

**DISEÑO DE INTERCONEXIÓN DE LAS SEDES DE LA UIS MEDIANTE
VIDEOCONFERENCIA Y VOZ CORPORATIVA**

**ADRIANA MARCELA RODRÍGUEZ MARIN
CARLOS ALBERTO VELANDIA VALERO**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECHANICAS
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES
BUCARAMANGA
2005**

**DISEÑO DE INTERCONEXIÓN DE LAS SEDES DE LA UIS MEDIANTE
VIDEOCONFERENCIA Y VOZ CORPORATIVA**

**ADRIANA MARCELA RODRÍGUEZ MARIN
CARLOS ALBERTO VELANDIA VALERO**

Trabajo de Grado

**Director:
Magíster. Jorge Hernando Ramón**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECHANICAS
ESCUELA DE INGENIERIA ELECTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES
BUCARAMANGA
2005**

A mis padres y hermanas, quienes siempre han apoyado mis decisiones y anhelos y que nunca han dejado de creer en mi, a mi esposa, mi hijo Carlos Andrés y mis sobrinos Alejandro y Valentina que son el motor de mi inspiración para cumplir las metas que cada día me propongo, para todos ellos cada triunfo en mi vida.

Carlos Alberto Velandia Valero

A Dios por mi vida, a mis padres por su dedicación y esfuerzos, mis hermanos por su apoyo, a mi esposo e hijo que son mi fuerza para seguir triunfando.

Adriana Marcela Rodríguez Marín

AGRADECIMIENTOS

Al Mg. Jorge Hernando Ramón director del proyecto quien fue pieza fundamental en la realización de pruebas sobre la red de la Universidad y en el desarrollo del diseño.

Al CIDLIS en cabeza del profesor Ricardo Llamosa quienes facilitaron los equipos de videoconferencia existentes en la Universidad.

Al Ingeniero Norberto Toledo, funcionario de la Universidad Industrial de Santander de la seccional Socorro en quien siempre se encontró disposición para la realización de pruebas en esta ciudad.

A la empresa ANS COMUNICACIONES LTDA quienes nos colaboraron con información técnica y el préstamo del equipo Analizador de Redes (Wandell), utilizado para probar el canal contra el Socorro.

TABLA DE CONTENIDO

	Pág.
INTRODUCCIÓN	18
1. DESCRIPCIÓN DEL PROYECTO	20
1.1 OBJETIVOS	20
1.1.1 Objetivo General	20
1.1.2 Objetivos específicos	20
1.2 JUSTIFICACION	21
2. MARCO TEORICO	24
2.1 ENRUTAMIENTO	24
2.1.1 Routers y comunicación entre redes	24
2.1.2 Pila de protocolos TCP/IP	24
2.1.3 Paquetes de datos	26
2.1.4 Comunicación entre ordenadores en una red	27
2.1.5 Comunicación entre ordenadores en dos redes. Routers	28
2.1.6 Cómo funciona un router	30
2.1.7 Componentes básicos de un router	32
2.1.8 Tipos de routers	33
2.1.9 Protocolos de enrutamiento	35
2.2 PROTOCOLO FRAME-RELAY	37
2.2.1 ¿Por qué usar “Frame Relay”?	39

2.2.2	Estructura de trama	40
2.2.3	Historia de Frame Relay	42
2.2.4	Redes PVC	44
2.2.5	Redes SVC	47
2.2.6	PVCs versus SVCs	48
2.2.7	Congestión	48
2.2.8	Tarifación	50
2.3	VOZ SOBRE IP	51
2.3.1	Determinación de los requisitos de número de enlaces principales (Trunking)	56
2.3.2	Determinación de los requisitos de ancho de banda de red	56
2.3.3	Determinación de la calidad de servicio (QoS)	57
2.3.4	Trayecto para las llamadas de voz	57
2.3.5	Algoritmo de codificación de voz	58
2.3.6	problemas del diseño de la calidad de voz	60
2.3.7	Latencia	61
2.3.8	Compresión	63
2.3.9	Retardo de procesamiento interno	64
2.3.10	Acceso a la red en el origen	65
2.3.11	Retardo de Transmisión de red	66
2.4	ESTÁNDAR H.323	68
2.4.1	Establecimiento y control de llamadas	71
2.4.1.1	H.225.0 para inicio de llamadas	71

2.4.1.2 H.245 media control	73
2.4.1.3 Establecimiento de una llamada con H.225.0 y H.245	74
2.4.1.4 Caso con gatekeeper. H.225.0 RAS.	76
2.4.2 Transmisión de datos durante la llamada	78
2.4.2.1 Los protocolos rtp/rtcp	78
2.4.3 Implementación de h.323 a nivel de puertos	80
2.4.4 La problemática de NAT. Connection Tracking	81
2.4.5 Codecs de audio en H.323	82
2.4.5.1 Waveform codecs	83
2.4.5.1.1 G.711	83
2.4.5.1.2 G.722	83
2.4.5.2 Codificadores mediante vocoders	84
2.4.5.2.1 G.723.1	85
2.4.5.2.2 G.728	85
2.4.5.2.3 G.729	85
2.4.6 Códecs de vídeo en H.323	86
2.4.6.1 H.261	86
2.4.6.2 H.263	87
2.4.7 Equipos para VoIP	87
2.4.7.1 Terminales	88
2.4.7.2 Gateways	88
2.4.7.3 Gatekeeper	91
2.4.7.3.1 Funciones principales del Gatekeeper.	91

2.4.8 Multipoint Control Units	94
2.4.8.1 Partes del MCU	95
3. DISEÑO	96
3.1 ANÁLISIS DE LA RED DE DATOS ACTUAL	96
3.1.1 Pruebas realizadas sobre la red actual	96
3.1.2 Pruebas de videoconferencia utilizando software	96
3.1.2.1 Programa Neetmeeting	98
3.1.2.2 Programa ISPQ	100
3.1.3 Pruebas de videoconferencia utilizando Hardware	101
3.1.4 Pruebas de voz a través de un canal de datos	105
3.2 PROYECTO PROPUESTO	105
3.3 PROPUESTA ECONÓMICA DE CANALES DE DATOS FRAME RELAY	106
3.3.1 Propuesta económica Telecom.	109
3.3.1.1 Propuesta económica canales Frame-Relay de Telecom .	109
3.3.1.2 Aspectos comerciales	110
3.3.1.3 Sanciones por no pago	111
3.3.1.4 Cancelación del contrato por uso indebido	111
3.3.1.5 Forma de Pago	112
3.4 EQUIPOS DE ENRUTAMIENTO REQUERIDOS	113
3.4.1 Costo de equipos de enrutamiento	116
3.5 CAMARAS DE VIDEOCONFERENCIA	117
3.5.1 Propuesta en Polycom	118
3.5.1.1 Equipo multipunto	118

3.5.2 Propuesta Tandberg	119
3.6 INTERCONEXIÓN DE LAS PLANTAS TELEFÓNICAS A LA RED DE DATOS	120
3.7 PROPUESTA ECONOMICA GENERAL	122
4. CONCLUSIONES	123
BIBLIOGRAFÍA	125
ANEXOS	126

LISTA DE FIGURAS

	Pág.
Figura 1 .Red de computadores	27
Figura 2 .Router cisco 1601	28
Figura 3 .Red conectada a router	29
Figura 4 .Router multipunto 2611	33
Figura 5 .Router wireless	34
Figura 6 .Estructura de trama Frame Relay	41
Figura 7 .Formato DLCI	42
Figura 8 .Evolución de Frame Relay	43
Figura 9 .Estándares Frame Relay	44
Figura 10.Autopruueba de calidad de Frame Relay	45
Figura 11.Señalización PVC	45
Figura 12.Estado “ status”	46
Figura 13.Opciones de ping	67
Figura 14.Torre de protocolos	71
Figura 15.Formato de trama H.225.0	72
Figura 16.Establecimiento de llamadas con H.225.0 y H.245	75
Figura 17.Protocolo RTP trama	79
Figura 18.Protocolo RTCP trama	80
Figura 19.Componentes red típica H.323	87
Figura 20.Gateway H.323	90

Figura 21. Señalización directa entre terminales	93
Figura 22. Señalización enrutada por el gatekeeper	94
Figura 23. Partes del MCU	95
Figura 24. Diagrama de conexión Socorro Bucaramanga	96
Figura 25. Presentación Netmeeting	99
Figura 26. Verificación registro ISPQ	100
Figura 27. Esquema de ISPQ	101
Figura 28. Mensaje detección de cortafuegos	102
Figura 29. Ping hacia el router de Bucaramanga	103
Figura 30. Ping introduciendo tráfico	104
Figura 31. Topología en estrella	107
Figura 32. Conexión router R2 y R3 a través de Frame Relay	108
Figura 33. Router cisco 1760	114
Figura 34. Modulo Vic 2FXS	114
Figura 35. Router cisco 2611 vista trasera	116
Figura 36. Equipo Polycom	118
Figura 37. Cámara Tandberg	119
Figura 38. Diagrama general del proyecto	121

LISTA DE TABLAS

	Pág.
Tabla 1 .Enrutamiento simple	32
Tabla 2 .Características de ancho de banda de los algoritmos de codificación de voz	58
Tabla 3 .Características de retardo de los algoritmos de codificación de voz	58
Tabla 4 .Sugerencias de segmentación de LF1 y FRF.12	59
Tabla 5 .Retardos de la red de paquetes	62
Tabla 6 .Resumen estándar	81
Tabla 7 .Valor canales Frame Relay	110
Tabla 8 .Valor equipos de enrutamiento	116
Tabla 9 .Valor equipos Polycom	118
Tabla 10.Valor equipos Tandberg	119
Tabla 11.Valor Total Proyecto	122

LISTA DE ANEXOS

	Pág.
Anexo A. Prueba de Bert enlace Socorro- Bucaramanga	126
Anexo B. Analizador de redes digitales (Wandell)	128
Anexo C. Routers modulares de acceso de la serie Cisco 2600	133
Anexo D. Router Cisco 1760	140
Anexo E. Polycom Serie VSX 7000	162
Anexo F. Sistema Tandberg 880 MXP IP	173
Anexo G. Acceso y verificación de puertos Router Cisco	190

TITULO: DISEÑO DE INTERCONEXIÓN DE LAS SEDES DE LA UIS MEDIANTE VIDEOCONFERENCIA Y VOZ CORPORATIVA*

Adriana Marcela Rodríguez Marín, Carlos Alberto Velandia**

Palabras Claves: Videoconferencia, Voz sobre IP, Frame-Relay, H.323, Enrutamiento.

RESUMEN

Las comunicaciones interactivas de video están siendo usadas en muchas partes del mundo para actividades académicas a todo nivel, al mismo tiempo son una herramienta indispensable en el sector empresarial para la gestión de negocios y la capacitación de su personal.

En el caso particular de la Universidad Industrial Santander la necesidad de cubrimiento de algunas cátedras en dependencias diferentes a la de Bucaramanga, presupone el desplazamiento de profesores hasta la sede en cuestión en donde el tiempo de espera en los terminales y el desplazamiento, entre otros, son factores que reducen la productividad de los profesores de la universidad y por lo tanto el nivel de la educación se ve afectado, sin tener en cuenta la pérdida de la disponibilidad del profesor en su sitio de trabajo.

Por otra parte otra falencia que existe en la actualidad en las comunicaciones de la Universidad Industrial de Santander es la no interconexión de voz corporativa entre sus sedes, lo que actualmente representa elevados costos en llamadas de larga distancia teniendo en cuenta que el proceso administrativo es centralizado a Bucaramanga, a partir de esto se visualiza la necesidad de convergencia en el canal de comunicaciones que integre videoconferencia y voz por un mismo canal.

El alcance de este proyecto es dejar planteado el diseño requerido para la interconexión de las sedes de la Universidad Industrial de Santander entre Bucaramanga, Socorro, Málaga, Barbosa, Barrancabermeja, para lograr comunicación de Voz corporativa y Videoconferencia durante las 24 horas del día, los 7 días de la semana, los 365 días del año. Esto a través de canales Frame-Relay en una topología en estrella con enrutadores Cisco, 4 cámaras de videoconferencia punto a punto y una multipunto.

* Trabajo de Grado.

** Facultad de Ingenierías Físico-Mecánicas, Ingeniería Electrónica, Magíster Jorge H. Ramón.

TITLE: DESIGN OF INTERCONNECTION OF THE HEADQUARTERS OF THE UIS
BY MEANS OF VIDEOCONFERENCE AND CORPORATE VOICE^{*}

Adriana Marcela Rodríguez Marín, Carlos Alberto Velandia^{**}

Key words: Videoconference, Voice Over IP, Frame-Relay, H.323, Routing.

SUMMARY

The interactive communications of video are being used in many parts of the world for academic activities at all level, at the same time they are an indispensable tool in the managerial sector for the administration of business and their personnel's training.

In the case peculiar of the Industrial University Santander the necessity to cover some classes in dependences different to that of Bucaramanga, presupposes the displacement of professors until the headquarters in question where the time of wait in the terminals and the displacement, among other, they are factors that reduce the productivity of the professors of the university and therefore the level of the education is affected, without keeping in mind the loss of the professor's readiness in its work place.

Another disadvantage that exists at the present time in the communications of the Industrial University of Santander is not the interconnection of corporate voice among its headquarters, at the moment represents high costs in calls of long distance keeping in mind that the administrative process is centralized Bucaramanga, starting from this the convergence necessity is visualized in the channel of communications that integrates videoconference and voice for oneself channel.

The reach of this project is to leave outlined the design required for the interconnection of the headquarters of the Industrial University of Santander among Bucaramanga, Socorro, Málaga, Barbosa, Barrancabermeja, to achieve communication of corporate Voice and Videoconference during the 24 hours of the day, the 7 days of the week, the 365 days of the year. This through channels Frame-Relay in a topology in star with routers Cisco, 4 cameras of videoconference point to point and a multipoint.

* Grade Work

** School of Physical-mechanical Engineerings, Electronic Engineering, Schoolmaster Jorge H. Ramón.

INTRODUCCIÓN

Desde la invención de los sistemas de Telecomunicaciones, uno de los primeros tipos de información enviados siempre ha sido la voz. Con la revolución tecnológica de Internet se buscaron nuevas tácticas para el transporte de voz a través de las redes de datos.

La convergencia de servicios es un factor preponderante hoy en día, la reducción de costos y la optimización de recursos hacen que las empresas busquen soluciones de comunicación integrales. En el caso particular de la Universidad Industrial de Santander su estructura centralizada crea la necesidad de interacción constante entre las diferentes sedes ubicadas en el departamento de Santander y su principal en Bucaramanga, este hecho implica un elevado costo en llamadas telefónicas de larga distancia a través de los operadores tradicionales para poder llevar a cabo estos procesos.

Por otra parte, la falta de personal docente capacitado para cubrir las clases de algunas materias en las sedes alternas obliga al desplazamiento de este, disminuyendo así su desempeño.

Diferentes instituciones del ámbito nacional e internacional han optado por aprovechar redes de datos para dictar clases virtuales y videoconferencia, de esta manera se pueden realizar clases magistrales donde se da la oportunidad a los alumnos de recibir cursos especializados desde sus aulas tradicionales, con la ventaja de estar interactuando en tiempo real con el docente que puede encontrarse a cientos de kilómetros de distancia con la percepción de tenerlo presente. La Universidad Industrial de Santander como institución educativa no esta exenta de beneficiarse de estos avances tecnológicos.

El alcance de este proyecto es crear una visión mediante un diseño de las opciones de mejoramiento que puede realizar la Universidad Industrial de Santander en el área de Telecomunicaciones, aprovechando las ventajas del mundo moderno con el fin de estar en línea todo el tiempo.

1. DESCRIPCIÓN DEL PROYECTO

Diseño de la interconexión de las sedes de la Universidad Industrial de Santander para servicios de videoconferencia y voz corporativa.

1.1 OBJETIVOS

1.1.1 Objetivo General. Realizar el diseño de interconexión de voz y videoconferencia para las sedes de la Universidad Industrial de Santander de Bucaramanga, Socorro, Barrancabermeja, Málaga y Barbosa.

1.1.2 Objetivos específicos:

- ❖ Realizar el diseño de interconexión multipunto para las sedes de la Universidad antes mencionadas.
- ❖ Establecer las características de los equipos de Videoconferencia requeridos.
- ❖ Determinar la marca de los equipos de enrutamiento necesarios para los requerimientos de interconexión de acuerdo al diseño planteado.
- ❖ Verificar las especificaciones técnicas de las plantas actuales y de las posibles actualizaciones con el fin de introducirlas al diseño de interconexión de las sedes.
- ❖ Determinar los requerimientos de ancho de banda actuales y los necesarios para montar la nueva infraestructura de voz y videoconferencia.

1.2 JUSTIFICACION

Las comunicaciones interactivas de video están siendo usadas en muchas partes del mundo para actividades académicas a todo nivel, al mismo tiempo son una herramienta indispensable en el sector empresarial para la gestión de negocios y la capacitación de su personal.

La videoconferencia posibilita la asistencia remota a sesiones de clase presencial, a actividades específicas para alumnos a distancia o a desarrollar trabajo colaborativo en el marco de la presencia motivada. La videoconferencia tiene unas posibilidades educativas enormes, puesto que permite una interacción permanente, en tiempo real, con imagen y sonido entre diferentes puntos, haciendo posible que, diferentes profesores, diferentes alumnos, diferentes centros escolares, etc. participen en el proceso de comunicación sin necesidad de desplazamiento alguno. De entre la multitud de tecnologías de posible aplicación que posibilitan la interactividad en el campo de la formación, la videoconferencia es, sin duda, una de las que mayor futuro tiene en lo referente a enseñanza no presencial. La videoconferencia es hoy por hoy la pieza fundamental para la reducción de costos en la gran mayoría de las empresas a nivel mundial. La tendencia a nivel mundial es la de reducir cada vez más el número de viajes, viáticos y costos hoteleros dentro de todos los niveles de las compañías.

En el caso particular de la Universidad Industrial Santander la necesidad de cubrimiento de algunas cátedras en dependencias diferentes a la de Bucaramanga, presupone el desplazamiento de profesores hasta la sede en cuestión en donde el tiempo de espera en los terminales y el desplazamiento, entre otros, son factores que reducen la productividad de los profesores de la universidad y por lo tanto el nivel de la educación se ve afectado, sin tener en cuenta la pérdida de la disponibilidad del profesor en su sitio de trabajo.

Enseñar a través de videoconferencia supone, no obstante, un cambio en cuanto a la metodología tradicional aplicada en los sistemas presenciales de enseñanza. Esta nueva tecnología necesita formas distintas de interacción, diferente comportamiento físico, distintas maneras de presentar la información y diferentes formas de juzgar los mensajes que se puedan transmitir en ambas direcciones. Por esto es necesario que los profesores se formen en el manejo de esta tecnología, que conozcan los elementos que la componen y, sobre todo, cuáles son los principales aspectos que tienen que tener en cuenta a la hora de utilizarla.

Finalmente una ventaja adicional de montar servicios de videoconferencia es que una vez la Universidad Industrial de Santander se integre a Internet 2 podrá intercambiar información no solo de datos sino también de voz y video en su sede Principal incluyendo sus demás sedes de Santander.

Por otra parte otra falencia que existe en la actualidad en las comunicaciones de la Universidad Industrial de Santander es la no interconexión de voz corporativa entre sus sedes, lo que actualmente representa elevados costos en llamadas de larga distancia teniendo en cuenta que el proceso administrativo es centralizado a Bucaramanga, a partir de esto se visualiza la necesidad de convergencia en el canal de comunicaciones que integre videoconferencia y voz por un mismo canal.

La principal ventaja es que la VoIP proporcionaría a las sedes de la Universidad, comunicaciones gratuitas entre ellas. Además, la red de comunicaciones de la UIS se vería enormemente simplificada, ya que los canales de voz entrarían a formar parte de la planta telefónica de campus. En una llamada telefónica IP estamos comprimiendo la señal de voz y utilizamos una red de paquetes sólo cuando es necesario. Los paquetes de datos de diferentes llamadas, e incluso de diferentes tipos de datos, pueden viajar por la misma línea al mismo tiempo aprovechando de

esta manera el recurso del canal aun cuando se este utilizando la videoconferencia.

El argumento inicial en favor de este modelo de redes se basa en la gran presencia actual de las infraestructuras IP en los entornos corporativos de datos, así como en la suposición de que parte de la capacidad de estas redes está siendo desaprovechada. Parece que nada hay mejor que emplear el ancho de banda inutilizado para soportar el tráfico de voz.

No obstante en la topología actual de datos de la Universidad y la capacidad de información que se transporta entre las sedes, presupone la necesidad de un canal independiente que transporte la voz y las necesidades de Videoconferencia teniendo como aditivo especial la necesidad que las comunicaciones sean multipunto para así permitir interconexión no solo con Bucaramanga sino entre las diferentes sedes.

2. MARCO TEORICO

2.1 ENRUTAMIENTO

2.1.1 Routers y comunicación entre redes. Un ordenador solitario, sin conexión con ningún otro, es una isla de información y de recursos que no resulta rentable, especialmente cuando para el trabajo diario se precisa recurrir a diferentes fuentes de datos.

De esto se dieron cuenta muy pronto las empresas, que solicitaron a las compañías de desarrollo de hardware y software un medio compartido de trabajo, en el que diferentes estaciones de trabajo, servidores e impresoras pudieran comunicarse entre ellos y compartir recursos. De este modo surgieron las primeras redes de ordenadores.

Una red está formada por una serie de estaciones de trabajo unidas entre sí por medios de transmisión físicos (cables) o basados en ondas (redes inalámbricas), coordinados por unas máquinas especiales, denominadas servidores, y por un conjunto variable de dispositivos de trabajo, como impresoras, escaners, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs.

2.1.2 Pila de protocolos TCP/IP. Las diferentes máquinas que forman una red se comunican entre sí usando un medio compartido, pudiendo tener además cada una de ellas características propias, como componentes de hardware, sistemas operativos y aplicaciones de usuario.

Para solventar estas diferencias se hizo necesaria la introducción de una serie de reglas que controlaran el acceso al medio compartido y la forma correcta en que

las máquinas se debían comunicar y transmitir los datos, surgiendo con ello diferentes protocolos de comunicación y control.

En un principio, cada empresa desarrolladora implementó un sistema propio de comunicación de red, con una arquitectura y unos protocolos diferentes, por lo que no fue posible, cuando se necesitó, unir redes de diferentes fabricantes. Simplemente, no se entendían entre ellas, pues hablaban “idiomas” diferentes.

Intentando solucionar este problema, la ISO (Organización Internacional de Estándares) creó un modelo de comunicación para redes dividido en una serie de niveles de trabajo, denominados capas, cada uno de los cuales se encargaría de uno o más aspectos concretos de la comunicación mediante una serie de protocolos específicos.

Este modelo se llamó OSI (Intercomunicación de Sistemas Abiertos) y, lamentablemente, no llegó a utilizarse en la práctica, debido a que cuando se publicó ya se habían desarrollado otras arquitecturas de comunicación en redes que funcionaban más o menos bien, y que fueron las que al final se usaron y extendieron.

De ellas, la más conocida y usada en la actualidad es la arquitectura TCP/IP, formada por un extenso conjunto de protocolos, cada uno de los cuales se encarga de un aspecto concreto de la comunicación entre máquinas en red. TCP/IP se basa en un modelo de capas, al igual que OSI, pero más reducido, actuando cada protocolo en una de las capas del mismo.

El número de capas en que se divide TCP/IP y el nombre de las mismas varía según el autor (recordemos que no es un estándar, si no una implementación “de facto”), pero podemos considerar la siguiente división:

- Capa de Aplicación: encargada de dar soporte de red a las aplicaciones de usuario, convirtiendo los datos de estas a un formato estándar apropiado para su transmisión por red. En ella actúan protocolos como HTTP (web), FTP (transferencia de ficheros) y SMTP (correo electrónico).
- Capa de Transporte: encargada de dividir los datos en unidades de información de tamaño apropiado y de controlar la correcta transmisión lógica de las mismas. Sus principales protocolos son TCP y UDP.
- Capa de Red: su misión principal es enrutar o dirigir los datos de una máquina a otra, usando para ello el protocolo IP, siendo el responsable principal del tráfico de datos entre diferentes redes interconectadas.
- Capa de Enlace de datos: se ocupa de identificar los datos transmitidos entre máquinas de una misma red y de controlar la validez de los mismos tras su emisión y recepción a través del medio físico.
- Capa Física: responsable de la conversión de los datos a transmitir en impulsos eléctricos o en ondas y de su transmisión física.

Cada capa trabaja independientemente de las otras, comunicándose entre ellas por medio de interfaces apropiadas.

2.1.3 Paquetes de datos. Cuando un host desea enviar una serie de datos a otro, estos son convertidos a un formato de red apropiado (capa de Aplicación) y divididos en una serie de unidades, denominadas segmentos (capa de Transporte), que son numerados para su correcto reensamble en la máquina destino.

Posteriormente, son pasados a la capa de Red, que les coloca las direcciones IP de la máquina origen y de la máquina destino. Las unidades así obtenidas se conocen con el nombre de paquetes. Entonces son pasados a la capa de Enlace de Datos, que les añade las direcciones MAC de ambas máquinas y un número calculado para la verificación posterior de errores en el envío, pasando entonces a denominarse tramas.

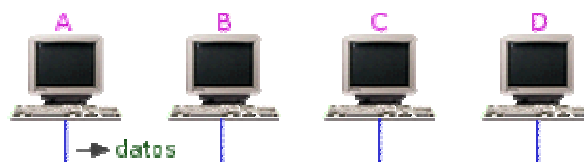
Por último, las tramas son pasadas a la capa Física que las une en trenes de bits apropiados para su transformación en impulsos eléctricos o en ondas, que posteriormente son enviados al medio.

Cuando los impulsos llegan a la máquina destino el proceso se invierte, obteniendo la aplicación receptora los datos en su formato original.

A pesar de que lo que se transmite por el medio físico son impulsos eléctricos, se suele hablar de paquetes transmitidos, ya que son las unidades de información con entidad propia.

2.1.4 Comunicación entre ordenadores en una red. Imaginemos una red formada por varios host, como la representada en la siguiente imagen:

Figura 1. Red de computadores.



Si el host A (IP=210.23.5.14) se desea comunicar con el host C (IP=210.23.5.27), construye sus paquetes de datos y la capa de Red les coloca su dirección IP

(emisor) y la de C (destinatario), pasándolos a la capa de Enlace de Datos, que no sabe la dirección MAC de C. Para averiguarla, envía un mensaje a todas las máquinas de la red, conocido como petición ARP, preguntando cuál es la dirección MAC correspondiente a la IP 210.23.5.27. Las peticiones ARP son de tipo broadcast, es decir, peticiones que son enviadas a todos y cada uno de los equipos en la red.

La pregunta llega a todas las máquinas, pero sólo C contesta, enviando una respuesta con su dirección MAC. Entonces, A añade ambas direcciones MAC a los paquetes y los pasa a la capa Física, que lo transmite al medio.

2.1.5 Comunicación entre ordenadores en dos redes. Imaginemos ahora que el host C (IP=190.200.23.5) no se encuentra en la misma red que A (IP=210.23.5.14). Cuando éste envíe el broadcast preguntando la dirección MAC de C nadie le responderá, por lo que, si no se hace nada al respecto, la comunicación entre ambas máquinas resultará imposible.

Los encargados de solucionar este problema son unos dispositivos de red especiales, llamados routers, que conectan dos o más redes, sirviendo de enlace entre ellas. Los routers trabajan en la capa de Red, encargándose de encaminar o enrutar paquetes de datos entre máquinas de redes diferentes.

Figura 2. Router Cisco 1601

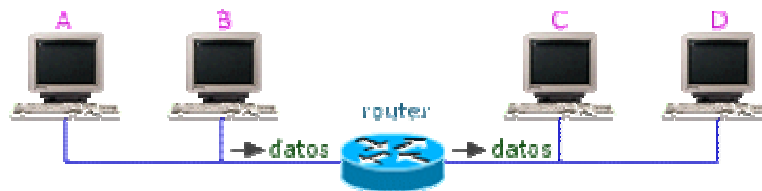


Router Cisco 1601-R

Para poder funcionar de esta forma deben pertenecer a cada una de las redes que conectan, como si fueran un host más de las mismas. De esta forma, un router que conecte dos redes debe tener una tarjeta de red diferente para cada una de las redes y, consecuentemente, dos direcciones MAC diferentes. También debe tener asignada una dirección IP en cada una de las dos redes, ya que si no sería imposible la comunicación con las máquinas de las mismas.

El esquema de dos redes conectadas por un router podría ser el representado en la siguiente imagen:

Figura 3. Red conectada con router.



Ahora, cuando un host envía una petición ARP para averiguar la dirección MAC correspondiente a una IP dada y no es respondido por ningún equipo de su red, envía los paquetes correspondientes a un router que tiene configurado para este tipo de envíos, denominado gateway por defecto.

Una vez que el router recibe los paquetes de datos utiliza un parámetro especial, denominado máscara de red, que sumado lógicamente a la dirección IP destino le da la red a la que pertenece el host buscado. Pasa entonces los paquetes a la red a la que pertenece C, haciendo una nueva petición de broadcast preguntando la MAC de C. Este le responde, y entonces el router le envía los paquetes directamente. Si C desea responder a A, el proceso se invierte.

