tráfico, mantener un nivel aceptable de saturación de la red. También es el responsable de controlar de ancho de banda lo que permite al administrador fijar un límite de utilización, por encima del cual se rechazan las llamadas bien sean internas o externas.

Otro aspecto importante que debe manejar el Gatekeeper es el enrutamiento de las llamadas. De esta forma, el propio Gatekeeper puede redireccionar las llamadas al Gateway más indicado o elegir un nuevo destino si el original no está disponible. En este punto es donde una solución software puede dotar al administrador del sistema de herramientas potentes de control y definición de reglas.

En cuanto a otras capacidades añadidas, podemos pensar en el control de costos de llamadas, control de centros de atención al cliente, etc.

#### **4.5.7.1.3. Gateways.**

En rigor es un dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. En VoIP es un punto extremo en la red que proporciona comunicaciones en ambos sentidos en tiempo real entre terminales H.323 de la red por paquetes y otros terminales UIT en una red con conmutación de circuitos, o con otra pasarela H.323. Otros terminales UIT son, por ejemplo, aquellos que cumplen con la Rec. UIT-T H.310 (H.320 sobre la RDSI-BA), H.320 (RDSI), H.321 (ATM), H.322 (LAN con GQOS), H.324 (RTGC), H.324M (Móviles) y V.70 (Señales vocales y datos simultáneos digitales).

Existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización

Todo el funcionamiento se produce de una forma totalmente transparente en ambos sentidos, pudiendo recibir y emitir llamadas directamente desde nuestro computador personal sin ningún problema.

#### **4.5.7.1.4. MCU (Multipoint Control Unit).**

Una unidad de control multipunto H.323 (MCU) es un extremo que proporciona la capacidad para que tres o más terminales (puntos) y Gateways participen en una conferencia multipunto. Una MCU se forma de dos partes: un controlador multipunto (MC) que es obligatorio y un procesador multipunto (MP) opcional. En el caso más simple, una MCU puede estar formada por un MC únicamente.

#### **4.5.7.1.5. MC (Multipoint Control).**

Un controlador multipunto (MC) es una entidad H.323 que proporciona las capacidades de negociación entre todos los terminales para conseguir la comunicación. Puede controlar así mismo recursos de la conferencia tales como el vídeo multicast. El MC no realiza mezcla ni conmutación de audio, vídeo o datos.

#### **4.5.7.1.6. MP (Multipoint Processor).**

Un procesador multipunto (MP) es la entidad H.323 cuyo hardware y software especializado mezclan, conmutan y procesan el audio, vídeo y/o los datos de los participantes en una conferencia multipunto. El MP puede procesar una única secuencia multimedia o varias simultáneamente, dependiente del tipo de conferencia soportada.

Es necesario además definir dos términos que se utilizan en toda la literatura relacionada con este tema.

#### **4.5.7.1.7. Entidad.**

Definido en la recomendación H.323 como: “Cualquier componente H.323, incluidos terminales, pasarelas, controladores de acceso, MC, MP y MCU”. Es decir, es el término genérico de entidad como cualquier componente que cumpla con el estándar.

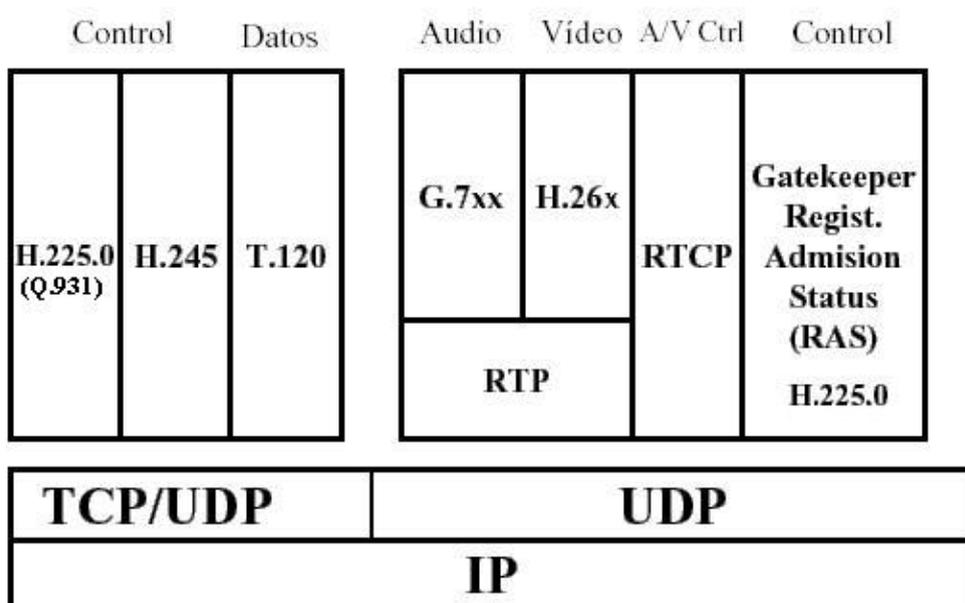
#### 4.5.7.1.8. Extremo.

Se define como: “Un terminal, una pasarela o una MCU H.323. Un punto extremo puede llamar y ser llamado. Genera y/o termina trenes de información.”.

#### 4.5.7.2. Canal de registros, admisión y situación (RAS, *registration, admission and status*).

Canal no fiable utilizado para transportar los mensajes de registro, admisiones, cambio de ancho de banda y situación (según la Rec. UIT-T H.225.0) entre dos entidades H.323.

##### 4.5.7.2.1. Pila de protocolos.



De acuerdo con la imagen anterior los protocolos de señalización H.323 son:

**H.225.0:** Define la señalización entre terminales/Gateways y Gatekeeper (RAS). También define la señalización para establecimiento y liberación de la llamada (Setup, Alerting,...) que va por el canal de señalización de llamada. En este caso se utiliza un subconjunto de las funciones proporcionadas por la Q.931.

**H.245:** Señalización de control extremo a extremo. La función principal es el intercambio de capacidades entre los terminales H.323 previa a la transmisión de información.

**H.235:** Trata sobre la seguridad en la comunicación incluyendo autenticación, autorización, control de llamada seguro y privacidad de los canales de voz

**RAS:** La función de señalización RAS utiliza mensajes H.225.0 para llevar a cabo los procedimientos de registro, admisiones, cambios de ancho de banda, situación y desligamiento entre puntos extremos y controladores de acceso.

**RTP (real time protocol):** Protocolo de tiempo real, maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

**RTCP (real time control protocol):** protocolo de control de tiempo real, se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras

#### Protocolos de compresión audio en tablas comparativas.

Formato	Frecuencia de muestreo	Canales	Kb/s	Uso
PCM (G.711)	8	1	64	Telefonía
ADPCM (G.721)	8	1	32	Telefonía
SB-ADPCM (G.722)	16	1	48/56/64	Videoconferencia
MP-MLQ (G.723.1)	8	1	6,3/5,3 variable	Telefonía Internet
ADPCM (G.726)	8	1	16/24/32/40	Telefonía
E-ADPCM (G.727)	8	1	16/24/32/40	Telefonía
LD-CELP (G.728)	8	1	16	Telefonía/Video
CS-ACELP (G.729)	8	1	8	Telefonía Internet

#### Protocolos de compresión de video

Sistema	Compresión espacial	Compresión temporal	Complejidad	Eficiencia	Retardo
M-JPEG	Si	No	Media	Baja	Muy pequeña
H.261	Si	Limitada (fotog I y P)	Elevada	Media	Pequeño
MPEG-1/2	Si	Extensa (fotog I, P y B)	Muy elevada	Alta	Grande
H.263 y MPEG-4	Si	Extensa (fotog I, P y B)	Enorme	Alta	Medio

### **4.5.7.3.Descripción de sistemas H.323.**

La recomendación H.323 describe los componentes de dicha recomendación y las características de su comunicación.

La información es transmitida por medio de trenes de información, que se clasifican en, trenes de audio, video, datos, control de las comunicaciones y control de llamada. Estos trenes de datos son formateados y enviados a la interfaz de red de acuerdo a la recomendación UIT-T H.225.0.

#### **4.5.7.3.1. Características de los terminales.**

Los terminales H.323, disponen de diversas facilidades siendo obligatoria en todos ellos una unidad de control del sistema, capa H.225.0, interfaz de red y códec de audio. La unidad de códec de video y las aplicaciones de datos son opcionales.

##### **4.5.7.3.1.1.Interfaz de red por paquetes.**

En relación a la interfaz de red está relacionada con la implementación y no es de competencia de la recomendación en estudio. Sin embargo, los requerimientos que deberá proporcionar son enumerados en la recomendación UIT-T H.225.0. Esto significa que el servicio de extremo a extremo fiable (por ejemplo, TCP, SPX) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada. El servicio de extremo a extremo no fiable (por ejemplo, UDP, IPX) es obligatorio para los canales de audio, los canales de vídeo y el canal de RAS. Estos servicios pueden ser dúplex o simplex y de unidifusión o multidifusión dependiendo de la aplicación, las capacidades de los terminales y la configuración de la red.

##### **4.5.7.3.1.2.Códecs de audio y video.**

Con relación a los códec, el de video se exige al menos la decodificación y codificación de QCIF H.261, sin descartar el uso de otro códec. El de códec de audio es obligatorio para todos los terminales H.323, los cuales deben ser capaces de codificar y decodificar señales de audio en conformidad con la recomendación el UIT-T G.711, además deben ser capaces de transmitir en ley A y ley  $\mu$ ; no es descartable la implementación de otros códecs de audio.

#### **4.5.7.3.1.3. Canal de datos.**

Los canales de datos (1 ó más) son opcionales. Este puede ser unidireccional o bidireccional, dependiendo de los requisitos de la aplicación de datos. La Recomendación UIT-T T.120 es la base por defecto de la interoperabilidad de datos entre un terminal H.323 y otro terminal H.323, H.324, H.320 o H.310.

#### **4.5.7.3.1.4. Función de control H.245.**

La recomendación H.245 realiza una función de control utilizando el canal de control H.245, para llevar los mensajes de control de extremo a extremo que manejan el funcionamiento de la entidad H.323, incluyendo el intercambio de capacidades, apertura y cierre de canales lógicos, peticiones de modo preferido, mensajes de control de flujo e instrucciones e indicaciones generales.

La señalización H.245 se establece entre dos puntos extremos, un punto extremo y un MC o un punto extremo y un Gatekeeper. El punto extremo establecerá un canal de control H.245 en cada sentido para cada llamada en la que él participe. Este canal utilizará los mensajes y procedimientos de la recomendación UIT-T H.245. Es preciso señalar que un terminal, una MCU, una pasarela o un Gatekeeper pueden soportar muchas llamadas y, por ello, muchos canales de control H.245.

La Recomendación UIT-T H.245 especifica varias entidades de protocolo independientes que soportan señalización de punto extremo a punto extremo. Una entidad de protocolo se especifica por su sintaxis (mensajes), su semántica y un conjunto de procedimientos que establecen el intercambio de mensajes y la interacción con el usuario. Los puntos extremos H.323 soportarán la sintaxis, la semántica y los procedimientos de las siguientes entidades de protocolo:

- Determinación maestro/esclavo.
- Intercambio de capacidades.
- Señalización de canal lógico unidireccional.
- Señalización de canal lógico bidireccional.
- Señalización de cierre de canal lógico.
- Petición de modo.
- Determinación de retardo de ida y vuelta.
- Señalización de bucle de mantenimiento.

Los mensajes H.245 se clasifican en cuatro categorías: de petición, respuesta, instrucción e indicación. Los mensajes de petición y respuesta son utilizados por las entidades de protocolo. Los mensajes de petición requieren una acción específica por parte del receptor, incluyendo una respuesta inmediata. Los mensajes de respuesta responden a una petición correspondiente. Los mensajes de instrucción requieren una acción específica, pero no una respuesta. Los mensajes de indicación son informativos solamente y no requieren ninguna acción o respuesta. Los terminales H.323 responderán a todas las instrucciones y peticiones H.245 (se especifica en el anexo A de la recomendación H.323) y transmitirán indicaciones que reflejen el estado del terminal.

Los terminales H.323 deben ser capaces de descomponer analíticamente todos los mensajes de mensajes de control de sistema multimedios H.245 y enviarán y recibirán todos los mensajes necesarios para implementar las funciones requeridas y aquellas funciones opcionales que soporte el terminal. Los terminales H.323 deben enviar el mensaje de "función no soportada" en respuesta a cualquier mensaje de petición, respuesta o instrucción no reconocida que reciban.

Se dispone de una indicación H.245, usuario, para el transporte de caracteres alfanuméricos de entrada del usuario desde un telemando o un teclado, equivalente a las señales multifrecuencia (DTMF, *dual-tone multifrequency*) utilizadas en telefonía analógica o mensajes de números SBE de la Rec. UIT-T H.230. Esto se puede utilizar para operar manualmente equipos distantes tales como los sistemas de correo vocal o correo vídeo, los servicios de información por medio de un menú, etc. Los terminales H.323 soportarán la transmisión de los caracteres de entrada de usuario 0-9, " ? y "?. La transmisión de otros caracteres es opcional.

#### **4.5.7.3.1.5. Función de señalización RAS.**

La función de señalización RAS utiliza mensajes H.225.0 para llevar a cabo los procedimientos de registro, admisiones, cambios de ancho de banda, situación y desligamiento entre puntos extremos y controladores de acceso. El canal de señalización RAS es independiente del canal de señalización de llamada y del canal de control H.245. En los entornos de red que no tienen un Gatekeeper, no se utiliza el canal de señalización RAS. En los entornos de red que sí tienen un Gatekeeper (una zona), el canal de señalización RAS se abre entre el punto extremo y el Gatekeeper. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

#### **4.5.7.3.1.6. Función de señalización de llamada.**

La función de señalización de llamada utiliza la señalización de llamada H.225.0 para establecer una conexión entre dos puntos extremos H.323. El canal de señalización de llamada es independiente del canal de RAS y del canal de control H.245. Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización de llamada. El canal de señalización de llamada se abre antes del establecimiento del canal H.245 y de cualquier otro canal lógico entre puntos extremos H.323. En los sistemas que no tienen un Gatekeeper, el canal de señalización de llamada se abre entre los dos puntos extremos que participan en la llamada. En los sistemas que sí tienen un Gatekeeper, el canal de señalización de llamada se abre entre el punto extremo y el Gatekeeper o entre los propios puntos extremos, según decida el Gatekeeper.

#### **4.5.7.3.2. Capa H.225.0.**

Los canales lógicos de información de vídeo, audio, datos o control se establecen de acuerdo con los procedimientos de la Rec. UIT-T H.245. Los canales lógicos son unidireccionales e independientes en cada sentido de la transmisión.

Además de los canales lógicos, los puntos extremos H.323 utilizan dos canales de señalización para el control de la llamada y las funciones relacionadas con el Gatekeeper. El formato dado a estos canales deberá ser conforme a la Rec. UIT-T H.225.0.

## **5. CAPÍTULO V. SEÑALIZACIÓN Y ESTABLECIMIENTO DE LLAMADA H.323.**

### **5.1. INTRODUCCIÓN.**

En este capítulo se explicará diferentes conceptos que se emplean en llamadas; también se incluirá los pasos de establecimiento de llamada, en forma general, que aplica en la recomendación UIT-T H.323.

Además se tratará de identificar los conceptos analizando paquetes de datos capturados. Para ello fue necesario un proveedor de servicios IP (CallManager<sup>†</sup>), un ATA<sup>‡</sup> (Analog Telephonic Adaptor) -ambos de CISCO-, un teléfono análogo, un software de captura (Packetyzer, Ethereal).

### **5.2. SEÑALIZACIÓN.**

La señalización de una llamada, en general, se conforma por mensajes y procedimientos. En particular una llamada IP está compuesta entre otros; pedir cambios de ancho de banda de la llamada, obtener el estado de los puntos extremos de la llamada y desconectar la llamada. El formato de los mensajes están consignados en la recomendación UIT-T H.225.0 y los procedimientos en la recomendación UIT-T H.323.

#### **5.2.1. Direcciones (identificadores).**

##### **5.2.1.1. Dirección de Red**

Cada entidad deberá tener, al menos una dirección de red. Dicha dirección identifica de manera exclusiva la entidad H.323 en la red además es específica del entorno de red en que está el punto extremo. Sin embargo entidades pueden compartir una dirección de red.

##### **5.2.1.2. Dirección de alias.**

Una dirección alias puede representar el punto extremo o puede representar conferencias que el punto extremo está acogiendo. Las direcciones alias son un método alternativo de direccionamiento del punto extremo. Dichas direcciones incluyen direcciones de dígitos marcados o de números de parte, incluyendo números telefónicos privados y plan de numeración telefónica pública, identidades H.323 (cadenas alfanuméricas que representan nombres, direcciones similares a las del correo electrónico, etc.) y cualesquiera otras direcciones definidas

---

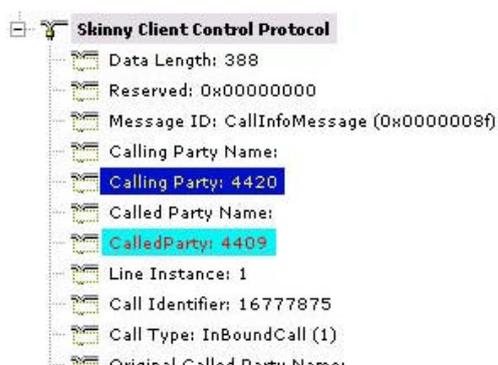
<sup>†</sup> Ver Anexo CISCO CallManager.

<sup>‡</sup> Ver Anexo.CISCO ATA 186.

en la Rec. UIT-T H.225.0. Las direcciones alias deberán ser únicas dentro de una zona, pero un punto extremo puede tener también una o más direcciones alias asociadas al mismo.

En las imágenes se muestra las direcciones de alias, estos números telefónicos son tanto del extremo llamado como el llamante.

▲	Source Ad...	Dest Addr...	Summary	Le...	Rel Time	Delta Time	AbsTime
32	172.16.10.10	172.16.10.28	SKINNY: DialedNumberM...	98	00:00:07.531.737	00:00:00.000.519	17:21:02.322.496
33	172.16.10.10	172.16.10.28	SKINNY: CallStateMessage	90	00:00:07.532.249	00:00:00.000.512	17:21:02.323.008
34	172.16.10.10	172.16.10.28	SKINNY: CallInfoMessage	450	00:00:07.532.251	00:00:00.000.002	17:21:02.323.010
35	172.16.10.10	172.16.10.28	SKINNY: StartToneMessa...	82	00:00:07.532.764	00:00:00.000.513	17:21:02.323.523
36	172.16.10.10	172.16.10.28	SKINNY: CallStateMessage	90	00:00:07.532.767	00:00:00.000.003	17:21:02.323.526



## 5.2.2. Canal de registro, admisiones y situaciones (RAS).

Este canal se utilizará para los procesos de descubrimiento de Gatekeeper y de registro de punto extremo que se asocian con un alias en un punto extremo. El canal de RAS es un canal no fiable.

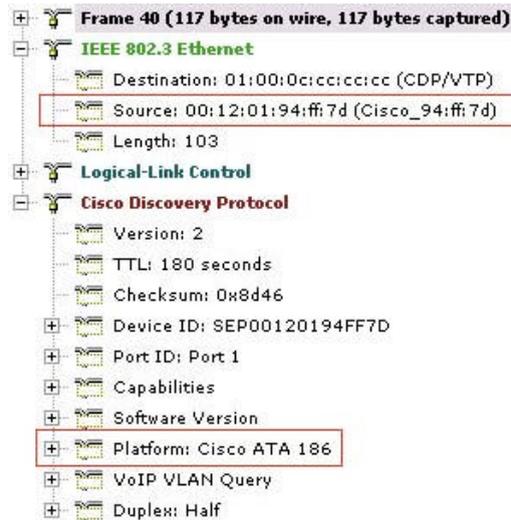
### 5.2.2.1. Descubrimiento del Gatekeeper (controlador de acceso).