Este proceso es necesario realizarlo sólo una vez, ya que en esta tanto los host A y C como el router anotan las parejas de direcciones MAC-IP en unas tablas especiales, denominadas tablas de enrutamiento, que usarán en envíos de datos posteriores para enrutar los paquetes directamente.

Resumiendo, los routers son los principales responsables de la correcta comunicación entre máquinas de diferentes redes, encargándose en este proceso de enrutar correctamente los paquetes de datos.

2.1.6 Cómo funciona un router. Los routers son dispositivos de red que raramente se encuentran aislados entre sí. Al contrario, suelen estar interconectados, formando una especie de “telaraña” que hace posible el tráfico de datos entre redes separadas físicamente.

Tomando como ejemplo la Red de redes, Internet, cuando un ordenador envía una serie de paquetes de datos a otro situado en otra ciudad o país, estos son encaminados de router a router a lo largo del camino entre ambas máquinas. Cada paso de un paquete de un router a otro se denomina “salto”, y el principal objetivo de todos y cada uno de los routers que intervienen en la transferencia del paquete es que éste llegue a su destino en el menor número posible de saltos, por la mejor ruta posible.

Para poder realizar esta tarea, los routers se comunican constantemente entre sí, informándose de las rutas bloqueadas, de las máquinas intermedias que se encuentran caídas o saturadas de tráfico, aprendiendo con ello cuál es el router idóneo para enviarle los paquetes recibidos.

Si consideramos ahora el caso de un router segmentando una red local (LAN), aunque ahora no debe enviar los paquetes a otro router, sí que tiene que saber por qué puerto debe enviar los datos para que lleguen a la máquina local destino.

Esta habilidad de “saber” a dónde tienen que enviar los paquetes de datos que reciben la consiguen almacenando en su interior una tabla especial, conocida como tabla de ruteo, en la que van anotando las direcciones IP de las máquinas que se comunican con él y el puerto por el que está accesible esa máquina.

Así, cuando a un router llega un paquete, mira en su tabla de ruteo. Si está en ella referenciada la dirección IP de la máquina destino, también lo estará el puerto por el que ésta es accesible, con lo que envía por él el paquete. En caso de no estar la IP en la tabla, manda una petición de respuesta por todos los puertos, preguntando en cuál de ellos se encuentra la máquina destino, y una vez obtenido el puerto de acceso, ingresa la nueva pareja IP/PUERTO en su tabla de ruteo, con lo que los próximos paquetes para esa máquina los enviará directamente.

Podemos buscar una analogía del funcionamiento de los routers con el de las oficinas de correos. Cuando enviamos una carta desde Mérida (Badajoz) a Linares (Jaén), ésta llega en primer lugar a la oficina local de Mérida, que la reenvía a la de Badajoz, que a su vez la manda a la de Jaén, que la remite a la oficina de Linares, que hace la entrega. Si la oficina de correos de Jaén está cerrada por obras, la de Badajoz la enviará a la de Madrid, que la remitirá a la de Andujar, que a su vez se encargará de mandarla a la de Linares, haciendo ésta de nuevo la entrega. Cierre la oficina que cierre, siempre se encontrará un camino para entregar la carta.

Para evitar mantener en su tabla direcciones IP que hayan quedado obsoletas, cada cierto tiempo borra aquellas que no tienen actividad y las que, tras enviarles paquetes, no han respondido. Esto lo consiguen manteniendo “conversaciones” entre ellos, en unos lenguajes especiales denominados “protocolos de enrutamiento”.

Tabla 1. Enrutamiento simple.

Destino	Métrica	Interfase
210.100.12.0	0	Ethernet0
210.100.12.5	0	Etehernet0
192.80.26.13	8	Serial0
135.0.25.124	5	Serial 1

2.1.7 Componentes básicos de un router. Básicamente, podemos considerar un router como un ordenador especial que funciona solo en las tres primeras capas de la arquitectura TCP/IP, al que se le han eliminado una serie de componentes físicos y funcionalidades lógicas que no necesita para su trabajo, mientras que se le han añadido otros componentes de hardware y de software que le ayudan en su trabajo de enrutamiento.

Como todo ordenador, un router necesita un sistema de arranque (bootstrap), encargado de realizar un chequeo del resto de los componentes antes de pasar el control a un sistema operativo (Cisco IOS, en el caso de los routers Cisco).

El sistema de arranque se almacena en una memoria ROM (Read Only Memory=Memoria de Solo Lectura), junto con una parte básica del sistema operativo, la que toma el control inicialmente, mientras que el cuerpo principal de éste se almacena en una memoria especial, de tipo FLASH, que se puede borrar y reprogramar, permitiendo con ello las actualizaciones necesarias. El contenido de la memoria Flash se conserva en caso de cortes de energía o durante los reinicios del router.

Por otra parte, las funcionalidades operativas de los routers son configurables mediante una serie de instrucciones escritas en un fichero de texto, denominado

archivo de configuración, que se almacena en un módulo de memoria de tipo NVRAM (No Volatil RAM), cuyo contenido se conserva durante un corte de energía o si se reinicia el equipo.

Una vez inicializado un router, el fichero de configuración es cargado en una memoria RAM (Random Access Memory=Memoria de Acceso Aleatorio), desde la que se va ejecutando el conjunto de órdenes en él contenido. También se almacenan en esta memoria las tablas de enrutamiento, encargadas de almacenar los puertos del router por los que son accesibles las diferentes máquinas.

Por último, el router posee una serie de puertos o interfaces físicas, puntos de conexión del mismo con las diferentes redes a las que está unido, y a través de los cuales se produce la entrada y salida de datos al equipo. El número de interfaces depende del tipo y funcionalidades del router (y de su precio, claro).

Figura 4 Router multipuerto Cisco 2611.



2.1.8 Tipos de routers. Los tipos de router a usar en una red varían dependiendo del tipo de ésta, del número de usuarios y de la función o funciones que deba desempeñar, pudiendo variar mucho la complejidad y el precio de ellos en función del tipo elegido.

Si queremos segmentar nuestra red en diferentes subredes, nos hará falta un router de segmentación, con tantos puertos Ethernet como subredes queremos

crear (más los de enlace con otros routers), siendo siempre conveniente que nos sobren puertos, con vista a futuras ampliaciones en la red. Cada subred utilizará luego un hub concentrador o un switch para dar acceso a sus clientes individuales. Podemos desear un ancho de banda dedicado para un número elevado de equipos individuales, prescindiendo así de los hubs. Necesitaremos entonces un routers de concentración, que precisa aún más puertos Ethernet, aunque no suele ser necesario que sean de alta velocidad de transmisión.

Para conectar una red corporativa a Internet necesitaremos un router de frontera, que actuará como gateway de la red interna, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

En caso de tener que conectar dos redes WAN o dos segmentos de red en sucursales o campus diferentes, necesitaremos un routers de backbone, que proporciona transporte óptimo entre nodos de la red, con interfaces de alta velocidad que proporcionan un elevado ancho de banda. Generalmente estarán basados en tecnología de fibra óptica.

Por último, también es posible al acceso a redes inalámbrico a redes mediante routers con tecnología wireless, un medio práctico de liberar los equipos de las limitaciones de los cables físicos.

Figura 5. Router Wireless



Router wireless Barricade 7004AWBR

2.1.9 Protocolos de enrutamiento. Hemos visto antes que los routers mantienen unas tablas de enrutamiento, en las que van anotando las direcciones IP de las máquinas destino y los puertos adecuados para darles salida de forma óptima.

Los routers suelen encontrarse interconectados entre ellos, pasándose los paquetes de datos de uno a otro, hasta llegar a la máquina destino. Como cada router tan solo es responsable de las máquinas directamente conectadas a él (incluyendo los routers vecinos), se hace necesario un mecanismo que permita a los routers comunicarse entre sí, para evitar que cada uno tenga en sus tablas registros inválidos.

Esto se consigue por medio de una serie de protocolos de enrutamiento, responsables de que los diferentes routers mantengan sus tablas de enrutamiento acordes, obteniéndose una red convergente. Con ello se consigue, por ejemplo, que si un ordenador o un servidor se apaga en una red, los routers sepan que ya no está accesible, evitando el envío de datos que no llegarán a su destino, y disminuyendo con ello el tráfico de red.

Para mantener las tablas de enrutamiento actualizadas, un router pueden mandar a los routers vecinos una copia de su tabla cada determinado periodo de tiempo (enrutamientos por vector de distancia) y también cuando alguna máquina en su red sufre algún cambio (enrutamiento por estado de enlace). Depende del protocolo de enrutamiento con que funcione.

Existen diferentes protocolos de comunicación entre routers, cada uno de los cuales utiliza mecanismos propios para conseguir la convergencia en la red y para determinar el mejor camino que puede seguir un paquete de datos en su viaje hasta la máquina destino, y cada uno utiliza un sistema de determinación de mejor ruta (métrica) diferente.

Según su misión en una red podemos diferenciar dos tipos principales de protocolos de enrutamiento: los protocolos de gateway interior (IGP), encargados de la comunicación entre routers de una misma red, entre los que destacan RIP e IGRP, y los protocolos de gateway exterior (EGP) o de frontera, encargados de la comunicación entre routers de redes diferentes.

Entre los más importantes protocolos de enrutamiento podemos destacar los siguientes:

RIP (Protocolo de Información de Enrutamiento), es un protocolo de enrutamiento por vector de distancia que calcula las distancias hacia la máquina destino en función de cuántos routers debe atravesar un paquete para llegar a su destino (saltos), enviando cada paquete de datos por el camino que en cada momento muestre una menor distancia. RIP actualiza las tablas de enrutamiento a intervalos programables, generalmente cada 30 segundos. Es un buen protocolo de enrutamiento, pero necesita que constantemente se conecten los routers vecinos, generándose con ello una gran cantidad de tráfico de red.

IGRP (Protocolo de Enrutamiento de Gateway Interior), desarrollado por Cisco System, es un protocolo de enrutamiento por vector de distancia que usa una métrica compuesta basada en diferentes variables de red, como ancho de banda, unidades máximas de transmisión (MTU), confiabilidad, etc. Envía actualizaciones de las tablas de enrutamiento cada 90 segundos.

EIGRP (Protocolo de Enrutamiento de Gateway Interior Mejorado), protocolo mixto basado en IGRP, basado en una métrica de vector distancia, pero que manda actualizaciones de las entradas de las tablas que han cambiado por haber sido alterado el estado de alguna máquina de su red.

OSPF, protocolo puro de estado de enlace, que calcula las rutas más cortas y accesibles mediante la construcción de un mapa de la red y el mantenimiento unas bases de datos con información sobre su sistema local y sobre los vecinos. Cuando una máquina de su sistema cambia, se envía esa entrada de la tabla a los routers vecinos.

El protocolo de enrutamiento a elegir en cada caso depende del tipo de red (LAN, WAN, etc.), de su topología y del uso de la misma, siendo posible en la mayoría de los casos configurar varios protocolos en un mismo router.

2.2 PROTOCOLO FRAME-RELAY

Frame Relay es una interfaz de redes. Es aproximadamente análoga a una versión reducida de X.25 con una interfaz conmutadas por paquetes de velocidad variable entre 56 Kb/s y 45 Mb/s. Como X.25, Frame Relay multiplexa estadísticamente paquetes o tramas hacia destinos diferentes con una sola interfaz. Esta orientada a la conexión, lo que significa que un circuito virtual debe estar configurado para comunicaciones. Esto se hace típicamente mediante un enlace de señalización en banda.

No existe nada en los estándares que diga que una red Frame Relay debe ser una red rápida por paquetes. Frame Relay podría ser una interfaz usada por una red rápida SMDS por paquetes. Los estándares de Frame Relay establecen pocas premisas.

Existen algunas implicaciones debidas al diseño de la interfaz. La interfaz no intenta corregir errores, no existen vías para la retransmisión de datos, lo cual implica que Frame Relay no ejecuta una retransmisión de mensajes contaminados. Los protocolos de redes locales que Frame Relay esta diseñando, tiene ya incluidas rutinas de corrección y retransmisión de mensajes contaminados. Los protocolos de redes locales que Frame Relay esta diseñando, tienen ya incluidas rutinas de corrección y retransmisión por lo que realizar de nuevo todo ese trabajo en las capas de red es ineficiente y redundante. Aunque es inevitable que las interfaces Frame Relay sean eventualmente colocadas en arquitecturas de red que dispongan de reconocimiento de mensajes y entrega confiable, hacer esto anularía una de las ventajas clave de Frame Relay. La ausencia de mecanismos de corrección de errores de transmisión es un beneficio que conduce a un mejor desempeño de la red.

Otra implicación de Frame Relay y del amplio soporte industrial que ha acumulado en poco tiempo, es que existirá un buen grado de compatibilidad entre redes publicas y privadas. Las arquitecturas de redes híbridas públicas / privadas darán a los administradores de redes más herramientas para afrontar efectivamente los retos de ingeniería que impone su trabajo.

En palabras más simples, Frame Relay es un servicio rápido de conmutación de paquetes de longitud variable, para transportar datos sobre áreas extensas. Es una evolución de X.25 que tiene la ventaja de una transmisión de mejor calidad, con mayor rapidez y reduciendo el encabezado de chequeo de errores. Frame Relay soporta tasas de transmisión de hasta 2 Mb/s. Esta controlado por los estándares ANSI T1.617 anexo D y por el UIT-T Q.933 anexo A. El foro de Frame Relay esta trabajando en una alta capacidad de 45 Mb/s para la interfase red-red.

Frame Relay tiene servicios con conexiones permanentes y conexiones virtuales conmutadas (PVC y SVC). Los elementos típicos de la red Frame Relay son: los

dispositivos de acceso a Frame Relay (FRAD) y los conmutadores de Frame Relay (FRS).

Permite la implementación de servicios de acceso por demanda, reduciendo costos en la transmisión de ráfagas de datos. Los usuarios pagan por el cargo de una Tasa de Información Convenida o Compromiso CIR baja, pudiendo enviar datos a tasas mucho mayores cuando lo necesiten.

La mayoría de las implementaciones de FR son una alternativa de bajo costo para las conexiones de líneas alquiladas y otras redes de datos.

Las aplicaciones WAN de Frame Relay son muchísimas a nivel mundial. Los estándares de la interacción de FR/ATM están muy avanzados ya que el despliegue de ambas tecnologías esta marcado por una rápida expansión, que fuerza su interacción; y, los Foros de Frame Relay y ATM han cooperado para producir un acuerdo común. Este acuerdo permite el diseño de las unidades de interacción FR/ATM ínter operables.

Las funciones de interacción IWFs que traducen FR a ATM y viceversa están definidas en las Rec. UIT-T I.555 y en el acuerdo de implementación del Foro de Frame Relay, FRF.5 de diciembre 20 de 1994.

2.2.1 ¿Por qué usar “Frame Relay”? La razón principal para usar Frame Relay es obtener una mejor conectividad entre redes de área local por un precio menor. Cambiar los componentes de las redes a Frame Relay es un proceso relativamente simple, Frame Relay usa la infraestructura de comunicaciones existente; a menudo se trata típicamente de una actualización del “software” de los enrutadores, y una actualización menor del “software” y del “hardware” de algunos conmutadores de paquetes.

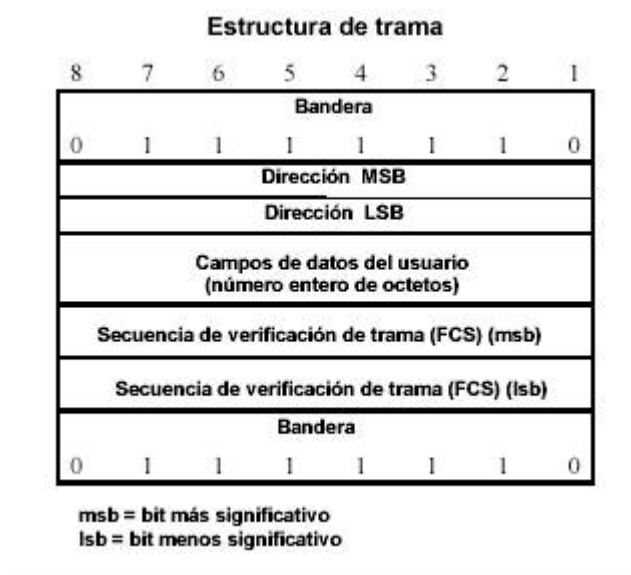
Los servicios públicos de Frame Relay pueden constituir un reemplazo (con ventajas en los costos) de las líneas dedicadas, o pueden ser una buena interfaz para ser usada sobre estas líneas. Los servicios públicos de Frame Relay podrían permitir la justificación de un enlace con localidades remotas que de otra forma quedarían incomunicadas. Frame Relay ofrece ahorros inmediatos a los usuarios de multiplexadores, porque ofrece un mejor control sobre su ancho de banda y costos menores, gracias a un mejor uso de la línea. Frame Relay permite un mejor desempeño y menos lastre en las tareas de interconexión de redes de área local.

2.2.2 Estructura de trama. Parte del atractivo de Frame Relay es su estructura directa. Una trama de Frame Relay puede ser enviada sobre cualquier enlace serial de bits. Cada trama esta delimitada por dos secuencias de bit de 011111110, llamadas banderas (“flags”), cuya unicidad en el caudal de bits está garantizada. Sólo puede existir una bandera entre tramas. Al igual que en otros protocolos tipo HDLC orientados hacia el bit, los circuitos de envío y recepción insertan ceros en el caudal de bits luego de cualquier sucesión de cinco unos consecutivos para mantener la irrepetibilidad de la secuencia bandera. Otra secuencia especial (siete unos seguidos) se emplea para señalar el aborto de la trama.

Aparte de los datos del usuario, existen solo dos campos en una trama: el encabezado y cola. El encabezado viene después de la bandera de inicio y contiene la dirección, llamada Identificador de Conexión del Enlace de Datos (“Datos Link Connection Identifier”, DLCI), además de algunos bits de señalización. El otro campo se llama Secuencia de Verificación de Trama (“Frame Séquence Check”, FSC), la cual es una comprobación de redundancia cíclica UIT-T (CRC 16) que representa la suma del contenido total de la trama (incluyendo la DLCI). La secuencia de verificación de trama se usa para determinar si la trama ha sido corrompida durante la transmisión. No existe ningún campo de longitud; la

longitud de una trama se deriva del número de byte/octetos enviados entre dos banderas. En una trama puede haber hasta 8 Kbytes de datos del usuario, aunque algunas redes pueden tener límites inferiores.

Figura 6. Estructura de trama Frame-Relay



La dirección numérica especificada para una trama por la DLCI identifica hacia cual circuito va dirigida, y por el número del circuito, la red Frame Relay conoce tanto el origen como el destino de la trama. Estas son las tres variantes del identificador de conexión de enlace de datos (DLCI): 2 bytes, 3 bytes y 4 bytes. El bit menos significativo de cada byte de encabezado se hace cero para indicar una extensión hacia el próximo bit, y si es uno, esto quiere decir que se trata del último byte del encabezado. Cada byte añade progresivamente más espacio para la dirección. La variante usada más comúnmente es la de 2 bytes.

Figura 7. Formato DLCI.

DLCI de 2 bytes				
(segmento superior DLCI)			C/R	EA 0
(segmento inferior DLCI)	FECN	BECN	DE	EA 1

Formato de dirección por defecto 2 bytes

DLCI de 3 bytes				
(segmento superior DLCI)			C/R	EA 0
DLCI	FECN	BECN	DE	EA 0
(segmento inferior DLCI)			D/C	EA 1

Formato de dirección de 3 bytes

DLCI de 4 bytes				
(segmento superior DLCI)			C/R	EA 0
DLCI	FECN	BECN	DE	EA 0
DLCI				EA 0
(segmento inferior DLCI)			D/C	EA 1

Formato de dirección de 4 bytes

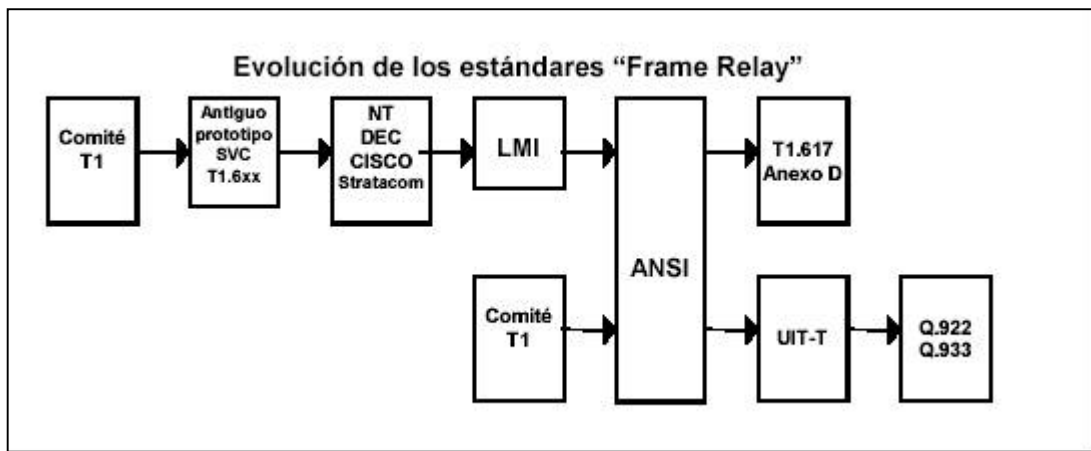
En el encabezado existen tres bits dedicados a especificar la información de congestión. Elegible para Descartar (“Discard Eligible, DE), Notificación de Error por congestión hacia Adelante (“Forward Error congestión Notificación”, FECN) y Notificación de Error por congestión hacia atrás (“Backward Error congestión Notifiacion”, BECN). En la variante de 2 bytes de la DLCI, se deja un espacio de 10 bits para la dirección, lo cual significa que cualquier nodo puede mantener hasta 1024 conexiones activas. De estas, la superior y la inferior se reservan para señalización y otros usos. Un circuito virtual especial (el Circuito 0) se usa para transferir información de señalización.

Debido a razones históricas, algunos equipos antiguos emplean la dirección 1023 para señalización.

2.2.3 Historia de Frame Relay. Frame Relay provino originalmente de trabajos en ISDN. Se pensó que se emplearía en canales Portadores de 64 Kb/s con

señalización en el canal D del sistema ISDN. Algunos de los conceptos de Frame Relay fueron tomados de cuatro fabricantes: Cisco Systems, Northern Telecom., DEC y Stratcom, quienes presentaron una variante reducida que ha sido bautizada como Interfaz de Manejo Local (“Local Management Interface”, LMI).

Figura 8. Evolución de Frame- Relay



Mientras que los estándares originales ANSI para relevadores de trama (“Frame Relay”), T1.617 y T1.618, manejaban sólo redes SVC, la versión reducida LMI proponía una alternativa PVC mucho más simple. La interfaz LMI ganó popularidad industrial rápidamente engendrando su propio cuerpo de pseudocódigo estándares industriales a través del Foro de “Frame Relay”. Esta popularidad garantizó su incorporación a los estándares. Luego de cambios menores (principalmente se trasladó el circuito de señalización del 1023 al 0), LMI fue adoptado como el Anexo D de T1.617 y su correspondiente Q.933 del UIT-T.

Todas las redes “Frame Relay” disponibles ahora se basan en PVC, pero a medida que las redes vayan creciendo, estas conexiones permanentes deberán cambiarse a una operación mas dinámica tipo SVC (Conexiones Virtuales

Conmutadas). La tecnología SVC se encuentra ya avanzada por parte de muchos fabricantes de equipos.

Figura 9. Estándares Frame-Relay.

Estándares "Frame Relay"

UIT-T

I.122	Estructura para proporcionar Servicios Adicionales de Portadora en Modo de Paquete.
Q.922	Especificaciones de la Capa de Enlace de Datos ISDN para Servicios de Portadora en Modo de Trama.
Q.933	Especificación de Señalización ISDN para Servicios de Portadora en Modo de Trama.

ANSI

T1.606	Servicios de Portadora con Relevo de Trama.
T1.606	Manejo de Congestión.
T1.617	Especificación de Señalización para Servicios de Portadora con Relevo de Trama.
T1.618	Aspectos Centrales del Protocolo de Trama para uso en Servicios de Portadora con Relevo de Trama.

2.2.4 Redes PVC. En una red PVC los circuitos son configurados por operadores, siendo aquellos prácticamente permanentes. La información de señalización que debe ser distribuida consiste en una actualización del estado de los circuitos desde la red hacia los nodos terminales. De esta forma la red puede notificar a los usuarios de la incorporación de nuevos circuitos o de la eliminación de los antiguos. La información de estos("status") es distribuida a través de un procedimiento de control mediante una función de autoprueba de calidad de la señal que se denomina "heartbeat polling".

Figura 10. Autopruueba de calidad de Frame-Relay.

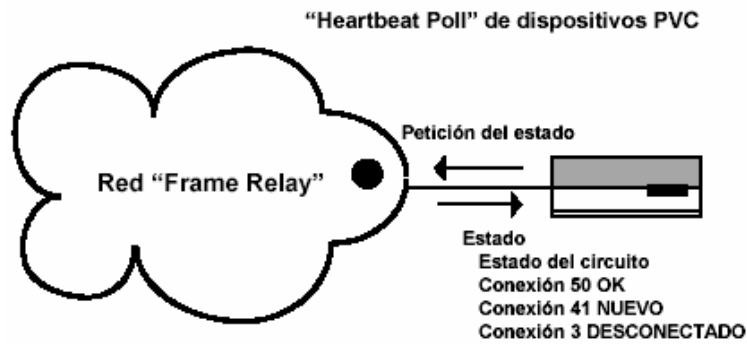
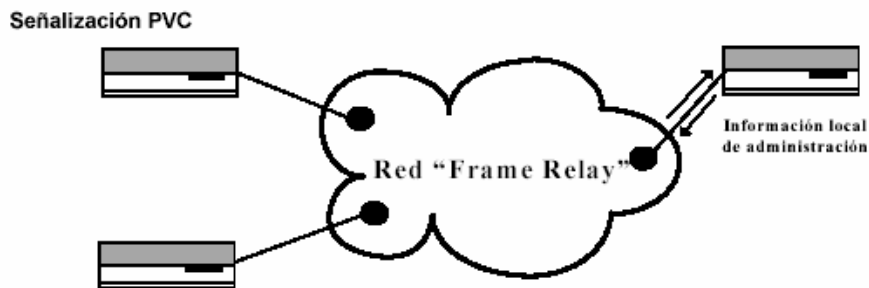
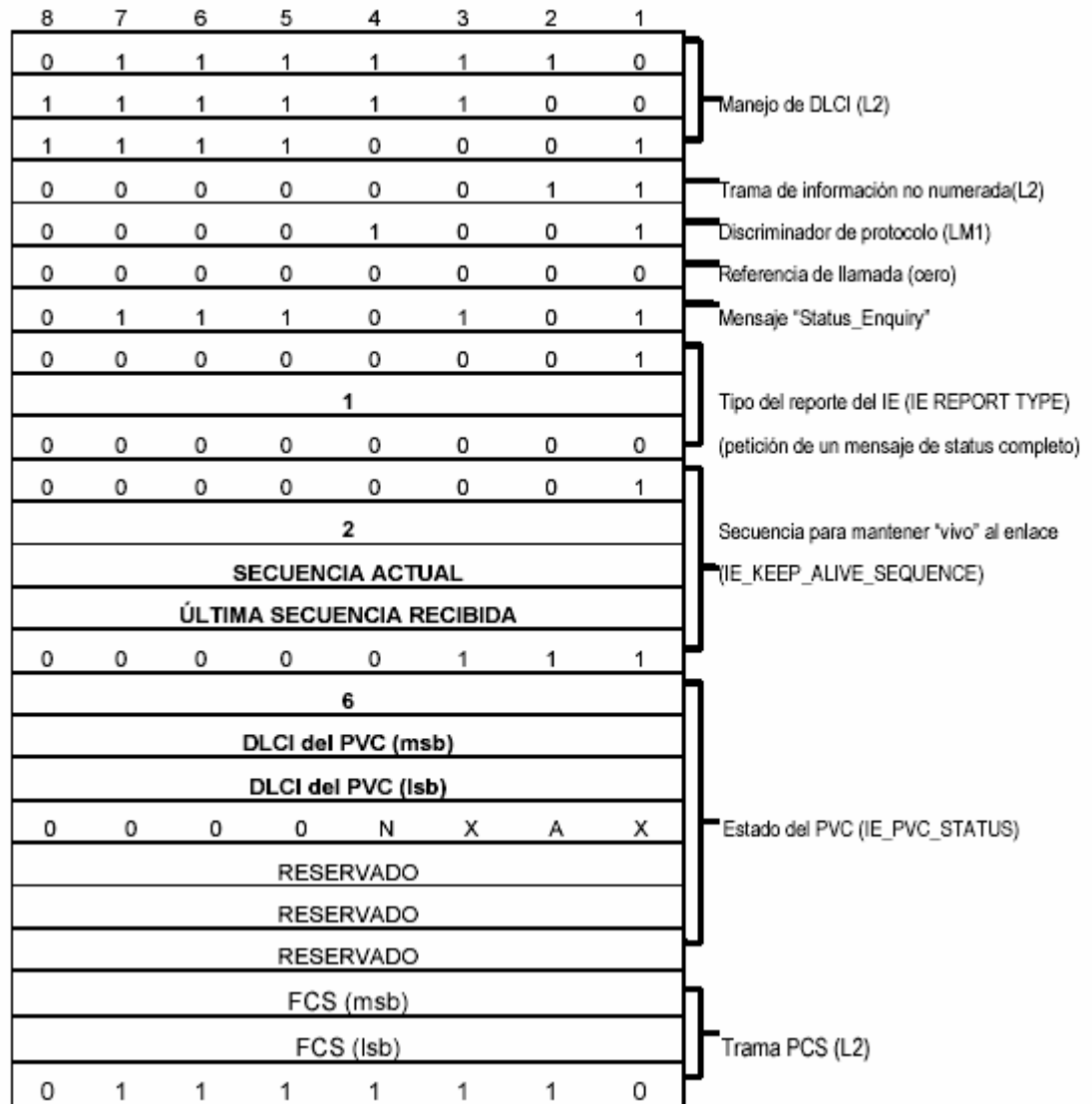


Figura 11. Señalización PVC



Es responsabilidad de los nodos terminales el pedir periódicamente a la red la información de estado (típicamente cada 30 segundos). La red responde a los mensajes de STATUS – ENQUIRY del nodo terminal con un mensaje de STATUS. Si transcurre un cierto número de ciclos de petición de estado sin recibirse ningún mensaje de STATUS – ENQUIRY, la red declara “muerto” al enlace respectivo, hasta que las peticiones se restablezcan. De forma similar, si la red tarda demasiado en responder con un mensaje de STATUS, el nodo terminal del usuario declara “muerto” al enlace.

Figura 12. ESTADO "STATUS"



Puesto que "Frame Relay" no garantiza una entrega confiable, se debe seguir una serie de pasos para asegurar que la información de estado ha sido recibida en el nodo del usuario. Esto se hace para evitar situaciones tales como las que ocurrirían con la eliminación de un circuito y la incorporación de uno nuevo bajo el

mismo número, mientras que la información de STATUS se ha perdido en tránsito; lo cual dejaría al usuario con la posibilidad de una conexión incorrecta.

La entrega confiable se logra mediante el intercambio de las secuencias numéricas del Elemento de Información (IE) KEEP_ALIVE_SÉQUENSE.

Existen dos secuencias de números en el IE KEEP-ALIVE, uno con la secuencia del mensaje actual, y otro con la última secuencia recibida por el otro extremo del enlace. Siguiendo la pista a estas dos secuencias numéricas, la red puede detectar si ha ocurrido la pérdida de la información de señalización y reenviarla o tomar cualquier otra acción correctiva que fuese necesaria (suspender la incorporación de nuevos circuitos con direcciones liberadas recientemente por la eliminación de otros).

El usuario puede elegir entre dos formas del mensaje de STATUS. Una de ellas es un mensaje breve para simplemente intercambiar las secuencias numéricas y mantener vivo el enlace, y la otra es un mensaje completo del estado, con un elemento de información (IE) para cada circuito que está conectado en ese instante a la red. Cada uno de estos IE de PVC_STATUS contiene información importante relativa al circuito, como por ejemplo su estado de congestión, la velocidad para la cual ha sido configurado y si se trata de un circuito nuevo o eliminado. La red tiene la opción de responder con un mensaje completo de estado, aún si el usuario pidió sólo el mensaje corto, si existiese la necesidad de informarle sobre adiciones o eliminaciones importantes.

2.2.5 Redes SVC. Mientras que las redes PVC son sencillas de implementar, existen limitaciones inherentes a su diseño que las hacen indeseables en redes de mayor tamaño. Por esta razón la tecnología "Frame Relay" SVC está estandarizada y en desarrollo.

La señalización SVC se parece a la señalización ISDN para llamadas telefónicas. Consiste en dos capas, enviadas sobre la dirección 0 de la DLCI. En la capa dos, un protocolo llamado Procedimientos de Acceso al Enlace para Tramas (“Link Access Procedures for Frames”, LAPF) asegura la confiabilidad de la entrega de los mensajes de señalización. LAPF es un protocolo basado en estado que reconoce la recepción de todos los mensajes y puede regular el tráfico.

La capa que está por encima de LAPF transmite los mensajes del circuito. Para preparar o eliminar circuitos, se intercambia una secuencia de mensajes entre los elementos de la red. El diagrama anterior describe brevemente los intercambios requeridos. Algunos campos del mensaje (IE) especifican, por ejemplo, lo relativo a la velocidad de información en el circuito, o cual dirección DLCI preferiría emplear el usuario para el circuito. Es potestad de la red tomar la decisión final sobre qué parámetros son concedidos, los cuales son especificados en el mensaje de respuesta CONNECT.

2.2.6 PVCs versus SVCs. Los PVCs son sencillos de implementar, pero a medida de que crece la complejidad de la red se incrementa la cantidad de esfuerzo por parte de los operadores y los recursos de conmutación necesarios para mantener controlado el crecimiento de la red. Desafortunadamente, la señalización SVC sufre de las mismas complicaciones de implementación que hacen que el “software” ISDN es complejo y difícil de probar. El desarrollo de SVC es una aplicación primordial de los probadores de protocolo para “Frame Relay”.

2.2.7 Congestión. Como se mencionó antes, tres bits en la DLCI se destinan a la notificación y el manejo de la congestión. La congestión es una consideración importante en redes “Frame Relay”. Además de la ausencia de mecanismos de corrección de errores, otra consecuencia básica de la remoción del lastre asociado a las arquitecturas de almacenamiento y reenvío de paquetes, es la ausencia de cualquier tipo de mecanismo implícito de control de flujo.

En una red “Frame Relay”, la única respuesta que puede dar la red al fenómeno de la congestión es enviar la notificación de congestión a los nodos afectados y descartar una parte de los datos. A medida que los nodos terminales se hacen más inteligentes, es más fácil implementar mecanismos de prevención de congestión más cercanos al “software” de aplicación que está generando el tráfico. Es difícil regular el tráfico de una red local sin conocer las aplicaciones que están involucradas. Es el “software” de aplicación quien mejor sabe cómo reducir sus demandas sobre la red.

Por esta razón, las redes “Frame Relay” modifican los bits FECN (Notificación de Error por congestión hacia delante) y BECN (Notificación de Error por Congestión hacia Atrás) de las tramas en circuito para indicar cuándo está verificándose una situación de congestión en algún lugar en el camino de un circuito virtual. El bit FECN notifica al receptor que el circuito del cual provino la trama está sufriendo de congestión en la dirección de entrada, de forma que el receptor pueda intentar disminuir sus solicitudes de datos a la fuente. El bit BECN notifica al receptor de una trama que los datos que está enviando en la otra dirección de ese circuito están experimentando congestión, de manera que el equipo transmisor puede reducir su tasa de envío.

El otro bit que puede ser usado en situaciones de congestión es el bit de Elección de Descargo (DE). Los nodos terminales pueden voluntariamente colocar este bit en el tráfico saliente para indicar cuales bloques de datos son menos importantes y por lo tanto pueden ser los primeros en descartarse (datos como los relativos a la actualización de las rutinas de enrutamiento, los cuales pueden perderse sin mayores consecuencias). Se supone que la red hará lo posible por descartar las tramas señaladas por el bit DE antes que las otras.

Desafortunadamente, esta filosofía de diseño no se ajusta del todo con los protocolos de redes actuales, cuyo diseño no contempla el concepto de congestión. Típicamente, la interfaz de red en la que se emplea “Frame Relay” es un enrutador multiprotocolo que no tiene ninguna comunicación real con el “software” de aplicación que esta generando el tráfico.

Más grave es que la respuesta típica de un protocolo LAN a una pérdida de datos sea transmitir aún más datos. Esto significa que una red que descarta tráfico LAN podría incrementar el tráfico. A menos que la red sea cuidadosamente diseñada para evitar situaciones de congestión, el descarte por congestión en cantidades suficientes podría disparar una condición en la que la red transmita cada vez menos datos efectivos, al provocarse más y más retransmisiones. No obstante, empleando instrumentos de prueba apropiados para supervisar la congestión y diseñando cuidadosamente el ancho de banda a ser empleado, esta situación debería ser muy poco frecuente.

2.2.8 Tarifación. El diseño de la red y el bit DE también entran en juego en la tarifación de “Frame Relay”. Todos los esquemas conocidos de tarifación relacionan el precio del enlace a un concepto llamado Tasa de Información Compromiso (“Committed Information Rate”, CIR). La CIR de un enlace es la cantidad de datos cuya entrega está garantizada por la red (sin descartar nada) sobre un periodo de tiempo. La información que se envía a la red se cobra en función de la CIR especificada para el circuito. Si se transmiten más datos que la CIR especificada en un intervalo de tiempo específico, este exceso de datos es marcado con el bit DE al entrar en la red. La red todavía intentará entregar este exceso hasta un cierto punto (llamado a veces Tasa de Información), después del cual los datos serán descartados hasta el inicio del próximo intervalo de medición. Esta capacidad de un enlace de enviar ocasionalmente más datos se llama Capacidad de Ráfagas de Exceso (Excess Burst Capacity).

Este esquema implica que la tasa de información compromiso (CIR) de un circuito sería menor que la tasa de transmisión física del enlace, de forma que las ráfagas por encima del CIR aún puedan ser transmitidas. No obstante, hacer a la tasa de información compromiso (CIR) igual a la tasa de transmisión (es decir, anular la capacidad de manejar ráfagas) no está excluida. Tampoco se excluye que la CIR agregada de todos los circuitos conectados a un enlace exceda la tasa física de transmisión, haciendo imposible que todos los circuitos ejerzan su CIR completa al mismo tiempo.

2.3 VOZ SOBRE IP

Tradicionalmente la transmisión de la voz y los datos se ha realizado a través de redes diferenciadas. En la actualidad se estima que el tráfico de datos crece a una velocidad diez veces superior al tráfico de voz, al tiempo que se observa un proceso de convergencia para que sea una única red la que soporte la transmisión de voz, datos y vídeo. La conversión de la voz en paquetes de datos utilizando Protocolo de Internet (IP) es lo que se ha dado en llamar la VoIP. Hasta el momento la transmisión de voz se ha venido realizando mediante la conmutación de circuitos; gracias al protocolo de Internet se puede transformar la voz en paquetes de datos y transmitirla, por tanto, como si de datos se tratara a través de una única red, dando lugar a lo que se denomina “red multi-servicio”. La convergencia de distintas redes en una sola representa un gran ahorro tanto en mantenimiento como en su gestión y uso. Hay que señalar que la tecnología IP no es nueva y, aunque su potencial ya se percibía desde hace tiempo, ha sido gracias al incremento del número de internautas y sobre todo el despegue de la banda ancha cuando se ha comenzado a considerar como una alternativa real de futuro.

Se entiende por la voz sobre IP o VoIP (del inglés Voice over Internet Protocol) a la digitalización de la voz y su transmisión a través de la red siguiendo el Protocolo

de Internet, es decir, mediante la conmutación de paquetes en los que la información se transfiere fragmentada. La conmutación de paquetes se basa en que la información transmitida (voz en este caso) se trocea y cada trozo o paquete se envía de forma independiente con la misma dirección de destino (receptor) donde vuelve a reagruparse y de esta forma, se recupera la información. La telefonía tradicional, sin embargo, se realiza a través de la denominada Red Telefónica Conmutada (RTC). En la telefonía tradicional, a diferencia de la VoIP, durante el tiempo que dura la comunicación se produce una asignación permanente de circuitos que quedan dedicados en exclusiva a esa comunicación hasta que finaliza.

La VoIP al tratar la voz como si de datos se tratara permite la utilización de una única red, por lo que su gestión y uso representa un importante ahorro económico para los usuarios. El número de usuarios con acceso a Internet y el despegue de la banda ancha están haciendo que aumente la demanda de este tipo de servicios. Se estima que en el año 2003 se cursaron más de 24.000 millones de minutos mediante VoIP.

Ha sido el sector empresarial el primero en percibir las ventajas y los potenciales ahorros que representa la migración de los sistemas tradicionales de telefonía a los servicios de voz sobre IP. Ahora bien, es el ahorro en costes la principal razón para que las empresas puedan realizar importantes ahorros, sobre todo aquellas que dispongan de varias sedes interconectadas, aunque su cuantificación efectiva es difícil de determinar.

Por tanto, las empresas encaminarán sus esfuerzos a integrar servicios y redes, lo que ha venido a denominarse como ALL OVER IP (todo sobre IP), aunque bien es verdad que en la actualidad el incentivo más importante para la implantación de la VoIP en las empresas es el ahorro de costes.

Las ventajas, además de las económicas, vienen del lado de las nuevas aplicaciones y de la integración de servicios entre los que se puede destacar: (1) el desarrollo de call centers que requieran de la unificación de voz y datos, (2) la integración de redes privadas virtuales como por ejemplo la de bancos y corporaciones, y (3) las aplicaciones de multiconferencias y fax para todo tipo de organizaciones. Todas ellas, aún siendo de difícil cuantificación en la cuenta de resultados, representan importantes ventajas competitivas de cara al futuro y están impulsando la implantación de la VoIP en las empresas.

La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

Cuando hacemos una llamada telefónica por IP, nuestra voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de Internet a la persona con la que estamos hablando. Cuando alcanzan su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

La utilización de la telefonía sobre IP como sustituto de la telefonía convencional se debe, principalmente, a su reducido coste.

A finales de 1997 el VoIP forum del IMTC ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red de

VoIP. Debido a la ya existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base de la VoIP. De este modo, la VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre la VoIP. La VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

La VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:
 1. RAS (Registration, Admission and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
 2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS
- Señalización:
 1. Q.931 Señalización inicial de llamada
 2. H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz
 3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

- Compresión de voz:
 1. Requeridos: G.711 y G.723
 2. Opcionales: G.728, G.729 y G.722

- Transmisión de voz:
 1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
 2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- Control de la transmisión:
 1. RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Un aspecto importante a reseñar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es de más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP, cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un router.

2.3.1 Determinación de los requisitos de número de enlaces principales (Trunking). La velocidad de flujo de llamadas para la hora ocupada se puede traducir a los requisitos aproximados de ancho de banda de la red de datos. Para determinar los requisitos de número de enlaces principales, el flujo de llamadas a la hora ocupada se debe convertir a una medida del tráfico llamada erlang. Un erlang es equivalente a la cantidad de tráfico que puede manejar un único enlace principal o troncal en una hora. Para convertir el cálculo de hora ocupada a erlang, se debe dividir la velocidad del flujo de llamadas de 1 hora por 60 minutos y se añade al resultado el 15 por 100. Se añade el 15 por 100 para compensar la sobrecarga del establecimiento y la desconexión de la llamada. La ecuación es la siguiente:

Hora Ocupada = $(A/60 \text{ min}) \times 1,15 = \text{erlangas}$; donde A es la velocidad del flujo de llamadas en una hora. Y a su vez $A = \text{número de llamadas iniciadas durante el intervalo de tiempo} \times \text{la duración media de la llamada durante el intervalo}$.

El resultado es una cantidad adimensional para la hora ocupada. El paso final es determinar lo que se llama categoría del servicio (GoS, grade of service). La GoS es básicamente una estimación del número de llamadas que se bloquearán. Habitualmente, el objetivo de diseño es que la GoS esté comprendida entre 0,01 y 0,05, que se traduce entre una y cinco llamadas descartadas de cada 100. Afortunadamente, el mercado de las telecomunicaciones proporciona unas instrucciones para la selección de enlaces principales, que se basan en el tráfico de la hora ocupada y en la GoS. Estas gráficas se obtienen utilizando análisis estadísticos complejos de las distribuciones para la selección de enlaces principales.

2.3.2 Determinación de los requisitos de ancho de banda de red. Una vez se han determinado los requisitos de enlaces principales, el paso final es convertir el número de enlaces principales en requisitos de ancho de banda para los enlaces entre emplazamientos. Es un paso directo que necesita la información de número

de enlaces principales (trunking) y el ancho de banda de cada llamada de voz. La fórmula es la siguiente:

Ancho de banda = número de enlaces principales x ancho de banda del CODEC

Para tráfico G.729 que utiliza el Protocolo comprimido de tiempo real (CRTP, Compressed Real-Time Protocol), la fórmula se convierte en:

Ancho de banda = número de enlaces principales x 11,2 Kbps.

2.3.3 Determinación de la calidad de servicio (QoS). Una de las tareas más difíciles en la configuración de las redes de VoIP es la determinación de qué tipo de mecanismo de QoS se debería utilizar y dónde aplicar. Esta decisión requiere gran cantidad de información que se debe recopilar de múltiples fuentes. Los factores claves son los siguientes:

- ❖ Trayecto de las llamadas de voz.
- ❖ Algoritmo de codificación de voz.
- ❖ Modelos de router desplegados en la red.
- ❖ Utilización relativa del procesador en los routers.
- ❖ Modo de conmutación de paquetes empleado en los routers.
- ❖ Transportes de WAN de Nivel 2.
- ❖ Problemas del diseño de la calidad de voz.
- ❖ QoS y modelos de colas existentes.
- ❖ Versión de software del router.

2.3.4 Trayecto para las llamadas de voz. El determinar el trayecto que seguirán las llamadas de voz en paquetes a través de la red de datos es importante porque identifica los routers y enlaces individuales que se requieren para finalizar la llamada. Una vez identificado, se analizan en mayor detalle los routers y enlaces individuales para determinar qué técnicas de QoS se deberían aplicar. Este proceso sirve para identificar los componentes críticos que admitirán el tráfico de

voz. Además, si el trayecto completo no está bajo el control del administrador porque es Internet, una WAN subcontratada, una *red privada virtual* (VPN) de IP o está bajo el control de otro departamento, se deben identificar estas condiciones para que se puedan tomar las medidas adecuadas. Se puede utilizar encaminamiento basado en directivas y/o otras técnicas para dirigir el tráfico a través de los enlaces deseados.

2.3.5 Algoritmo de codificación de voz. El algoritmo de codificación de voz utilizado determina los requisitos de ancho de banda, variabilidad y latencia para las llamadas de voz. Son todos ellos factores importantes cuando se determina la técnica de QoS adecuada a aplicar.

Tabla 2. Características de ancho de banda de los algoritmos de codificación de voz:

Algoritmo	Ancho de Banda (flujo de voz en kbps)	Anchos de Banda (en paquetes en Kbps)	Ancho de Banda (con CRTP en Kbps)
PCM-G.711	64	82	67
CS-ACELP- G.729	8	26	11,2
MP-MLQ-G.723.1	6,3	20	10

Tabla 3. Característica de retardo de los algoritmos de codificación de voz:

Algoritmo	Retardo del algoritmo,ms	Retardo de búfer de reproducción, ms	Retardo de VAD, ms	Tamaño de paquete(mejor),bytes
PCM-G.711	0,75	5	5	168
CS-ACELP- G.729	10	5	5	28
MP-MLQ- G.723.1	30	5	5	38

Esta información, junto con el perfil de tráfico de voz, ayuda a determinar la cantidad de ancho de banda requerido para permitir el tráfico de voz. Los requisitos de ancho de banda se determinan multiplicando el número esperado de llamadas concurrentes por el ancho de banda consumida por cada llamada. El resultado influye en decisiones sobre si utilizar o no CRTP, además de características de QoS que limitan la velocidad, como la conformación de tráfico Frame Relay, conformación genérica de tráfico, el Protocolo de configuración de reserva de recursos (RSVP, Resource Reservation Setup Protocol) y la Velocidad de acceso comprometida (CAR, committed access rate). Las características de retardo influyen en los mecanismos de asignación de prioridades y de eficiencia del enlace, como el protocolo de punto a punto (PPP, point-to-point protocol) de múltiples enlaces con la fragmentación de enlaces y el entremezclado o fragmentación de Frame Relay FRF.12.

Tabla 4. Sugerencia de segmentación de LFI y FRF.12

		Reserva de ancho de banda/ Tamaño máximo de fragmento recomendado / Número máximo de llamadas		
		G.711	G.729/G729a	
		G.723.1		
Velocidad del enlace o CIR	Mecanismo de eficiencia			
32 kbps	LFI	Ancho de banda insuficiente.	12 kbps/15 ms/1	11 kbps/15 ms/1
	FRF.12	Ancho de banda insuficiente	12 kbps/60 bytes/1	12 kbps/60 bytes/1

56 kbps	LFI	Ancho de banda insuficiente	24 kbps/20 ms/2	33 kbps/20 ms/3
	FRF.12	Ancho de banda insuficiente	24 kbps/140 bytes/2	33 kbps/140 bytes/3
128 kbps	LFI	70 kbps/20 ms/1	60 kbps/20 ms/5	66 kbps/20 ms/6
	FRF.12	70 kbps/20ms/1	60 kbps/320 bytes/5	66 kbps/320 bytes/6
256 kbps	LFI	140 kbps/20 ms/2	156 kbps/20 ms/13	154 kbps/20 ms/14
	FRF.12	140 kbps/320 bytes/2	156 kbps/640 bytes/13	154 kbps/640 bytes/14
512 kbps	LFI	280 kbps/20ms/4	264 kbps/20 ms/22	264 kbps/20 ms/24
	FRF.12	280 kbps/1.280 bytes/4	264 kbps/1.280 bytes/22	264 kbps/1.280 bytes/24

2.3.6 problemas del diseño de la calidad de voz. La integración de voz en una red basada en paquetes representa un reto para los diseñadores de red y administradores de Redes de área Local (LAN). En una red de voz convencional, se reserva un intervalo de tiempo de 64 Kbps para transportar voz digitalizada. Ese intervalo de tiempo se basa en la utilización de Modulación por impulsos codificados (PCM) como método de digitalización de voz. Aunque se considera que PCM representa voz de buena calidad, su utilización es ineficiente. Otros

métodos más modernos de codificación de voz, como una familia de codificadores híbridos basados en una técnica de predicción lineal modificada desarrollada originalmente durante los años sesenta, permite tener comunicaciones de calidad bastante buena a velocidades de datos inferiores a 16 Kbps. Considerando que el habla humana habitualmente es semidúplex, la reserva de intervalos de tiempo de 64 kbps para transportar voz digitalizada es ineficiente en la era de las redes de paquetes.

Cuando se considera la integración de voz en una red de paquetes, se debe considerar cuidadosamente la forma en la que fluyen los paquetes por la red. Como la voz en tiempo real es sensible al retardo, se transporta en un *Protocolo de datagrama de usuario*(UDP, User Datagram Protocol) en un entorno de red IP. Esto supone que no se retransmite un paquete que tiene errores y que simplemente se descarta. En realidad, los circuitos modernos de comunicaciones tienen una tasa de error relativamente baja y el oído humano tiene una capacidad de absorción de sonidos relativamente lenta, lo que supone que el descarte periódico de fragmentos pequeños de una conversación digitalizada tendrá un efecto insignificante en la comprensión de una conversación. En su lugar, el retardo o latencia de los paquetes cuando atraviesan una red de paquetes tiene un efecto primordial en la capacidad que tiene una persona de comprender una conversación.

2.3.7 Latencia. La capacidad de implementar una solución de VoIP depende de la latencia unidireccional o retardo entre el origen y el receptor de la llamada. Este retardo es variable. Depende de varios parámetros, algunos de los cuales estarán bajo control, pero otros, cuando se utiliza una red pública, no lo estarán.

La tabla enumera los principales componentes asociados a la codificación de analógico a digital, la transmisión de extremo a extremo y la decodificación del

paquete que transporta un fragmento digitalizado de una conversación para obtener a voz.

Tabla 5. Retardos de la red de paquetes

	Retardos fijos y variables (ms)
Compresión (codificación de voz)	10-45
Procesamiento interno (origen)	10
Acceso a red en el origen	0,25-7
Retardo de transmisión de red	20-200
Salida de la red en el destino	0,25-7
Búfer (configurable)	10
Descompresión	10
Retardos fijos y variables totales	60,50-289

Los retardos fijos y variables asociados a la transmisión de extremo a extremo de un paquete puede variar generalmente entre 60 y 289 milisegundos (ms). Para situar este valor en su contexto, se debe observar que un oído humano típico puede aceptar un retardo de hasta 250 ms de vez en cuando antes de que la conversación resulte molesta. Aunque una transmisión dúplex completa es algo deseable para la mayoría de las aplicaciones de datos, no resulta útil y, de hecho, provoca problemas cuando se transporta voz en una red. Se debe a que la gente no tiene conversaciones en las que ambas partes hablan a la vez. En su lugar, una persona espera que la otra termine antes de responder. Si la latencia o retardo comienza a superar un cuarto de segundo para un fragmento significativo de una conversación, la conversación comenzará a parecerse a una conversación por radio unidireccional, en la que cada persona tiene que decir “cambio” para informar a la otra de que puede hablar. En caso contrario, el retardo provoca que una parte piense periódicamente que la otra ha terminado de hablar cuando no es así, con lo que el resultado es una conversación dúplex completa que exige que

una parte se pare y la otra comience de nuevo. De hecho, el estándar de la *Unión internacional de telecomunicaciones*(ITU) para retardos unidireccionales en una llamada de voz exige una latencia máxima de 150 ms, que asegura que la llamada no se convierta en una conversación dúplex completa. Para la mayoría de las empresas, una latencia máxima de 200 ms y una latencia media que se acerca o está por debajo de 150 ms deben ser suficientes para proporcionar una voz reconstruida de buena calidad.

2.3.8 Compresión. Se pueden seleccionar varios métodos de compresión o codificación de baja velocidad binaria. De hecho, la mayoría de los fabricantes de equipos, admiten habitualmente entre cuatro y seis métodos de codificación de voz. La mayoría de estos métodos son miembros de la familia de *Predicción lineal excitada por código* (CELP, Code Excited Linear Prediction) de codificadores de voz. El codificador de voz CELP original era un híbrido, que incorporaba tanto una codificación de forma de onda similar a PCM, ADPCM y codificación por predicción lineal. Aunque el primer codificador de voz CELP funcionaba a una velocidad binaria relativamente baja en comparación a PCM y ADPCM, su retardo de codificación era relativamente elevado, casi 60 ms. Desde que se introdujo el primer codificador de voz CELP se han desarrollado diversas variantes, estando aproximadamente media docena estandarizadas por el ITU. Dos de los miembros más famosos de la familia CELP son el CELP de retardo reducido (LD, low delay) (G.723), que funciona a 16 Kbps pero tiene un retardo de 10 ms, y el multicodificador G.729.1, que funciona a 5,3 y 6,3 Kbps. El multicodificador G.729.1 tiene también un retardo de codificación de aproximadamente 30 ms. Otros codificadores tienen retardos de hasta 45 ms.

Si se examina en detalle las hojas de especificaciones asociadas a las diferentes técnicas de codificación de voz, observará que habitualmente existe una relación directa entre la velocidad binaria del codificador y su Puntuación óptima media (MOS, Mean Optimum Score), que es una medida de la calidad de la voz. Es decir, a mayor velocidad binaria mayor es la MOS. Además, se produce una

relación inversa entre la velocidad binaria del codificador y su retardo de codificación. Es decir, cuanto mayor sea la velocidad binaria resultante producida por el codificador, menor será el retardo de codificación. De este modo, una técnica que se puede utilizar para conseguir que funcione una aplicación de VoIP cuando existe demasiada latencia es cambiar el método de codificación de voz. En general, cambiar de un codificador que funciona a 5,3/6,3 Kbps a otro que funciona a 8 Kbps reduce el retardo de codificación en aproximadamente 10 ms. Si se cambia el codificador por un codificador LD-CELP, se pueden eliminar 10 ms adicionales de retardo. Aunque 20 ms no parece demasiado, puede ser suficiente para asegurar que la calidad de la voz reconstruida sea aceptable para la aplicación de VoIP. Además, se ahorra unos cuantos ms con otras técnicas, el efecto acumulado de estos ahorros realmente se notará.

El efecto de cambiar estos valores puede ser suficiente para proporcionar un nivel aceptable en la voz reconstruida, que en caso de no cambiarlos, podrían impedir que su empresa implementara una aplicación de VoIP.

2.3.9 Retardo de procesamiento interno. El retardo de procesamiento interno representa el tiempo requerido para formar un datagrama IP a partir de cada segmento de voz digitalizada generado por un codificador de voz a continuación encaminar el datagrama resultante a un router conectado a la red IP. El retardo total de procesamiento interno es aproximadamente 10 ms y representa un serie de retardos que pueden variar por el hecho de que el nivel de utilización de LAN, que conecta a la pasarela (gateway) de voz al router, determina el retardo de pasarela al router. Además del retardo de pasarela a router, la propia pasarela tiene cierto retardo de procesamiento cuando compone un datagrama antes de enviarlo hacia su destino.

La mayoría de las pasarelas de voz son dispositivos modulares, con tarjetas de procesamiento de voz que están insertadas en un PC. Aunque cada tarjeta de procesamiento de voz contiene su propio procesador, lo que permite admitir

métodos de codificación de voz diferentes y que realmente realiza conversión de analógico a digital, la composición y desplazamiento de datagramas a través de la pasarela es una función de su procesador principal.