Este proceso lo usa un punto extremo para determinar cual es el Gatekeeper que lo registrará (Gatekeeper). Existe dos métodos uno manual y otro automático para realizar este procedimiento.

Es posible que el punto extremo no conozca quién es su Gatekeeper, o quizás necesite identificar otro Gatekeeper debido a un fallo, lo que puede hacerse mediante el descubrimiento automático.

En el procedimiento automático se envía un mensaje de multidifusión como aparece a continuación, en este caso corresponde a un protocolo propietario de Cisco.

N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
39	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32768/00:0f:35:05:1b:85 Cost =...	68	00:00:04.414.708	00:00:00.001.822	19:35:04.431.810
40	Cisco_94:ff:7d	CDP/VTP	CDP: Cisco Discovery Protocol	117	00:00:04.745.883	00:00:00.331.175	19:35:04.762.985
41	Cisco_97:0e:03	CDP/VTP	CDP: Cisco Discovery Protocol	417	00:00:04.746.644	00:00:00.000.761	19:35:04.763.746
42	200.2.114.31	200.2.114.63	NBNS: Name query NB MONICA<00>	96	00:00:04.945.503	00:00:00.198.859	19:35:04.962.605



Es importante hacer notar que el origen del mensaje corresponda al ATA puesto que la dirección que aparece como fuente es la Mac Address Cisco\_97:0e:03 (00:12:05:94:ff:7d) corresponde a este dispositivo.

Luego de esto, se envía información mediante TCP de parte del CallManager. Como se ve en la siguiente figura. La dirección IP de origen (172.16.10.10) corresponde al CallManager y la de destino al ATA (172.16.10.20)

N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
43	200.2.114.1	224.0.0.10	EIGRP: Hello	78	00:00:05.632.533	00:00:00.687.030	19:35:05.649.635
44	Cisco_94:ff:7d	CDP/VTP	CDP: Cisco Discovery Protocol	117	00:00:05.745.615	00:00:00.113.082	19:35:05.762.717
45	Cisco_97:0e:03	CDP/VTP	CDP: Cisco Discovery Protocol	417	00:00:05.746.349	00:00:00.000.734	19:35:05.763.451
46	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32769/00:12:01:97:0e:00 Cost =...	68	00:00:06.037.583	00:00:00.291.234	19:35:06.054.685
47	Cisco_97:0e:03	Spanning-tree-(fo...	STP: Conf. Root = 32769/00:12:01:97:0e:00 Cost =...	60	00:00:06.038.096	00:00:00.000.513	19:35:06.055.198
48	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32798/00:12:01:97:0e:00 Cost =...	68	00:00:06.045.840	00:00:00.007.744	19:35:06.062.942
49	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32908/00:12:01:97:0e:00 Cost =...	64	00:00:06.047.247	00:00:00.001.407	19:35:06.064.349
50	Cisco_05:18:00	Broadcast	ARP: Who has 172.16.54.240? Tell 172.16.54.1	64	00:00:06.085.395	00:00:00.038.148	19:35:06.102.497
51	172.16.10.10	172.16.10.20	TCP: 2000 > 15104 [RST] Seq=4178817440 Ack=...	64	00:00:06.314.352	00:00:00.228.957	19:35:06.331.454
52	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32768/00:0f:35:05:18:0f Cost =...	68	00:00:06.407.777	00:00:00.093.425	19:35:06.424.879
53	Cisco_97:0e:03	01:00:0c:cccc:cd	STP: Conf. Root = 32768/00:0f:35:05:18:39 Cost =...	68	00:00:06.414.454	00:00:00.006.677	19:35:06.431.556

### 5.2.2.1.1. Registro de punto extremo.

El registro es el proceso por el cual un punto extremo se incorpora a una zona y se comunica al Gatekeeper sus direcciones de transporte y direcciones de alias. El registro se concibe como un proceso de configuración en el que todos los puntos extremos se registran al Gatekeeper identificado mediante el protocolo de descubrimiento. Este proceso se deberá realizar antes de efectuar cualquier llamada y puede producirse en forma periódica.

### 5.2.2.2. Empleo de mensajes RRQ ligeros.

El registro de un punto extremo puede tener una vida finita. Para esto el punto extremo puede solicita un tiempo de vida (Time To Live, TTL), el cual se expresa en segundos, en un mensaje al Gatekeeper, este responde con un tiempo de vida igual o menor. Transcurrido dicho tiempo el registro expira. Antes que el registro expire el punto extremo puede enviar un mensaje de mantener vivo (Keep Alive) activado, esto reiniciara el registro en el controlador, de otro modo se deberá registrar de nuevo.

A continuación se verifica esto mediante el análisis del datagrama que cumple esta función en el ATA. En el podemos apreciar destacado el tiempo del Keep Alive en segundos

▲	Source Addr...	Dest Addr...	Summary	Len...	Rel Time	Delta Time	AbsTime
128	172.16.10.20	172.16.10.10	SKINNY: RegisterMessage	110	00:00:13.640.391	00:00:00.096.261	19:35:13.657.493
129	172.16.10.10	172.16.10.20	TCP: 2000 > 14738 [ACK] Seq=73898402 Ack=60367005 ...	64	00:00:13.640.903	00:00:00.000.512	19:35:13.658.005
130	172.16.10.10	172.16.10.20	SKINNY: RegisterAckMessage	90	00:00:13.645.037	00:00:00.004.134	19:35:13.662.139
131	172.16.10.10	172.16.10.20	SKINNY: CapabilitiesReqMessage	70	00:00:13.645.549	00:00:00.000.512	19:35:13.662.651
132	172.16.10.20	172.16.10.10	SKINNY: VersionReqMessage	70	00:00:13.652.978	00:00:00.007.429	19:35:13.670.080

+ Frame 130 (90 bytes on wire, 90 bytes captured)  
 + Ethernet II, Src: 00:50:8b:f7:ec:df, Dst: 00:12:01:94:ff:7d  
 + 802.1q Virtual LAN  
 + Internet Protocol, Src Addr: 172.16.10.10 (172.16.10.10), Dst Addr: 172.16.10.20 (172.16.10.20)  
 + Transmission Control Protocol, Src Port: 2000 (2000), Dst Port: 14738 (14738), Seq: 73898402, Ack: 60367005, Len: 32  
 - Skinny Client Control Protocol

- Data Length: 24
- Reserved: 0x00000000
- Message ID: RegisterAckMessage (0x00000081)
- KeepAliveInterval: 30**
- DateTemplate: D/M/YA
- SecondaryKeepAliveInterval: 60

Consecuentemente con la información enviada en las imágenes anteriormente mostradas se puede observar el envío sistemático de mensajes Keep Alive cada 30 segundo. En la imagen los paquetes de información se ordenaron de acuerdo al enunciado del protocolo.

Num	Source Address	Dest Address	Summary	Le...	AbsTime
12799	172.16.10.10	172.16.10.20	SKINNY: KeepAliveAckMessage	70	12:10:10.651.071
12822	172.16.10.10	172.16.10.20	SKINNY: KeepAliveAckMessage	70	12:10:11.661.324
1123	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:07:40.539.939
1205	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:07:41.547.737
1988	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:08:10.559.449
2011	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:08:11.569.019
4744	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:08:40.583.994
4859	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:08:41.593.046
7589	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:09:10.605.361
7607	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:09:11.615.599
9648	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:09:40.629.136
9761	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:09:41.638.042
12798	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:10:10.650.555
12821	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	12:10:11.660.810
473	172.16.10.20	172.16.10.10	SKINNY: KeypadButtonMessage	74	12:07:30.140.860

La imagen que aparece a continuación corresponde al mensaje Keep Alive.

▲	Source Addr...	Dest Addr...	Summary	Len...	Rel Time	Delta Time	AbsTime
1140	172.16.9.2	172.16.10.20	UDP: Source port: 17836 Destination port: 16384	218	00:00:43.675.744	00:00:00.001.443	19:35:43.692.846
1141	172.16.10.20	172.16.10.10	SKINNY: KeepAliveMessage	70	00:00:43.678.507	00:00:00.002.763	19:35:43.695.609
1142	172.16.10.10	172.16.10.20	SKINNY: KeepAliveAckMessage	70	00:00:43.679.014	00:00:00.000.507	19:35:43.696.116
1143	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 17836	218	00:00:43.682.841	00:00:00.003.827	19:35:43.699.943
1144	172.16.9.2	172.16.10.20	UDP: Source port: 17836 Destination port: 16384	218	00:00:43.695.691	00:00:00.012.850	19:35:43.712.793

+	🔗	<b>Frame 1142 (70 bytes on wire, 70 bytes captured)</b>
+	🔗	<b>Ethernet II, Src: 00:50:8b:f7:ec:df, Dst: 00:12:01:94:ff:7d</b>
+	🔗	<b>802.1q Virtual LAN</b>
+	🔗	<b>Internet Protocol, Src Addr: 172.16.10.10 (172.16.10.10), Dst Addr: 172.16.10.20 (172.16.10.20)</b>
+	🔗	<b>Transmission Control Protocol, Src Port: 2000 (2000), Dst Port: 14738 (14738), Seq: 73903574, Ack: 60367757, Len: 12</b>
+	🔗	<b>Skiny Client Control Protocol</b>
	🔗	Data Length: 4
	🔗	Reserved: 0x00000000
	🔗	Message ID: KeepAliveAckMessage (0x00000100)

### 5.2.2.3. Canal de señalización de llamada.

El canal de señalización de llamada se empleará para transportar mensajes de control de llamada H.225.0. El canal de señalización será un canal fiable.

#### **5.2.2.3.1. Encaminamiento del canal de señalización.**

Los mensajes de señalización de llamada se pueden transferir según dos métodos. El primero de ellos es el de señalización de llamada por el Gatekeeper. En este método, los mensajes de señalización de llamada se encaminan a través del Gatekeeper entre los puntos. El segundo método es el de señalización de llamada de puntos extremos directa. En este método, los mensajes de señalización de llamada se pasan directamente entre los puntos extremos. La elección del método a utilizar es de responsabilidad del Gatekeeper.

Ambos métodos utilizan las mismas clases de conexiones para los mismos fines y los mismos mensajes. Los mensajes de admisión son intercambiados en canales RAS con el Gatekeeper, seguidos de un intercambio de mensajes de señalización de llamada en un canal de señalización de llamada.

En el método de señalización de llamada encaminada por el Gatekeeper, el Gatekeeper puede optar por el cierre del canal de señalización de llamada una vez que se haya completado el establecimiento de la comunicación, o puede optar por mantenerlo abierto mientras dure la llamada para soportar los servicios suplementarios. Solamente el Gatekeeper cerrará el canal de señalización de llamada, que no se debería cerrar cuando una Gateway participe en la llamada. Si el Gatekeeper cierra el canal de señalización de llamada, las entidades que participan mantendrán el estado actual de la llamada. El Gatekeeper puede reabrir el canal de señalización de llamada en cualquier momento durante la llamada.

Se puede deducir que el canal de señalización de los equipos estudiados es el encaminado por Gatekeeper dado que toda señalización es enviada y recibida en el CallManager.

#### **5.2.2.3.2. Encaminamiento del canal de control.**

Cuando se utiliza la señalización de llamada encaminada por Gatekeeper, se dispone de dos métodos para encaminar el canal de control H.245. En el primero de ellos, el canal de control H.245 se establece directamente entre los puntos extremos. En el segundo método, el canal de control H.245 es encaminado entre los puntos extremos a través del Gatekeeper. Este método permite al Gatekeeper reencaminar el canal de control H.245 a un MC cuando una conferencia multipunto ad hoc pasa de conferencia punto a punto a conferencia multipunto. El Gatekeeper

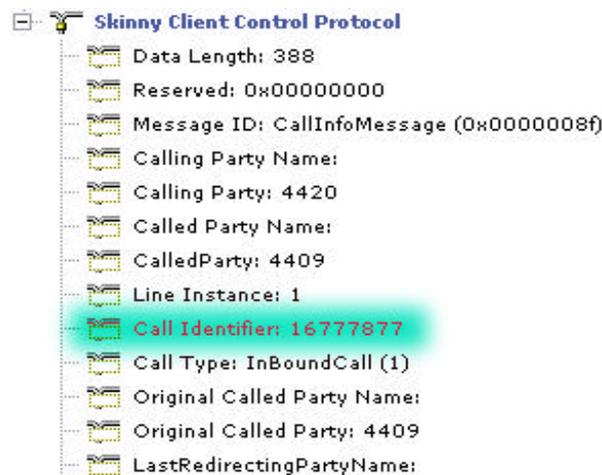
realiza esta elección. Cuando se utiliza la señalización de llamada de punto extremo directa, el canal de control H.245 sólo puede ser conectado directamente entre los puntos extremos.

### 5.2.3. Identificador (ID) de llamada.

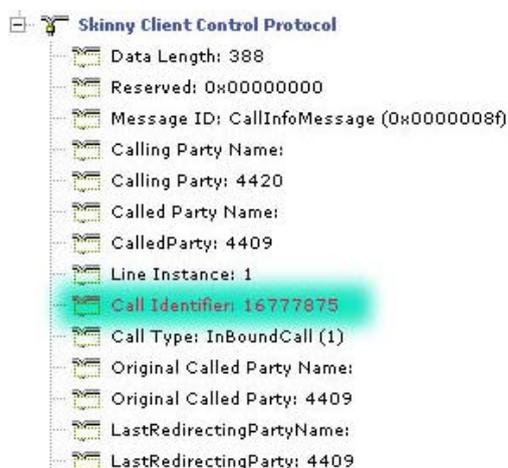
Este es un valor diferente de cero, es único. Este número es creado por el punto extremo llamante. El ID de llamada identifica la llamada con la que está asociado el mensaje. Además se utiliza para asociar todos los mensajes RAS y de señalización de llamada relacionados con la misma llamada. Este número no se altera dentro de una llamada, pero puede verse alterado al volver a realizar una llamada, ver figuras a continuación. Todos los mensajes del punto extremo llamante a su Gatekeeper, del punto extremo llamante al punto extremo llamado, y del punto extremo llamado a su Gatekeeper relativos a la misma llamada contendrán el mismo ID de llamada.

El ID de llamada es analizado en dos llamadas distintas.

...	Source Ad...	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
45	172.16.10.10	172.16.10.28	SKINNY: DisplayPromptStatusM...	110	00:00:31.474.248	00:00:00.000.002	17:17:03.172.734
46	172.16.10.10	172.16.10.28	SKINNY: DisplayPriNotifyMessa...	106	00:00:31.474.251	00:00:00.000.003	17:17:03.172.737
47	172.16.10.10	172.16.10.28	SKINNY: CallInfoMessage	450	00:00:31.474.759	00:00:00.000.508	17:17:03.173.245
48	172.16.10.10	172.16.10.28	SKINNY: SetLampMessage	78	00:00:31.474.762	00:00:00.000.003	17:17:03.173.248
49	172.16.10.10	172.16.10.28	SKINNY: SetRingerMessage	82	00:00:31.474.764	00:00:00.000.002	17:17:03.173.250



▲	Source Ad...	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
10	172.16.10.10	172.16.10.28	SKINNY: DisplayPromptStatu...	110	00:00:04.993.690	00:00:00.000.003	17:15:23.163.905
11	172.16.10.10	172.16.10.28	SKINNY: DisplayPriNotifyMes...	106	00:00:04.993.692	00:00:00.000.002	17:15:23.163.907
12	172.16.10.10	172.16.10.28	SKINNY: CallInfoMessage	450	00:00:04.993.832	00:00:00.000.140	17:15:23.164.047
13	172.16.10.10	172.16.10.28	SKINNY: SetLampMessage	78	00:00:04.994.340	00:00:00.000.508	17:15:23.164.555
14	172.16.10.10	172.16.10.28	SKINNY: SetRingerMessage	82	00:00:04.994.343	00:00:00.000.003	17:15:23.164.558



#### 5.2.4. Capacidad de llamada de un punto extremo .

La capacidad de llamada, señala la capacidad de aceptar que posee un punto extremo para cada uno de los tipos de llamada que el punto extremo soporta (voz, datos, voz, datos T.120, H.320, etc.). Aunque cualquier punto extremo puede comunicar capacidad de llamada a través de varios mensajes H.225.0, los Gateways deben comunicar información de capacidad de llamada al Gatekeeper para ayudar en el encaminamiento de las llamadas, específicamente, en el reparto de carga entre Gateways y en la reducción del número de intentos de llamada fallidos.

La capacidad máxima y actual del punto extremo debe indicarse en el momento del registro.

Además, la capacidad actual puede también indicarse en cada llamada. Para representar esta capacidad dinámica, se desea considerar los modelos de llamada siguientes:

- Modelo de llamada directa con admisión por llamada – En este caso, el punto extremo puede indicar capacidad remanente en los mensajes ARQ, DRQ o BRQ.
- Modelo de llamada directa con admisión previamente concedida. En este caso, el punto extremo puede indicar capacidad en los mensajes RRQ (petición de registro) o RAI (si el punto extremo es un Gateway).
- Modelo de llamada encaminada por el Gatekeeper con admisión por llamada. El punto extremo puede proporcionar información de capacidad en los mensajes ARQ, DRQ, o BRQ.
- Modelo de llamada encaminada por el Gatekeeper con admisión concedida previamente.

El punto extremo puede incluir información de capacidad en los mensajes de señalización de llamada, tales como establecimiento y liberación completa. En este caso, el punto extremo origen

puede proveer su información de capacidad en un mensaje establecimiento, mientras que el punto extremo de terminación puede proporcionar su información de capacidad en los mensajes de aviso o conexión. Cada punto extremo puede entregar información de capacidad actualizada utilizando el mensaje liberación completa.

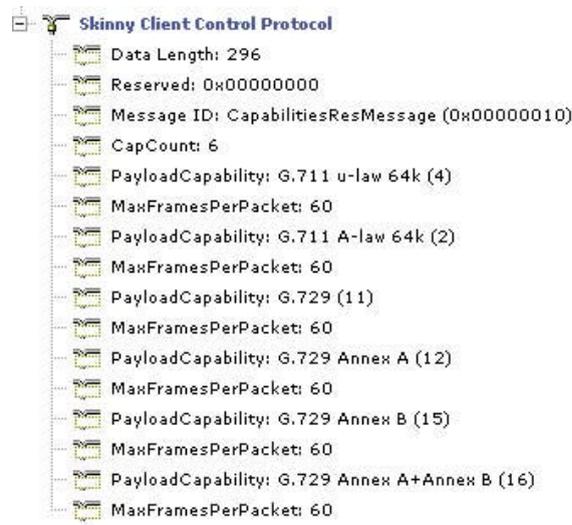
Un punto extremo puede señalar que tiene capacidades diferentes para los distintos protocolos que pueda soportar (T.120, H.320, H.321, voz, etc.).

En las siguientes imágenes el Gatekeeper requiere sus capacidades del punto extremo, este llega en el mensaje siguiente y actualizado antes de entablar una llamada.