2.3.10 Acceso a la red en el origen. Una conversación de voz digitalizada consta de un flujo de datagramas pequeños para reducir el impacto de que se pierda uno o más de ellos. Si el router está conectado a Internet a 56 Kbps y la longitud media del datagrama es 49 bytes, entonces el retardo de acceso a la red en el origen es 7,0 ms ($49 \text{ bytes} * 8 \text{ bits / byte} / 56 \text{ Kbps}$).

De los 49 bytes de un datagrama típico, 20 representan la cabecera de IP y ocho representan la cabecera UDP, quedando 21 bytes reales para el transporte de voz digitalizada. Aunque es posible que encuentre referencias a la utilización de TCP y UDP para transportar voz, en realidad se utiliza TCP para el establecimiento de la conexión, mientras que se utiliza UDP para el transporte real de la voz digitalizada. Como no se pueden retransmitir los datagramas perdidos o erróneos, se utiliza UDP para el transporte de voz digitalizada porque es un protocolo orientado a conexión y de mejor esfuerzo. Como es muy importante asegurar que se reciba correctamente la información del establecimiento de la llamada, como el número marcado, TCP, que es un protocolo orientado a conexión y libre de errores, se utiliza para transportar la información de establecimiento de llamada.

Si se actualiza la línea de acceso a una línea T1 que funciona a 1,544 Mbps, entonces el retardo del acceso a la red es igual a 0,25 ms ($49 \text{ bytes} * 8 \text{ bits / byte} / 1,536 \text{ Mbps}$). Se utiliza un divisor de 1,536 Mbps en vez de 1,544 Mbps para la línea T1 porque se utilizan 8 Kbps para sincronización y no están disponibles para la transferencia de datos.

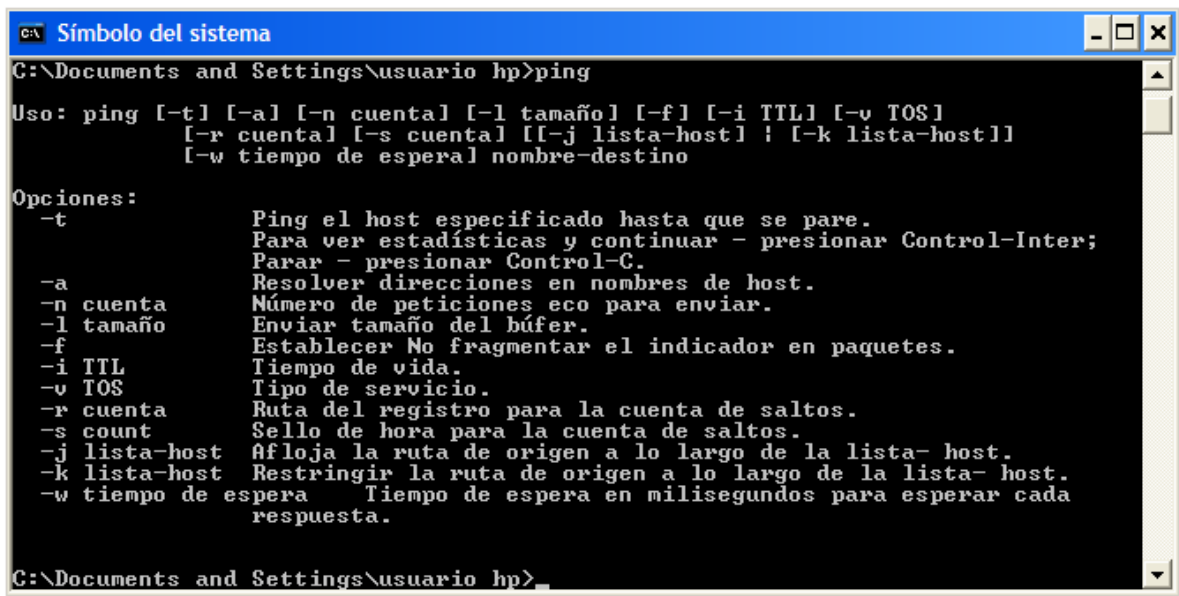
Cuando se transmite desde la frontera de una red, se debe considerar cuidadosamente la utilización de un protocolo del encaminamiento. Cuando un router es un dispositivo frontera, normalmente tendremos pocas razones para

utilizar un protocolo de encaminamiento que provoque un intercambio periódico de actualizaciones de tabla de encaminamiento. En su lugar, la utilización de encaminamiento estático evita los intercambios de actualizaciones de tabla y puede eliminar cambios periódicos en la latencia debidos al transporte de un segmento de voz digitalizada por un paquete que se retarda debido a una actualización de tabla de encaminamiento. Aunque la utilización del encaminamiento estático supone una ganancia mínima cuando se emplea en un enlace de comunicaciones de relativamente baja velocidad como un circuito de 64 Kbps, su utilización puede reducir la latencia de forma considerable.

2.3.11 Retardo de Transmisión de red. Como rara vez se utiliza VoIP en comunicaciones internas a la ciudad, se puede asumir que la red IP encaminará los datos entre áreas geográficas diferentes. Como al menos estarán implicados dos routers de red troncal en el proceso de encaminamiento, se puede esperar un retardo mínimo de 20 ms. Se pueden utilizar dos herramientas claves para determinar el retardo de la red: Ping y Traceroute.

Ping: Es una de las herramientas claves que se pueden utilizar por adelantado para determinar la viabilidad de una aplicación de VoIP, hacerlo proporciona la latencia de ida y vuelta desde el router hasta el dispositivo objetivo. Como los paquetes de VoIP fluyen a través de una red hasta el router, una forma más precisa de calcular la latencia es utilizar Ping desde una estación de trabajo de la LAN en la que reside una pasarela de voz, ya que de esta manera se pueden observar todos los retardos de la red. Basta con introducir Ping con un nombre de host (anfitrión) o dirección IP, o se puede introducir una o más de las opciones enumeradas a en el siguiente cuadro:

Figura 13. Opciones de ping



```
CA Smbolo del sistema
C:\Documents and Settings\usuario hp>ping

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v IOS]
        [-r cuenta] [-s cuenta] [[-j lista-host] ! [-k lista-host]]
        [-w tiempo de espera] nombre-destino

Opciones:
-t          Ping el host especificado hasta que se pare.
            Para ver estadísticas y continuar - presionar Control-Inter;
            Parar - presionar Control-C.
-a          Resolver direcciones en nombres de host.
-n cuenta  Número de peticiones eco para enviar.
-l tamaño  Enviar tamaño del búfer.
-f          Establecer No fragmentar el indicador en paquetes.
-i TTL     Tiempo de vida.
-v IOS     Tipo de servicio.
-r cuenta  Ruta del registro para la cuenta de saltos.
-s count   Sello de hora para la cuenta de saltos.
-j lista-host Afloja la ruta de origen a lo largo de la lista- host.
-k lista-host Restringir la ruta de origen a lo largo de la lista- host.
-w tiempo de espera Tiempo de espera en milisegundos para esperar cada
            respuesta.

C:\Documents and Settings\usuario hp>
```

Aunque la utilización primaria de Ping es determinar el estado operativo del host o dirección objetivo, también proporciona el retardo de ida y vuelta desde el origen hasta el destino.

En realidad, si se introduce un nombre de host que no ha sido resuelto previamente, la obtención de la dirección IP del nombre de host provoca que el primer retardo de ida y vuelta sea superior al de los retardos posteriores. La única excepción es cuando el tráfico o el procesamiento en un router llega a un punto en el que retardos significativos provocan que Ping sufra un fin de temporización.

Por tanto, cuando se utiliza Ping para determinar el retardo de ida y vuelta a través de una red siempre se debe descartar el primer retardo porque puede incluir el tiempo de resolución de la dirección IP del host. Además, se deberá ejecutar Ping varias veces a lo largo del día para determinar si existen uno o más periodos de tiempo durante los cuales los retardos aumentan. Se puede escribir una secuencia de órdenes que ejecute Ping en momentos diferentes o se puede utilizar la opción `-t` para ejecutarlo continuamente durante el día.

Tracert: Tracert funciona transmitiendo inicialmente una serie de paquetes con un valor de campo *Tiempo de vida* (TTL, time to live) igual a uno. Los routers decrementan automáticamente el valor del campo TTL. Si su valor es cero, se descarta el paquete y el router devuelve un mensaje de error al origen junto con la dirección IP del router, información acerca del router e información acerca de su conexión de red. El origen transmite entonces una nueva serie de paquetes con el valor de campo TTL incrementado en uno o dos. Los paquetes fluyen a través del primer router del trayecto hasta el destino, donde el valor del campo TTL de cada paquete se decrementa en uno. De este modo, el segundo router que está en el camino hasta el destino descarta la serie de paquetes y devuelve mensajes de error al origen. Este proceso continúa hasta que una secuencia de paquetes llega a su destino o se alcanza el valor máximo predeterminado del campo TTL.

2.4 ESTÁNDAR H.323

El estándar H.323 constituye la base para la transmisión de audio, video y datos sobre redes IP, lo cual, por lo tanto, incluye Internet. El objetivo es que los productos y aplicaciones que cumplan con dicho estándar puedan comunicarse entre sí, de modo que los usuarios no tengan que preocuparse por problemas de compatibilidad.

H.323 es una recomendación de la Unión internacional de Telecomunicaciones (ITU) que fija los estándares para comunicaciones multimedia sobre LANs que no ofrezcan una calidad de servicio (QoS) garantizada. Estas redes dominan la mayoría de ordenadores de las empresas de hoy en día y funcionan no solo con redes TCP/IP, sino también IPX sobre ethernet, Fast Ethernet y Token Ring. Por lo tanto, H.323 es un importante bloque para toda una nueva área de aplicaciones LAN para comunicaciones multimedia.

Esta recomendación fue aprobada por en el 1996 (H.323v1) y revisada de nuevo en el 1998 (H.323 v2), 1999 (H.323 v3) y finalmente en el 2000 (H.323 v4), y ha

demostrado ya ser ideal para la transmisión de voz en redes IP. De hecho, H.323 es parte de una serie de estándares conocida como H.32X, que incluye el H.320 y el H.324 para ISDN o redes públicas de telefonía (PSTN) respectivamente.

Hay una serie de aspectos que hacen del H.323 un estándar con numerosos beneficios:

Estandarización de Códecs: H.323 establece los estándares para compresión y descompresión de audio, video y datos, asegurando que los equipos de múltiples vendedores tengan formatos comunes.

Interoperabilidad: Los usuarios quieren poder hablar si preocuparse por la compatibilidad con el punto receptor. Por tanto, además de asegurarnos que el receptor es capaz de descomprimir la información, H.323 establece formas de negociar las capacidades de ambos terminales, así como establecer unos protocolos de inicio de llamada.

Independencia de la red: H.323 está diseñado para funcionar sobre las arquitecturas de redes habituales. A medida que la tecnología de red avance, y las técnicas de gestión del ancho de banda mejoren, las soluciones basadas en H.323 podrán irse adaptando.

Independencia de la aplicación y de la plataforma: H.323 no está atado al hardware o al sistema operativo. Las plataformas que cumplan con el estándar tendrán múltiples formas y tamaños, incluyendo ordenadores personales con capacidad de grabar video hasta teléfonos comunes con compatibilidad IP o los propios decodificadores de televisión a los que ya estamos acostumbrados (set-top Boxes).

Soporte Multipunto: H.323 puede soportar conferencias con 3 o más participantes sin una unidad especial de multipunto, pero los MCUs proporcionan una arquitectura flexible para llevarlas a cabo más eficazmente.

Gestión del Ancho de Banda: el envío de streams multimedia puede generar cantidades ingentes de tráfico, que saturarían nuestra red. Por eso es importante poder controlar cuanto ancho de banda van a consumir, y poder limitarlo, respetando así el resto de sistemas de la red.

Soporte Multicast: H.323 está preparado para hacer transporte multicast en conferencias multipunto. De este modo, enviaremos un solo paquete a una serie de destinos de la red sin tener que repetirlos. Es por tanto mucho más eficiente en cuanto a consumo de ancho de banda.

Flexibilidad: Podremos tener terminales H.323 con especificaciones muy diferentes, como por ejemplo terminales que solo soporten audio, conferenciando con terminales que sí pueden recibir video, enviar datos a un terminal que solo soporte datos, y a la vez enviar video y audio al resto de participantes que si lo soporten.

Conferencia Inter-red: en muchas ocasiones vamos a querer comunicar terminales que se encuentran en diferentes redes. Esto será posible mediante el uso de gateways.

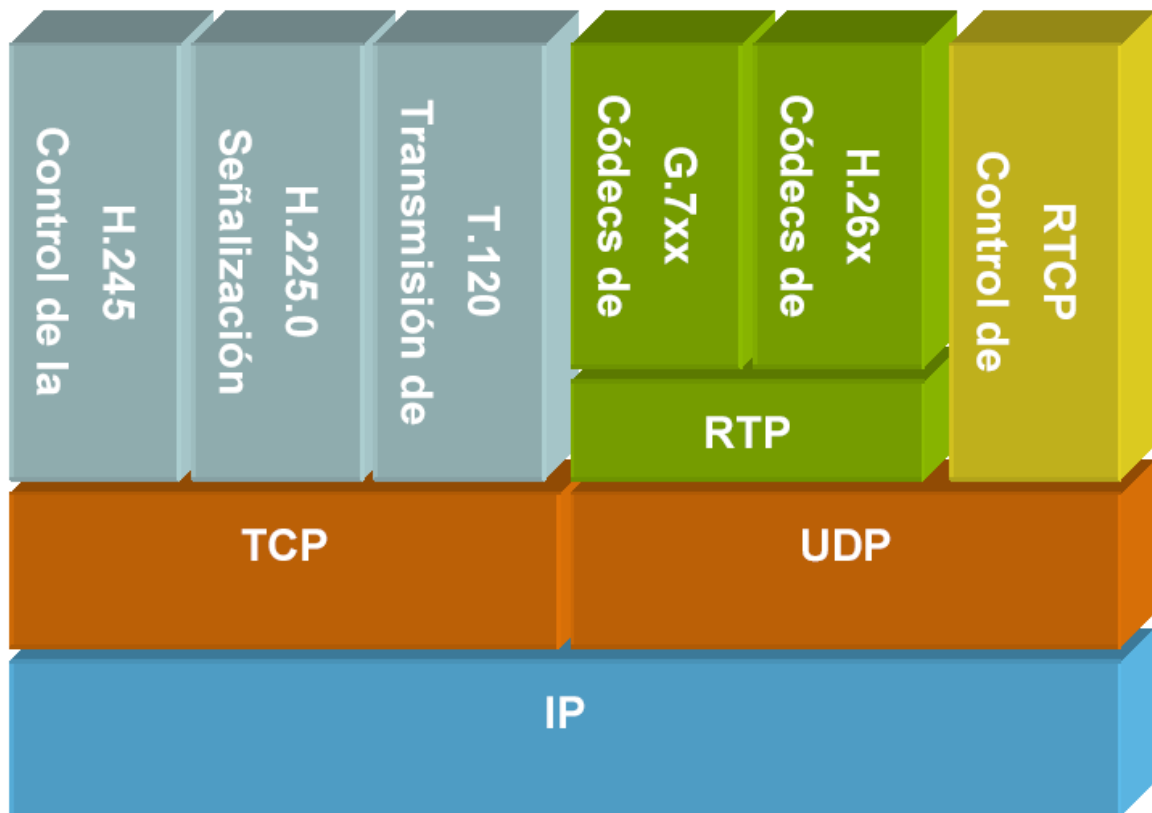
El estándar no solo cubre la capa software del sistema, sino también la arquitectura de la red y los equipos implicados. Más adelante veremos el papel de los bloques hardware constituyentes: Terminales, Gatekeepers, Gateways y MUCs.

Se verán a continuación los protocolos usados en la comunicación:

- Control de las llamadas: H.245, H.225.0
- Datos: T.120
- Audio: G.711, G.722, G.723.1, G.728, G.729.
- Vídeo: H.261, H.263.

La torre de protocolos queda estructurada de la siguiente forma:

Figura 14. Torre de protocolos.



2.4.1 Establecimiento y control de llamadas

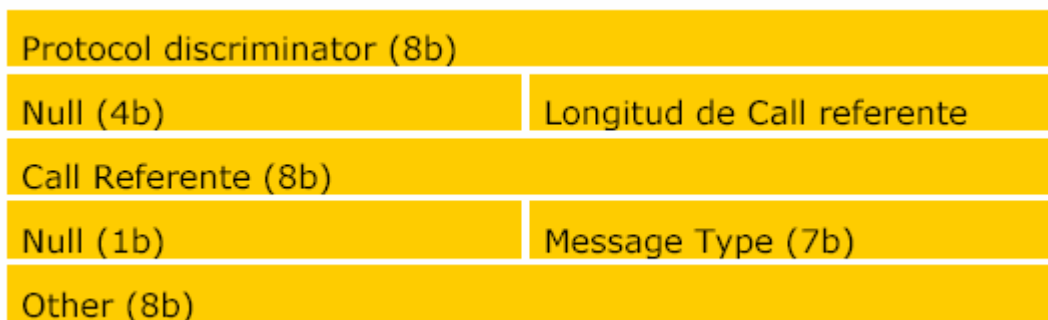
2.4.1.1 H.225.0 para inicio de llamadas. Hay dos partes en H.225.0 empezaremos con la de “Call Signaling” (señalización de llamada) para establecer

las llamadas entre dos terminales. El protocolo utilizará Q.932 para iniciar y finalizar las llamadas, si bien Q.932 se diseñó inicialmente para redes RDSI, H.225.0 adopta su formato.

Las llamadas podrán realizarse directamente de terminal a terminal, o bien pasar por un gatekeeper que las enrutará. El uso del call signaling es obligatorio para el establecimiento de una llamada entre dos puntos terminales.

La trama tendrá el siguiente formato:

Figura 15. Formato de trama H.225.0



Protocol Discriminator: El H.225.0 usa 0x8h.

Call Referente: numero identificador de la llamada, constante durante toda la transmisión.

Message type: tipo del mensaje.

Other: campo con informaciones dependientes del tipo de mensaje

Dado que estos mensajes son críticos para el establecimiento de la llamada, se realizarán sobre TCP, orientado a conexión, y con garantía de recepción. Los mensajes posibles serán:

Mensaje de establecimiento:

- Alerta, aviso de llamada (alerting).

- Proseguir llamada (Call proceeding).
- Conectar (connect).
- Configuración del establecimiento (setup).

Mensaje de desconexión:

- Finalización de la llamada completa (release complete).

Otros mensajes:

- Estado (state)
- Estado de la búsqueda (state inquiry)
- Mensajes de información (information)

2.4.1.2 H.245 media control. Una vez establecida la llamada, esta se transmitirá sobre los protocolos RTP y RTCP, pero aún tendremos que negociar los canales a usar en la comunicación. Esto se consigue mediante H.245, cuyas funciones incluyen:

Evitar conflictos: Determina que terminal podrá decidir quien y cuándo puede tomar una acción (maestro) a diferencia del resto de terminales (esclavos). Esto durará toda la llamada y evitará que surjan conflictos posteriores cuando los terminales quieran llevar a cabo acciones incompatibles a la vez.

Decidir qué transmitir y cómo: Los terminales negociarán sus capacidades en cuanto a recepción y transmisión, informando del tipo de comunicación que soporta y los codificadores disponibles, velocidad de la comunicación (bit rate) etc.. Permitirá también renegociar dichas capacidades en cualquier momento.

Gestión de los canales: estos pueden ser uni o bidireccionales, y vienen marcados por un identificador (son pues, canales lógicos). El protocolo decidirá que canales abrir o cerrar, manteniendo siempre el 0, para uso propio.

Al igual que en el caso del H.225.0, los mensajes de H.245 se transmitirán mediante TCP, para garantizar su recepción.

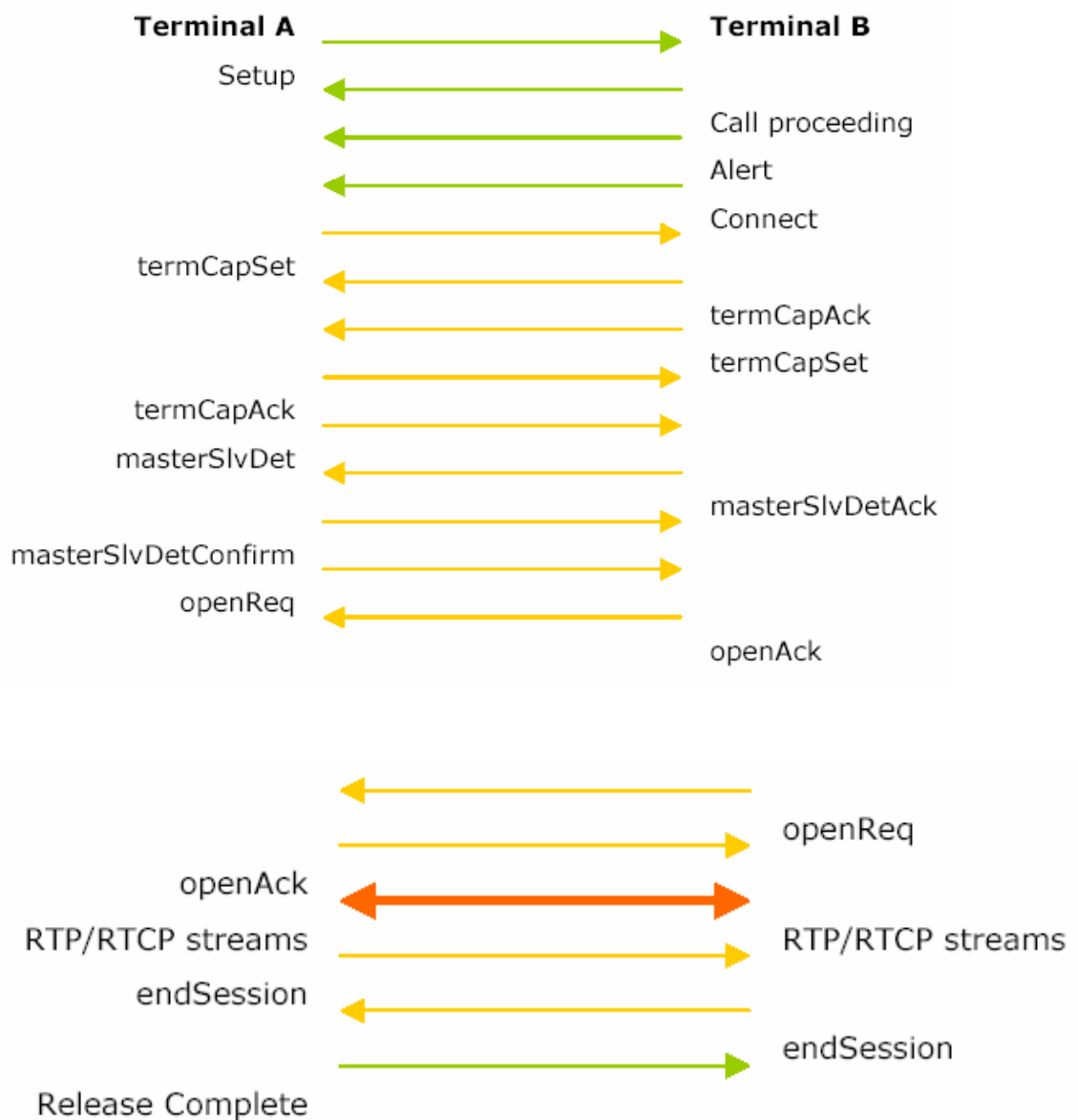
Cabe destacar que el protocolo H.245 no es imprescindible desde la versión 2, en la que se habilita un nuevo método, el *fase-connect*, que tan solo usará mensajes de H.225.0.

Para ello, el terminal incluye una petición de faststart en el campo de setup del mensaje inicial, que ya indica al receptor los canales lógicos y las capacidades de cada canal (tanto la velocidad como el codificador). En caso de que esto sea compatible con el receptor, se mandará un mensaje de vuelta donde el campo faststart indicará que se acepta la conexión, que quedará entonces establecida. Como en todos los casos, la conexión termina con un *release complete*.

Es recomendable, sin embargo, no prescindir del H.245 pese al ligero overhead que puede suponer, pues proporciona gran flexibilidad.

2.4.1.3 Establecimiento de una llamada con H.225.0 y H.245. Se verá a continuación como se combinan los protocolos mencionados para realizar una llamada. Para simplificar, veremos el caso en que dos equipos se comunican directamente, sin hacer uso del gatekeeper. El caso con gatekeeper es muy parecido, y en realidad es bastante común, pues los equipos terminales a menudo incorporan un gatekeeper que, por H.323, debe ser deshabilitable para evitar que cada equipo quiera usar el suyo propio.

Figura 16. Establecimiento de llamada con H.225.0 y H.245



Los mensajes correspondientes a H.225.0 se detallan en verde, mientras que en amarillo podemos ver las de H.245.

Bien pues, analicemos la llamada iniciada por A:

Un mensaje de *setup* a B inicia la llamada. Éste incluye la petición TSAP (dirección de transporte) para la conexión H.245. B responderá con *call proceeding* que indica a A que está disponible y que la llamada sigue adelante. El mensaje *Alert* de B a A va a continuación (opcional) y el de *connect*, indicando que se realizó la comunicación. Este es el que nos indica si el proceso tuvo éxito o no, y solo se envía si se acepta la petición TSAP.

A partir de aquí la conexión H.245 seguirá por la dirección TSAP, y negociará las capacidades con *TermCapSet* y *TermCapAck*. También fijará quien es el maestro y quien el esclavo con *masterSlvDet*, *masterSlvDetAck* y *masterSlvDetConfirm* y por último abrirá los canales lógicos con *openReg* y *OpenAck*. Hecho esto se inicia el flujo de datos sobre RTP y RTCP para la transmisión de voz video y datos, y finalmente *endSession* indica al terminal de destino que quiere terminar la llamada. Cuando este es correspondido, y de nuevo en H.225.0, se indica la finalización de conexión y la liberación de recursos con un *ReleaseComplete*,

2.4.1.4 Caso con gatekeeper. H.225.0 RAS. En ocasiones nos interesará enrutar nuestra llamada a través de un gatekeeper, y para ello usaremos el protocolo RAS, de *Registration*, *Admission* y *Status*. La principal diferencia radica en que las comunicaciones entre los terminales se establecen con un gatekeeper en medio, en el cual tendrán que registrarse y ser aceptados. Aquí es donde contamos con los elementos de control de QoS y tráfico en red para proteger nuestra red.

En concreto, el protocolo incorporará las funciones de descubrimiento de gatekeeper, registro de los terminales, localización de los destinos y control de capacidades.

Gatekeeper discovery: Permite localizar el gatekeeper que se usará. Básicamente, consiste en el envío de un mensaje GRQ (Gatekeeper Request) que será visto por todos los gatekeepers, que responderán con GCF (Gatekeeper confirmation) o GRJ (Gatekeeper Reject) en función de si pueden o no ser el gatekeeper para esa llamada. En caso de aceptarla, se incluirá en el mensaje el canal RAS que va a usar ese Gatekeeper. Si se recibe más de una confirmación, el terminal deberá decidir con cual quedarse. Es importante recordar que el estándar H.323 indica que en caso de tener un gatekeeper incorporado en el terminal, deberemos poder deshabilitarlo. Tal funcionalidad queda ahora clara. Si no se reciben confirmaciones, el terminal deberá reintentar la llamada de GRQ.

Endpoint registration: una vez elegido un gatekeeper, el terminal debe registrarse. Para ello, indica al gatekeeper su dirección IP y el nombre asociado, mediante un mensaje RRQ (Registration Request). A ello responderá el gatekeeper con un RCF (Registration Confirmation) o un RRJ (Registration Reject). Del mismo modo, el terminal puede des-registrarse o ser des-registrado por el gatekeeper mediante URQ (Unregistration Request) y UCF (Unregistration Confirm).

Endpoint Location: se usa para encontrar el terminal destino, ya sea el terminal de origen o el gatekeeper quien los busquen. Para ello se usa LRQ (Location Request) y LCF (Location Confirmation). Como en los casos análogos, LRQ indicará que se busca un punto terminal, y LCF nos dará la información de donde se encuentra. Análogamente un mensaje LRJ indicará que no se ha encontrado dicho terminal.

Admissions, Bandwith change, Status and Disengage: dichas funcionalidades vienen dadas también por el canal RAS. El mensaje ARQ (Admissions Request) especifica el ancho de banda a usar por por el terminal que llama. Como respuesta se manda un ACF (Admissions Confirmation) que indicará si se acepta

la petición y si el ancho de banda es factible, ya sea por carga de la red o por limitaciones impuestas sobre el tráfico multimedia. En caso de no serlo, se pedirá una reducción. Un BRQ (Bandwidth Change Request) nos permitirá cambiar este ancho de banda durante una llamada.

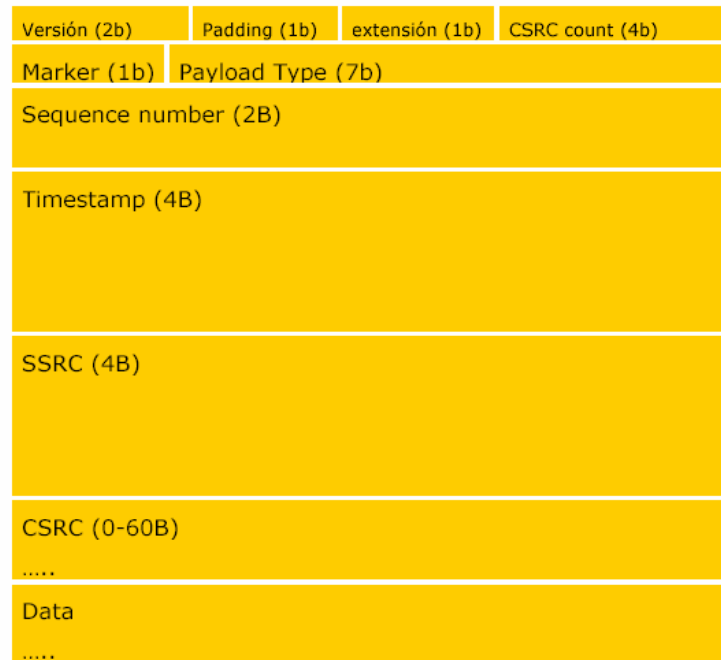
2.4.2 Transmisión de datos durante la llamada.

2.4.2.1 Los protocolos rtp/rtcp. El protocolo RTP trabaja sobre UDP, y se utilizará durante la llamada en sí para enviar los flujos de datos, voz y video. El protocolo da información que permitirá al receptor re-sincronizar los datos para poder sincronizar, por ejemplo, el movimiento de los labios con la voz, o para que un texto aparezca en el momento adecuado (como por ejemplo un subtítulo). Dado que RTP se puede configurar para tener una muy baja latencia, es muy útil para conversaciones interactivas o para envío de contenidos multimedia.

Por otra parte, RTCP trabaja con RTP para realizar estadísticas del tráfico, como por ejemplo el número de bytes enviados, los paquetes enviados y perdidos, el jitter o desorden de llegada, o el tiempo de latencia. Con ello, las aplicaciones extremas podrán juzgar la calidad de la conexión y ajustarlas según sea necesaria, cambiando entre codecs de alta compresión para malos canales a otros de mayor calidad cuando mejoren las condiciones.

Detallando ambos protocolos mirando sus tramas. En el caso de RTP se tiene:

Figura 17. Protocolos rtp trama.



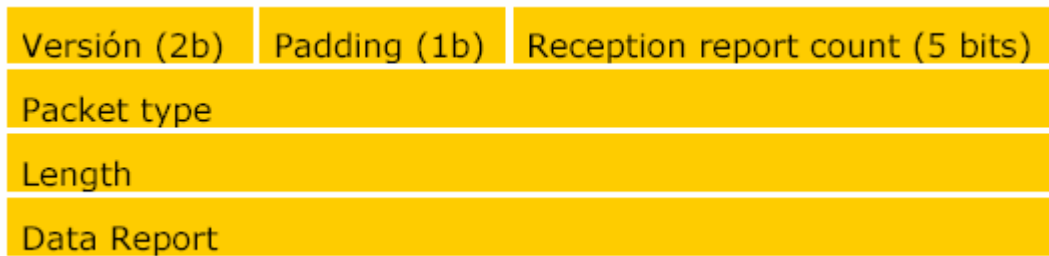
Los campos corresponden a:

- Versión: actualmente, la 1
- Padding bit/Extensión bit: Indica si hay bits de relleno o de Extensión
- CSRC count: indica el número de contribuyentes en el flujo, con un máximo de 15.
- Marker: podría ser usado arbitrariamente por las aplicaciones.
- Payload type: indica si el paquete lleva datos, voz o audio, y con qué códecs
- Timestamp: indica el tiempo de envío, que podrá ser usado en el receptor para resincronizarse
- SSRC: indica quien es el emisor del mensaje
- CSRC: indica quienes son cada uno de los contribuyentes. A 4B por contribuyente, tendremos un máximo de 60B

- Data: los datos en sí

Por otro lado, el RTCP:

Figura 18. Protocolo RTCP trama.



Tendrá los siguientes campos extra:

- Reception report count: indica cuantos informes se transmiten
- Packet type: indica el tipo de paquete RTCP
- Length: longitud del informe, en bytes
- Data Report: el informe en sí, con información sobre el jitter, los paquetes recibidos y perdidos, etc..

RTP constituye pues el protocolo básico para la transmisión de los datos, y se verá complementado por los informes mediante RTCP.

2.4.3 Implementación de h.323 a nivel de puertos. Ya teniendo una idea general de los diferentes canales que va a usar una llamada con el protocolo H.323, de modo que es conveniente hacer un repaso general, que nos permitirá situarnos e identificar cada parte de la comunicación.

Tabla 6. Resumen estándar H.323

Canal	Protocolo	Tipo de conexión	Destino
Establecimiento de la llamada	H.225.0	TCP	Terminal o Gatekeeper (RAS UDP)
Control de la llamada	H.245	TCP	Terminal
Media Control Channel	RTCP	UDP	Terminal
Media Channel (uno para cada flujo de datos)	RTP	UDP	Terminal

A nivel de TCP/IP vamos a tener que establecer unos puertos de destino para cada canal, ya que TCP/UDP nos permiten crear canales lógicos mediante dicho número (el puerto).

En general nos interesaría que estos fueran dinámicos, para no saturar nunca un puerto, pero esto dificultaría el descubrimiento de servicios. Es pues conveniente tener el H.225.0, ya sea para establecimiento de llamada, o para RAS, en puertos conocidos. El resto, en cambio, podrán negociarse una vez establecida la llamada, y por tanto, podrán ser dinámicos.

Tendremos pues los puertos 1720 (H.225.0 Call signaling), 1718 (RAS – Discovery) y 1719 (RAS – Registration and Status).

El puerto dinámico para H.245 se establecerá en H.225, y los canales de RTP/RTCP, se establecerán mediante H.245 cuando se abran los canales lógicos, salvo en el caso de *Fast Connect*.

2.4.4 La problemática de NAT. Connection Tracking. Muchas redes usan hoy en día NAT (Network Address Translation) para asignar direcciones IP privadas a

los terminales del interior de la red, que saldrán al exterior mediante un servidor NAT, que traducirá dichas IP's a su dirección pública.

Esto en sí no es un problema, ya que cuando un equipo interior hace una petición al exterior, el servidor de NAT envía la petición al exterior con una dirección pública enrutable, por un puerto dinámico. El flujo de retorno va dirigido a dicho puerto, y el servidor NAT lo enviará a la dirección privada correspondiente.

El problema en H.323 es más complicado, ya que una petición de llamada con H.225 se realizará con normalidad, pero cuando se asigne el puerto dinámico de H.245, el servidor NAT, que no mira el contenido de los paquetes que reenvía, no tendrá ninguna información al respecto, y el próximo paquete H.245 que el terminal exterior trate de enviar al interior, será rechazado.

Para ello, será necesario implementar un módulo en el gestor de NAT que lea el contenido de los paquetes y se prepare para aceptar y enrutar las conexiones a medida que se vayan decidiendo los puertos.

Un buen ejemplo es el caso de Linux, que soporta NAT mediante el módulo de Netfilter incorporado en el Kernel. Desde la versión 2.4.19 es posible implementar un módulo de connection tracking para H.323, que enrutará correctamente las conexiones.

2.4.5 Codecs de audio en H.323. En el caso de VoIP estricto, tan solo vamos a enviar voz, ya que habitualmente queremos contactar con terminales de la RTB. Empecemos pues con los codificadores soportados por el estándar.

Estos van a ser de dos tipos: Waveform Codecs o Vocoders. Los primeros van a tratar de comprimir la forma de onda que tengan a la entrada, muestreándola y tratando con dichos valores. Naturalmente, van a funcionar con cualquier voz, ruido o sonido que introduzcamos. Los Vocoders en cambio van a ser capaces de

“entender” la voz humana, adaptando la onda de entrada a un modelo vocal. Los parámetros de dicho modelo se enviarán al receptor, el cual sintetizará una voz basada en ese modelo vocal. Típicamente, los Vocoders van a basar su funcionamiento en filtrar una señal base. Esto es análogo a tomar el sonido emitido por las cuerdas vocales y filtrarlos con labios, dientes o posición de la lengua). Los Vocoders tendrán pues problemas para adaptar sonidos que no sean voces a su modelo vocal.

2.4.5.1 Waveform codecs. Destacaremos de estos que:

- Se utilizan circuitos estándar muy conocidos, rápidos y poco complejos.
- No introducen prácticamente retardo algorítmico.
- Son muy adecuados para emplear en sistemas TDM.
- No son tan útiles para voz paquetizada, ya que una sola muestra es demasiada poca información como para justificar la cabecera de un paquete entero, y tener que reunir varias muestras implica introducir un retardo.
- De este tipo se permiten G.711 y G.722

2.4.5.1.1 G.711. Es el estándar para enviar audio en un canal de 64kbps. Muestrea la señal a 8Khz, es decir, transmitirá la banda de 0 a 4KHz de la voz. A una muestra cada 0.125ms es comprensible que no podamos esperar mucho para llenar varios paquetes. Se usan 8 bits por muestra, de forma fija. Trabaja en PCM (Pulse Code Modulation).

Sobre paquetes, se suelen usar tramas de 40 muestras (5 ms de voz) o de 80 (10ms).

2.4.5.1.2 G.722. También conocido como SB-ADPCM (SubBand – Adaptive Differential Pulse Code Modulation), nos aportará mejores respecto al G.711. Su velocidad de muestreo se dobla, a 16KHz, ofreciendo un ancho de banda de

8KHz. En realidad, la señal se va a dividir en dos bandas, y cada una de ellas se enviará mediante un ADPCM, que al ser diferencial, funciona mejor para bandas reducidas. Encontraremos tres velocidades posibles:

- 64 kbps (2 bpm para la banda inferior y 6 bpm para la banda superior).
- 56 kbps (con 8 kbps libres opcionales para datos) (2 y 5 bits/muestra).
- 48 kbps (con 16 kbps para datos) (2 y 4 bits/ muestra).

2.4.5.2 Codificadores mediante vocoders. Resultan mucho más eficaces con el ancho de banda, puesto que nos permitirán eliminar o comprimir los silencios, generar ruido de confort (hace la conversación más apacible al usuario) y ocultar las tramas perdidas. Sin embargo, a veces la voz se oirá mal, debido a la mala codificación o a la falta de recursos de envío, y definitivamente tendremos problemas con otros sonidos que no sean voz. En concreto, no vamos a poder transmitir fax o datos de MODEM.

Encontraremos típicamente, los siguientes algoritmos:

- LPC (Linear Predictive Coding): Este modelo convierte el trato vocal en un filtro excitado por una señal de entrada. La señal generada será simplemente el resultado de filtrar dicha señal. Así pues, el LPC codificará la señal de excitación y el filtro.
- CELP (Code Excited Linear Predictor): La idea básica es la del LPC, pero la señal de excitación se codifica mejor, diferenciando entre sonidos sonoros, con intervención de las cuerdas vocales, de las sordas, que no son más que ruido blanco. Para las excitaciones sonoras definimos un *codebook* de señales de excitación, de modo que tan solo tendremos que enviar el índice dentro de dicha tabla. Por otro lado, el filtro se codifica con predicción lineal, es decir, como variación respecto al filtro anterior.
- ACELP (Algebraic CELP): Se trata de un CELP para DSP's más simples, y usa un *codebook* simplificado.

- CS-ACELP (Conjugate Structure - ACELP): Divide la señal de excitación en dos contribuciones: "adaptive codebook" (una versión retrasada de la excitación usada en la trama anterior) y "fixed codebook" (tabla prefijada).
- MP-MLQ (Multipulse maximum likelihood quantization): Usa un conjunto de pulsos (o ruido) como señal de excitación.

Los permitidos por el estándar son: G.723.1, G.728 y G.729

2.4.5.2.1 G.723.1. Usa dos algoritmos, en función de si es la versión de 5.3Kbps o 6.3Kbps. Para la primera, un MP-MLQ, y para el segundo un ACELP. El bloque de voz codificado es de 30ms y 158bits o 189bits para 5.3Kbps o 6.3Kbps respectivamente.

De por sí, el algoritmo introduce un retardo de 47.5ms, a los que habrá que añadir los retardos de transmisión.

Por otro lado, el algoritmo incluye VAD (Voice Activity Detection) que detectará cuando no se está hablando, para ahorrar el ancho de banda; CNG (Comfort noise Generation) que generará ruido aleatorio de fondo durante esos instantes de silencio, en beneficio del oyente. Durante los silencios se mandarían tramas SID (Silence Insertion Descriptor) que solo ocupan 5bytes por trama, y llevan los parámetros necesarios para generar el ruido de confort.

2.4.5.2.2 G.728. Usará algoritmo Low Delay CELP (LD-CELP) con un bitrate de 16Kbps, 12.8Kbps o 9.6Kbps. La trama es de 0.625ms y 10 bits. El retardo algorítmico es mínimo: 0.625ms y a la práctica nunca es mayor que 2 o 3 ms.

2.4.5.2.3 G.729. Dispone de varios bitrates: (8kbps: G.729, G.729A. 6.4Kbps: G.729D. 11.8Kbps G.729E). Usa el algoritmo CS-ACELP. G.729A es una versión ligeramente más simple de G.729. D y E son extensiones para otros bitrates.

En G.729, la trama es de 10ms, o sea, 10bytes. El retardo algorítmico es de 15ms, y una vez implementado en la realidad, de unos 20ms. En caso de perder una trama, el algoritmo repite la última trama, pero ligeramente atenuada para que no se note tanto. Usa también VAD, CNG y SID.

Las tramas SID, en este caso, serán de 15 bits (contra los 80 de la trama de voz) pero solo se envían si el ruido de fondo ha cambiado.

2.4.6 Códecs de vídeo en H.323. El envío de vídeo no es exactamente parte de VoIP, pero lo comentamos para redondear la explicación sobre H.323, y porque cada vez más van a querer ampliarse las funcionalidades de VoIP hacia la imagen y la transmisión de datos.

Los estándares permitidos son: H.261 y H.263.

2.4.6.1 H.261. Es un estándar de codificación de la ITU, publicado en 1990. Está diseñado para bitrates múltiples de 64Kbps, típicamente entre 1 y 30 veces 64Kbps.

El algoritmo es un híbrido de predicción cuadro a cuadro, codificación con transformada y compensación de movimiento. La primera, reducirá la redundancia temporal. La segunda, la redundancia espacial. Por último los vectores de movimiento se usan para compensar el movimiento. Para acabar de eliminar la redundancia, se utilizan longitudes de la codificación variables. La transformación es del tipo DCT (Discrete Cosene Transform).

Soportaremos dos resoluciones, QCIF (Quarter Common Interchange format) y CIF (Common Interchange format). Recomendamos visitar la página web [6] para muestras de las diferentes calidades.

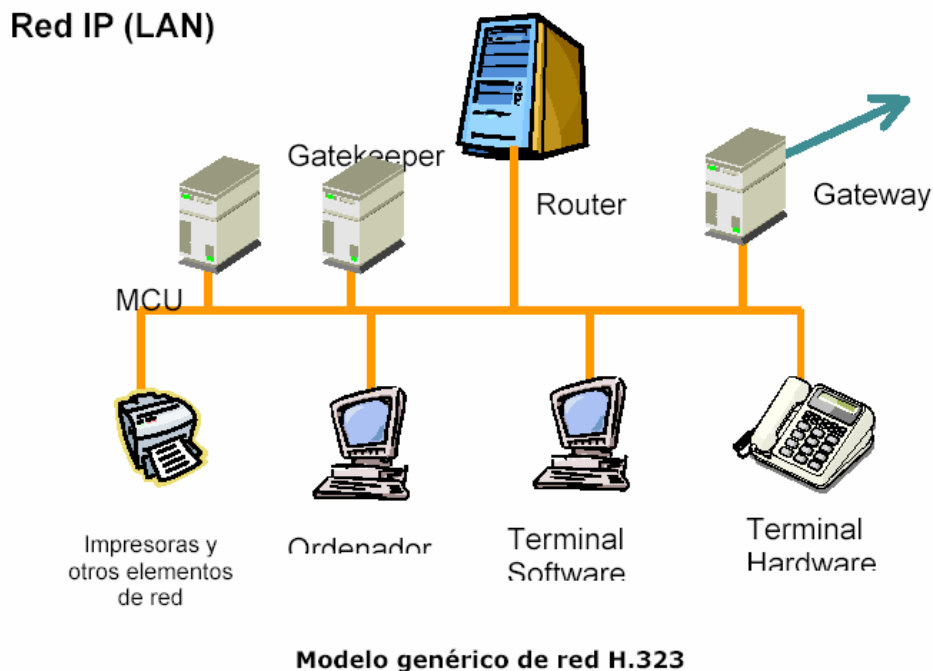
2.4.6.2 H.263. Es específico para canales muy lentos, a menos de 64kbps. El algoritmo es muy parecido al de H.261, pero con numerosas mejoras para mejorar el rendimiento y la recuperación de errores.

Las resoluciones soportadas serán: CIF progresivo a 352 x 288 píxels a 29.97 fps, QCIF progresivo a 176 x 144 píxels a 29.97 fps y Sub-QCIF progresivo a 128 x 96 píxels a 29.97 fps.

2.4.7 Equipos para VoIP. Una red típica H.323 podría ilustrarse mediante la siguiente Figura, donde se ven reflejados los elementos básicos que la componen:

- Terminales
- Gateways (GW)
- Gatekeepers (GK)
- Multipoint Control Units (MCU)

Figura 19. Componentes red típica H.323



2.4.7.1 Terminales. Un terminal H.323 es la interfaz entre el usuario final y la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y / o datos entre los dos terminales. El terminal se comunica con el Gateway VoIP usando H.245 para el control de llamada, Q.931 para el establecimiento de llamada, y RAS para el registro y administración con su Gatekeeper local.

Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo. Se puede hacer otra clasificación de terminales VoIP: los terminales software (como el popular *Microsoft NetMeeting*, que incluye capacidad para transmitir vídeo, audio y datos T.120) y los terminales hardware, que presentan una apariencia similar a los teléfonos convencionales pero incorporan las funcionalidades requeridas para transmitir sobre IP.

2.4.7.2 Gateways. El Gateway es básicamente un dispositivo lógico que actúa como pasarela de interconexión entre la red telefónica clásica (modo circuito) y las redes de datos (modo paquete). Este dispositivo es fundamental durante la necesaria fase de coexistencia entre la telefonía analógica y la telefonía digital sobre IP, pues no es coherente pretender implantar una tecnología totalmente digital sin prever una fase de introducción donde, de alguna manera, podamos decir que seguimos llamando desde un teléfono analógico a otro teléfono analógico prescindiendo del método de transmisión que se emplee entre ambos terminales y sin tener que comprar un terminal.

Podemos ver el Gateway como un dispositivo que por un lado tiene una interfaz LAN y por el otro dispone de una o varias de las siguientes interfaces:

- FXO: para conexión a extensiones de centralitas o a la red telefónica básica.

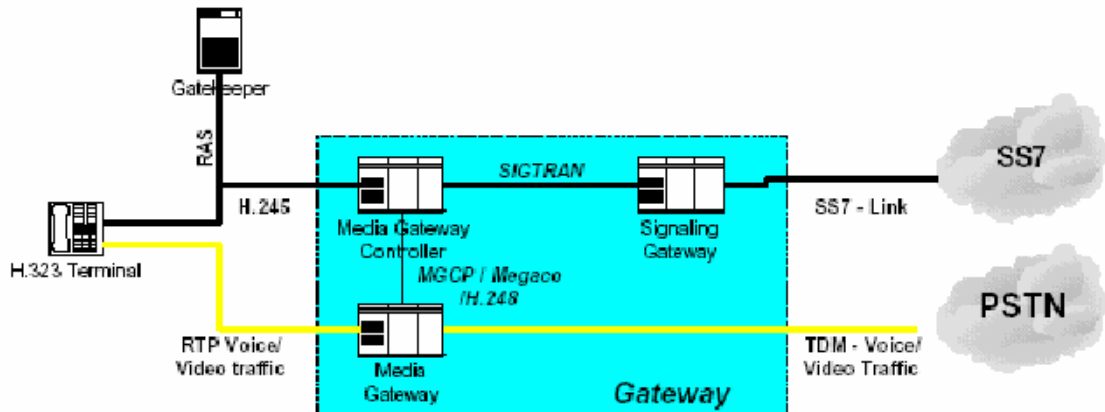
- FXS: para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M: para conexión específica a centralitas.
- BRI: acceso básico RDSI (2B+D)
- PRI: acceso primario RDSI (30B+D)

Los gateways se caracterizan por una serie de atributos que caracterizan el volumen y tipos de servicios que pueden proveer:

- Capacidad: número máximo de llamadas simultáneas que puede manejar. Depende del número de puertos del Gateway y de la velocidad del enlace de acceso.
- Protocolos de señalización soportados.
- Códecs de voz utilizados.
- Algoritmos de encriptado que soporta.
- Rango de direccionado

Un modelo genérico para un Gateway H.323 puede ser una caja como la de la figura:

Figura 20. Gateway H.323



Podemos descomponer el modelo de la figura en tres componentes, que corren en tres plataformas diferentes:

- **Media Gateway:** por un lado está conectado a una red de área local como Ethernet 10/100 BT y del otro asume una conexión a la red telefónica como un troncal T1 o línea RDSI para comunicación de video con un equipo compatible con H.320. Esta plataforma debe permanecer activa todo el tiempo para evitar cualquier interrupción de servicio entre dos terminales conectados. Este nodo controla el jitter, el retardo, la cancelación de eco y cualquier otro componente que constituye la calidad de servicio (QoS).
- **Media Gateway Controller:** proporciona el control general del Gateway. Se comunica con el Gatekeeper para solicitar información referente al mapeado entre una dirección IP y la red telefónica.
- **Signalling Gateway:** responsable de la interfaz entre la red de señalización SS7 y la señalización VoIP, como H.323.

Finalmente, cabe mencionar que existen unos gateways denominados especiales en tanto que se posicionan entre redes IP para desempeñar determinadas funciones de mapping, por ejemplo en la capa IP. Dentro de esta categoría podemos citar los proxies VoIP, transcodificadores VoIP, traductores de direcciones de red VoIP, etc.

2.4.7.3 Gatekeeper. El Gatekeeper es una entidad que se encarga del control, el enrutamiento y la seguridad de la comunicación, de manera que no se produzcan situaciones de saturación en la red. Es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de éste. Éstas son sus funciones principales:

2.4.7.3.1 Funciones principales del Gatekeeper.

- **Traducción de direcciones:** esta función permite a cualquier terminal o Gateway recuperar la dirección IP a partir de una dirección alias, o viceversa. Además, evita que el terminal o el Gateway tenga que hacer la traducción localmente, evitando de esta manera errores de conexión o direcciones IP desconocidas.
- **Control de admisión (RAS: Registration Admission and Status):** El Gatekeeper gestiona el control de admisión basándose en criterios como el ancho de banda disponible en la red y otros criterios.
- **Gestión del ancho de banda:** para garantizar una buena calidad de la comunicación entre terminales.
- **Gestión de su zona:** define qué terminales H.323 están registrados en este Gatekeeper. Cada terminal es responsable de registrarse a un Gatekeeper.

También puede realizar funciones de:

- Enrutamiento de la señal de llamada.
- Funciones de control de la red. El Gateway consulta y resuelve cuestiones como:
 - Pueden todos los usuarios establecer teleconferencias o sólo los que se han registrado anteriormente?
 - Usa la red DHCP, forzando así la autenticación por alias?
 - Cuál es el máximo ancho de banda autorizado para cada usuario?
 - Cuál es el máximo ancho de banda total en la red?
- Autorización de llamadas
- Servicios de directorio
- Call Logging (CDR)

El Gatekeeper utiliza los siguientes protocolos:

- **H.225.0**
 - Mensajes Q.931 para el establecimiento de llamada.
 - RAS para la señalización entre el terminal y el Gatekeeper.
- **H.245** es el protocolo de control de conferencia.
 - RTP / RTCP para el transporte de información:
 - Terminal a Terminal después del establecimiento de llamada.
- **Abriendo múltiples canales lógicos de transmisión de datos.**
- **H.225.0**

- Mensajes Q.931 para el establecimiento de llamada.
- RAS para la señalización entre el terminal y el Gatekeeper.
- T.120 para la transmisión de información.

El Gatekeeper tiene dos modos de funcionamiento en función de cómo se establezca la comunicación entre terminales:

La llamada se establece directamente entre los terminales en cuyo caso el Gatekeeper no es más que un mero intermediario en la comunicación para poner en contacto ambos extremos al inicio de ésta.

El Gatekeeper enruta la llamada (normalmente porque el terminal destino está fuera de su zona o está registrado en otro Gatekeeper) y realiza funciones como follow-me / find-me, forward on busy, etc.

Figura 21. Señalización directa entre terminales

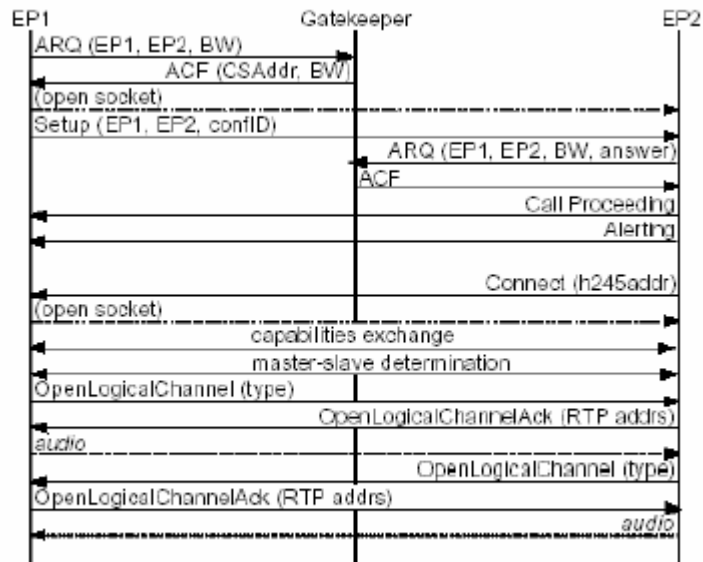
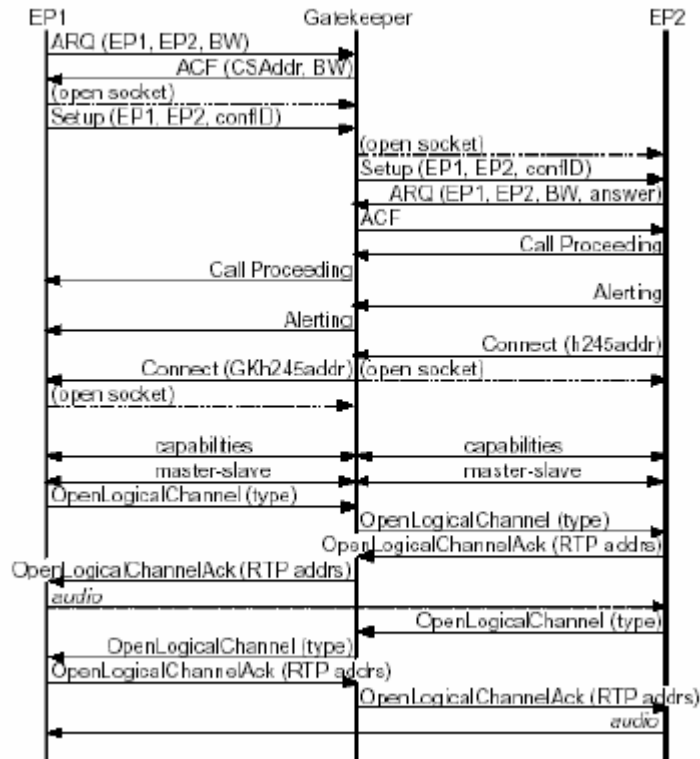


Figura 22. Señalización enrutada por el Gatekeeper



2.4.8 Multipoint Control Units. El MCU es el elemento encargado de controlar las diferentes situaciones que pueden producirse a lo largo de una comunicación (conferencia) y facilitar que ésta se pueda llevar a cabo. Sus características más importantes son:

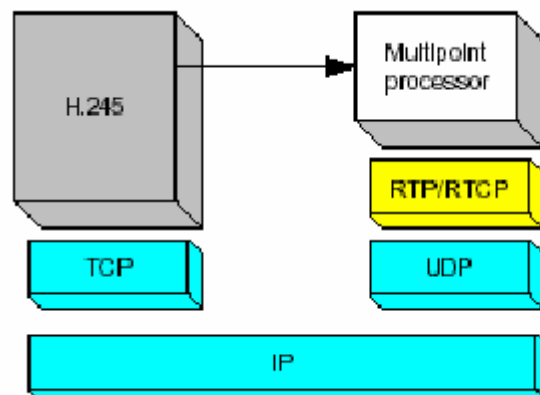
- Soporta conferencia entre 3 o más terminales.
- Realiza la distribución de comunicaciones unicast, multi-cast o híbridos, ahorrando ancho de banda.

- Controla el dinamismo de llamadas multimedia (*join, invite*, controles de la conferencia).
- A menudo, las funciones del MCU son llevadas a cabo por un terminal (el usuario que se conecta a una conferencia permite a los otros usuarios que se conecten con él).
- El MCU consta de dos partes.