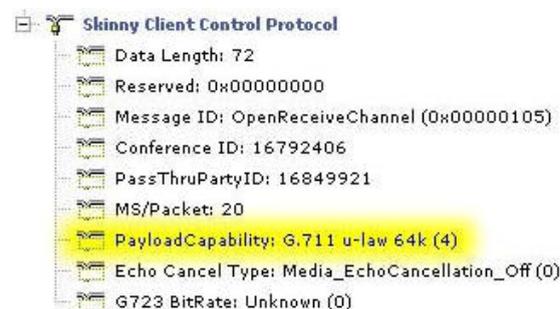
N...	Source Address	Dest Address	Summary	Le...	Rel Time	Delta Time	AbsTime
129	172.16.10.10	172.16.10.20	TCP: 2000 > 14738 [ACK] Seq=738...	64	00:00:13.640.903	00:00:00.000.512	19:35:13.658.005
130	172.16.10.10	172.16.10.20	SKINNY: RegisterAckMessage	90	00:00:13.645.037	00:00:00.004.134	19:35:13.662.139
131	172.16.10.10	172.16.10.20	SKINNY: CapabilitiesReqMessage	70	00:00:13.645.549	00:00:00.000.512	19:35:13.662.651
132	172.16.10.20	172.16.10.10	SKINNY: VersionReqMessage	70	00:00:13.652.978	00:00:00.007.429	19:35:13.670.080
133	172.16.10.10	172.16.10.20	SKINNY: VersionMessage	86	00:00:13.653.569	00:00:00.000.591	19:35:13.670.671



N...	Source Address	Dest Address	Summary	Le...	Rel Time	Delta Time	AbsTime
132	172.16.10.20	172.16.10.10	SKINNY: VersionReqMessage	70	00:00:13.652.978	00:00:00.007.429	19:35:13.670.080
133	172.16.10.10	172.16.10.20	SKINNY: VersionMessage	86	00:00:13.653.569	00:00:00.000.591	19:35:13.670.671
134	172.16.10.20	172.16.10.10	SKINNY: CapabilitiesResMessage	362	00:00:13.655.809	00:00:00.002.240	19:35:13.672.911
135	172.16.10.20	172.16.10.10	SKINNY: ButtonTemplateReqMessage	70	00:00:13.656.619	00:00:00.000.810	19:35:13.673.721
136	172.16.10.10	172.16.10.20	TCP: 2000 > 14738 [ACK] Seq=738...	64	00:00:13.657.137	00:00:00.000.518	19:35:13.674.239



N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
553	Cisco_05:18:00	Broadcast	ARP: Who has 172.16.54.173? Tell 172.1...	64	00:01:05.123.366	00:00:00.015.453	12:07:35.395.777
554	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:01:05.150.840	00:00:00.027.474	12:07:35.423.251
555	172.16.10.10	172.16.10.20	SKINNY: OpenReceiveChannel	138	00:01:05.151.352	00:00:00.000.512	12:07:35.423.763
556	172.16.10.10	172.16.10.20	SKINNY: StartMediaTransmission	154	00:01:05.153.452	00:00:00.002.100	12:07:35.425.863
557	172.16.10.20	172.16.10.10	SKINNY: OpenReceiveChannelAck	86	00:01:05.163.904	00:00:00.010.452	12:07:35.436.315



## 5.2.5. Servicio de presentación y restricción

### 5.2.5.1. Presentación de la dirección de la parte llamante.

La presentación de la parte llamante es una característica que proporciona la dirección alias de la parte llamante a la parte llamada. La dirección de la parte llamante puede ser proporcionada por el punto extremo llamante o por el Gatekeeper en caso de llamadas encaminadas por el Gatekeeper que se originan en la red de paquetes. Cuando la llamada se encamina a través del Gatekeeper al que está registrado el punto extremo llamante, el Gatekeeper puede proporcionar un servicio de supervisión que asegure que la dirección proporcionada es realmente la de la parte llamante. El Gatekeeper puede también proporcionar la dirección de la

parte llamante cuando ésta no proporciona dirección alguna o cuando la parte llamante proporciona una dirección distinta de aquella con la que dicha parte se registró.

Cuando una llamada se origina en la Red de Conmutación de Circuitos y accede a la red de paquetes a través de un Gateway, ésta pasará a la red de paquetes la información del número de la parte llamante que se facilita desde la Red de Conmutación de Circuitos.

En las imágenes que siguen se puede observar la información enviada desde el Gatekeeper al punto extremo analizado, al ser realizada una llamada telefónica, desde fuera de la zona. Se puede apreciar los números de origen y de destino mas no los alias porque los puntos extremos no cuentan con ellos.

N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
382	172.16.10.10	172.16.10.20	SKINNY: DisplayPromptStatusMessage	114	00:00:38.673.200	00:00:00.003.734	19:40:14.719.076
383	172.16.10.10	172.16.10.20	SKINNY: DisplayPriNotifyMessage	110	00:00:38.673.824	00:00:00.000.624	19:40:14.719.700
384	172.16.10.10	172.16.10.20	SKINNY: CallInfoMessage	454	00:00:38.674.335	00:00:00.000.511	19:40:14.720.211
385	172.16.10.10	172.16.10.20	SKINNY: SetLampMessage	82	00:00:38.674.339	00:00:00.000.004	19:40:14.720.215
386	172.16.10.10	172.16.10.20	SKINNY: SetRingerMessage	86	00:00:38.674.846	00:00:00.000.507	19:40:14.720.722



A este servicio se le pueden agregar otros que proporcionan funciones similares estos son de restricción y presentación de la dirección de la parte llamante, de la parte conectada, de la parte llamada (avisada) o de la parte ocupada. Estas corresponden a la restricción o a la entrega de información relacionadas con los extremos de la llamada; que son proporcionados o por el Gatekeeper o por el punto extremo que corresponda.

A continuación los bits que indicas dichas funciones.

▲	Source Ad...	Dest Addr...	Summary	Le...	Rel Time	Delta Time	AbsTime
31	172.16.10.10	172.16.10.28	SKINNY: SelectOrderkeysmessam...	82	00:00:07.531.718	00:00:00.000.512	17:21:02.321.711
32	172.16.10.10	172.16.10.28	SKINNY: DialedNumberMessag...	98	00:00:07.531.737	00:00:00.000.519	17:21:02.322.496
33	172.16.10.10	172.16.10.28	SKINNY: CallStateMessage	90	00:00:07.532.249	00:00:00.000.512	17:21:02.323.008
34	172.16.10.10	172.16.10.28	SKINNY: CallInfoMessage	450	00:00:07.532.251	00:00:00.000.002	17:21:02.323.010
35	172.16.10.10	172.16.10.28	SKINNY: StartToneMessage	82	00:00:07.532.764	00:00:00.000.513	17:21:02.323.523
36	172.16.10.10	172.16.10.28	SKINNY: CallStateMessage	90	00:00:07.532.767	00:00:00.000.003	17:21:02.323.526



### 5.2.6. Mensajes y elementos de información

Los mensajes y elementos de información son los que permiten a los dispositivos H.323 proporcionar los servicios de presentación y restricción de dirección. A saber los mensajes y elementos son denominados: Información de dirección de la parte llamante, Información de dirección de la parte conectada, Información de dirección de la parte llamada (avisada), Información de dirección de la parte ocupada; todos esos mensajes provienen del establecimiento de la llamada, la información de dirección proporcionada puede ser número de la parte llamante,

número llamado, etc., según corresponda al tipo de mensaje, esta puede ser un número telefónico o no teniendo en cada caso procesos alternativos de funcionamiento en el envío de mensajes.

Más adelante, en presentación de la dirección de la parte llamante, se analiza una imagen que también sirve para reflejar este servicio en las opciones Calling Party Name o Called Party Name deberían aparecer –al ser habilitados- los alias cuando no son números telefónicos.

### **5.2.7. Acciones en el punto extremo de terminación.**

Se describen los aspectos de procedimiento necesarios para proporcionar servicios de identificación del llamante en el punto extremo de terminación. Este puede ser como el Gateway o el terminal o MCU como punto extremo de terminación.

En el primer caso se trata de un Gateway de la Red Conmutada que recibe un mensaje de establecimiento de la red de paquetes, copiará la información del IE (elemento de información) número de la parte llamante del mensaje establecimiento al formato de señalización soportado por la Red de Conmutación de Circuitos. Si el IE número de la parte llamante no está presente en el mensaje establecimiento, el Gateway formará dicho IE utilizando otro campo del mensaje que sea considerado un tipo de alias de número telefónico.

El Gateway enviará un mensaje conexión a la red de paquetes en el que el IE número conectado tiene la misma información que existía en el formato de señalización soportado en la red telefónica. En el caso de que en el Gateway reciba un mensaje conexión procedente de la RDSI, la información de la parte conectada reside en el IE número conectado.

En el caso de que un terminal o una MCU reciba un mensaje establecimiento debe respetar el indicador de presentación cuando se presente al usuario la información del llamante.

En caso de encaminamiento por el Gatekeeper, el Gatekeeper de la parte que responde puede añadir esta información si no está presente o si es incorrecta y el Gatekeeper de la parte llamante puede suprimir la información de dirección de la parte que responde si ello es pertinente.

### **5.2.8. Acciones en un Gatekeeper:**

En los casos de encaminamiento por Gatekeeper, éste puede proporcionar información de identificación o puede proporcionar un servicio de supervisión. Los servicios que puede proporcionar un Gatekeeper dependen del tipo de punto extremo servido.

Con el Gateway como punto extremo de origen el Gatekeeper no debe modificar la información del mensaje de establecimiento, se considera que la red telefónica ha proporcionado información correcta.

En el caso de un terminal o una MCU sea el extremo de origen, el Gatekeeper puede proporcionar información de la parte llamante cuando esta no es un Gateway. El Gatekeeper puede proporcionar la dirección de la parte llamante bajo diferentes circunstancias -si es proporcionada o no, si es correcta o no lo es, si el Gatekeeper proporciona una distinta- en cada caso se fijará un indicador de supervisión específico para cada situación

En los casos con un Gateway como punto extremo de terminación, un Gatekeeper no debería modificar la información del mensaje conexión enviada desde una Gateway. Se considera que la red telefónica ha proporcionado información correcta.

En los casos que un terminal o una MCU como punto extremo de terminación, el Gatekeeper puede proporcionar información de la parte conectada, avisada u ocupada cuando la parte conectada, avisada u ocupada no es de una Gateway. El Gatekeeper puede proporcionar la dirección de la parte conectada (la parte avisada u ocupada) si la parte conectada (la parte avisada u ocupada) no proporcionó una o si el Gatekeeper determina que la dirección no es correcta; en este caso se fijaran indicadores de supervisión específicos.

### **5.3. PROCEDIMIENTOS DE SEÑALIZACIÓN DE LA LLAMADA.**

La comunicación se efectúa siguiendo los pasos que a continuación se indican:

- Fase A: Establecimiento de la comunicación.
- Fase B: Comunicación inicial e intercambio de capacidad.
- Fase C: Establecimiento de comunicación audiovisual.
- Fase D: Servicios de la llamada.
- Fase E: Terminación de la llamada.

### **5.3.1. Fase A – Establecimiento de la llamada.**

El establecimiento de la comunicación se efectúa utilizando los mensajes de control de llamada definidos en la Rec. UIT-T H.225.0, de acuerdo con los procedimientos de control de llamada.

Si se especifican la dirección alias y la dirección de transporte, se preferirá la dirección alias.

No hay ninguna sincronización explícita ni enganche entre dos puntos extremos durante el procedimiento de establecimiento de la comunicación. Esto significa que el punto extremo **A** puede enviar un mensaje establecimiento al punto extremo **B** exactamente al mismo tiempo que el punto extremo **B** envía un mensaje establecimiento al punto extremo **A**. Corresponde a la aplicación de terminal determinar si sólo se desea una llamada y ejercer la acción apropiada. Esta acción puede ser para un punto extremo indicar que está ocupado siempre que tiene un mensaje establecimiento pendiente. Si un punto extremo puede soportar más de una llamada simultánea, debe indicar que está ocupado siempre que recibe un mensaje establecimiento del mismo punto extremo con el cual tiene un mensaje establecimiento pendiente.

Un punto extremo será capaz de enviar el mensaje aviso. Aviso tiene el significado de que la parte llamada (usuario) ha sido avisada de una llamada entrante. En el caso de interfuncionamiento a través de un Gateway, el Gateway enviará aviso cuando reciba una indicación de llamada de la Red de Conmutación de Circuitos. Si un punto extremo puede responder a un mensaje establecimiento con un mensaje conexión, llamada en curso, o liberación completa en el plazo de 4 segundos, no es necesario enviar el mensaje aviso. Un punto extremo que envía el mensaje establecimiento puede esperar recibir un mensaje aviso, conexión, llamada en curso o liberación completa en un plazo de 4 segundos después de su transmisión con éxito.

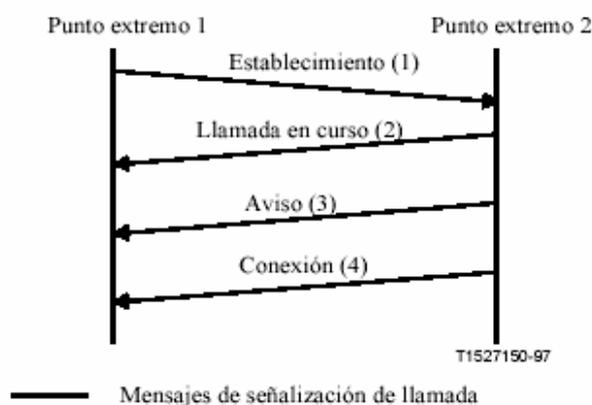
El mensaje conexión debe enviarse sólo si se está seguro de que el intercambio de capacidades H.245 concluirá con éxito y puede existir un nivel mínimo de comunicaciones, con el objeto de mantener la coherencia del significado del mensaje conexión entre redes por paquetes y redes con conmutación de circuitos.

Dentro del establecimiento de llamada existen diferentes posibilidades, por ejemplo que los extremos no estén registrados, ambos puntos extremos registrados en el mismo Gatekeeper,

solo el extremo llamante tenga Gatekeeper, sólo el extremo llamado tenga Gatekeeper, ambos controladores de acceso estén registrados en Gatekeeper diferentes.

#### 5.3.1.1. Ningún punto extremo está registrado en un Gatekeeper.

Cuando ninguno de los puntos extremos está registrado en un Gatekeeper. Los dos puntos extremos comunican directamente. El punto extremo 1 (punto extremo llamante) envía el mensaje establecimiento (1) al canal de señalización de llamada conocido del punto extremo 2. El punto extremo 2 responde con el mensaje conexión (4) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.

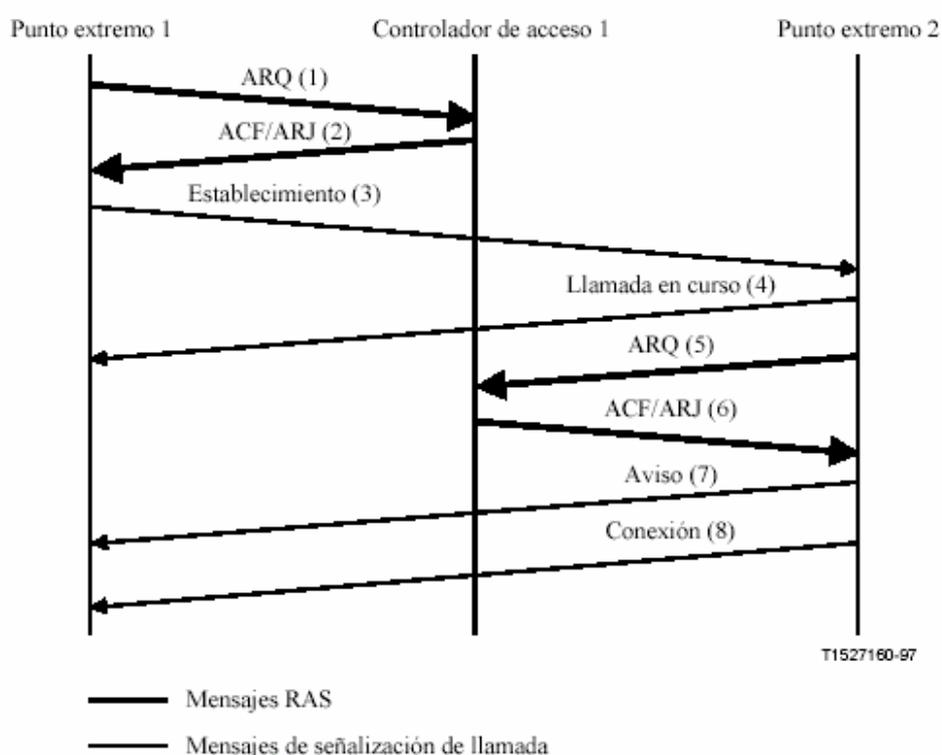


#### 5.3.1.2. Ambos puntos están registrados en el mismo Gatekeeper.

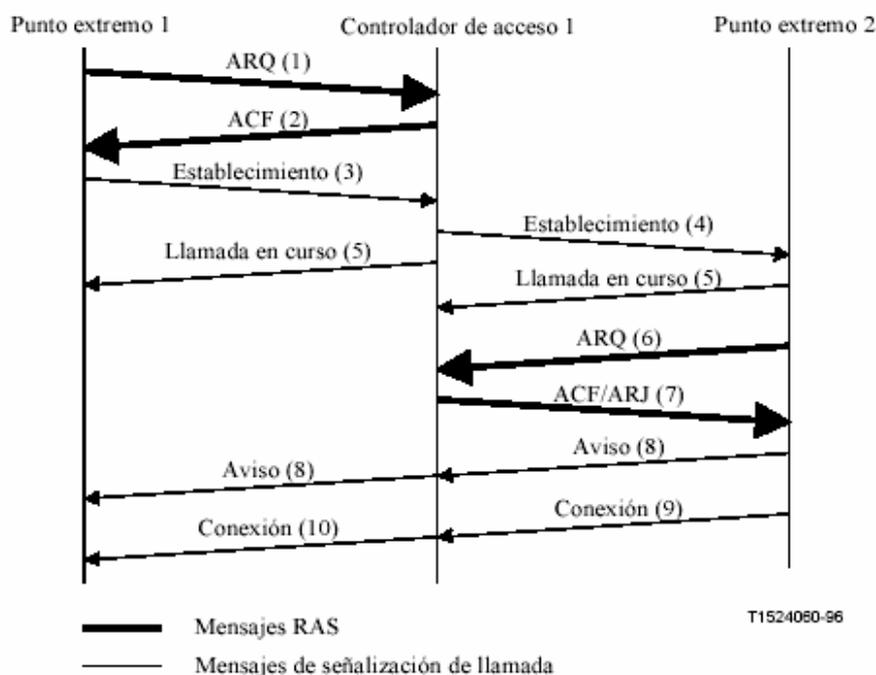
Cuando ambos puntos extremos están registrados en el mismo Gatekeeper; existen dos opciones una que el Gatekeeper ha optado por señalización de llamada directa y la otra que la llamada sea encaminada por el Gatekeeper.

Mediante señalización de llamada directa, el punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ -petición de admisión- (1)/ACF -confirmación de admisión- (2) con ese Gatekeeper. El Gatekeeper devolverá la dirección de transporte de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF. El punto extremo 1 envía entonces el mensaje establecimiento (3) al punto extremo 2 utilizando esa dirección de transporte. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (5)/ACF (6) con el Gatekeeper. Es posible que el punto extremo 2 reciba un ARJ -rechazo de admisión-. (6) en cuyo caso envía el mensaje liberación completa al punto extremo 1. El punto extremo 2 responde con

el mensaje conexión (8) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.