2.4.8.1 Partes del MCU.

- El Multipoint Controller.
- El Multipoint Processor: es opcional. commuta los datos de audio/video de todos los terminales H.323 bajo el control de H.245. Tiene las mismas funciones de audio/video Vocoder que las incluidas en todos los otros terminales o Gateways H.323. El MCU se puede integrar en un Gateway o Gatekeeper local.

Figura 23. Partes del MCU.



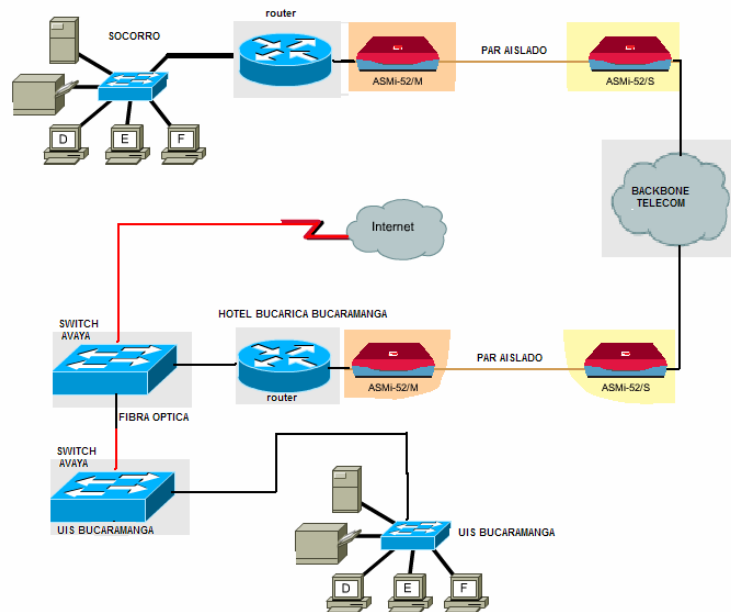
3. DISEÑO

3.1 ANÁLISIS DE LA RED DE DATOS ACTUAL

La Universidad Industrial de Santander cuenta actualmente con enlaces dedicados entre las sedes de Barrancabermeja – Bucaramanga; Socorro – Bucaramanga; Málaga- Bucaramanga y Barbosa – Bucaramanga, los dos primeros con una capacidad de 256 KBPS y los otros dos a 128 KBPS, todos ellos contratados con la Empresa Colombiana de Telecomunicaciones-Telecom.

Se describe a continuación la topología básica de uno de los enlaces como referencia de la conexión que existe actualmente entre las sedes alternas y la principal de Bucaramanga.

Figura 24. Diagrama conexión Socorro – Bucaramanga:



Como se puede observar la red LAN del Socorro se interconecta al Backbone de Telecom por medio de módems vía par aislado de cobre, al igual que la última milla desde Telecom Bucaramanga a la sede administrativa del Hotel Bucarica, el siguiente segmento de la conexión corresponde a un enlace de Fibra Óptica utilizando switch Avaya, este último conectado a la red principal de la UIS Bucaramanga.

Para que los equipos del Socorro tengan acceso al Internet provisto en Bucaramanga y a los aplicativos administrativos se hace necesaria la presencia de los routers que sirven para conectar las redes sirviendo de enlace entre ellas.

En las sedes de Barrancabermeja, Málaga y Barbosa la topología es similar llegando también a converger en el switch de fibra óptica del Hotel Bucarica.

En la actualidad la Universidad solo cuenta con canales de transporte de datos y se comparte el enlace de Internet contratado en la sede de Bucaramanga. La comunicación de voz entre las sedes de la UIS se realiza mediante los operadores convencionales, tales como Telecom., Orbitel y ETB, lo cual genera un costo alto en este servicio. Por otra parte, los docentes especializados tienen que desplazarse desde Bucaramanga para suplir la falta de personal en las diferentes sedes, asumiéndose un costo en viáticos. Por estas razones se sugieren enlaces con servicio de voz corporativa y videoconferencia para las sedes de Socorro, Barbosa, Málaga y Barrancabermeja todas estas en continua interacción con la sede principal de Bucaramanga, de esta manera una clase tal como electromagnetismo puede ser recibida de forma simultanea por los estudiantes de diferentes sedes evitándose el desplazamiento del docente hasta la ciudad correspondiente. En cuanto a la voz se refiere se podrán realizar llamadas entre sedes por medio del canal de datos como si se tratase de una llamada interna.

3.1.1 Pruebas realizadas sobre la red actual. En el mes de octubre de 2004 se realizó una prueba al enlace del Socorro con la ayuda de un analizador de BERT (Bit Error Rate Test). El analizador de BERT genera un ráfaga de bits, los cuales son enviados por intermedio de la interfase V.35 del MODEM A (Bucarica) el cual tiene salida por un medio físico (pares aislados y Backbone de Telecom.) para la comunicación con el MODEM B en el lado del Socorro. Al MODEM B se le colocó un loop (cruce de señales) en su interfase de salida de datos, el cual devuelve los datos enviados por el MODEM A. El primer MODEM (A) devuelve también los datos al Analizador; el cual hace una comparación de la Tasa de Bit de Errores (TEB) de los datos recibidos con los datos enviados anteriormente, esta comparación nos indicara el estado actual del enlace de comunicaciones.

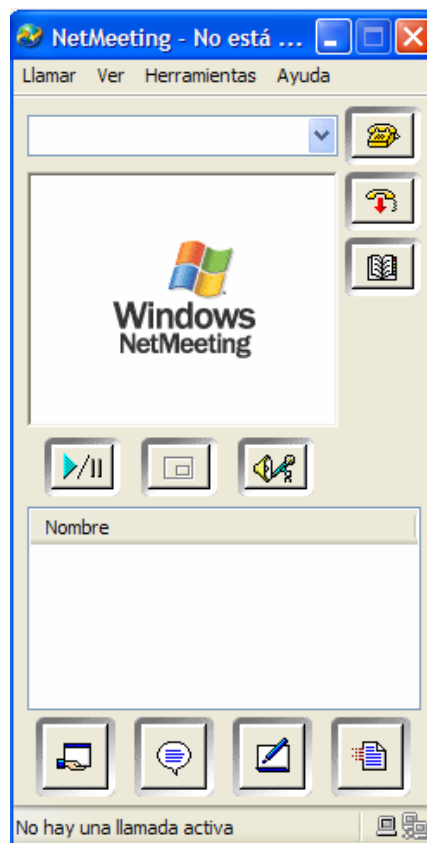
La prueba se corrió durante dos horas, en las cuales no se generaron errores ni perdidas de sincronismo, esto nos garantiza que el proveedor nos esta suministrando los 128 KBPS del contrato en el momento de realizada la prueba y que el canal se encuentra en óptimas condiciones. Ver Anexo 1.

3.1.2 Pruebas de videoconferencia utilizando software

3.1.2.1 Programa Neetmeeting. En enero de 2005 se realizaron las primeras pruebas de videoconferencia utilizando el programa Neetmeeting de Microsoft, instalando una cámara Web en Socorro y otra ubicada en el edificio de Ingenierías Físico-Mecánicas, se configuraron direcciones estáticas sobre los PC y se realizó una marcación IP a través de la red existente, las pruebas se realizaron sin mayor flujo de trafico en la red hacia Socorro con lo cual los resultados en cuanto a voz y movimientos de imagen obtenidos fueron aceptables, no obstante la resolución de video no es muy buena ya que está sujeta a la resolución de la cámara Web y de la velocidad de procesamiento del computador.

Otra desventaja de este programa es que solo permite una videoconferencia punto a punto, además el tamaño máximo de ventana deteriora la resolución en pantalla ya que es un zoom digital que se realiza a nivel de píxeles, por lo cual se requeriría un equipo adicional como un video bean para ampliar la imagen que a su vez se vera dentro de un entorno de página de computador que puede generar distracción en los asistentes. De igual forma requiere un buen sistema de multimedia en cuanto a micrófono y parlantes, el movimiento de la cámara se hace de manera manual y no se tiene la opción de hacer acercamiento ni seguimiento al conferencista.

Figura 25. Presentación NetMeeting



3.1.2.2 Programa ISPQ. Con el fin de superar algunas de las falencias del Neetmeeting, se buscó otra opción de software utilizando un demo del programa ISPQ, el cual permite videoconferencia hasta con cuatro participantes en simultanea (figura 27) desplegando las cuatro ventanas sobre una pantalla de PC.

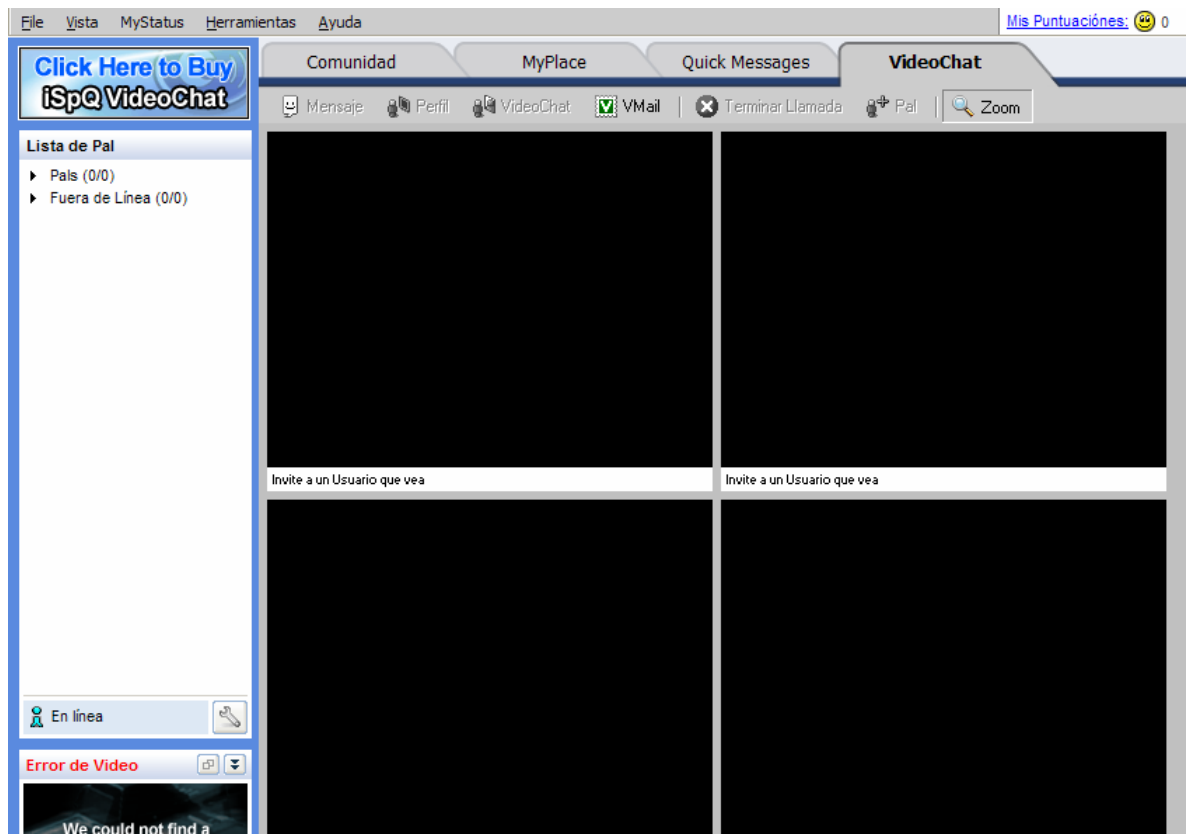
Figura 26. Verificación registro ISPQ



La plataforma funciona sobre un servidor ubicado en Internet donde se pueden generar grupos de participantes para interactuar utilizando voz, video y texto, además se puede realizar el envío de archivos al igual que Neetmeeting. En la pantalla del computador se pueden observar los cuatro puntos remotos en simultanea y se debe oprimir la opción de video chat para poder hablar, en este caso la voz funciona como con equipos trunking en donde se requiere esperar que el otro participante termine de hablar para poder hablar.

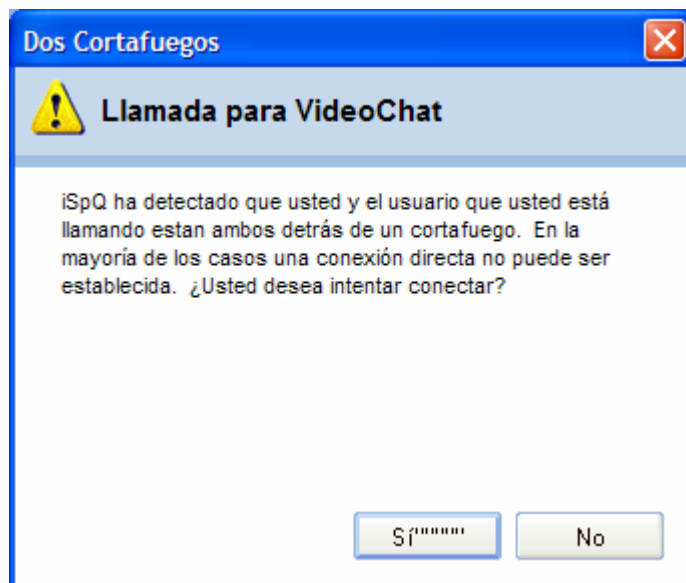
A continuación se observa la presentación que dispone el software para su uso en multiconferencia con cuatro puntos.

Figura 27. Esquema de ISPQ



La desventaja de este software radica en que el servidor está ubicado en Internet si la comunicación se hace entre dos usuarios con ISP diferentes los firewall propios de estos filtran el video imposibilitando así la comunicación (figura 4), adicionalmente si el servidor por algún motivo se encuentra fuera de servicio no se podrán realizar las videoconferencias, sin olvidar además que es un recurso compartido sobre el cual no se tiene control ya que a este acceden múltiples usuarios a través de Internet.

Figura 28 . Mensaje detección de Cortafuegos



3.1.3 Pruebas de videoconferencia utilizando Hardware. La primeras pruebas con Hardware se realizaron gracias a la colaboración del CIDLIS quienes facilitaron un par de cámaras Polycom viewstation 128 con las cuales se probó la comunicación a través a través de la LAN de la Universidad, gracias a la integración con fibra óptica existente entre El Bucarica y la sede de la Cra 27.

En febrero luego de verificar el funcionamiento de los equipos (cámaras) con el canal de Socorro ampliado a 256 KBPS se realizan pruebas de conectividad, nuevamente se hace un día sábado donde se tiene a disposición gran parte del canal desde Socorro, se hacen pruebas de ping hacia el equipo en Bucaramanga, previamente para ver en que condiciones de tráfico se realizaran las pruebas (Figura 29).

Las cámaras se conectan a la red directamente actuando como si fuera un host mas en la red, la conexión se hace por medio del puerto 10/100 ethernet que posee el equipo, al cual a su vez se le asigna una dirección IP, la comunicación entre ellas se hace por medio de una llamada IP, la cámara se puede conectar a

un televisor por medio las salidas de video por medio de conectores RCA, también tiene la posibilidad de conectar directamente a un PC o a un video bean.

Figura 29. Ping hacia el router de Bucaramanga

```
C:\WINDOWS\System32\ping.exe
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=41ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=14ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=15ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=38ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=18ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=19ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=35ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=46ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=37ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=17ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=33ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
```

Se observan tiempos de respuesta bastante buenos para este canal, no obstante el trafico se ve afectado por algunas solicitudes de páginas web en la red.

Figura 30. Ping introduciendo tráfico

```
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=439ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=553ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=917ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=1047ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=156ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=30ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=13ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=18ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=187ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=55ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=232ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=279ms TTL=28

Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=3195ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=19ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=38ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=12ms TTL=28
Respuesta desde 192.168.94.1: bytes=32 tiempo=68ms TTL=28
```

Con la colaboración de personal de CIDLIS se realiza videoconferencia entre Socorro y el Hotel Bucarica, los resultados de resolución y respuesta en tiempo real son satisfactorios, sin embargo en los momentos en que se introducía tráfico de Internet en el canal de datos se observan retardos grandes en el video, donde la imagen queda estática durante unos segundos.

El tráfico entre lunes y viernes es bastante alto debido a que se utiliza el canal en acceso a Internet y programas de aplicativos administrativos, con tiempos de respuesta muy elevados no es posible realizar una videoconferencia fluida ya que no queda ancho de banda suficiente para el tráfico de voz y video, además, como se tienen tiempos de respuesta superiores a 250 ms los cuales rebasan la latencia permitida para una aplicación de VoIP.

La resolución de videoconferencia obtenida con las cámaras Polycom fue superior al obtenido mediante las cámaras Web con software de videoconferencia, la voz y el video son más nítidos y debido a la posibilidad de tener un televisor en el cual la

imagen del remoto es completa se elimina la distracción de elementos en la imagen diferentes al salón de clases remoto.

3.1.4 Pruebas de voz a través de un canal de datos. Con la colaboración de una empresa del sector privado la cual posee en su infraestructura canales de voz corporativos, se verifico la calidad y nitidez de la voz por medio de un canal de datos, esta empresa se maneja a nivel nacional y comparte su aplicación de correo electrónico y bases de datos junto con el transporte de voz sobre IP, lo cual reduce sustancialmente los costos en el servicio telefónico, ya que dentro del monto de alquiler del canal de datos va agregada la voz corporativa.

Las llamadas realizadas a otras sedes de otra ciudad se realizan como si se tratara de una extensión local de acuerdo a una programación de marcación, de esta forma se integran las plantas telefónicas de las diferentes sedes, con la posibilidad de marcar directamente a una extensión ubicada en una localidad remota. Las pruebas se realizaron en compañía del Ingeniero Jorge Vidal jefe de planta física y del Mg. Jorge Hernando Ramón Director del proyecto.

3.2 PROYECTO PROPUESTO

La idea general del proyecto es interconectar las sedes de Bucaramanga, Barbosa, Málaga, Barrancabermeja y Socorro para poder tener servicios de videoconferencia y voz privada entre todas ellas, de esta manera un usuario ubicado en cualquiera de las sedes se pueda comunicar con cualquier otra sede marcando la extensión de la persona con la cual se desea conversar, esto gracias a que se integrara al sistema de plantas telefónicas de la Universidad.

Para realizar el plan de marcación se requiere de la colaboración del personal de Planta Física de la Universidad para el trabajo con las plantas telefónicas las cuales tienen su software propietario, pues una vez la llamada llegue proveniente

de la conexión router a router estos entregarán señalización a la planta para que esta envíe la solicitud a la extensión correspondiente.

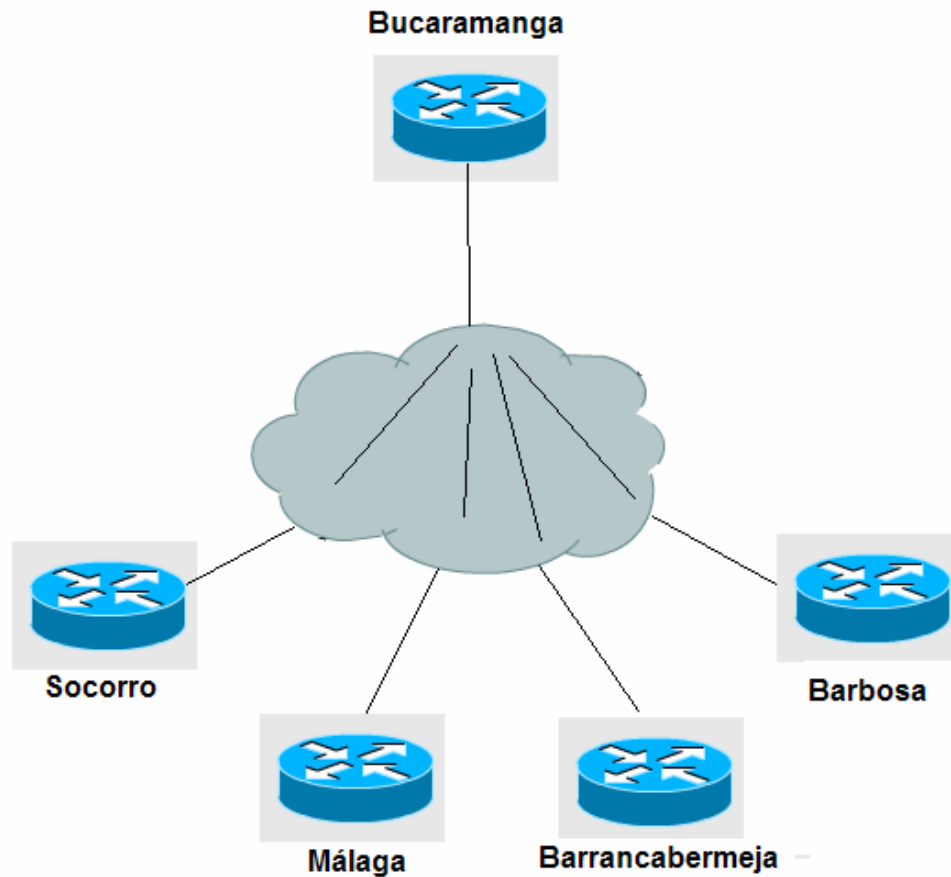
Por otra parte en cada sede se ubicará una cámara de videoconferencia teniendo un multipunto en Bucaramanga para permitir en simultánea conexión de todas las sedes, no obstante si se requiere una videoconferencia entre dos sedes se puede realizar sin inconveniente, pues las cámaras ubicadas en puntos como el Socorro, Málaga, Barbosa y Barrancabermeja permiten comunicación punto a punto, si en algún momento se quisieran enlazar tres (3) de estos puntos se requiere la intervención del equipo de Bucaramanga el cual opera como MCU (Multipoint control Unit). A continuación se detallan los componentes necesarios para ejecutar lo planteado.

3.3 PROPUESTA ECONÓMICA DE CANALES DE DATOS FRAME RELAY

Debido a que la idea es poder interconectar las sedes de Bucaramanga, Socorro, Málaga, Barbosa y Barrancabermeja y que inicialmente no se tocara la infraestructura de datos actualmente montada, se requiere entonces una topología que permita comunicación multipunto.

Para esto se hará uso de Frame-Relay con una Topología en estrella donde habrá una conexión de todas las sedes con la ubicación central en Bucaramanga. De esta forma se minimizan el número de enlaces necesarios para interconectar todos los puntos entre sí.

Figura 31. Topología en estrella



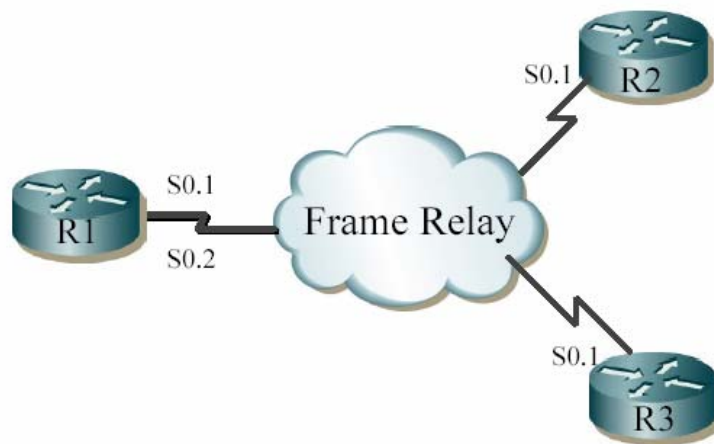
Una ventaja de esta topología es su facilidad de gestión. La desventaja es que el router de Bucaramanga es un punto único de avería por ser el núcleo de la estrella.

Con esta topología se puede tener comunicación de voz o videoconferencia entre las sedes de Socorro y Málaga y demás combinaciones posibles entre las diferentes ciudades donde la UIS tiene presencia, sin que exista físicamente un enlace entre estos dos puntos.

La idea es que el enlace de Bucaramanga tenga la suma de los anchos de banda de cada uno de los puntos externos. Como Bucaramanga tendrá un solo enlace físico que conectara a cuatro puntos remotos se deben crear PVC's (circuitos virtuales permanentes) y DLCI's (Identificador de conexión del enlace de datos) con el fin que cada conexión llegue sin inconveniente a través del único canal existente.

La familia Cisco tiene dentro de su sistema operativo (IOS) la opción de permitir por una sola interfaz física múltiples interfaces virtuales. Estos router utilizan subinterfaces que permiten aplicar atributos de interfaz física a cada interfaz virtual. Gracias a esto se puede intercambiar información entre dos router R2 y R3 pues se evita la regla del horizonte dividido en Frame-Relay.

Figura 32. Conexión Router R2 y R3 a través de Frame-Relay



Se plantea para las sedes de Socorro, Málaga, Barbosa y Barrancabermeja enlaces a 256 kbps, con el fin de proveer 4 canales de voz en cada uno de ellos utilizando algoritmo de codificación G.729, el cual se presenta como la mejor opción cuando se trabaja sobre una red Frame-Relay, de esta manera en el caso más crítico que estén en operación las cuatro (4) llamadas en simultanea se

ocupara un ancho de banda de 72 kbps, quedando un ancho de banda de 184 kbps disponibles para videoconferencia, ahora bien para el caso de Bucaramanga se sugiere un ancho de banda de 1024 kbps, para el caso mas critico de tener las 16 llamadas en simultanea utilizara 288 kbps, quedando así un total de 736 kbps con los cuales se puede tener videoconferencia en simultanea con los otros cuatro puntos los 7 días de la semana, 24 horas al día, los 365 días del año.

Se revisaron varias propuestas de diferentes proveedores de Backbone para enlaces Frame-Relay, los cuales ofrecen enlaces satelitales los cuales presentan el inconveniente de presentar un retardo natural de 250 ms aproximadamente de subida y bajada al satélite, lo cual representa una desventaja debido a que las aplicaciones a utilizar como son voz y videoconferencia, no toleran retardos tan altos, por otra parte el costo de tener un enlace satelitales con esta velocidades es demasiado alto, sin contar que la infraestructura necesaria también en considerable teniendo en cuenta que se montarían antenas con un diámetro igual o superior a 2,4 mts, lo cual exige espacio para su montaje. Debido a esto se ve como viable la propuesta de La Empresa Colombiana de Telecomunicaciones (Telecom.), quienes ofrecen enlaces terrestres mediante enlaces por pares de cobre en las últimas millas, y microondas a través de su Backbone.

3.3.1 Propuesta económica Telecom. Dentro de los requerimientos en la interconexión de videoconferencia y voz de las sedes de la UIS el presupuesto de gasto es el siguiente:

**3.3.1.1 Propuesta económica canales Frame-Relay de Telecom .
Canales Frame Relay Puros (AB = CIR)**

Tabla 7. Valor canales Frame-Relay

CANALES	AB	CIR	CARGO INSTALACIÓN	C F MENSUAL ACTUAL
Bucaramanga	1.024k	1.024k	\$ 1.879.000	\$ 1.441.000
Málaga	256k	256k	\$ 1.384.000	\$ 931.000
Socorro	256k	256k	\$ 1.384.000	\$ 931.000
Barbosa	256k	256k	\$ 1.384.000	\$ 931.000
Barrancabermeja	256k	256k	\$ 1.384.000	\$ 931.000
Valor Total			\$ 7.415.000	\$ 5.165.000

Los anteriores valores no incluyen IVA ni enrutadores, por lo que se les deberán agregar los precios correspondientes.

No incluye:

- Equipos adicionales no previstos y que por circunstancias de cambio de solución puedan ser necesarios, ni convertidores de interfase no contemplados.
- Las obras civiles para la acometida interna que sea necesaria realizar en las oficinas de **LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.**
- Conectores y cables para la conexión de sus equipos a los puertos entregados por COLOMBIA TELECOMUNICACIONES S.A. ESP.
- Instalación de tierras.

3.3.1.2 Aspectos comerciales. Los valores no incluyen el IVA.

- **Validez de la oferta:** Treinta (30) días calendario.

- **Terminación del contrato:** Si el cliente da por terminado el contrato en forma anticipada, deberá cancelar a Colombia Telecomunicaciones todos los valores que estén pendientes a la fecha, así como el monto que falte del valor total del contrato.
- **Renovación del contrato:** Los contratos se entenderán prorrogados en las condiciones y términos originalmente pactados. El valor de los servicios de dicha prórroga se ajustará a las tarifas vigentes al momento de la misma (será por lo menos el valor del contrato original + IPC).

3.3.1.3 Sanciones por no pago. El no pago de la factura genera los intereses de mora correspondientes.

- **Suspensión temporal del servicio por no pago:** El servicio se suspenderá temporalmente después del vencimiento de la segunda factura no pagada.
- **Suspensión temporal voluntaria:** La suspensión temporal del servicio a voluntad del cliente será por sólo una vez hasta de dos meses para toda la duración del contrato. El cliente deberá cancelar el equivalente al 15% del valor de un mes de servicio (cargo fijo de suspensión) y notificar con 30 días de anticipación a la fecha de suspensión deseada.
- **Cancelación del contrato por no pago:** El contrato se considerará unilateralmente terminado por el NO pago de la factura vencida 30 días después de la suspensión temporal del servicio, sin perjuicio de las sanciones pactadas en el contrato.