Por el método de señalización encaminada por el Gatekeeper, el punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper. El Gatekeeper devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF. El punto extremo 1 envía entonces el mensaje establecimiento (3) utilizando esa dirección de transporte. El Gatekeeper envía a continuación el mensaje establecimiento (4) al punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (6)/ACF (7) con el Gatekeeper. Es posible que el punto extremo 2 reciba un ARJ (7), en cuyo caso envía el mensaje liberación completa al Gatekeeper. El punto extremo 2 responde con el mensaje conexión (9) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper envía al punto extremo 1 el mensaje conexión (10) que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de Gatekeeper, dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245.

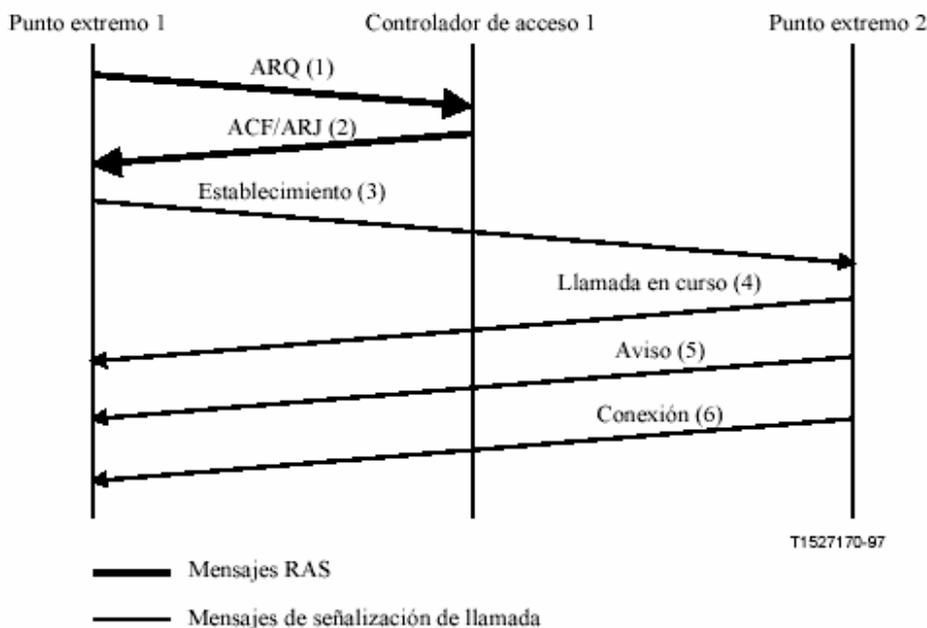


### 5.3.1.3. Solamente un punto extremo posee Gatekeeper.

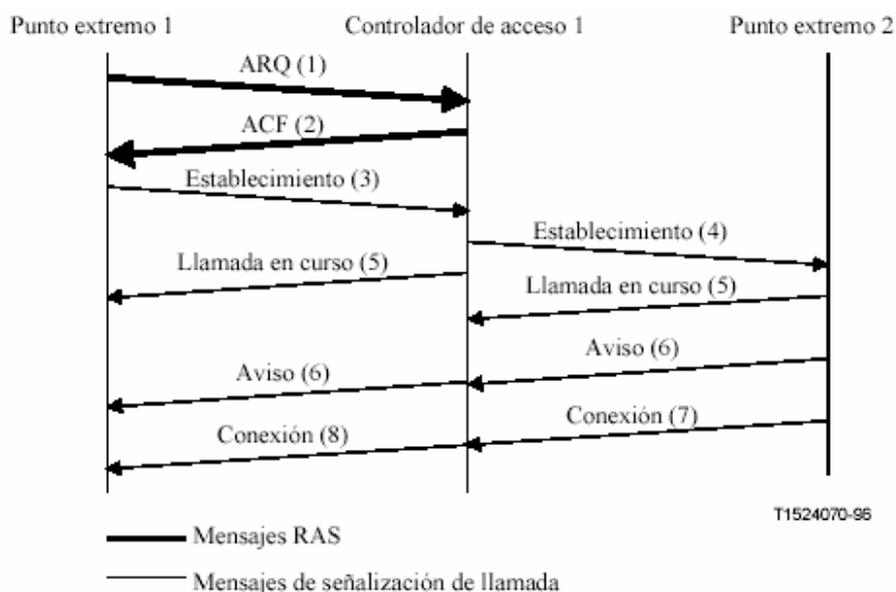
#### 5.3.1.3.1. Punto extremo llamante cuenta con Gatekeeper.

Cuando sólo un punto extremo llamante tiene Gatekeeper, existen dos alternativas de señalización la señalización de llamada directa y la señalización por encaminamiento por Gatekeeper.

En la primera situación el punto extremo 1 (punto extremo llamante) está registrado en un Gatekeeper, el punto extremo 2 (punto extremo llamado) no está registrado en un Gatekeeper y el Gatekeeper ha optado por señalización de llamada directa. El punto extremo 1 inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper. El punto extremo 1 envía entonces el mensaje establecimiento (3) al punto extremo 2 utilizando la dirección de transporte de canal de señalización de llamada conocida. Si el punto extremo 2 desea aceptar la llamada, responde con el mensaje conexión (6) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.



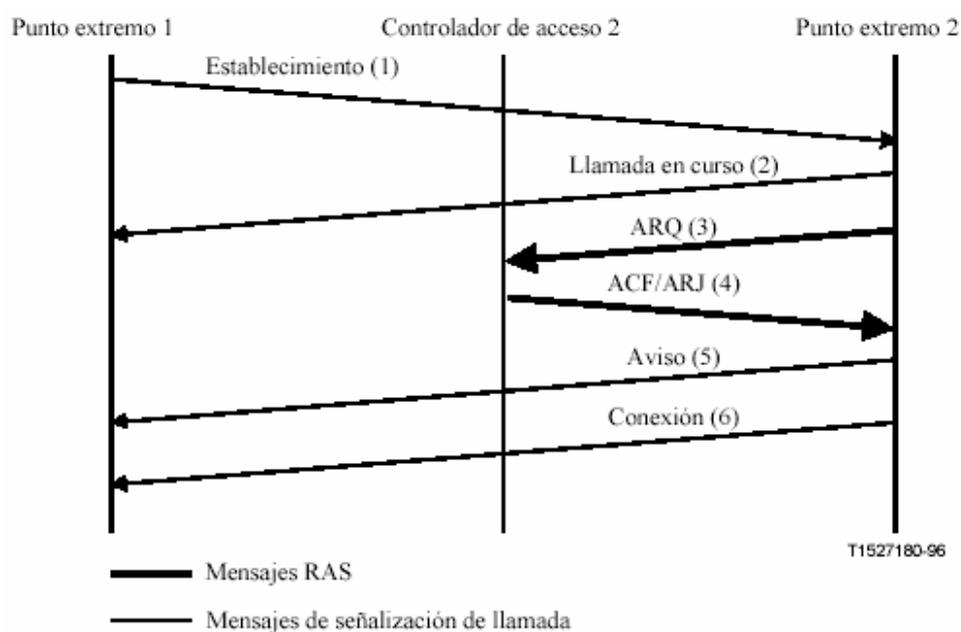
En el segundo caso en donde el punto extremo 1 (punto extremo llamante) está registrado en un Gatekeeper, el punto extremo 2 (punto extremo llamado) no está registrado en un Gatekeeper y el Gatekeeper ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con ese Gatekeeper. El Gatekeeper devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje establecimiento (3) utilizando esa dirección de transporte. El Gatekeeper envía a continuación el mensaje establecimiento (4) a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, responde con el mensaje conexión (7) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper envía el mensaje conexión (8) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de Gatekeeper, dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245.



#### 5.3.1.3.2. Punto extremo llamado cuenta con Gatekeeper.

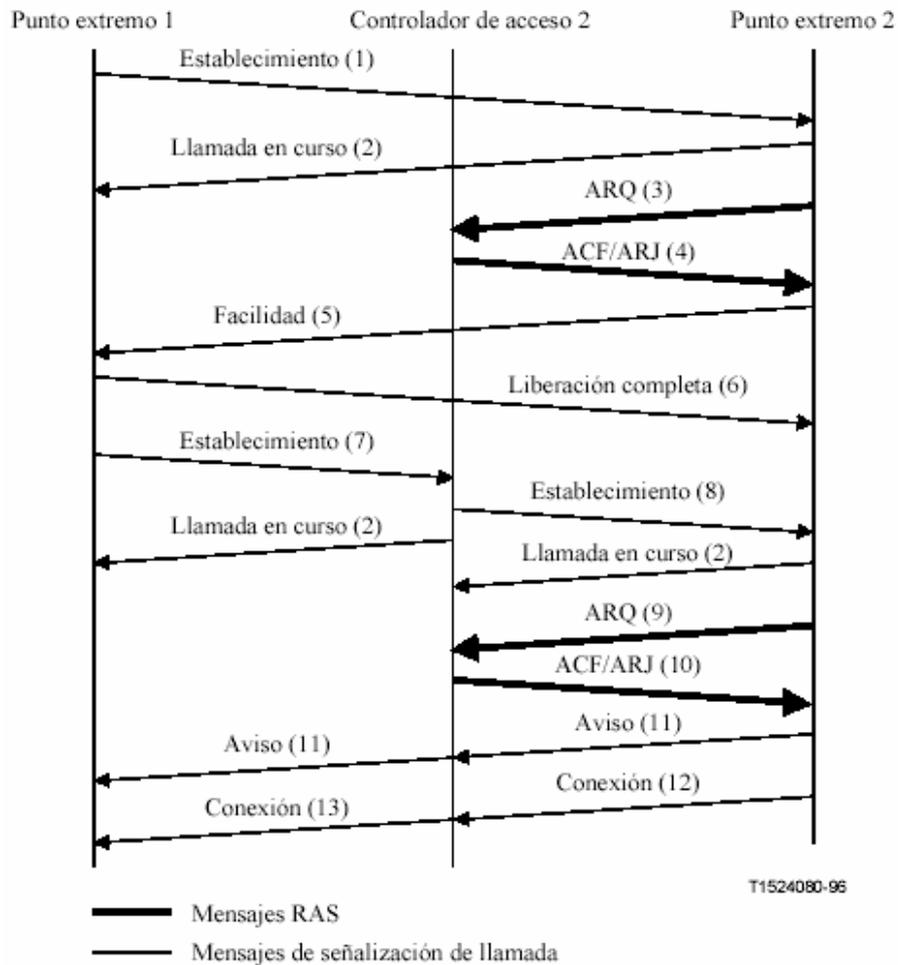
Si sólo el punto extremo llamado tiene Gatekeeper, aparece dos alternativas una es señalización de llamada directa y la otra es señalización de llamada por encaminamiento por el Gatekeeper

Si el punto extremo 1 (punto extremo llamante) no está registrado en un Gatekeeper, el punto extremo 2 (punto extremo llamado) está registrado en un Gatekeeper y el Gatekeeper ha optado por la señalización de llamada directo. El punto extremo 1 envía el mensaje establecimiento (1) al punto extremo 2 utilizando la dirección de transporte de canal de señalización de llamada conocida. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (3)/ACF (4) con el Gatekeeper. Es posible que el punto extremo 2 reciba un ARJ (4), en cuyo caso envía un mensaje liberación completa al punto extremo 1. El punto extremo 2 responde con el mensaje conexión (6) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.



En el caso de que el punto extremo 1 (punto extremo llamante) no está registrado en un Gatekeeper, el punto extremo 2 (punto extremo llamado) está registrado en un Gatekeeper y el Gatekeeper ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) envía un mensaje establecimiento (1) a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (3)/ACF (4) con el Gatekeeper. Si es aceptable, el Gatekeeper devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (4) con un código de causa de encaminamiento de llamada a Gatekeeper. El punto extremo 2 responde al punto extremo 1 con un mensaje facilidad (5) que contiene la dirección de transporte de señalización de llamada de su Gatekeeper. El punto extremo 1 envía entonces el mensaje liberación completa (6) al punto extremo 2. El punto extremo 1 responde con un mensaje establecimiento (7) a la dirección de transporte de canal de señalización de llamada del Gatekeeper. El Gatekeeper envía el mensaje establecimiento (8) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (9)/ACF (10) con ese Gatekeeper. El punto extremo 2 responde después con el mensaje conexión (12) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper envía el mensaje conexión (13) al punto extremo 1 que puede contener la dirección de transporte de canal de

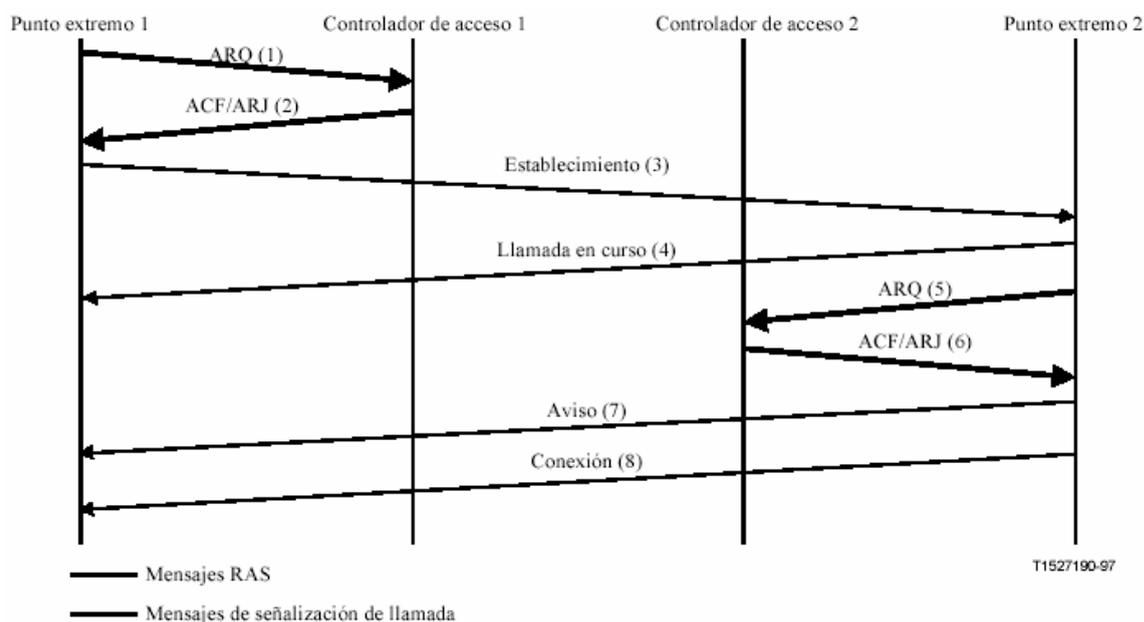
control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 de Gatekeeper dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245.



### 5.3.1.3.3. Ambos puntos extremos están registrados pero en diferentes Gatekeeper.

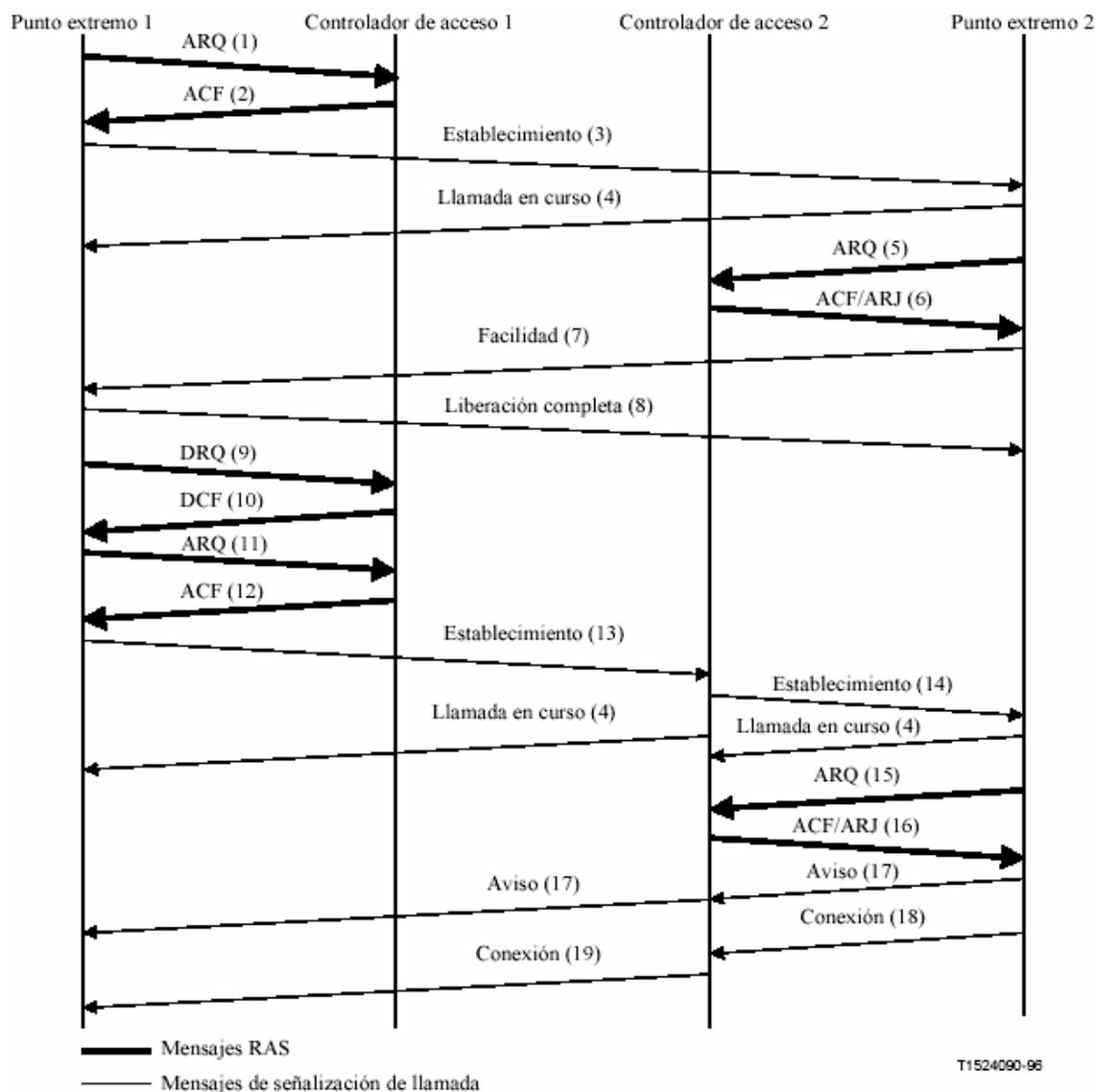
Si sucede que ambos extremos estén registrados Gatekeeper diferentes son cuatro las alternativas en el establecimiento de la llamada estas corresponden a: señalización de llamada directa en ambos Gatekeeper, señalización de llamada directa por parte del Gatekeeper de origen y encaminada en el segundo Gatekeeper, señalización de llamada encaminada por el primer Gatekeeper y directa por el Gatekeeper de destino, y por ultimo señalización de llamada encaminada en ambos Gatekeeper.

En este primer caso, ambos puntos extremos están registrados en controladores de acceso diferentes y ambos controladores de acceso han optado por la señalización de llamada directa. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper 1. El Gatekeeper 1 puede devolver la dirección de transporte de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF si el Gatekeeper 1 tiene una manera de comunicar con el Gatekeeper 2. El punto extremo 1 envía entonces el mensaje establecimiento (3) bien a la dirección de transporte devuelta por el Gatekeeper (si está disponible) o bien a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia un intercambio ARQ (5)/ACF (6) con el Gatekeeper 2. Es posible que el punto extremo 2 reciba un ARJ (6), en cuyo caso envía un mensaje liberación completa al punto extremo 1. El punto extremo 2 responde con el mensaje conexión (8) que contiene una dirección de transporte de canal de control H.245 para su utilización en la señalización H.245.



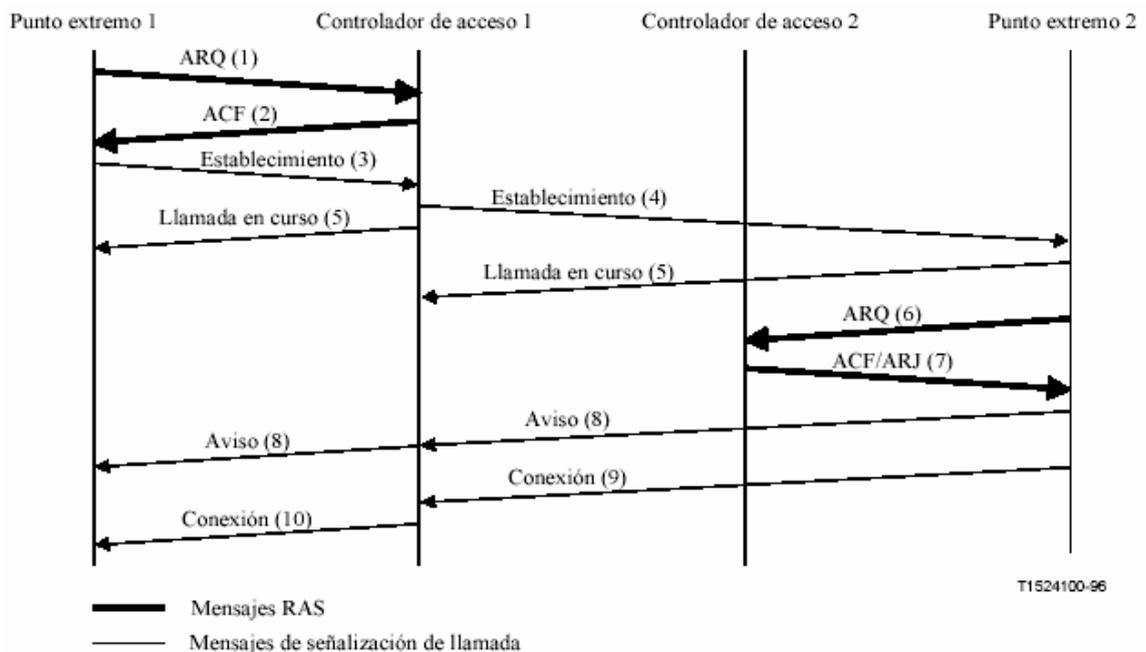
En la segunda alternativa, ambos puntos extremos están registrados en diferentes controladores de acceso, el Gatekeeper del punto extremo llamante ha optado por la señalización de llamada directa y el Gatekeeper del punto extremo llamado ha optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper 1. El Gatekeeper 1 puede devolver la dirección de transporte

de canal de señalización de llamada del punto extremo 2 (punto extremo llamado) en la ACF (2) si el Gatekeeper 1 tiene una manera de comunicar con el Gatekeeper 2. El punto extremo 1 envía entonces el mensaje establecimiento (3) bien a la dirección de transporte devuelta por el Gatekeeper (si está disponible) o bien a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (5)/ACF (6) con el Gatekeeper 2. Si es aceptable, el Gatekeeper 2 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (6) con un código de causa relacionado con el camino de la llamada al Gatekeeper. El punto extremo 2 responde al punto extremo 1 con un mensaje facilidad (7) que contiene la dirección de transporte de señalización de llamada del Gatekeeper 2. El punto extremo 1 envía entonces el mensaje liberación completa (8) al punto extremo 2. El punto extremo 1 enviará DRQ (9) al Gatekeeper 1 que responde con DCF (10). El punto extremo 1 inicia después un nuevo intercambio de ARQ (11)/ACF (12) con el Gatekeeper 1. El punto extremo 1 envía un mensaje establecimiento (13) a la dirección de transporte de canal de señalización de llamada del Gatekeeper. El Gatekeeper 2 envía el mensaje establecimiento (14) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (15)/ACF (16) con el Gatekeeper 2. El punto extremo 2 responde después con el mensaje conexión (18) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper 2 envía el mensaje conexión (19) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del Gatekeeper 2, dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245.



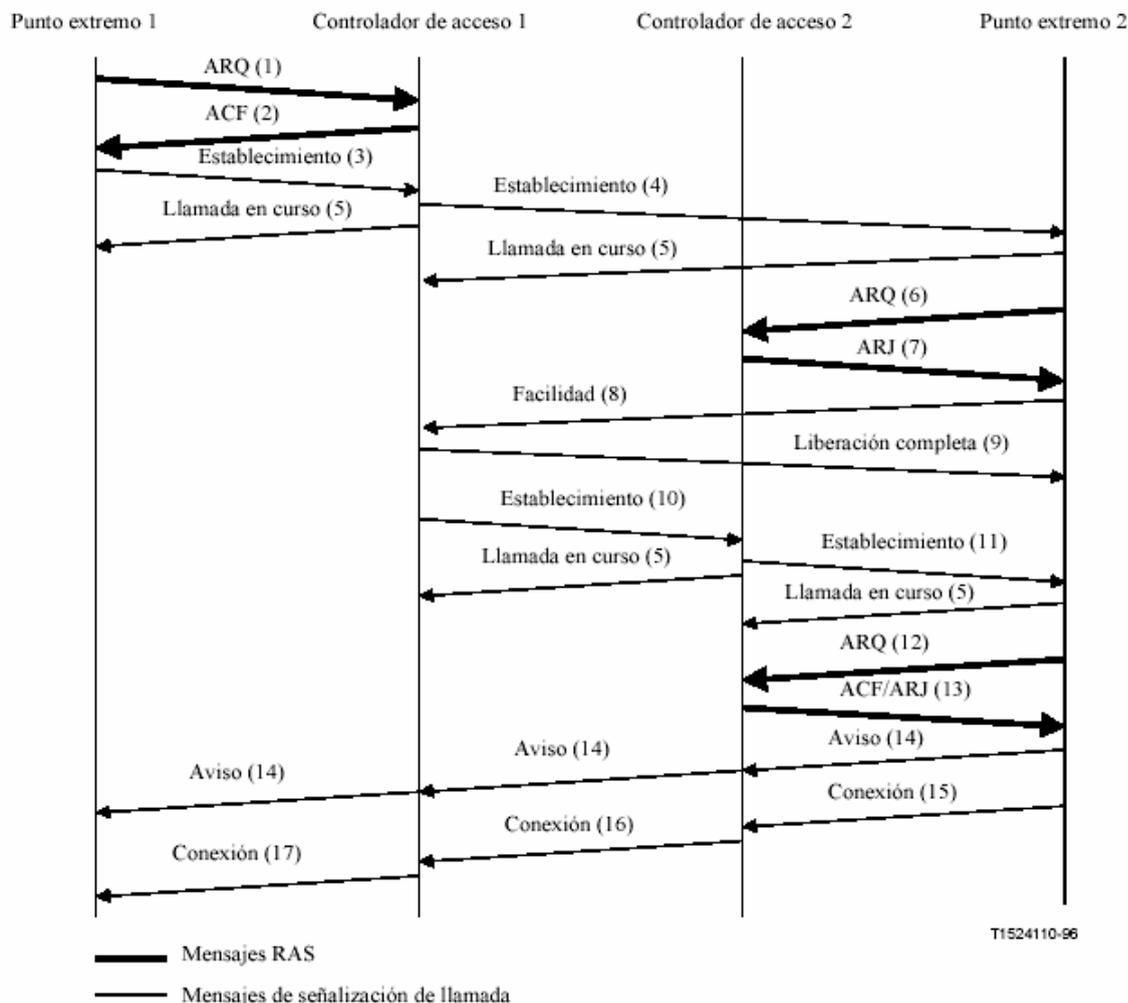
En esta tercera posibilidad, ambos puntos extremos están registrados en controladores de acceso diferentes, el Gatekeeper del punto extremo llamante ha optado por encaminar la señalización de la llamada y el Gatekeeper del punto extremo llamado ha optado por la señalización de llamada directa. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper 1. El Gatekeeper 1 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje establecimiento (3) utilizando esa dirección de transporte. El Gatekeeper 1 envía entonces el mensaje establecimiento (4) que contiene su dirección de

transporte de canal de señalización de llamada a la dirección de transporte de canal de señalización de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (6)/ACF (7) con el Gatekeeper 2. Es posible que el punto extremo 2 reciba un ARJ (7), en cuyo caso envía un mensaje liberación completa al punto extremo 1. El punto extremo 2 responde al Gatekeeper 1 con el mensaje conexión (9) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper 1 envía el mensaje conexión (10) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del Gatekeeper 1, dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245.



Por ultimo, cuando ambos puntos extremos están registrados en controladores de acceso diferentes y ambos controladores de acceso han optado por encaminar la señalización de la llamada. El punto extremo 1 (punto extremo llamante) inicia el intercambio ARQ (1)/ACF (2) con el Gatekeeper 1. El Gatekeeper 1 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en la ACF (2). El punto extremo 1 envía entonces el mensaje establecimiento (3) utilizando esa dirección de transporte. El Gatekeeper 1 envía a continuación el mensaje establecimiento (4) a la dirección de transporte de canal de señalización

de llamada conocida del punto extremo 2. Si el punto extremo 2 desea aceptar la llamada, inicia el intercambio ARQ (6)/ACF (7) con el Gatekeeper 2. Si es aceptable, el Gatekeeper 2 devolverá una dirección de transporte de canal de señalización de llamada de él mismo en ARJ (7) con un código de causa de encaminamiento de llamada a Gatekeeper. El punto extremo 2 responde al Gatekeeper 1 con un mensaje facilidad (8) que contiene la dirección de transporte de señalización de llamada del Gatekeeper 2. El Gatekeeper 1 envía después el mensaje liberación completa (9) al punto extremo 2. El Gatekeeper 1 envía un mensaje establecimiento (10) a la dirección de transporte de canal de señalización de llamada del Gatekeeper 2. El Gatekeeper 2 envía el mensaje establecimiento (11) al punto extremo 2. El punto extremo 2 inicia el intercambio de ARQ (12)/ACF (13) con el Gatekeeper 2. El punto extremo 2 responde después al Gatekeeper 2 con el mensaje conexión (15) que contiene su dirección de transporte de canal de control H.245 para su utilización en la señalización H.245. El Gatekeeper 2 envía el mensaje conexión (16) al Gatekeeper 1 que puede contener la dirección de transporte de canal de control H.245 del punto extremo 2 o una dirección de transporte de canal de control H.245 del Gatekeeper 2, dependiendo de si el Gatekeeper decide encaminar o no el canal de control H.245. El Gatekeeper 1 envía el mensaje conexión (17) al punto extremo 1 que puede contener la dirección de transporte de canal de control H.245 enviada por el Gatekeeper 2 o una dirección de transporte de canal de control H.245 del Gatekeeper 1, dependiendo de si el Gatekeeper 1 decide encaminar o no el canal de control H.245.



#### 5.3.1.4. Establecimiento de una comunicación a través de Gateways.

##### 5.3.1.4.1. Establecimiento de comunicación entrante a través de Gateway.

Cuando un terminal externo llama a un punto extremo de red a través del Gateway, el establecimiento de la comunicación entre el Gateway y el punto extremo de red se produce de la misma manera que el establecimiento de llamada de punto extremo a punto extremo. Es posible que el Gateway tenga que emitir mensajes llamada en curso al terminal externo mientras establece la llamada en la red.

Una Gateway que no pueda encaminar directamente una llamada de la Red de Conmutación de Circuitos entrante a un punto extremo H.323 deberá ser capaz de aceptar la marcación en dos etapas, por ejemplo la marcación de un primer número para alcanzar el

Gateway y un segundo número –el real- para acceder al punto extremo a llamar. En el caso de Gateways hacia terminales sólo vocales, el Gateway aceptará números DTMF del terminal sólo vocal. Estos números indicarán un número de marcación de segunda etapa para acceder al punto extremo individual en la red.

#### **5.3.1.4.2. Establecimiento de comunicación saliente a través de Gateway.**

Cuando un punto extremo de red llama a un terminal externo a través del Gateway, el establecimiento de la comunicación entre el punto extremo de red y el Gateway se produce de la misma manera que el establecimiento de comunicación de punto extremo a punto extremo. El Gateway recibirá la información de numeración de destino en el mensaje establecimiento. A continuación utilizará esa dirección para efectuar la llamada saliente. El Gateway puede devolver mensajes llamada en curso al punto extremo de red mientras establece la comunicación saliente.

Existirá un elemento de información indicador de progreso se utiliza para indicar que se está produciendo el interfuncionamiento entre redes. El Gateway emitirá un elemento de información indicador de progreso dentro de los mensajes aviso, llamada en curso o conexión. Esta información también puede ser enviada en un mensaje progreso.

El punto extremo de red enviará todas las direcciones de numeración que está llamando en el mensaje establecimiento. El fallo de la llamada en la Red de Conmutación de Circuitos se notificará al punto extremo de red en el mensaje liberación completa.

#### **5.3.1.5.Reenvío de llamada.**

Un punto extremo que desea reenviar una llamada a otro punto extremo puede utilizar un mensaje facilidad indicando la dirección de transporte del nuevo punto extremo. El punto extremo receptor de esa indicación de facilidad debe enviar un mensaje liberación completa y recomenzar después los procedimientos de la fase A con el nuevo punto extremo.

### **5.3.2. Fase B – Comunicación inicial e intercambio de capacidad**

Una vez que ambos lados han intercambiado los mensajes de establecimiento de llamada de la fase A, los puntos extremos, si proyectan emplear H.245, establecerán el canal de control H.245. Se utilizan los procedimientos de la Rec. UIT-T H.245 en el canal de control H.245 para el intercambio de capacidad y la apertura de canales de medios.

Los puntos extremos soportarán el procedimiento de intercambio de capacidades H.245, como se describe a continuación.

Las capacidades de recepción y transmisión serán separadas también existirá un método mediante el cual el terminal puede describir su aptitud para funcionar con diversas combinaciones de modos simultáneamente.

Las capacidades de recepción describen la posibilidad que tiene el terminal de recibir y procesar trenes de información entrantes. Los transmisores limitarán el contenido de la información que transmiten a lo que el receptor haya indicado que es capaz de recibir. La ausencia de una capacidad de recepción indica que el terminal no puede recibir (es transmisor solamente).

Las capacidades de transmisión describen la posibilidad que tiene el terminal de transmitir trenes de información. Las capacidades de transmisión sirven para ofrecer a los receptores la elección entre posibles modos de funcionamiento, de manera que el receptor pueda pedir el modo en el que prefiere recibir. La ausencia de una capacidad de transmisión indica que el terminal no ofrece la elección del modo preferido al receptor (pero puede aún transmitir cualquier cosa que se halle dentro de la capacidad del receptor).

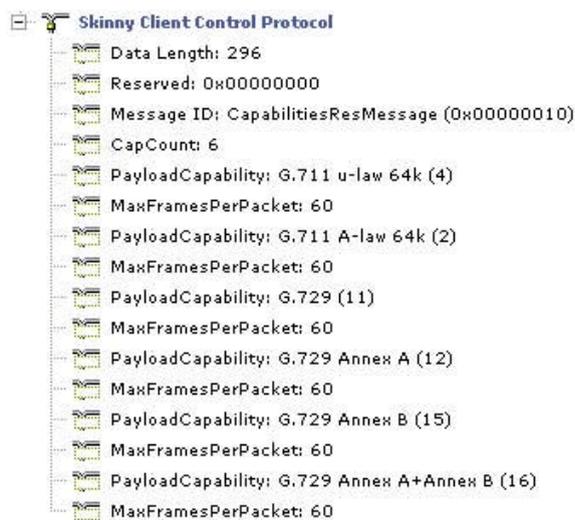
Las capacidades de recepción y transmisión describen la posibilidad que tiene el terminal de recibir y transmitir trenes de información cuando esas capacidades no son independientes y hace falta que sean las mismas en ambos sentidos.

Como podemos observar en la siguiente imagen, las capacidades son requeridas por el Gatekeeper al ser registrado el punto extremo, y al establecer una llamada el Gatekeeper envía un mensaje con las capacidades del punto extremo llamante al punto extremo H.323.

N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
171	172.16.10.10	172.16.10.20	TCP: 2000 > 3481 [ACK] Seq=33455061...	64	00:00:40.224.629	00:00:00.000.524	12:07:10.497.040
172	172.16.10.10	172.16.10.20	SKINNY: RegisterAckMessage	90	00:00:40.228.353	00:00:00.003.724	12:07:10.500.764
173	172.16.10.10	172.16.10.20	SKINNY: CapabilitiesReqMessage	70	00:00:40.228.863	00:00:00.000.510	12:07:10.501.274
174	172.16.10.20	172.16.10.10	SKINNY: VersionReqMessage	70	00:00:40.235.777	00:00:00.006.914	12:07:10.508.188
175	172.16.10.10	172.16.10.20	SKINNY: VersionMessage	86	00:00:40.237.458	00:00:00.001.681	12:07:10.509.869



N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
174	172.16.10.20	172.16.10.10	SKINNY: VersionReqMessage	70	00:00:40.235.777	00:00:00.006.914	12:07:10.508.188
175	172.16.10.10	172.16.10.20	SKINNY: VersionMessage	86	00:00:40.237.458	00:00:00.001.681	12:07:10.509.869
176	172.16.10.20	172.16.10.10	SKINNY: CapabilitiesResMessage	362	00:00:40.238.711	00:00:00.001.253	12:07:10.511.122
177	172.16.10.20	172.16.10.10	SKINNY: ButtonTemplateReqMessage	70	00:00:40.239.516	00:00:00.000.805	12:07:10.511.927
178	172.16.10.10	172.16.10.20	TCP: 2000 > 3481 [ACK] Seq=33455062...	64	00:00:40.240.022	00:00:00.000.506	12:07:10.512.433
179	172.16.10.20	172.16.10.10	SKINNY: IpPortMessage	74	00:00:40.244.234	00:00:00.004.212	12:07:10.516.645



N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
553	Cisco_05:18:00	Broadcast	ARP: Who has 172.16.54.173? Tell 172.1...	64	00:01:05.123.366	00:00:00.015.453	12:07:35.395.777
554	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:01:05.150.840	00:00:00.027.474	12:07:35.423.251
555	172.16.10.10	172.16.10.20	SKINNY: OpenReceiveChannel	138	00:01:05.151.352	00:00:00.000.512	12:07:35.423.763
556	172.16.10.10	172.16.10.20	SKINNY: StartMediaTransmission	154	00:01:05.153.452	00:00:00.002.100	12:07:35.425.863
557	172.16.10.20	172.16.10.10	SKINNY: OpenReceiveChannelAck	86	00:01:05.163.904	00:00:00.010.452	12:07:35.436.315



N...	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
554	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:01:05.150.840	00:00:00.027.474	12:07:35.423.251
555	172.16.10.10	172.16.10.20	SKINNY: OpenReceiveChannel	138	00:01:05.151.352	00:00:00.000.512	12:07:35.423.763
556	172.16.10.10	172.16.10.20	SKINNY: StartMediaTransmission	154	00:01:05.153.452	00:00:00.002.100	12:07:35.425.863
557	172.16.10.20	172.16.10.10	SKINNY: OpenReceiveChannelAck	86	00:01:05.163.904	00:00:00.010.452	12:07:35.436.315
558	Cisco_dcr61:c7	Broadcast	ARP: Who has 172.16.10.20? Tell 172.16...	64	00:01:05.187.620	00:00:00.023.716	12:07:35.460.031



Las capacidades de los sistemas de punto extremo se intercambian mediante la transmisión un mensaje H.245. Si antes de la terminación satisfactoria de intercambio de capacidad terminal, cualquier otro procedimiento presenta un fallo (es decir, rechazado, no comprendido, no soportado) el punto extremo de origen se ha de iniciar y completar satisfactoriamente el intercambio de capacidad terminal antes de intentar cualquier otro procedimiento.