3.3.1.4 Cancelación del contrato por uso indebido. Está prohibido que el SUSCRIPTOR aloje contenidos de pornografía infantil, use o permita usar el

servicio con fines de explotación, pornografía, turismo sexual y demás forma de abuso sexual contra menores de edad. Asimismo, El SUSCRIPTOR no podrá utilizar los enlaces y demás equipos para establecer métodos de comunicación no autorizados (cualquiera tendiente a violar en forma directa o indirecta el régimen de telecomunicaciones, entre otros: "call back"; "by pass" ó tercer país; re-orignamiento de llamadas de "TPBC" para su posterior comercialización; reventa de servicios de "TPBC" sin autorización de Colombia Telecomunicaciones S.A. ESP; distorsión del tráfico; alteración de las señales de los equipos terminales o abonados; alteración de cualquier equipo, sistema o dispositivo de acceso de tal forma que se modifique la medición del consumo facturable; acceso no autorizado a códigos de acceso o números de identificación personal; acceso a servicios suplementarios o a categorías de programación sin previa autorización de Colombia Telecomunicaciones S.A. ESP; interceptación de comunicaciones sin orden de autoridad competente; acceso a los servicios para realizar denuncias o manifestaciones tendenciosas, o cualquier modalidad similar o de uso ilegal de la RTPBC y de fraude en su utilización). El uso indebido facultará al OPERADOR para dar por terminado el contrato, en consecuencia se suspenderá y retirará el enlace y los demás equipos que se hayan instalado, sin perjuicio de iniciar las acciones legales correspondientes.

- **Reconexión del servicio:** El servicio suspendido por no pago, se reconectará en 3 días hábiles después de la legalización del pago correspondiente.
- **Adiciones al contrato:** Los nuevos servicios o adiciones al contrato exigen una nueva oferta, la cual se formalizará como un anexo al contrato original, junto con los acuerdos de servicio respectivos.

3.3.1.5 Forma de Pago: El pago se hará por mensualidades vencidas. Los precios de la presente oferta están en Pesos Colombianos.

3.4 EQUIPOS DE ENRUTAMIENTO REQUERIDOS

Debido a que la propuesta concreta implica cuatro canales de voz y ya se nombro una de las ventajas de los router Cisco con respecto a sus competidores en el mercado, se busco dentro de esta familia equipos versátiles que nos ofrezcan las ventajas de manejar 256 KBPS con encapsulación Frame – Relay y que a su vez proporcione la plataforma para incluir Voz sobre IP.

Dentro de la serie Cisco 1700 se encuentra el CISCO 1750 y 1760, siendo el Router más pequeño que puede implementar VoIP al poder introducirle módulos FXS, FXO ó E&M, siendo estos los mismos para los Routers 2600 y 3600. La familia de Routers CISCO 1700 permiten integrar tarjetas de interfaz WAN soportando una gran variedad de tecnologías (RDSI, xDSL, Serie Sínc/Asinc para líneas dedicadas, Frame Relay, X.25 y SMDS).

Dentro de esta familia de Routers podemos destacar los siguientes equipos:

- **CISCO 1710** (2 puertos autosensing 10/100)
- **CISCO 1720** (1 puerto autosensing 10/100 y 2 slots WAN)
- **CISCO 1750** (1 puerto autosensing 10/100, 2 slots VIC/WIC y 1 slot VIC)
- **CISCO 1760** (1 puerto autosensing 10/100, 2 slots VIC/WIC y 2 slots VIC)

Como se puede apreciar el modelo 1760 permite conexión mediante puerto FastEthernet 10/100 con cuatro slots para tarjetas dentro de las cuales se puede introducir 2 tarjetas de interfase Wan (WIC) y 2 para VIC (Voz), que pueden ser como se mencionó anteriormente FXS, FXO ó E&M, por tal motivo este se convierte en el enrutador elegido de nuestro diseño para las sedes alternas de la Universidad.

Figura 33. Router Cisco 1760.



Para el caso de la voz corporativa, se instalarán 2 módulos VIC-2FXS (tarjeta de interfaz de voz FXS de dos puertos), los cuales se utilizan para conectar directamente con teléfonos y maquinas de fax. La tarjeta de interfaz de voz funciona con el equipamiento existente de teléfono y fax a fin de proporcionar servicios de voz y fax a través de IP; además es compatible con el estándar H.323 para conferencia y videoconferencia. Para conectar a la WAN se instalará una WIC-1T.

Figura 34 . Modulo Vic 2FXS.



Para la sede de Bucaramanga, se escoge la serie Cisco 2600: Es una serie de routers de media capacidad, multiservicio (voz y datos) y casi completamente modular, además se garantiza integración en cualquier momento con la red actual que también esta compuesta por estos equipos.

Al igual que en las líneas de routers más bajas, soporta módulos WIC. En esta línea aparecen los Network Modules (NM), que son módulos o placas más grandes que permiten ampliar la variedad y cantidad de interfaces (LAN, WAN o mixtas).

También poseen un slot interno para Advanced Integration Module (AIM); este módulo se utiliza para brindar servicios de compresión o encriptación de datos.

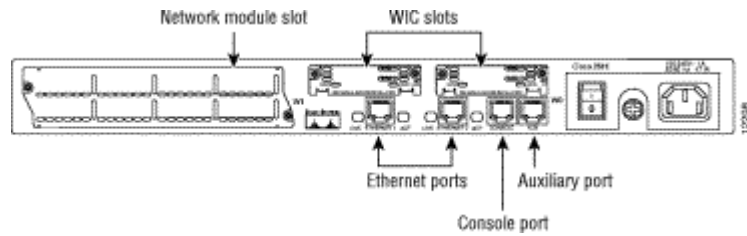
Según el modelo de chasis, vienen con distintas interfaces de LAN:

- ▶ El **2610** posee **1** interface ethernet.
- ▶ El **2611** posee **2** interfaces ethernet.
- ▶ El **2612** posee **1** interface ethernet y **1** interface token ring.
- ▶ El **2613** posee **1** interface token ring.
- ▶ El **2620** posee **1** interface fastethernet (10/100 Mbps autosensing).
- ▶ El **2621** posee **2** interfaces fastEthernet (10/100 Mbps autosensing).
- ▶ **Todos los modelos** tienen **2** slots para placas WIC, **1** slot para módulos NM, y **1** slot (interno) para módulo AIM.

Vista trasera:

(Todos los modelos son muy similares, se muestra sólo uno como ejemplo)

Figura 35. Router Cisco 2611 vista trasera



Se instalará una tarjeta WIC V.35 para recibir el canal de 1024 kbps Frame-Relay que se piensa contratar con Telecom, para conectar la planta telefónica Siemens de la Universidad Industrial de Santander se hará uso de un módulo de red de un solo puerto y 30 canales mejorados de enlace troncal E1 de paquetes e voz digital NM-HDV-1E1-30E.

3.4.1 Costo de equipos de enrutamiento.

Tabla 8. Valor equipos de enrutamiento

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO EN DOLARES
10/100 Modular Router w/Voice, 19-in Chassis, 32MB FL/96MB DR	4	2,049
Cisco 1700 IOS IP/VOICE PLUS	4	-
1-Port Serial WAN Interface Card	5	316
Two-port Voice Interface Card – FXS	8	316
V.35 Cable, DTE, Male, 10 Feet	5	316
Power Cord, 110V	4	79

Cisco 1700 64MB to 96MB DRAM Factory Upgrade	4	-
4-Channel Packet Voice/Fax DSP Module	4	-
10/100 Modular Router w/Voice,19-in Chassis,32MB FL/96MB DR	4	171
10/100 Ethernet Modular Router with 2 WIC Slots & 1 NM Slot CISCO2611XM	1	2156
1-Port E1 30 Channel Voice/Fax Network Module NM-HDV-1E1-30	1	6900
TOTAL EN DOLARES:		23940

3.5 CAMARAS DE VIDEOCONFERENCIA

Como se observó dentro de las pruebas de videoconferencia realizadas, la opción de software no se encuentra tan atractiva debido a sus limitaciones debido a que la resolución y calidad depende mucho de las cámaras web que se instalan y a que tipo de equipo de computo se conectan, por otra parte cabe resaltar que estos software no son gratuitos para el caso de conexiones multipunto, se realizaron algunas pruebas con un proveedor del programa Click to Meet que ofrece la interconexión de 4 o mas puntos por medio de videoconferencia, donde el servidor se encuentra en una dirección publica de Internet, con las desventajas antes mencionadas. El monto para 4 equipos con el software de videoconferencia Click to Meet supera los 10.300 dólares.

El Cidlis posee un par de cámaras Polycom Viewstation 128sp para videoconferencia con las cuales se realizaron pruebas sobre el enlace Bucaramanga-Socorro, a partir de los resultados obtenidos con estos equipos se eligió la opción de incluir dentro del diseño total cámaras especializadas de videoconferencia que cumplan con los estándares multimedia en cuanto a

codificación y compresión de audio y video se refiere. De acuerdo a esto se realizó un serie de visitas a diferente empresas que utilizan videoconferencia dando como resultado proveedores de equipos para estas soluciones.

Se tienen dos opciones de cámaras de videoconferencia, la primera son de la reconocida marca Polycom y la segunda es la serie de cámaras Tandberg.

3.5.1 Propuesta en Polycom

3.5.1.1 Equipo multipunto. Polycom VSX7000 H.323 VSX MULTIPPOINT PLUS MULTIPUNTO PARA CUATRO PUNTOS.

Figura 36. Equipo Polycom



Tabla 9. Valor Equipos Polycom.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO EN DOLARES
Polycom VSX7000 MULTIPPOINT PLUS multipunto para 4 puntos	1	8.998.00

Polycom VSX7000 H.323	4	23.996.00
Valor total oferta sin iva		32.994.00

Nota: Los precios anteriores no incluyen IVA.

3.5.2 Propuesta Tandberg

Figura 36. Cámara Tandberg



Tabla 10. Valor equipos Tandberg.

DESCRIPCION	CANTIDAD	PRECIO UNITARIO EN DOLARES
Sistema Tandberg 880 MXP IP hasta 4 de videoconferencia, y 3 en audio	1	11.100.00
Sistema Tandberg 550 IP Punto a punto	4	22.000.00
Valor Total de la Oferta sin IVA		33.100.00

Nota: Los precios anteriores no incluyen IVA.

Como se puede observar los precios de los equipos finalmente tiene un costo similar y las características ofrecidas son muy similares en cuanto a integración con otras marcas de equipos de videoconferencia y servicio de presentación de diapositivas, videos, etc. Ver anexo.

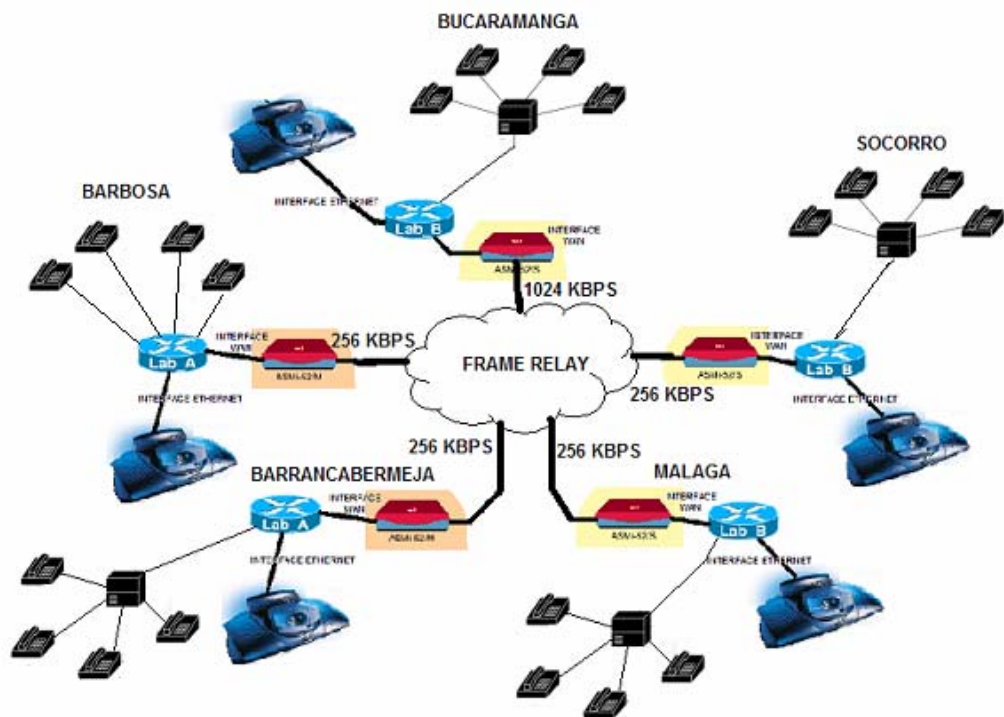
3.6 INTERCONEXIÓN DE LAS PLANTAS TELEFÓNICAS A LA RED DE DATOS

La universidad Industrial de Santander cuenta con plantas telefónicas marca Siemens en sus sedes. El diseño propuesto pretende integrar las plantas de las diferentes localidades. Tal como se había mencionado los router Cisco 1760 de las sedes de Socorro, Barbosa, Barrancabermeja y Málaga tendrán 4 puertos de voz FXS cada uno de ellos, estos puertos generan señalización y timbre, por lo cual se pueden comportar como troncales telefónicas analógicas, de esta manera se pueden integrar a las plantas como si fueran una entrada de línea troncal analógica convencional para que el tono sea tomado desde cualquier extensión, en el caso de Barbosa donde no se posee planta telefónica se pueden cablear desde los puertos del router para conectar teléfonos en las oficinas que se requiera generar y recibir las llamadas.

En la sede de Bucaramanga se hará uso de un módulo de red de un solo puerto y 30 canales mejorados de enlace troncal E1 de paquetes e voz digital NM-HDV-1E1-30E, el cual se debe conectar a una tarjeta digital por instalar adicional en la planta Siemens de Bucaramanga, de esta manera por una sola tarjeta se integran los canales de voz de todas las sedes con la principal permitiendo las 16 llamadas en simultanea en Bucaramanga contra todas las sedes, quedando espacio para 14 llamadas mas en caso de ampliación de los servicios o integración de una nueva regional.

La Universidad Industrial Santander se encuentra en estudio de actualización de las plantas telefónicas con el mismo proveedor actual, sin embargo la infraestructura propuesta sirve como pilar de la nueva red de voz si esta se llega a efectuar, pues de acuerdo a la propuesta del fabricante de la planta, una gran proporción de los módulos de la actual se pueden integrar a la nueva línea, de igual manera si dentro de la actualización de las plantas se incluyen adaptadores de conversión a paquetes IP de la voz, se estaría manejando voz sobre IP generada directamente desde la planta, los equipos de enrutamiento propuestos poseen la versatilidad suficiente para poder suplir los cambios correspondientes.

Figura 37. Diagrama general del Proyecto.



3.7 PROPUESTA ECONOMICA GENERAL

De acuerdo a los requerimientos de infraestructura y equipos necesarios para montar una red de voz y videoconferencia con disponibilidad del servicio 7 días a la semana, las 24 horas del día durante todo el año, el presupuesto es el siguiente:

Tabla 11. Valor total del proyecto.

DESCRIPCIÓN	VALOR EN DOLARES APROXIMADO
EQUIPOS DE ENRUTAMIENTO	23.940
EQUIPOS DE VIDEOCONFERENCIA	32.994
CANALES FRAME RELAY INSTALACIÓN MAS PRIMERA MENSUALIDAD	5.470
TOTAL	62.404

4. CONCLUSIONES

Dentro de las pruebas realizadas sobre la red existente, se encuentra que los canales actuales en las regionales tienen copada su capacidad en el servicio de Internet y de aplicativos administrativos, lo cual implica que no hay disponibilidad para incluir más servicios como los propuestos en este proyecto, por otra parte no se planteó la opción de ampliar los anchos de banda en cada punto, debido a que el proveedor no garantiza que los pares de cobre por donde van los enlaces sean de alta calidad para soportar 512 Kbps, esto para las sedes diferentes a la de Bucaramanga.

Para servicios que requieren respuesta en tiempo real como lo son la videoconferencia y servicios de voz, son necesarios canales con retardos y tiempos de respuesta mínimos entre los puntos, razón por la cual no se eligen enlaces satelitales en este diseño, sin contar que además los costos son demasiado altos comparados con enlaces terrestres. Debido a esto la mejor opción encontrada es contratar nuevos canales de cobre con el proveedor actual.

En toda red de datos actual los equipos de enrutamiento son pieza fundamental, para este caso la elección de la marca Cisco Systems se basa en que están a la vanguardia en tecnología a nivel mundial y permiten compatibilidad con la red actual, la cual también esta basada en estos. Además la posibilidad de actualizaciones permanentes en cuanto a su sistema operativo (IOS), permite que los equipos que se adquieran no se vuelvan obsoletos rápidamente.

La elección del modelo de enrutador depende de las necesidades del momento, pero siempre teniendo en cuenta futuras ampliaciones de servicios, sin llegar a sub-utilizar los mismos, por esta razón se encogieron los modelos 1760-V para las sedes alternas y el 2611 para la principal de Bucaramanga.

Si bien hoy en día la inclinación es tener infraestructuras a base de Software, no siempre es ésta opción la más ventajosa, pues depende mucho del Hardware sobre la cual se piensa montar, tal como se observó en las pruebas realizadas, el desempeño obtenido por las cámaras de videoconferencia fue superior al de los software analizados, los cuales son funcionales para casos de entretenimiento por ejemplo Internet.

La integración de los sistemas de voz de la Universidad, más específicamente de las plantas telefónicas, exige que la infraestructura sobre la cual se monte permita cambios y actualizaciones de los sistemas telefónicos, por esto se plantean canales de voz corporativos flexibles independientemente de la marca o modelo de planta que se piense adquirir en un futuro, pues los equipos de enrutamiento sugeridos permiten el transporte de voz de extremo a extremo y una fácil integración con los sistemas de plantas telefónicas actuales y futuras.

Finalmente, las necesidades de comunicación e interacción directa con todas las dependencias de la Universidad, con el fin que se haga una integración total, promueve el planteamiento de soluciones que cumplan con los requerimientos actuales.

BIBLIOGRAFÍA

SACKETT, George. Manual de routers Cisco. Primera Edición en Español (2002); p.129-158.

STALLINGS, William. Comunicaciones y redes de computadores. Sexta edición (2000); p. 352-356.

Disponible en Internet: <http://www.iec.gov>

Disponible en Internet: http://www.sunrisetelecom.com/espanol/frame_relay.pdf

Disponible en Internet: <http://www.telenorma.com.co/videoconferencia/02h.htm>

Disponible en Internet: <http://www.telenorma.com.co/videoconferencia/02a.htm>

Disponible en Internet:

<http://www.comunicaciones.unitronics.es/tecnologia/H.323.html>

Disponible en Internet:

http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a0080088713.html

Disponible en Internet:

http://www.ims.es/imatges/pdf/telecom/polyspan/Folleto_Polycom_VSX7000%20MP.pdf

ANEXO A

PRUEBA DE BERT AL ENLACE DE SOCORRO – BUCARAMANGA

Archivo entregado por el Analizador de Redes Digitales Wandel:

WANDEL & GOLTERMANN PFA-35 ANALIZADOR DE REDES DIGITALES
12:26 26 Oct 2004

Impresion de resultados de prueba numero:	4	
Hora inicio	9:00 23 Oct 2004	
Hora parada	11:00 23 Feb 2004	
Tiempo total medida (en segundos)	7200	
Velocidad de linea		
Veloc. transmision	128000	
Total bit recibidos	9.216E 8	
Total errores bit recibidos	0	
Tasa media errores de bit	0.000E 0	
Segundos de No Reloj	0	
Segundos de perdida de sincro	0	
Segundos de todo "1"	0	
Segundos de todo "0"	0	
Segundos de Deslizamiento		
Tiempo disponible	7200	100.00000%
Tiempo indisponible	0	0.00000%
Segundos sin error	7200	100.00000%
Segundos con error	0	0.00000%

Segundos severamente errados	0	0.00000%
Segundos No-severam. errados	7200	100.00000%
Minutos degradados		
Minutos no degradados	120	100.00000%

ANEXO B.

ANALIZADOR DE REDES DIGITALES (WANDELL)



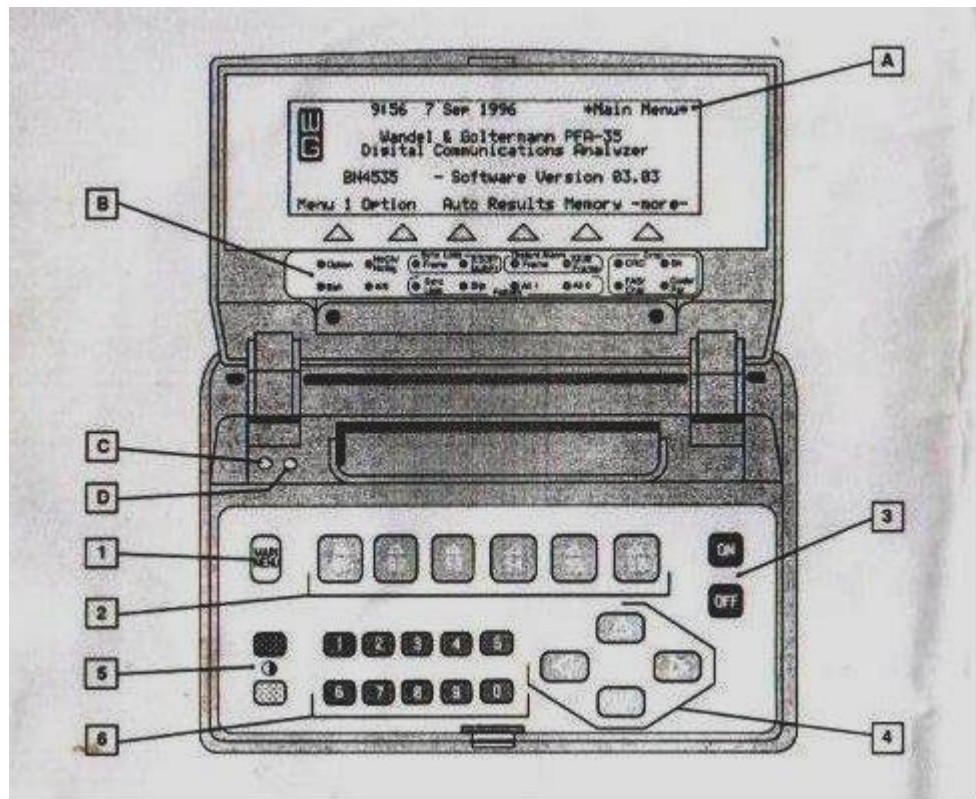
El wandell o generador de pruebas de Bert (Bit Error Rate Test) es un equipo como su nombre lo indica que genera una ráfaga de bits, los cuales son enviados por intermedio de una interfaz a un modem (lado A) el cual tendrá salida por un medio físico para la comunicación con otro modem (lado B) en un lado remoto. El modem (lado B) deberá tener en su interfaz de salida de datos un loop (cruce de señales), el cual devolverá los datos enviados por el modem (lado A). El primer modem mencionado devolverá también los datos al wandell; el cual hará una comparación (TEB) de los datos recibidos con los datos enviados anteriormente, esta comparación nos indicara el estado actual del enlace de comunicaciones.

A medida que el TEB sea mayor el enlace tendrá un mayor rendimiento.

TEB	RESULTADO
0	Exitoso
Exp -8	Aceptable
Exp -6	Regular
<= Exp -5	Ineficiente

La prueba de un buen enlace de comunicaciones debe brindar un resultado exitoso para garantizar la transmisión de datos.

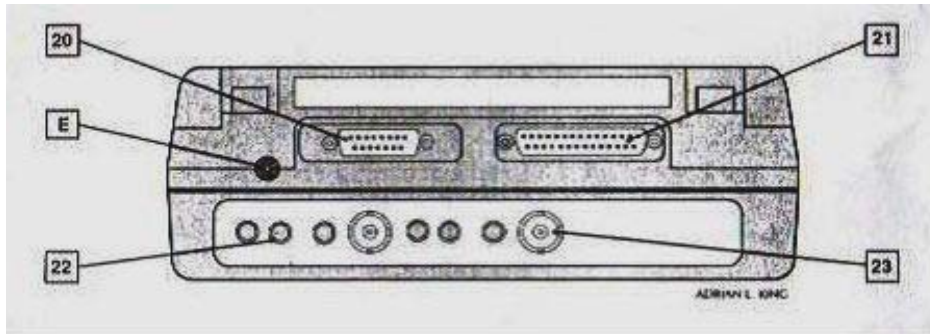
DESCRIPCIÓN FÍSICA DEL EQUIPO



PANTALLA Y TECLADO

- A. Pagina de presentación en el display: En la cual observamos el nombre del equipo, la versión del software, hora y fecha, y el menu principal: menú 1, result, memoria, menu 2, utilits, hora-día, menu 3, configuración, lengua.
 - B. Leds. Indican y especifican alarmas, errores de eventos específicos. El led rojo indica dicha alarma con su respectivo parámetro, el led amarillo en la opción batt indica que la batería se encuentra baja.
 - C. Led Indicador 1. Enciende en color rojo visualizando una alarma o un evento.
 - D. Led Indicador 2. Enciende en color verde indicando que no existe hasta el momento alarmas ni eventos durante la prueba.
1. Tecla Main Menu. Muestra la pagina de presentación y el menú principal.
 2. Teclas S1-S6. Con las cuales se ingresan a las diferentes funciones del menú principal.
 3. Teclas ON y OFF. Encender y apagar el equipo.
 4. Cursor. Cuatro teclas que sirven para el desplazamiento dentro de las diferentes funciones.
 5. Teclas de Contraste. Aumentar o disminuir el contraste del display (pantalla).
 6. Teclado Numérico. Contiene 10 dígitos, que comprenden 0-9.

PANEL POSTERIOR



20. Puerto para interfaz V.35.

21. Puerto para interfaz Rs-232.

22. Puerto BNC entrada interfaz G.703.

23. Puerto BNC salida interfaz G.703.

E. Puerto externo para conexión de fuente de alimentación.

Posee un submenú TEB (Tasa Error de Bit). Habilita el PRBS (Patrones que simulan tráfico real en las redes, dependiendo de la velocidad)

PRBS	VELOCIDADES
2^9-1	Hasta 14400 bps
$2^{11}-1$	64 kbps y n.64 kbps
$2^{15}-1$	1544-2048-6132-8448- 32064-404736 kbps
$2^{20}-1$	Hasta 62 Kbps
$2^{23}-1$	34368 y 139264 kbps

Para la prueba se selecciona **2⁹-1**.

En el momento en que esta corriendo el Bert el display (pantalla) muestra los siguientes parámetros:

- RX/TX
- V.35, DTE
- RTX: INT
- RX: EXT
- Segundos de la prueba: xxxxxx
- Velocidad en línea: xxxxxx
- TEB: xxxxxx
- OK en resolución mayor. Indica que la prueba esta ejecutándose sin ningún error hasta el momento.

También en el display tenemos las siguientes opciones:

- Reset: Reinicio de la prueba.
- Stop: Fin de la prueba

Al terminar la prueba el Wandell automáticamente guardar los resultados en un espacio de su memoria, la cual se asigno en el paso numero dos al mismo tiempo presenta en la pantalla los resultados obtenidos en la prueba:

- Segundos totales: xxxxxx
- Velocidad línea: xxxxxx
- TEB: xxxxxx
- Error Bit: xxxxxxx

ANEXO C

ROUTERS MODULARES DE ACCESO DE LA SERIE CISCO 2600

Cisco Systems extiende la versatilidad, integración y alimentación de clase empresarial a las sucursales y a las pequeñas y medianas empresas (PYMES) con la familia de routers modulares de la serie Cisco 2600. Ofrece a los administradores de redes y a los proveedores de servicios nuevos niveles de flexibilidad y protección de la inversión en una solución compacta integrada.

Mediante la implementación de una Power Branch Solution modular, el cliente está tranquilo sabiendo que si cambian las circunstancias de su empresa, el producto Cisco simplemente necesitará un cambio de componentes de poca trascendencia.

Resumen de las características de toda la serie Cisco 2600			
Procesador	CPU Power PC RISC	Ranuras de la tarjeta de interfaz WAN (WICS)	2 WICS
Memoria Flash,	8 MB, ampliables a SIMM de 16 MB	Ranura para módulo de red	1
		Ranura del módulo de integración avanzada (AIM)	1
Memoria DRAM del sistema	24 MB de DRAM, ampliables a DIMM de 64 MB de DRAM	Sistema de alimentación interno	Corriente alterna (CA), de corriente continua (CC) o adaptador RPS
Puertos LAN	Cisco 2621: 2 Ethernet 10/100 Cisco 2620: 1 Ethernet 10/100 Cisco 2613: 1 Token Ring Cisco 2612: 1 Ethernet + 1 Token Ring Cisco 2611: 2 Ethernet Cisco 2610: 1 Ethernet	Dimensiones (Al x An x Pr)	1,69 x 17,5 x 11,8 pulgadas
		Rendimiento	Entre 15 y 25 Kpps
		Puertos auxiliares y de consola	115,2 Kbps con acceso telefónico activado Enrutamiento bajo demanda (aux)

Ventajas principales

- **Integración/capacidad de gestión:** reduce el coste de propiedad y mejora la facilidad de gestión remota, lo que proporciona una red integrada "branch-in-a-box" que combina varias CSU/DSU, multiplexores, módems, NT-1 ISDN (RDSI), compresión, dispositivos de cifrado, VPN/firewalls y gateways de voz/datos en un solo dispositivo.