Tras la compleción satisfactoria de los requisitos de la fase B, los puntos extremos pasarán directamente al modo de funcionamiento deseado, normalmente a la fase C.

### 5.3.3. Fase C – Establecimiento de comunicación audiovisual

Después del intercambio de capacidades, se utilizarán los procedimientos de la Rec. UIT-T H.245 para abrir canales lógicos para los diversos trenes de información. Los trenes de audio y vídeo, que se transmiten por los canales lógicos establecidos en la Rec. H.245, se transportan utilizando un protocolo no fiable (véase UIT-T H.225.0). Las comunicaciones de datos, que se transmiten por los canales lógicos establecidos en H.245, se transportan utilizando un protocolo fiable (véase la Rec. UIT-T H.225.0).

Esto se puede analizar en las imágenes anteriores en donde abre los canales de recepción y da inicio a la transmisión.

A	Source Addr...	Dest Address	Summary	Le...	Rel Time	Delta Time	AbsTime
450	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:00:48.529.258	00:00:00.018.407	19:40:24.575.134
451	172.16.10.10	172.16.10.20	SKINNY: CallStateMessage	94	00:00:48.529.783	00:00:00.000.525	19:40:24.575.659
452	172.16.10.10	172.16.10.20	SKINNY: SelectSoftKeysMessage	86	00:00:48.529.788	00:00:00.000.005	19:40:24.575.664
453	172.16.10.10	172.16.10.20	SKINNY: DisplayPromptStatusMessage	114	00:00:48.529.790	00:00:00.000.002	19:40:24.575.666
454	172.16.10.10	172.16.10.20	SKINNY: CallInfoMessage	454	00:00:48.530.298	00:00:00.000.508	19:40:24.576.174
455	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:00:48.575.029	00:00:00.044.731	19:40:24.620.905
456	172.16.10.10	172.16.10.20	SKINNY: OpenReceiveChannel	138	00:00:48.575.542	00:00:00.000.513	19:40:24.621.418
457	172.16.10.10	172.16.10.20	SKINNY: StartMediaTransmission	154	00:00:48.578.062	00:00:00.002.520	19:40:24.623.938
458	172.16.10.20	172.16.10.10	SKINNY: OpenReceiveChannelAck	86	00:00:48.587.680	00:00:00.009.618	19:40:24.633.556
459	Cisco_94:ff:7d	Broadcast	ARP: Who has 172.16.10.1? Tell 172.16.10.20	64	00:00:48.614.815	00:00:00.027.135	19:40:24.660.691
460	Cisco_dc:61:c7	Cisco_94:ff:7d	ARP: 172.16.10.1 is at 00:0f:90:dc:61:c7	64	00:00:48.615.336	00:00:00.000.521	19:40:24.661.212
461	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:48.619.543	00:00:00.004.207	19:40:24.665.419
462	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:48.623.469	00:00:00.003.926	19:40:24.669.345
463	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:48.634.505	00:00:00.011.036	19:40:24.680.381
464	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:48.639.507	00:00:00.005.002	19:40:24.685.383
465	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:48.654.748	00:00:00.015.241	19:40:24.700.624
466	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:48.659.474	00:00:00.004.726	19:40:24.705.350
467	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:48.674.756	00:00:00.015.282	19:40:24.720.632

### 5.3.4. Fase D – Servicios de la llamada.

#### 5.3.4.1. Cambios de l ancho de banda.

El ancho de banda de la llamada la establece y aprueba inicialmente el Gatekeeper, durante el intercambio de admisiones. Un punto extremo deberá asegurar que la suma correspondiente a todos los canales transmitidos y recibidos de audio y de vídeo excluidos cualesquiera encabezamientos RTP, encabezamientos de cabida útil RTP, encabezamientos de red y otra tara, se halla dentro de ese ancho de banda. Los canales de datos y de control no se incluyen en ese límite.

En cualquier momento durante una conferencia, los puntos extremos o el Gatekeeper pueden solicitar un aumento o una disminución del ancho de banda de la llamada. Un punto extremo puede cambiar la velocidad binaria de un canal lógico sin solicitar un cambio del ancho de banda por el Gatekeeper si la suma de las velocidades binarias de todos los canales transmitidos y recibidos no supera al ancho de banda de llamada existente. Si el cambio da lugar a una velocidad binaria agregada que supera al ancho de banda de llamada existente, el punto extremo deberá pedir a su Gatekeeper un cambio de ancho de banda de la llamada y esperar la confirmación antes de aumentar efectivamente cualquier velocidad binaria. Se recomienda pedir un cambio de ancho de banda cuando un punto extremo utilice un ancho de banda reducida durante un periodo de tiempo prolongado, liberando así ancho de banda para otras llamadas.

### 5.3.4.2.Estado.

Para determinar si un punto extremo se ha desconectado o ha pasado a un modo fallo, el controlador de acceso puede utilizar la secuencia de mensajes de petición de información (IRQ, information request) o de respuesta a petición de información (IRR, information request response) (Rec. UIT-T H.225.0), a fin de sondear secuencialmente los puntos extremos con un intervalo establecido por el fabricante.

Mientras dura una llamada, el punto extremo o el Gatekeeper pueden indagar periódicamente el estado de aquélla desde otro punto extremo. El punto extremo o el controlador de acceso solicitante emiten un mensaje indagación de estado. El punto extremo receptor del mensaje indagación de estado responderá con un mensaje estado indicando el estado en que en esos momentos se encuentra la llamada. Este procedimiento puede ser utilizado por el controlador de acceso para verificar periódicamente si una llamada sigue estando activa. Los puntos extremos podrán aceptar cualesquiera valores de estado válidos recibidos en el mensaje estado, incluidos los que no pueden ser capaces de introducir. Adviértase que se trata de un mensaje H.225.0 enviado por el canal de señalización de llamada y no debe confundirse con un mensaje IRR, que es un mensaje RAS enviado por el canal RAS.

▲	Source Ad...	Dest Address	Summary	Len...	Rel Time	Delta Time	AbsTime
2267	172.16.10.20	172.16.9.2	UDP: Source port: 16386 Destination port: 17660	218	00:01:47.551.177	00:00:00.001.868	12:08:17.823.588
2268	172.16.9.2	172.16.10.20	UDP: Source port: 17660 Destination port: 16386	218	00:01:47.569.354	00:00:00.018.177	12:08:17.841.765
2269	172.16.10.10	172.16.10.20	SKINNY: CallStateMessage	94	00:01:47.570.557	00:00:00.001.203	12:08:17.842.968
2270	172.16.10.10	172.16.10.20	SKINNY: SelectSoftKeysMessage	86	00:01:47.571.063	00:00:00.000.506	12:08:17.843.474
2271	172.16.10.10	172.16.10.20	SKINNY: DisplayPromptStatusMessage	114	00:01:47.571.194	00:00:00.000.131	12:08:17.843.605



### 5.3.4.3.Servicios suplementarios.

El soporte de los servicios suplementarios es opcional. Las Recomendaciones de la serie H.450 describen un método de proveer servicios suplementarios en el entorno H.323.

### 5.3.5. Fase E – Terminación de la llamada.

Cualquiera de los puntos extremos puede terminar una llamada. La terminación de la llamada se realizará mediante el procedimiento siguiente:

- 1) Interrumpir la transmisión de vídeo al final de una imagen completa y a continuación cerrar todos los canales lógicos de vídeo.
- 2) Interrumpir la transmisión de datos y a continuación cerrar todos los canales lógicos de datos.
- 3) Interrumpir la transmisión de audio y a continuación cerrar todos los canales lógicos de audio.
- 4) Transmitir el mensaje instrucción finalizar sesión H.245 por el canal de control H.245, indicando al extremo distante que desea desconectarse de la llamada, interrumpiendo entonces la transmisión de mensajes H.245.
- 5) Esperar recibir el mensaje finalizar sesión del otro punto extremo y cerrar el canal de control H.245.
- 6) Si el canal de señalización de llamada está abierto, se enviará un mensaje liberación completa y se cerrará el canal de control H.245.
- 7) Liberar la llamada utilizando los procedimientos que se indican más adelante.

Un punto extremo que reciba una instrucción finalizar sesión sin haberla transmitido primero, realizará los pasos 1) a 7) anteriores, con la salvedad de que en el paso 5) esperará el mensaje instrucción finalizar sesión procedente del primer punto extremo.

La terminación de una llamada puede no terminar una conferencia; una conferencia puede ser terminada explícitamente utilizando un mensaje H.245 (abandono de conferencia). En este caso, los puntos extremos esperarán que el MC termine la llamada como se describe anteriormente.

#### **5.3.5.1.Liberación de la llamada sin un Gatekeeper.**

En las redes que no contienen un Gatekeeper, después de los pasos 1) a 6) anteriores se termina la llamada. No se requiere ninguna acción posterior.

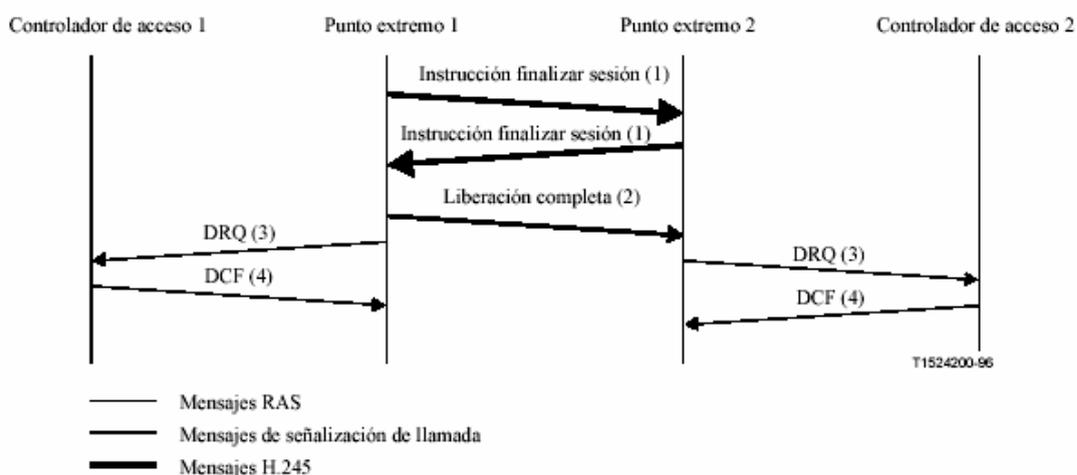
#### **5.3.5.2.Liberación de la llamada con un Gatekeeper.**

En las redes que contienen un Gatekeeper, no es preciso que el Gatekeeper esté al tanto de la liberación de ancho de banda. Después de ejecutar los pasos 1) a 6), cada punto extremo transmitirá un mensaje de petición de desligamiento (DRQ, disengage request) (3) H.225.0 a su Gatekeeper. El Gatekeeper responderá con un mensaje de confirmación de desligamiento (DCF,

disengage confirm) (4). Después de enviar el mensaje DRQ, los puntos extremos no enviarán más mensajes IRR no solicitados al Gatekeeper.

En este punto la llamada está terminada. La figura muestra el modelo de llamada directa, se sigue un procedimiento similar para el modelo encaminado por el Gatekeeper.

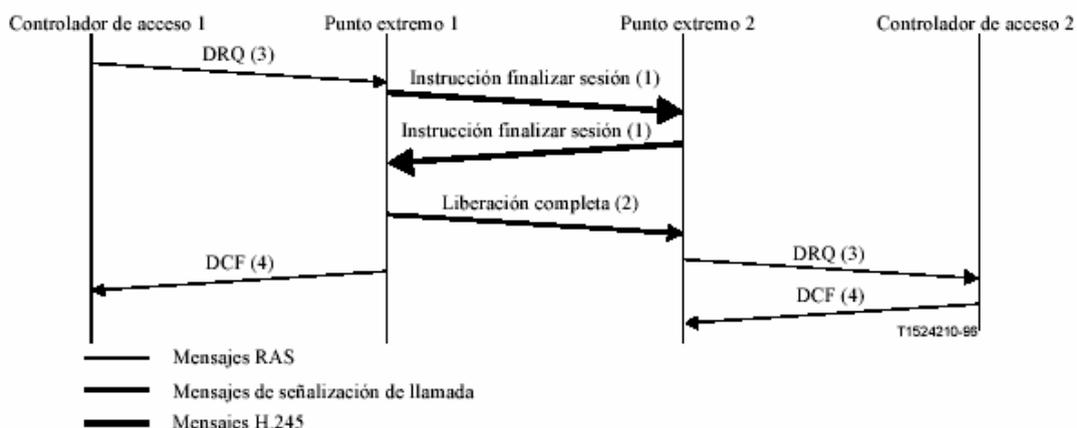
Los mensajes DRQ y DCF serán enviados por el canal RAS.



### 5.3.5.3. Liberación de la llamada por el Gatekeeper.

El Gatekeeper puede terminar cualquier conferencia enviando un DRQ a un punto extremo. El punto extremo seguirá inmediatamente los pasos 1) a 6) anteriores y responderá a continuación al Gatekeeper con un DCF. El otro punto extremo, al recibir la el comando de finalización de sesión seguirá el procedimiento descrito más arriba. En el modelo de llamada directa; se sigue un procedimiento similar para el modelo encaminado por el controlador de acceso.

Si la conferencia es una conferencia multipunto, el Gatekeeper debe enviar un DRQ a cada punto extremo de la conferencia, para cerrar toda la conferencia.



NOTA – El controlador de acceso 1 y el controlador de acceso 2 pueden ser el mismo controlador de acceso.

En el caso estudiado la liberación de llamada comprende una serie de mensajes de o para el Gatekeeper. Comienza con un mensaje evento de teclado, con el código **EndCall**, después un cierre del canal de recepción y una finalización de la transmisión tal como aparece detallado más abajo.

▲	Source Addr...	Dest Address	Summary	Le...	Rel Time	Delta Time	AbsTime
1020	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:53.849.404	00:00:00.009.603	19:40:29.895.280
1023	172.16.10.20	172.16.10.10	SKINNY: SoftKeyEventMessage	82	00:00:53.859.594	00:00:00.006.788	19:40:29.905.470
1024	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:53.860.108	00:00:00.000.514	19:40:29.905.984
1025	172.16.10.20	172.16.9.2	UDP: Source port: 16384 Destination port: 19384	218	00:00:53.869.858	00:00:00.009.750	19:40:29.915.734
1026	172.16.10.10	172.16.10.20	SKINNY: StopToneMessage	78	00:00:53.871.049	00:00:00.001.191	19:40:29.916.925
1027	172.16.10.10	172.16.10.20	SKINNY: SetLampMessage	82	00:00:53.878.302	00:00:00.007.253	19:40:29.924.178
1028	172.16.10.10	172.16.10.20	SKINNY: ClearPromptStatusMessage	78	00:00:53.879.342	00:00:00.001.040	19:40:29.925.218
1029	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:53.879.884	00:00:00.000.542	19:40:29.925.760
1030	172.16.10.10	172.16.10.20	SKINNY: CloseReceiveChannel	82	00:00:53.880.657	00:00:00.000.773	19:40:29.926.533
1031	172.16.10.10	172.16.10.20	SKINNY: StopMediaTransmission	82	00:00:53.882.184	00:00:00.001.527	19:40:29.928.060
1032	172.16.10.10	172.16.10.20	SKINNY: CallStateMessage	94	00:00:53.883.574	00:00:00.001.390	19:40:29.929.450
1033	172.16.10.10	172.16.10.20	SKINNY: SelectSoftKeysMessage	86	00:00:53.886.205	00:00:00.002.631	19:40:29.932.081
1034	172.16.10.10	172.16.10.20	SKINNY: DefineTimeDate	106	00:00:53.892.942	00:00:00.006.737	19:40:29.938.818
1035	172.16.10.10	172.16.10.20	SKINNY: SetSpeakerModeMessage	74	00:00:53.893.945	00:00:00.001.003	19:40:29.939.821
1036	172.16.10.10	172.16.10.20	SKINNY: SetRingerMessage	86	00:00:53.895.760	00:00:00.001.815	19:40:29.941.636
1037	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:53.899.865	00:00:00.004.105	19:40:29.945.741
1038	172.16.9.2	172.16.10.20	UDP: Source port: 19384 Destination port: 16384	218	00:00:53.919.845	00:00:00.019.980	19:40:29.965.721
1039	172.16.9.2	172.16.10.20	UDP: Source port: 19385 Destination port: 16385	114	00:00:53.934.831	00:00:00.014.986	19:40:29.980.707
1040	200.2.114.142	200.2.114.1...	NBNS: Name query NB GRUPO_TRABAJO<1b>	96	00:00:54.020.771	00:00:00.085.940	19:40:30.066.647





### 5.3.6. Tratamiento de fallo de protocolo.

El protocolo fiable subyacente del canal de control H.245 realiza el esfuerzo necesario para entregar o recibir datos por el canal antes de notificar un fallo de protocolo. Por consiguiente, si se notifica un fallo de protocolo en el canal, se deberán cerrar el canal de control H.245 y todos los canales lógicos asociados. Para ello se seguirán los procedimientos de la fase E, como si el otro punto extremo hubiera emitido el comando de finalización de sesión H.245. Esto incluye la transmisión del mensaje DRQ (petición de desligamiento) al Gatekeeper y la terminación del canal de señalización de llamada. Si el Gatekeeper detecta el fallo, tratará de restablecer el canal de control de llamada. Esto significa que el punto extremo tendrá siempre la posibilidad de establecer un canal en su dirección de transporte de canal de señalización de llamada.

Después del restablecimiento del canal de señalización de llamada, el Gatekeeper puede enviar un mensaje estado preguntando cuál es el estado de la llamada del extremo distante, para asegurarse de que están en sincronismo.

Si el punto extremo detecta el fallo, puede optar por terminar la llamada como se describe en la fase E, o intentar el restablecimiento del canal de señalización de llamada como se ha descrito más arriba.

Si durante una llamada un punto extremo desea saber si el otro punto extremo está todavía conectado y funcionando, puede enviar el mensaje de petición de retardo de ida y vuelta H.245. Puesto que el transporte del canal de control H.245 se realiza un canal fiable, esto dará lugar a una respuesta proveniente del otro punto extremo o a un error de la interfaz de transporte. En este último caso se utilizarán los procedimientos descritos anteriormente.

## 6. CAPÍTULO VI. CONCLUSIONES.

Recordar que el objetivo del presente trabajo es realizar un análisis de los principios y teoría que rigen en la integración de redes de voz sobre circuitos conmutados con redes de voz paquetizadas, además de los protocolos que se utilicen en ambos medios.

De este análisis se concluye:

La señalización, como tal, está presente en ambas redes. En la red telefónica conmutada la Señalización por Canal Común N° 7 está cada vez más extendida por la razón que puede proveer de voz y datos; este tipo de señalización también es capaz de proveer soporte a nuevas tecnologías de información. En la red IP existen varios métodos de señalización dependiendo del transporte de los datos. En ambas redes los datos transmitidos están en forma digital.

En telefonía IP existen varias normas, protocolos o recomendaciones, dentro de ella la UIT-T H.323, extensa recomendación base que abarca desde elementos mínimos hasta el desarrollo de posibles nuevas aplicaciones, incluye además de la transmisión de voz, la transmisión de datos y video. La recomendación UIT-T H.323, también describe la forma de enlazar una llamada de dos extremos, pertenezcan o no a la misma zona H.323.

La interacción entre las dos redes crea algunas dificultades. Una de ellas aparece con los datos de señalización; por ejemplo, al intentar realizar una llamada desde un extremo ubicado en la Red de Telefonía Pública hacia un terminal situado dentro de la Red IP, debe existir una entidad que sea capaz de entender y reflejar los diversos, al menos los básicos, datos de señalización con el objetivo de poder realizar una llamada. Este problema se soluciona empleando un Gateway, o Pasarela, que es un elemento que enlaza dos redes –a modo de ejemplo un Gateway es un elemento que por un lado tienen una interfaz Ethernet y por el otro una interfaz RDSI–, además realiza algunas aplicaciones de interfuncionamiento en ambas redes, por él pasan todos los datos. Otro equipo que se pudo observar su uso fue el Gatekeeper, o controlador de acceso, cuya función principal es de facilitar la traducción de direcciones y controlar el acceso a la red, el Gatekeeper conversa con el Gateway para realizar una llamada, y para configurarlo si corresponde; aun siendo un elemento opcional dentro de una red de Telefonía IP si está presente todos los demás elementos deben hacer uso de él.

Dentro de la denominación de Gateway también se incluye el ATA, Analog Telephonic Adaptator, un equipo que permite la utilización de teléfono y/o fax corrientes, dentro de una zona H.323 (soporta múltiples protocolo VoIP). El Gateway refleja las señales que genera el teléfono,

descolgar, marcar un número, colgar; y emular en el auricular las señales que vendrían de una central telefónica, como son: tono de ocupado, el ring, tono de marcar, etc., toda esta información está codificada y a cada acción le corresponde un código que interpretado y enviado hacia el elemento que corresponda o viene hacia el Gateway que descifra y genera en el teléfono los tonos asociados a cada señal.

Este estudio puede dejar desafíos, como en crear o implementar un elemento de monitoreo y control de llamadas telefónicas dentro de la Red IP que existe en la Universidad, si bien en la recomendación incluye un aparatado relativo a tarificación y la información del Gatekeeper, esto se podría lograr capturando los paquetes de información que se genera desde el Gatekeeper hacia los puntos extremos y asociándolos. Otro reto, que sigue al anterior, ¿Cuál es la forma más conveniente de cobrar el tráfico de llamadas de Telefonía IP, por tiempo como en la telefonía tradicional, por ancho de banda como los ISP o por volumen de información?

## **ANEXO. CISCO CallManager.**

### **HOJA de DATOS**

#### **VISTA GENERAL de PRODUCTO**

El Cisco® CallManager Express es una solución encajada en Software Cisco IO® que proporciona procesamiento de llamada para teléfonos IP de Cisco. Esta solución permite al gran portafolio de routers de acceso Cisco para entregar las características de telefonía que son utilizadas comúnmente por usuarios de negocio para encontrar los requerimientos de la oficina de pequeño o mediano tamaño. CallManager Express permite la implementación de un rentable, altamente segura, solución de Comunicaciones IP utilizando un solo router del acceso Cisco.

Los clientes ahora pueden escalar telefonía IP en una pequeña o mediana oficina con una solución que es muy sencilla de implementar, administrar, y mantener. El Cisco CallManager Express la solución que mejor conviene para clientes que buscan una solución de bajo costo, segura y rico en características de telefonía hasta 240 usuarios.

#### **Elementos claves y beneficios**

La telefonía de IP experimenta actualmente un crecimiento tremendo, acelerado por características de valor agregado de acceso y aplicaciones que sólo telefonía IP puede proporcionar al usuario final. Adicionalmente, los beneficios del costo de hacer converger voz, video, y datos en una sola red entregan la rápida aceptación de esta tecnología. Porque se integra en un router, la solución Cisco CallManager Express aumenta las ventajas de convergencia ofreciendo los beneficios extraordinarios siguientes:

- Las rentables operaciones por una sola plataforma integrada de la voz y datos para todas las necesidades – routers de acceso altamente seguros tales como el Cisco 1700, 2600XM, y 3700 plataformas de la serie ya proveídos en la industria- dirigir las características, inclusive robusta calidad del servicio (QoS), seguridad de red, la codificación, el firewall, y módulos de red que entregan el contenido de trabajo de red y los servicios habilitados de VPN para dirigir las necesidades de negocio de una pequeña sucursal. Ahora estos routers pueden entregar también telefonía IP integrada, buzón de voz, y asistente automatizado. Esto permite a clientes para implementar un dispositivo para dirigir todas sus necesidades de negocio, simplificando la administración, el

mantenimiento, y las operaciones, y entregar un costo total más bajo al propietario (TCO). La próxima generación 2800 y 3800 series integradas atienden a routers aumentan la solución CallManager Express entregando características avanzadas tal como la terminación integrada de la voz, transcoding, V3PN y seguridad de voz.

- El robusto conjunto de sistema clave comúnmente utilizado y bajo – el final de las capacidades de la PBX -pequeñas oficinas tienen volúmenes diferentes de trabajo y requieren las características especializadas para sostener sus prácticas de trabajo. Cisco CallManager Express entrega un conjunto robusto de características de telefonía para la pequeña oficina, y entrega las capacidades extraordinarias del valor agregado por el lenguaje (XML) eso aumenta la productividad del usuario final y del negocio, eso no puede ser entregado por soluciones tradicionales.
- La interoperabilidad con Cisco Callmanager –los clientes de puede implementar Cisco CallManager en sitios más grande e implementar y Cisco CallManager Express en sucursales donde procesamiento local de llamada se requiere. Utilizando H.323 las llamadas de larga distancia se pueden dirigir sobre la red WAN con party number y el número.
- La protección de la inversión y la facilita de actualizaciones centraliza las soluciones del procesamiento de llamada – realizando un sencillo cambio de configuración en el software en el router, un sistema con Cisco CallManager Express puede ser convertido un robusto Gateway de voz para un sitio remoto en una arquitectura centralizada implementación de Cisco CallManager. Esta flexibilidad ayuda a asegurar completamente la protección de la inversión a negocios exitosos que quizás crezcan más que la capacidad de sistema.
- El mantenimiento remoto y la localización de fallas en la interfase de línea de comando de Cisco IO Software (CLI) o la Interfaz gráfica (GUI) basada en Web– los clientes

tienen la opción de utilizar el Software estándar industrial de Cisco IOS CLI o GUI fácil de manejar para configurar y administrar Cisco CallManager Express.

- Cisco CallManager Express permite a un router de acceso de Cisco proporcionar el procesamiento de llamada IP conectado localmente y teléfonos analógicos. Todos los archivos y las configuraciones necesarios para teléfonos IP se almacenan internamente en el router, así que no es necesario ninguna base de datos ni el servidor de archivos externos. Además, la solución ofrece un conjunto robusto para la interfase a la red telefónica pública conmutada (PSTN), un amplio surtido de interfaces WAN, buzón de voz integrado y asistente automatizado, y una lista repleta de teléfono. El Cisco IO Software ofrece un conjunto robusto de características de dirección industrial de voz diseñadas para sistemas basados en telefonía IP, tal como señalización H.323, QoS avanzado, e interworking con un Gatekeeper H.323, todo disponible para el uso con implementaciones Cisco CallManager Express. Además, las funciones integradas tales como el canal de servicio unidad/digital unidad de servicio (CSU/DSU) y la Terminación de Red 1 (NT1) dispositivos disponibles en las tarjetas interfaz PSTN para proporcionar los servicios flexibles y robustos de la voz.

### **Soporte de Telefonía IP**

Mientras el Cisco CallManager Express es típicamente conveniente para menos de 200 usuarios, a un máximo de 240 teléfonos IP se puede soportada a través de una elección de plataformas con CallManager Express. La operación del teléfono IP es semejante a la comodidad de usar Cisco CallManager el fácil entrenamiento de usuario debe emigrar clientes a Cisco CallManager como ellos crecen más que la solución Cisco CallManager Express. Los números máximos de teléfonos contenidos en cada plataforma CallManager Express 3,2 son listados en la Tabla 1.

**Tabla 1. El soporte de Teléfono IP por la Plataforma**

Plataforma	El máximo de teléfonos
Cisco IAD 2430 Serie integró dispositivos de acceso	24
Cisco 2801 Integrado Atienden a Router, Routers de 1760 V y de 1751 V de Acceso	24
Cisco 2811 Integrado Atienden a Router, 261xXM y Routers de Acceso de Serie 262xXM	36
Cisco 2821 Integrado Atienden a Router, Router de Acceso 265xXM	48
Cisco 2691 Conseguir acceso a Router	72
Cisco 2851 Integrado Atienden a Router	72*/96**
Cisco 3725 Conseguir acceso a Router	96*/144**
Cisco 3745 Conseguir acceso a Router	120*/192**
Cisco 3825 Integrado Atienden a Router	168
Cisco 3845 Integrado Atienden a Router	240

\* Disponible con versión IO 12.3 (8) T4-August 2004

\*\* Disponible con versión de IO 12.3 (11) T-September 2004

**Figura 1. Familia de Teléfono de Cisco IP**



Cisco CallManager Express soporta los Teléfonos IP 7902G, 7905G, 7912G, 7910G, 7914 Módulo de Expansión, Teléfono IP inalámbricos 7920, Teléfono IP Color 7970, Estación de Conferencia IP 7936, 7940G, y 7960G. Estos teléfonos inteligentes IP Cisco de próxima generación, (Figura 2) soportan las siguientes características:

- El visor se basó las características con la facilidad de utilizar softkeys.
- Localización de Idioma y personalización de característica junto con apoyo para aplicaciones basadas en XML.
- El Cisco Power Over Ethernet del Switch Catalyst de Cisco, Módulos de Red Cisco EtherSwitch® o tarjetas interfaz WAN de alta velocidad disponibles en los routers de las series Cisco 2800, 3700 y 3800.

### **Características del producto**

Cisco CallManager Express proporciona un conjunto repleto del sistema clave, utilizado y común y características de telefonía PBX especialmente diseñado para la ubicación pequeña y media oficina o sucursal. Proporciona también varias características industriales extraordinarias que no están disponibles de otras soluciones tradicionales de telefonía. Actualmente, las características siguientes (Tabla 2) están disponibles con Cisco CallManager Express la Versión 3,2, consulta por favor con un navegador las características en <http://www.cisco.com> para última versión de IOS.

**Tabla 2. Características CallManager Express 3,2.**

Las características teléfono.	Máximo de 240 teléfonos por sistema, hasta 34 línea de apariencias por teléfono, la funcionalidad atención de consola utiliza 7914, transferencia rápida ciega o consulta, bussy lamp, opciones de alarma silenciosa, la selección Automática de línea para llamadas hacia afuera, redireccionador de llamada por No respuesta/ Ocupado/ Ningún/ Todas, todas el control de las restricciones del redireccionador de llamada, No Molestar (DND), características de ring con DND, el Display de teléfono IP del estado de DND, Desvío Llamadas dirigidas a
-------------------------------	--

	<p>VM, Personalización de softkeys, Activa/desactiva llamada espera notificación por línea, espera de llamada con cobertura DN, ring llamada en espera, apariencias dual de línea por botón, barra de tiempo, formatos europeos de fecha, enganchan paso rápido por llamadas laraga distancia analógicas de PSTN, identificación URL- mensajes insertados periódicamente o gráficos en teléfonos IP, rediscado último número, búsqueda guía Local, llamar de En-Gancho, estado velocidad de discado , velocidad discado de sistema, cambios de configuración de Velocidad-discado de teléfono IP, silencio y opciones de característica de ring, Apoyo para teléfonos analógicos que utilizan Cisco analógico en modo skinny. El apoyo de maquinas FAX en puertos de FXS o ATA en H. 323 modo. XML atiende a en teléfonos de Cisco IP.</p>
Características de enlace.	<p>FXO analógico (el lazo &amp; inicio en tierra), DID, E&amp;M, BRI/PRI apoyo (NI2, 4ESS, 5ESS, EuroISDN, DMS100, DMS250, y varios otros tipos de switch soportan actualmente el Software de Cisco IOS), identificación de la persona que llama, identificación automática de número (ANI), llamando el nombre, soporte llamada de larga distancia digital (T1/E1), discado directo interno, discado directo externo, soporte E1 R2, la troncal dedicada a llamar de botón, troncal H.323 con soporte H.450, H.450.12 soporte de descubrimiento automático de H.450 para end-point H.323 remotos, discado de llamada para non-H.450 y los end-point H.323, protocolo SIP troncales y soporte RFC2833, Transcoding G.711, G.729a, G.723.</p>
Características de sistema	<p>Cuenta Codificada y entrada de campo de Registro Detalle Llama (CDR), llamar de vuelta a Suscriptor Ocupado, mantención Llamada y Recuperar, Call Park - Personal y Dirigido, Call pickup Dirigido Call pickup grupo local, Call pickup grupo explícito, transferencia de llamada consultivo y ciego, llamada que espera, conferencia tripartita, integración (CTI) de telefonía de computadora con Microsoft CRM y Outlook usando Telefonía Cisco IOS a TSP, servicios de guía que utilizan XML,</p>

	Hunt Groups-Secuencial, circular, y identificación extensa y Hunt Group Dynamic login/logout, intercomunicador, apoyo internacional de idioma: alemán, francés, italiano, español, portugués, holandés, danés, noruego, sueco y ruso, música en espera (MoH)- fuente interna o la externa, alarma servicio de noche, extensiones de cubierta para alcance aumentado de llamada, despliegue nombre llamada para extensiones de cubierta, de identificación de bloqueo por llamada, señal de marcar Secundaria, transferencia estándares basado de llamada de red y Call Forwarding por H.450.2 y H.450.3, opción de velocidad de discado de servicio XML, el hora de día, el día de la semana, bloqueo de llamada, nombre personalizado en pantalla, Basic ACD (3 queues) con la estadística de llamada.
Características de buzón de voz.	La Solución integrada del buzón de voz con la Cisco Unity Express, la Integración con buzón de voz de Cisco Unity unifica mensajería, o la integración (H.323 de buzón de voz de terceros, SORBO, o DTMF) con Octel, Voz Activa, Stonevoice, Comverse.
Características de administración.	Asignación automática de extensiones a teléfonos IP, una internas GUI basada en Web-Basó para movimientos, agrega, y cambia para el sistema y buzón de voz integrado, Administración Centralizada de Red que utiliza Motor de Configuración de Cisco CNE, servicio de telefonía setup wizard, Tres niveles de la Administración de GUI; administrador de Sistema, Administrador de Cliente, y el Usuario.

## RESUMEN

Cisco CallManager Express entrega las características de telefonía requeridas por usuarios de negocio para encontrar los requisitos de la ubicación pequeña de la oficina o sucursal. Cisco Intergrated Service Router ofrece alta certeza y aplicaciones avanzadas incluyendo; VPN, Firewall, codificación, discado por acceso, Ethernet switching con Power Over Ethernet, y el contención de red, con todo en un sola plataforma. Como una sola plataforma es fácil de implementar y mantener tiene como resultado un coste total más bajo al propietario (TCO).

Cuando el negocio expande Cisco CallManager Express puede emigrar fácilmente a un Cisco CallManager la solución a gran escala de telefonía de IP. Todo hardware y el software utilizados por esta solución son completamente compatibles con Cisco CallManager y Cisco Survivable Remote Site Telephony (SRST), dando la protección de la inversión de cliente.

### **Características de servicio**

Cisco ofrece una gran variedad de programas de servicios para acelerar éxito de cliente. Estos programas innovadores de servicios se entregan por una combinación extraordinaria de personas, de los procesos, de los instrumentos, y de los socios, teniendo como resultado los niveles altos de la satisfacción del cliente. Cisco atiende a ayuda usted proteger su inversión de la red, optimizar las operaciones de la red, y preparar la red para aplicaciones nuevas para extender la red la inteligencia y el poder de su negocio. Para más información acerca de Cisco Services, vea Cisco Technical Support Services o Cisco Advanced Services.

### **PARA MÁS INFORMACIÓN**

Para más información acerca de Cisco CallManager Express, por favor visita <http://www.cisco.com/go/ccme>.

Si usted tiene las preguntas mandan correo electrónico a [access-ccme-cue@cisco.com](mailto:access-ccme-cue@cisco.com).

## **ANEXO. Adaptador Telefónico Analógico, CISCO ATA 186.**

### **Data Sheet.**

#### **Adaptador Del Teléfono Del Análogo Del Cisco ATA 186.**



El Adaptador de Teléfono Análogo de Cisco ATA 186 es un adaptador de microteléfono a Ethernet que convierte a los dispositivos telefónicos tradicionales en dispositivos IP. Los clientes pueden aprovecharse de los nuevos y excitantes usos de la telefonía IP conectando sus dispositivos análogos con ATA de Cisco.

Los Cisco ATA son dispositivos basados en estándares de comunicación que entregan exactas, terminales de próxima generación voz-sobre-IP (VoIP) a negocios y residencias por todo el mundo.

#### **Protege La Inversión Del Teléfono De la Herencia**

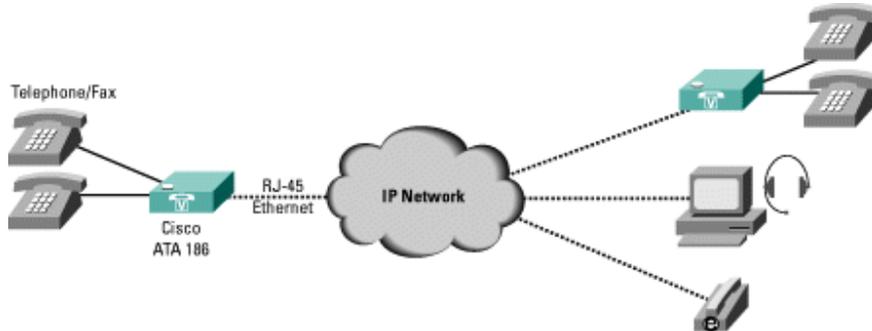
Cisco ATA 186 soporta dos puertos de la voz, cada uno con su propio número de teléfono independiente, y un solo puerto Ethernet 10/100BaseT. Este adaptador puede hacer uso Ethernet en LAN existente, además las líneas de banda ancha tales como línea digital de suscriptor (DSL), wireless e implementación del cable módem.

#### **Rentable**

Los Cisco ATA 186 ayudan a los clientes a convertir sus dispositivos análogos de teléfono en los dispositivos IP rentable y son la solución preferida para tratar las necesidades de los clientes que conectan con las redes de la empresa, ambientes de pequeña oficina, o la emergente administración VoIP de servicios de voz que emerge y mercado local de servicios.

Los clientes de empresa están utilizando el Cisco ATA 186 para conectar los teléfonos y las máquinas de FAX análogos con su red de VoIP. Los proveedores de servicio se están aprovechando de usos de la telefonía que emergen y de la facilidad de implementar servicios de la segunda línea usando el Cisco ATA 186.

**Figura 1 Cisco ATA 186 – Endpoint para un sistema de banda ancha end-to-end.**



El Cisco ATA 186 permite que usted conecte los teléfonos y los faxes análogos con una red de la telefonía del IP.

Tabla 1: Características y ventajas Características	Ventajas
<p>Dos puertos de voz soportan legado teléfonos (análogo) "touch tone".</p> <p>Conexión Rj-45 al hub o al switch Ethernet 10/100Base-T</p>	<p>Conecta los teléfonos heredados con las redes basadas en IP.</p>
<p>Autoprovisionamiento con servidores (TFTP)</p> <p>Asignación automática de dirección IP, ruteo de red IP, y mascara de subred vía DHCP.</p> <p>Configuración Web con Web Server incorporado.</p> <p>Configuración "touch tone" del teclado numérico del teléfono con aviso de la voz.</p> <p>Contraseña de la administración para proteger la configuración y el acceso.</p> <p>Actualizaciones remotas a través de la red.</p>	<p>Configuración flexible y opciones de aprovisionamiento.</p>
<p>Pre-proceso avanzado para optimizar la compresión full-duplex de la voz.</p> <p>La cancelación del eco de línea de alto rendimiento</p>	<p>Claro, sonido calidad de voz natural.</p>

<p>elimina ruido y eco.</p> <p>Detector de actividad de voz (VAD) y generador de ruido confortable (CNG) ahorra ancho de banda por la voz que entrega, no silencio.</p> <p>Monitoreo de red dinámico reduce jitter tal como la pérdida de paquete.</p>	
<p>H.323.</p> <p>Session Initiation Protocol (Sip).</p> <p>Media Gateway Control Protocol (MGCP).</p> <p>Skinny Client Control Protocol (SCCP) tecnología del Cisco CallManager.</p>	<p>Soporta múltiples protocolos para interoperabilidad y flexibilidad de implementación.</p>
<p>Ajustes en la mayoría de los ambientes.</p>	<p>Diseño pequeño del factor de forma.</p>
<p>Contraseñas exhibidas como asteriscos en vez del texto legible.</p>	<p>Seguridad realzada</p>
<p>Página del estado de la red</p>	<p>Seguimientos de paquetes Entrada, salida y errores.</p>

## Requisitos Del Sistema:



- A Teléfonos análogos, de "touch tone" regulares
- B el cable de 10/100Base-T category-3 o mejora (acceso a una red del IP)
- C Energía para el adaptador de la energía de AC/DC

## Especificaciones Del Software

### Protocolos Voz-sobre-IP (VoIP)

- H.323 v2.
- H.323 v4.
- SIP (RFC 2543 bis).
- MGCP 1,0 (RFC 2705).
- MGCP 1.0/network-based call signaling (NCS) 1.0 Profile.
- MGCP 0,1
- SCCP

### Códecs de voz

- G.729, G.729A, G.729AB2
- G.723.1
- G.711a-law
- G.711 $\mu$ -law

### Aprovisionamiento y configuración

- DHCP (RFC 2131).
- Configuración Web vía Web Server incorporado.
- Configuración "touch tone" del teclado numérico del teléfono con aviso de la voz.

- Aprovisionamiento básico del boot (RFC 1350 TFTP profiling).
- Aprovisionamiento del plan de numeración.
- Protocolo del descubrimiento del Cisco para SCCP.

#### Seguridad.

- H.235 para H.323.
- Cifrado RC4 para los perfiles de la configuración de TFTP.

#### Dual-tono de múltiples frecuencias (DTMF).

- Detección y generación del tono de DTMF.

#### DTMF Out-of-band.

- H.245 DTMF out-of-band para H.323.
- Tonos del RFC 2833 AVT para SIP, MGCP, SCCP.

#### Tonos de progreso de llamada.

- Configurable para dos sistemas de frecuencias y un sistema de cadencia on/off.

#### Cancelación de eco de línea.

- Cancelación de eco para cada puerto.
- Longitud del eco de 8 ms.
- Supresión no lineal del eco (ERL mayor que 28 dB para  $f = 300$  a 3400 hertzios).
- Tiempo de la convergencia = ms 250.
- ERLE = 10 a 20 dB.
- Doble-talk la detección.

#### Características de voz.

- Detector de actividad de voz (VAD).
- Generador de ruido confortable (CNG).
- Jitter buffer dinámico (adaptante).

#### Fax.

- Paso de fax G.711.
- Modo de fax G.711.

### **Especificaciones Físicas.**

Cliquee aquí [<http://wwwin.cisco.com/voice/evvbu/pdf/ata186.pdf>] para ver las especificaciones físicas del producto y la información reguladora de la conformidad en formato de PDF.

### **Información para ordenar.**

Tabla 2: Adaptadores Análogos Del Teléfono Del Cisco

ATA 186 Descripción	Número De Pieza
Cisco ATA 186 con impedancia de 600 ohmios	ATA186-I1
Cisco ATA 186 con la impedancia compleja (270 ohmios en serie con 750 ohmios y 150 NF en paralelo)	ATA186-I2
Licencia de la unidad de CallManager para el solo puerto análogo	SW-CCM-UL-ANA
Licencia de la unidad de CallManager para los puertos análogos duales	SW-CCM-UL-ANA

Tabla 3: Cables De la Fuente De Alimentación Del Cisco ATA 186

Descripción	Número De Pieza
Cable de la fuente de alimentación de ATA para Norteamérica	ATACAB-NA
Cable de la fuente de alimentación de ATA para Europa continental	ATACAB-EU
Cable de la fuente de alimentación de ATA para el reino unido	ATACAB-UK

Cable de la fuente de alimentación de ATA para Australia	ATACAB-AU
Cable de la fuente de alimentación de ATA para la Argentina	ATACAB-AR
Cable de la fuente de alimentación de ATA para Japón	ATACAB-JP

Cliquee aquí [<http://www.in.cisco.com/voice/evvbu/pricing.shtml#ata>] para la información de precios.

### **Servicios y soporte.**

Los servicios y el soporte de las comunicaciones IP de Cisco reducen el coste, el tiempo, y la complejidad de implementar una red en ejecución convergida, y pueden ayudarle a crear una infraestructura resistente a las comunicaciones del IP que resuelva sus necesidades del negocio hoy y en el futuro.

Cisco y sus socios han diseñado y han implementado algunas de las redes IP comunicaciones más grandes de hoy - entienden cómo integrar una solución de las comunicaciones IP en su infraestructura de la red, una solución que le ayudará más rápidamente a realizar resultados del negocio y a ganar una ventaja competitiva.

Estos resultados se entregan a través de una flexible suite de ofertas de colaboración que le ayudan a planificar, a diseñar, a implementar, a operar, y a crecer una solución de comunicación IP.

Las herramientas de diseño de Cisco y las mejores prácticas aseguran la solución caben lo mejor posible dentro de sus necesidades de negocio desde el inicio, eliminando reajustes costosos y tiempo muerto. Los métodos probados Cisco aseguran una puesta en marcha que entregue las funciones y las características que usted espera en el tiempo. Los servicios de ayuda incluyen operaciones de red remota, las herramientas de dirección de la red para administrar la aplicación de la convergencia de la infraestructura de red, y los servicios de ayuda técnicos.

El Cisco proporciona la flexibilidad que usted necesita para emplear una estrategia de servicios que resuelva sus requerimientos específicos.

Posted: Sun Aug 25 19:21:37 PDT 2002.

All contents are Copyright © 1992--2002 Cisco Systems, Inc. All rights reserved.

[Important Notices](#) and [Privacy Statement](#).

## **ANEXO. Calidad de servicio, QOS.**

### **INTRODUCCIÓN.**

Aún cuando, se escapa al espíritu del trabajo un aspecto importante dentro de la Telefonía IP es soporte que la recomendación UIT-T H.323 proporciona a los requisitos técnicos para la comunicación multimediales basado en paquetes redes que no garantizan correctamente la calidad de servicio. Esta Recomendación recomienda el uso de mecanismos de reserva de recursos a nivel de transporte para cumplir los requisitos de QOS de trenes de vídeo y audio en tiempo real.

La recomendación UIT-T H.323, data de 1996 (versión 1) y 1998 (versión 2). Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de muy importante ya que los primeros servicios de voz sobre protocolo Internet (VoIP) utilizan esta norma. En la versión 1 del protocolo H.323v1 disponía de un servicio con calidad de servicio (QoS) no garantizada sobre redes LAN. En la versión 2 se definió la aplicación VoIP independiente de la multimedia. Una versión 3 posterior incluye el servicio de fax sobre IP (FoIP) y conexiones rápidas entre otros.

### **FACTORES DE CALIDAD DE SERVICIO (QoS).**

La entrega de señales de voz, vídeo y fax desde un punto a otro no se puede considerar realizada con un éxito total a menos que la calidad de las señales transmitidas satisfaga al receptor. Entre los factores que afectan a la calidad se encuentran los siguientes:

**Requerimientos de ancho de banda:** la velocidad de transmisión de la infraestructura de red y su topología física.

**Funciones de control:** incluye la reserva de recursos, provisión y monitorización requeridos para establecer y mantener la conexión multimedia.

**Latencia o retardo:** de la fuente al destino de la señal a través de la red.

**Jitter:** variación en los tiempos de llegada entre los paquetes. Para minimizar este factor los paquetes entrantes han de ser introducidos en un buffer y, desde allí, enviados a intervalos estándar.

**Pérdida de paquetes:** cuando un paquete de vídeo o de voz se pierde en la red es preciso disponer de algún tipo de compensación de la señal en el extremo receptor.

## **PROCEDIMIENTOS DE RESERVA DE RECURSOS A NIVEL DE TRANSPORTE**

RSVP es el protocolo de señalización a nivel de transporte para reservar recursos en redes IP no fiables. Utilizando el RSVP, los puntos extremos H.323 pueden reservar recursos para un determinado tren de tráfico en tiempo real basados en sus propios requisitos de QoS. Si la red no consigue reservar los recursos requeridos, o en ausencia de RSVP, sólo es posible la entrega de los paquetes utilizando el mecanismo de entrega del mayor esfuerzo posible.

### **Soporte de QoS para H.323.**

Cuando un punto extremo solicita la admisión a un Gatekeeper, debe indicar en el mensaje ARQ si es capaz o no de reservar recursos. El Gatekeeper debe entonces decidir, sobre la base de la información que recibe del punto extremo y de la información que tiene sobre el estado de la red, si:

- Permite al punto extremo aplicar sus propios mecanismos de reserva para su sesión H.323; o.
- Efectúa la reserva de recursos en nombre del punto extremo; o
- No se necesita ninguna reserva de recursos. Es suficiente el mejor procedimiento posible.

Esta decisión es transmitida al punto extremo en el mensaje ACF. El punto extremo aceptará la decisión del Gatekeeper a fin de efectuar una llamada.

El Gatekeeper debe rechazar un ARQ de punto extremo, si el punto extremo no indica que es capaz de efectuar la reserva de recursos y el Gatekeeper decide que la reserva de recursos debe ser controlada por el punto extremo. En este caso, el Gatekeeper debe devolver ARJ al punto extremo.

El campo específico en la señalización RAS H.225.0 para permitir esta funcionalidad es el campo **QOS de transporte (transportQOS)**.

Además de **transportQOS**, un punto extremo debe también calcular y comunicar el ancho de banda que en ese momento pretende utilizar en todos los canales de la llamada. Este ancho de banda debe comunicarse en el campo **ancho de banda (bandWidth)** del mensaje ARQ independientemente de la decisión del punto extremo de utilizar o no

señalización RSVP. Además, si los requisitos de ancho de banda cambian en el curso de la llamada, el punto extremo debe comunicar al Gatekeeper los cambios de requisitos de ancho de banda utilizando BRQ independientemente de la decisión de utilizar RSVP.

Las reservas RSVP sólo pueden ser efectuadas por entidades de red que están en el trayecto del flujo de medios entre puntos extremos. Es posible encaminar, mediante señalización de llamada encaminada por el Gatekeeper, trenes de medios a través de un Gatekeeper. Sin embargo, la mayoría de los canales de medios de tiempo se encaminarán entre puntos extremos sin pasar a través del Gatekeeper. Si un Gatekeeper decide encaminar trenes de medios, los procedimientos seguidos deben entonces ser idénticos a los aplicados para la señalización RSVP directamente desde los puntos extremos. Lo mejor es que las reservas RSVP sean efectuadas directamente por los puntos extremos, ya que así se reservarán recursos a lo largo de todo el trayecto de encaminamiento de la llamada. El resto de este apéndice trata la utilización del RSVP por los puntos extremos H.323.

Algunos de los puntos sobresalientes del RSVP son los siguientes:

- RSVP soporta entornos unidifusión y multidifusión;
- RSVP está ligado a trenes concretos (es decir, pares concretos de direcciones de transportes);
- RSVP es de carácter flexible, por lo cual se adapta dinámicamente al cambio de la composición de los grupos y las rutas;
- RSVP es unidireccional;
- RSVP está orientado al receptor, es decir, el destinatario del tren de medios hace la reserva (escalable).

Durante la fase de intercambio de capacidades H.245, cada punto extremo indica sus capacidades de transmisión y recepción al otro punto extremo. La **capacidad de QOS (qOSCapability)**, es parte del intercambio de capacidades. Sin embargo, no es específica del tren. Por tanto, si en la **qOSCapability** se especificasen los parámetros RSVP, representarían un agregado de todos los trenes (ya sean los transmitidos o los recibidos). Dichos parámetros no serán de ninguna utilidad para el otro punto extremo. Por tanto, la única información relacionada con el RSVP que un punto extremo debe transmitir al otro

punto extremo en el conjunto de capacidades es si está o no capacitado para manejar el RSVP.

Para señalar la capacidad RSVP, un punto extremo fijará los campos **modo QOS (qOSMode)** disponibles dentro de la PDU capacidad durante el intercambio de capacidades. Los puntos extremos que no reciben capacidades RSVP del punto extremo receptor no utilizarán RSVP cuando abran canales lógicos.

### **Apertura de canal lógico y establecimiento de reservas**

Se describen los pasos que deben seguirse para abrir un canal lógico H.245 y reservar recursos para un determinado tren de tráfico. Las reservas se establecen sólo si ambos puntos extremos indican, durante el intercambio de capacidades, que están capacitados para el RSVP. Se considera sólo el caso punto a punto.

El emisor especificará en el campo **qOSCapability** del mensaje **openLogicalChannel** los parámetros RSVP del tren a transmitir, y los servicios integrados que soporta el emisor. En el caso de un tren punto a punto, el emisor no especifica un ID de puerto receptor en el mensaje **openLogicalChannel**. El receptor selecciona este ID después de recibir el mensaje **openLogicalChannel**, que se devuelve al emisor en el mensaje **openLogicalChannelAck**. Sólo entonces puede el emisor crear una sesión RSVP para ese tren (crear una sesión RSVP para un determinado tren significa que el punto extremo se registra en el RSVP para que se le notifique la llegada de los mensajes que puedan afectar al estado de la reserva RSVP para ese tren), y empezar a emitir mensajes RSVP trayecto. El receptor tiene suficiente información para crear una sesión RSVP para el mismo tren antes de enviar el mensaje **openLogicalChannelAck**. La información necesaria para crear una sesión RSVP e iniciar el procesamiento RSVP es la dirección IP del receptor en caso de punto a punto, o la dirección IP multidifusión de grupo en caso de punto a multipunto, el ID de puerto del receptor y el protocolo (siempre UDP en caso de trenes de audio y vídeo H.323 en redes IP).

Un receptor puede no desear empezar a recibir paquetes de trenes hasta que estén hechas las reservas RSVP. Para conseguirlo, el receptor puede poner el campo booleano **control de flujo a cero (flowcontrolToZero)** del mensaje **openLogicalChannelAck** a VERDADERO para indicar que no desea recibir ningún tráfico en ese canal antes de que estén completas las reservas de recursos.

Cuando un emisor recibe un mensaje **openLogicalChannelAck** cuyo **flowControlToZero** está puesto a VERDADERO, el emisor no transmitirá ningún tráfico por ese canal.

Cuando el receptor empieza a recibir los mensajes trayecto del emisor, debe iniciar la emisión de mensajes RSVP reserva. Cuando el receptor recibe un mensaje RSVP reserva conferencia (*ResvConf*) confirmando que se han establecido reservas, puede enviar una **instrucción de control de flujo (flowControlCommand)** al emisor restringiendo la velocidad binaria del tren de tráfico, es decir, suprimiendo el efecto del campo **flowcontrolToZero** anterior en el mensaje **openLogicalChannelAck**. Cuando el receptor recibe **flowControlCommand**, empieza a transmitir paquetes.

Adviértase todos demás mensajes RSVP, se transmiten no fiablemente. Por consiguiente, pueden retrasarse e incluso perderse. Un punto extremo debe conocer esa posibilidad, y fijar temporizadores con un valor apropiado mientras se espera un mensaje reserva conferencia. En caso de que venza la temporización del punto extremo sin haber recibido un mensaje reserva conferencia, la acción ejercida corresponde a los distintos vendedores de puntos extremos.

Si las reservas RSVP fallan en cualquier punto durante una llamada H.323, el comportamiento de un punto extremo no se especifican en este apéndice, y se deja a criterio de los vendedores. Sin embargo, si falla una reserva RSVP y el punto extremo receptor decide que el nivel de servicio de mayor esfuerzo posible no es aceptable, puede solicitar el cierre de su canal lógico utilizando el mensaje **petición de cierre de canal (requestChannelClose)**. El campo **motivo del cierre (closeReason)** está disponible en el mensaje **requestChannelClose** para que el receptor pueda señalar al emisor que la reserva RSVP ha fallado. Junto con la indicación de fallo, **requestChannelClose** incluye **qOSCapability**, que puede utilizar el receptor para comunicar al emisor los recursos que en ese momento están realmente disponibles en el trayecto del emisor al receptor. En este punto, el emisor puede decidir tratar de reabrir el canal con un códec de menor anchura de banda y/o formato de datos inferiores y someterse de nuevo a procedimiento de apertura de canal lógico.

Todas las peticiones RSVP reserva utilizarán el mismo estilo de reserva, el estilo de **filtro fijo (Fixed Filter)**, por los motivos siguientes:

- Los estilos de filtro compartido se reducen a filtros fijos en caso de llamadas punto a punto.
- No pueden mezclarse en la red estilos de reserva diferentes en la misma sesión. Por ejemplo, si en una llamada multipunto algunos de los receptores solicitan reservas de filtros fijos mientras que el resto solicitan reservas explícitas compartidas, fallarán las reservas de filtros fijos o las reservas explícitas compartidas.
- Las reservas compartidas, creadas por estilos de filtro comodín y de filtro explícito compartido, son apropiadas para aquellas aplicaciones multidifusión en las que es improbable que múltiples fuentes de datos transmitan simultáneamente. En las llamadas H.323 multipunto distribuidas, no existe ningún mecanismo que permita exclusivamente a una fuente transmitir en un momento determinado. En cambio, en las llamadas H.323 multipunto centralizadas, la MCU es la única fuente multidifusión. Los estilos de reserva compartida no son adecuados para ninguno de los casos.

Corresponde a los vendedores de puntos extremos elegir qué servicio QOS intserv (QOS garantizada o carga controlada) ha de utilizarse. Sin embargo, cualquier punto extremo H.323 con capacidad de utilizar RSVP, soportará el servicio de carga controlada como el servicio menos común. Este requisito es necesario para evitar problemas de interoperabilidad que puedan surgir de puntos extremos H.323 habilitados para RSVP que no soporten un servicio QOS intserv.

### **Cierre de canal lógico y cancelación de reservas**

Antes de enviar un mensaje **closeLogicalChannel** para un determinado tren de tráfico, un punto extremo emisor debe enviar un mensaje romper trayecto si se ha creado previamente una sesión RSVP para ese tren. Cuando un punto extremo receptor recibe un **closeLogicalChannel** para un determinado tren de tráfico, debe enviar un mensaje romper reserva si se ha creado previamente una sesión RSVP para ese tren.