- **Versatilidad / protección de la inversión:** miles de soluciones personalizadas que pueden actualizarse en las instalaciones ofrecen una sencilla migración a los futuros requisitos de la red. Los productos de la serie Cisco 3600 comparten más de 60 tarjetas de interfaz WAN (WIC) y módulos de red; los módulos pueden intercambiarse entre sucursales pequeñas, de tamaño medio y regionales. La ranura del módulo de integración avanzada (AIM) admite la compresión de datos asistida por hardware y, en el futuro, otros servicios avanzados como el cifrado.
- **Redes multiservicio de voz/datos:** reducen o eliminan los costes de las llamadas entre las oficinas. Utilizando las características de calidad de servicio (QoS) de Cisco IOS®, como por ejemplo WFQ, CAR y RSVP, Custom y Priority Queuing, el tráfico de voz se digitaliza y encapsula en paquetes Frame Relay o IP y se consolida con el tráfico de datos para extender la infraestructura multiservicio a las sucursales.
- **Alimentación:** total compatibilidad a Cisco IOS. Ofrece un rendimiento cinco veces mayor que otras soluciones para routers de sucursales, ya que admite enrutamiento LAN a LAN a velocidad de cable (velocidades de envío de paquetes de hasta 25.000 pps) y compresión de datos de alto rendimiento basada en hardware, o cifrado y compresión de datos basadas en software.
- **Interoperatividad/compatibilidad con varios protocolos:** ofrece un amplio conjunto de protocolos y servicios, incluyendo redes privadas virtuales, firewall, cifrado, optimización WAN y características de soporte multimedia mejoradas.
- **Gestión/monitorización remota:** el Protocolo simple de administración de redes (SNMP), telnet y el puerto de consola local funcionan con varias herramientas de gestión y configuración de Cisco, entre las que se incluyen Fast Step™, Cisco Voice Manager, Configmaker, CiscoView, CiscoWorks y Cisco Resource Manager.

- **Soluciones de extremo a extremo apilables:** la utilización de CiscoView o CiscoWorks permite que una solución de apilado de Cisco que incluye las series Catalyst 1900, 2820 o 2900 XL se gestione como un solo objeto.

Cuándo instalar

- **Serie Cisco 2600:** cuando lo que la empresa necesita es un router modular de alto rendimiento, un servidor de acceso o gateway de voz y:

- Una solución rentable a largo plazo que se adapte a los cambiantes requisitos de red;
- Acceso a la red privada virtual (VPN)/Extranet con firewall para reducir costes y aumentar la seguridad de los asociados y empleados;
- Concentración de acceso telefónico con módems asíncronos, ISDN (RDSI) o analógicos;
- Integración multiservicio de voz/fax/datos;
- Acceso a Internet;
- Concentración de dispositivos serie de los dispositivos de punto de venta, ATM, controladores SDLC con terminales de propietario y dispositivos LAN que comparten una única conexión WAN;
 - Aplicaciones de mayor rendimiento, como DLSW, cifrado L2TP, compresión, QoS y gestión del ancho de banda.

- **Cisco 2621–2** Ethernet 10/100 con detección automática y compatibilidad con VLAN

- **Cisco 2620–1** Ethernet 10/100 con detección automática y compatibilidad con VLAN

- **Cisco 2613–1** puerto Token Ring

- **Cisco 2612**–1 puerto Ethernet y 1 puerto Token Ring para requisitos de LAN mixtos y la capacidad de migrar de Token Ring a Ethernet

- **Cisco 2611**–2 puertos Ethernet para la segmentación LAN o para aislar a una LAN interna segura de una LAN de perímetro (expuesta a Internet)

- **Cisco 2610**–1 puerto Ethernet

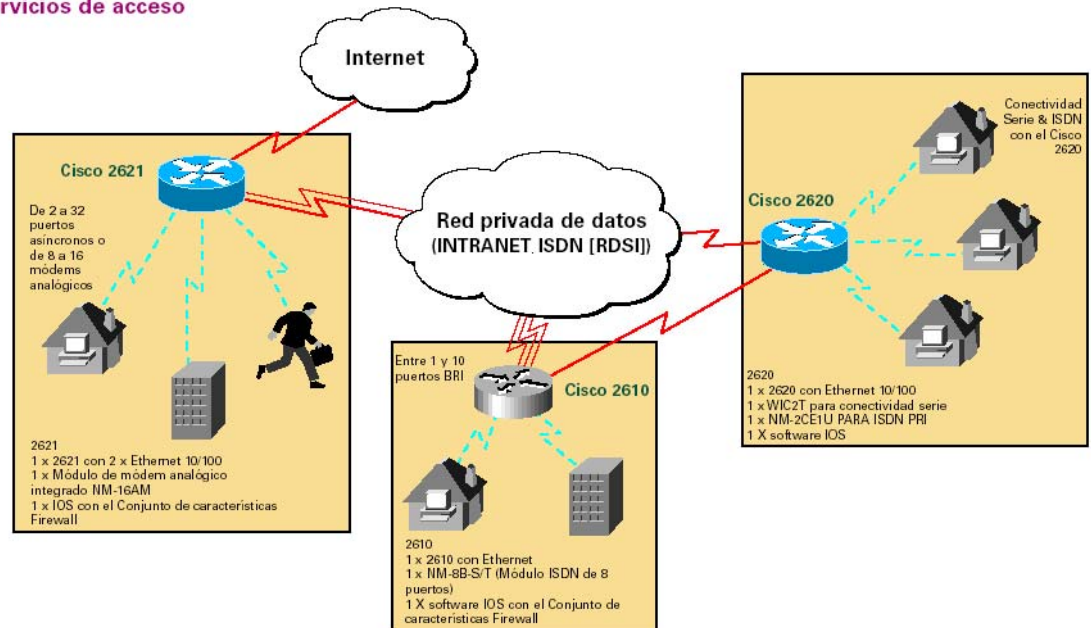
- **Tarjetas de interfaz WAN, módulos de integración de red y avanzados**
 - Conexiones serie (asínc/sínc), conectividad BRI y PRI ISDN (RDSI), CSU/DSU integradas, módems analógicos integrados, integración de voz/fax/datos, conectividad CPE ADSL a través de ATM-25, Ethernet, conexiones asíncronas y síncronas de alta densidad y compresión de datos.

- **Conjunto de características del software** – Cuando un cliente necesita:
 - Enrutamiento IP con NAT (conjunto de características IP)
 - Enrutamiento IP, IPX, AppleTalk y DEC para puesto de trabajo (conjunto de características IP/IPX/AT/DEC)
 - Características IBM, VPDN/L2F, ISL, RMON, MMP, ATM y de voz (conjunto de características Plus)
 - El conjunto más extenso de características de enrutamiento (conjunto de características Enterprise Plus)
 - Servicios avanzados de IBM (conjunto de características Enterprise/APPN Plus)
 - Completos servicios de acceso remoto, incluyendo la conversión de protocolos (conjunto de características RAS)
 - Cifrado DES IPsec y 3DES de 40 bits 56 bits de las capas de red (todos los conjuntos de características de cifrado Plus)

- Seguridad adicional firewall contra la intrusión en la red, especialmente cuando se conecta a Internet (todos los conjuntos de características Firewall)

Posicionamiento de los productos Cisco

Servicios de acceso



Ventajas de la serie Cisco 2600	Categoría	Serie Cisco 2600
<ul style="list-style-type: none"> • Flexibilidad y profundidad sin igual que proporciona el amplio abanico de módulos compartidos • Proporciona una densidad de interfaces mucho más alta para la concentración LAN a LAN, de acceso telefónico, serie y WAN • Cisco IOS ofrece una amplitud y una profundidad de protocolos y capacidades inigualable (QoS, RSVP, WFQ y otras muchas) para administrar de forma eficaz el ancho de banda y desarrollar productos rentables para redes • La solución VoIP y VoFR basada en los routers de Cisco reduce los retrasos, lo que tiene como consecuencia una mejor calidad de la voz • Facilidad de administración a través de Cisco Voice Manager, CiscoWorks y CiscoView • Cisco es líder en el mercado, con más de un 70 por ciento de cuota en el mercado de routers de bajo nivel 	Configuración base	Fijo sencillo, dual, mixto Puertos (Ethernet, 10/100 Ethernet, Token Ring) con 4 ranuras modulares
	Número máximo de puertos Ethernet	6
	Número máximo de puertos Ethernet 10/100	2
	Número máximo de puertos Token Ring	1
	Número máximo de conexiones serie de alta velocidad (hasta 2 Mbps)	4
	Número máximo de conexiones serie de baja velocidad (hasta 128 kbps)	12 sínc, 37 asínc
	Compatibilidad con voz/datos	Si
	Módems integrados	16
	Número máximo de puertos BRI ISDN (RDSI)	10
	Número máximo de puertos PRI ISDN (RDSI)	2
	CSU/DSU integradas (T1/T1 fraccional y 56k/64k)	Si
	Compresión por hardware o software	Hardware-8Mbps y software
	Cifrado	Software + hardware
Sistema de alimentación redundante	Si	

Información para los pedidos	Producto	Descripción	Aplicación			
			Acceso LAN a LAN	teléfono	Proprietario	Multi-Servicio
<p>La serie Cisco 2600 se solicita por componentes: Es necesario solicitar:</p> <ul style="list-style-type: none"> Un chasis (Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621) Un CD con el conjunto de características de software Un cable de alimentación <p>Los elementos opcionales son:</p> <ul style="list-style-type: none"> Una actualización o revisión del conjunto de características Cisco IOS (el conjunto de características IP es el predeterminado y el que se incluye con el chasis) Una o dos tarjetas de interfaz WAN (WICS) Un módulo de red Un módulo de integración avanzada Una o dos tarjetas de interfaz de voz para un módulo de red de voz/fax Actualizaciones de la memoria Cables Corriente continua (CC) o adaptador del sistema de alimentación redundante (RPS) Kit de compatibilidad con NEBS/ETSI <p>Todos los chasis Cisco 2600 incluyen de serie la memoria mínima necesaria para el conjunto de características IP por defecto, documentación, consola, cables LAN y auxiliares, abrazaderas para el montaje en bastidor, convertidores RJ45 a DB-9 y DB-25, y paneles de cubierta que protegen cualquier tarjeta de interfaz WAN y/o ranura de módulo de red no utilizada.</p>	Serie Cisco 2600					
	Cisco 2610	Router modular Ethernet con software IP Cisco IOS	x	x	x	x
	Cisco 2611	Router modular dual Ethernet con IP Cisco IOS Software	x	x	x	x
	Cisco 2612	Router modular Ethernet/Token Ring con Cisco Software IP IOS	x	x	x	x
	Cisco 2613	Router modular Token Ring con Cisco IOS Software IP	x	x	x	x
	Cisco 2620	Router modular Ethernet 10/100 con Cisco Software IP IOS	x	x	x	x
	Cisco 2621	Router modular dual Ethernet 10/100 con Cisco Software IP IOS	x	x	x	x
	Tarjetas de interfaz WAN/WIC compartidas con las series Cisco 1600, 1720 y 3600					
	WIC-1T=	Serie sínc. de un puerto	x	x	x	x
	WIC-2T=	Tarjeta de interfaz WAN serie de dos puertos para la serie Cisco 2600	x	x	x	x
	WIC-2A/S=	Tarjeta de interfaz WAN serie asínc/sínc de dos puertos para Cisco 2600	x	x	x	x
	WIC-IDSU-56K4=	56-64 kbps de 4 hilos y 1 puerto con integrado CSU/DSU	x	x	x	x
	WIC-1DSU-T1=	T1/T1 fraccional de un puerto con CSU/DSU	x	x	x	x
	WIC-1B-S/T=	ISDN (RDSI) BRI de un puerto	x	x	x	x
	WIC-1B-U=	ISDN (RDSI) BRI de un puerto con NT1	x	x	x	x
Módulos de integración avanzada (no ocupa ninguna ranura WIC o NM externa)						
AIM-COMPR2	AIM para compresión de datos para la serie Cisco 2600	x	x	x	x	

<p>WIC-1T: tarjeta de interfaz WAN serie de un puerto</p> <p>La tarjeta de interfaz WAN serie de 1 puerto admite una sola conexión serie a velocidades de hasta T1/E1. El conector DB-60 admite cualquiera de los cinco tipos de interfaces (RS-232, RS-449, RS-530, V.35, X.21) tanto en modo DTE como DCE. Esta tarjeta de interfaz se inserta en un módulo de red de medios mixtos de Cisco o directamente en la ranura de expansión de una tarjeta de interfaz WAN (WIC) de Cisco.</p>	<p>Soluciones VPN y Firewall de enrutamiento LAN a LAN</p> 	<p>3660 - 12.0(5)T 3640 - 11.1(7)AA 3620 - 11.1(7)AA Serie 2600 - 11.3(2)XA</p>	<p>Requiere un router Cisco 2600 o, para su uso en un router Cisco 3600, un módulo de red LAN/WAN NM-1E2W, NM-2E2W o NM-1E1R2W.</p>
---	--	---	---

SOLUCIONES DE VOZ DIGITAL

NM-HDV-1E1-30

Módulo de red de un solo puerto y 30 canales de enlace troncal E1 de paquetes de voz digitales

Este módulo de red de voz/fax proporciona una única conexión E1 y soporte para 30 canales de compresión de voz de complejidad media utilizando cualquiera de los siguientes VoCoders: G.711, G.729a/b, G.726 y fax. También se puede utilizar este módulo para ofrecer 12 canales de compresión de voz de complejidad alta y/o media utilizando cualquiera de los siguientes VoCoders: G.711, G.729, G.729a/b, G.726, G.728, G.723.1 y fax. La NM-HDV-1E1-30 se compone de un módulo de red, una tarjeta de interfaz de voz y procesadores de señal digital.

Soluciones VPN y Firewall de integración de voz y fax



Serie 3660 - 12.07XK ó 12.1.1T

Serie 3640 - 12.07XK ó 12.1.1T

Serie 3620 - 12.07XK ó 12.1.1T

Serie 2600 - 12.07XK ó 12.1.1T

Necesita un conjunto de características "PLUS" del Cisco IOS

ANEXO D

ROUTER CISCO 1760

Cisco **1760** Modular Access Router

Introduction

The Cisco 1760 Modular Access Router offers small and medium-sized businesses and enterprise small branch offices a 19-inch rack-mount access solution designed to enable them to grow their e-business capabilities. The two different versions of the Cisco 1760 Modular Access Router, the base version Cisco 1760 router and the preconfigured multiservice-ready Cisco 1760-V router, address the needs of customers who want to deploy e-business applications—now or in the future.

The Cisco 1760 router, as a modular platform in a 19-inch rack-mount form factor, offers customers secure Internet and intranet access, as well as the capability to implement a variety of e-business and

voice applications. This includes voice over IP (VoIP), virtual private network (VPN) access, and business-class digital subscriber line (DSL) as required (refer to Figure 1).

The Cisco 1760 router is part of a broad portfolio of access routers optimized to deliver intelligent services such as quality of service (QoS), manageability, availability, and security.

The two different versions of the Cisco 1760 Modular Access Router, the base version Cisco 1760 router and the Cisco 1760-V router, address the needs of customers who want to deploy transformation technologies such as converged voice and data, IP telephony, or videoconferencing.

Figure 1
Cisco 1760 Modular
Access Router



Key Benefits and Features

The key benefits and features of the Cisco 1760 Modular Access Router are listed in Table 1.

Table 1 Key Benefits and Features of Cisco 1760 Modular Access Router

Key Benefits	Key Features
Investment protection	<ul style="list-style-type: none"> Offers field-upgradable WICs and VICs¹ Provides Cisco IOS® Software upgradable feature sets
Flexibility	<ul style="list-style-type: none"> Provides full Cisco IOS Software support, including multiprotocol routing (IP, IPX², Apple Talk, IBM/SNA³) and bridging Provides customization through wide range of WICs and VICs Offers modular data and voice slots
Lower cost of ownership	<ul style="list-style-type: none"> Combines optional functions, including a voice gateway, dynamic firewall, VPN tunnel server, DSU/CSU⁴ (56 or 64 kbps or T1/FT1) and ISDN NT1⁵ device Supports remote management applications such as CiscoView (part of CiscoWorks2000)
Security	<ul style="list-style-type: none"> Offers Cisco IOS Firewall Provides VPN IPSec (DES⁶ and 3DES⁷) Enables wire-speed (T1/E1) encryption using optional VPN module
Voice traffic migration to data networks	<ul style="list-style-type: none"> Supports IP telephony Interoperates with next-generation voice-enabled applications such as integrated messaging and Web-based call centers Works with the existing telephone infrastructure: phones, fax machines, KTS⁸ units, and PBX⁹ (including digital PBXs)
Business-class broadband access for value-added services such as voice over broadband	<ul style="list-style-type: none"> Supports ADSL¹⁰ and symmetric single pair high bit rate digital subscriber line (G.shdsl) support Provides efficient utilization of bandwidth Offers prioritization of voice traffic
Ideal for small/medium-sized businesses and small enterprise branch offices to deploy transformational technologies such as converged data and voice applications	<ul style="list-style-type: none"> Provides greater analog voice port density (four slots) than Cisco 1751 (three slots), enabling more connections to analog end stations, PBXs, key switches, and basic telephone service (POTS) lines Supports maximum 30 digital DSD channels through T1/E1 VWICs 19-inch rack-mount form factor

1. WAN interface cards and voice interface cards

2. Internetwork Packet Exchange

3. Systems Network Architecture

4. DataChannel service unit

5. Network Termination 1

6. Digital Encryption Standard

7. Triple DES

8. Key telephone system

9. Private branch exchange

10. Asymmetric DSL

Cisco 1700 Series Routers

The Cisco 1700 Series routers enables a cost-effective, seamless network infrastructure for the small and medium-sized business and small enterprise branch office.

The Cisco 1700 Series of access routers includes the Cisco 1710, 1721, 1751 (includes a base model, the Cisco 1751, and a multiservice-ready model, the Cisco 1751-V), and Cisco 1760 (includes the base version, Cisco 1760, and the multiservice-ready version, Cisco 1760-V). Table 2 compares the Cisco 1760 and Cisco 1760-V routers.

The Cisco 1710 Security Access Router features comprehensive security with VPNs, a Cisco IOS Firewall, and advanced routing functionality in an all-in-one device.

The Cisco 1721 router is a modular device optimized for data-only connections. The Cisco 1751 and Cisco 1760 modular access routers are optimized for multiservice data and voice solutions.

The Cisco 1760 router is the preferred multiservice data and voice solution when a 19-inch rack-mount form factor is required. Compared to the Cisco 1751 router, it offers an additional VIC slot.

Table 2 Cisco 1760 Modular Access Router—Two Versions

Cisco 1760	Cisco 1760-V
Base version	Multiservice-ready version
Includes everything for data networking	Includes all the features needed for <i>immediate</i> integration of voice and data
32-MB Flash memory (on board)	32-MB Flash memory (16 MB on board, 16 MB in Flash SIMM ¹ socket)
64-MB DRAM (on board)	96-MB DRAM (64 MB on board, 32 MB in DRAM DIMM ² socket)
Cisco IOS IP Software Feature Set	Cisco IOS IP/Voice Plus feature set
Two DSP ³ module slots available DSPs available separately	Two DSP module slots available Comes with one DSP (PVDM-256K-4) inserted in one DSP module slot DSPs available separately for further upgrades
VICs available separately	VICs available separately
Flash memory and DRAM upgrades available separately	Flash memory and DRAM upgrades available separately
WICs available separately	WICs available separately

1. Single in-line memory module
2. Double in-line memory module
3. Digital signal processor

High-Performance Architecture

Cisco IOS Software features and a robust RISC architecture enables the Cisco 1760 router to support applications as shown in Figures 2 and 3.

Figure 2

The Cisco 1760 router enables a multiservice solution

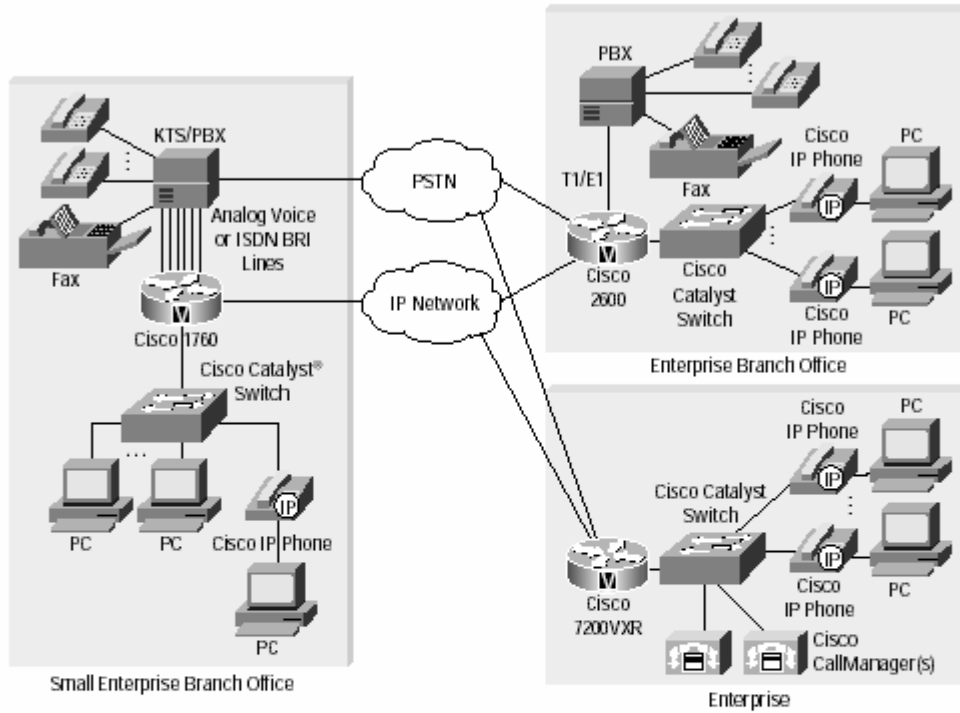
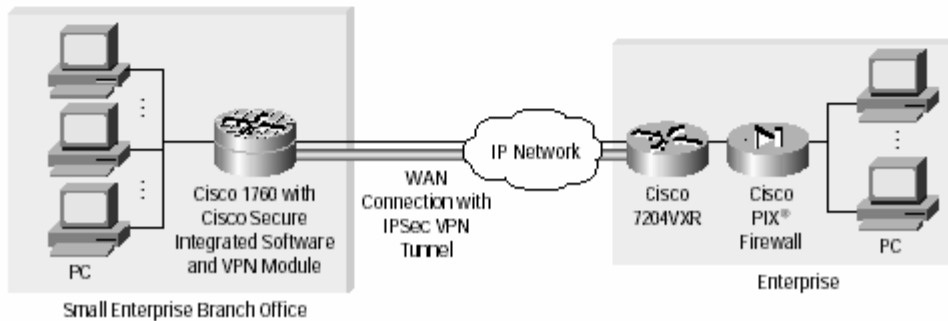


Figure 3

The Cisco 1760 router provides secure connectivity



Comprehensive Feature Set and Benefits

The Cisco 1760 router offers a broad feature set designed to allow businesses not only to attain maximum benefit on their investment but also to easily deploy e-business and voice solutions.

The following tables and figures provide details on the Cisco 1760 router features. Table 3 gives a comprehensive list of features and benefits, and Table 4 gives information on the physical architecture of the Cisco 1760 router. Physical interfaces, including WAN support, voice interface cards, and memory are delineated in Tables 5 through 7. The modular slots and router appearance are detailed in Figure 4.

Table 3 Benefits and Features of Cisco 1760 Modular Access Router

Benefits	Features
Cisco IOS Software support	
<ul style="list-style-type: none"> Provides the industry's most robust, scalable, and feature-rich internetworking software support Uses the industry-accepted standard networking software for the Internet and private WANs Improves network reliability and enables scalability to large networks Offers part of the Cisco end-to-end network solution 	<ul style="list-style-type: none"> Offers multiprotocol routing (IP, IPX, AppleTalk, IBM/SNA) and bridging Dial-on-demand routing Dual-bank Flash memory Scalable routing protocols such as OSPF¹, EIGRP², and HSRP³
Voice	
Integrated voice and data networking	
<ul style="list-style-type: none"> Reduces long-distance toll charges because data network carries interoffice voice and fax traffic Provides easy deployment of IP telephony solutions Eliminates the need for costly phone-equipment upgrade Allows expandability to support additional voice channels Enables unified messaging 	<ul style="list-style-type: none"> Offers integrated voice and data networking Cisco 1760 Router chassis accepts both WICs and VICs Supports IP telephony Works with existing handsets, key units, and PBXs Provides dual DSP slots
Voice support	
<ul style="list-style-type: none"> Transmits data, voice, and video across a single IP network 	<ul style="list-style-type: none"> Supports VoIP and VoFR⁴ (FRF.11) Supports SRST⁵
Gateway signaling	
<ul style="list-style-type: none"> Connects to H.323 networks and devices Provides open standards-based voice signaling 	<ul style="list-style-type: none"> Supports H.323 Versions 1 and 2 Supports SIP⁶ version 2.0 and MGCP⁷ Version 1.0
Codec ⁸ support	
<ul style="list-style-type: none"> Interoperates with a range of CPE⁹ Supports various compression algorithms 	<ul style="list-style-type: none"> Supports G.711 Supports G.723 Supports G.726 Supports G.728 Supports G.729 (interoperates with G.729a) Supports G.729.b (interoperates with G.729ab)

Table 3 Benefits and Features of Cisco 1760 Modular Access Router

Benefits	Features
Security	
<p>Cisco IOS Software security</p> <ul style="list-style-type: none"> • Enables secure access to the Internet with per-application-based, dynamic access control • Prevents unauthorized access to the internal LAN • Enables creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network • Supports up to 168-bit encryption • Simplifies router and security configuration through smart wizards, enabling customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of IOS Command Line Interface (CLI). 	<ul style="list-style-type: none"> • Simplifies VPN deployment through elimination of complex remote-side configurations • Accepts VPN connections from Cisco VPN Software clients and Cisco Easy VPN Remote devices • Provides Cisco IOS Firewall feature set context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, IDS¹⁰, and encryption • Offers IPSec¹¹ DES, and 3DES support • Offers Cisco Easy VPN Remote support • Offers Cisco Easy VPN Server support as of Q2 CY '02 • Offers Cisco Security Device Manager (SDM) support
<p>Hardware-accelerated VPN encryption</p> <ul style="list-style-type: none"> • Supports wire-speed encryption up to T1/E1 speeds 	<ul style="list-style-type: none"> • Offers hardware-based encryption using optional VPN module
<p>Device authentication and key management</p> <ul style="list-style-type: none"> • Ensures proper identity and authenticity of devices and data • Enables scalability to very large IPSec networks through automated key management 	<ul style="list-style-type: none"> • Supports IKE¹², X.509v3 digital certification, and CEP¹³ with certification authorities such as Verisign and Entrust
<p>User authentication</p> <ul style="list-style-type: none"> • Supports all leading user-identity verification schemes 	<ul style="list-style-type: none"> • Supports PAP/CHAP¹⁴, RADIUS¹⁵, and TACACS+
<p>VPN tunneling</p> <ul style="list-style-type: none"> • Offers choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic • Allows standards-based IPSec or L2TP¹⁶ client to interoperate with Cisco IOS tunneling technologies • Interoperates with public certification authorities and IPSec standards-based products • Fits as part of the scalable Cisco end-to-end VPN solution portfolio 	<ul style="list-style-type: none"> • Supports IPSec, GRE¹⁷, L2TP, and L2F¹⁸
Business-class DSL	
<ul style="list-style-type: none"> • Delivers business-class broadband access • Enables voice and video over DSL 	<ul style="list-style-type: none"> • Supports ADSL WAN and G.shdsl interface card with following QoS features: <ul style="list-style-type: none"> - LF¹⁹ using MLP²⁰ over ATM - LLQ²¹ (also called PQ/CBWFQ) - WRED²² - CAR²³ - Differentiated services (class-based marking)

Table 3 Benefits and Features of Cisco 1760 Modular Access Router

Benefits	Features
Security	
<p>Cisco IOS Software security</p> <ul style="list-style-type: none"> Enables secure access to the Internet with per-application-based, dynamic access control Prevents unauthorized access to the Internal LAN Enables creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network Supports up to 168-bit encryption Simplifies router and security configuration through smart wizards, enabling customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of IOS Command Line Interface (CLI). 	<ul style="list-style-type: none"> Simplifies VPN deployment through elimination of complex remote-side configurations Accepts VPN connections from Cisco VPN Software clients and Cisco Easy VPN Remote devices Provides Cisco IOS Firewall feature set context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, IDS¹⁰, and encryption Offers IPSec¹¹ DES, and 3DES support Offers Cisco Easy VPN Remote support Offers Cisco Easy VPN Server support as of Q2 CY '02 Offers Cisco Security Device Manager (SDM) support
<p>Hardware-accelerated VPN encryption</p> <ul style="list-style-type: none"> Supports wire-speed encryption up to T1/E1 speeds 	<ul style="list-style-type: none"> Offers hardware-based encryption using optional VPN module
<p>Device authentication and key management</p> <ul style="list-style-type: none"> Ensures proper identity and authenticity of devices and data Enables scalability to very large IPSec networks through automated key management 	<ul style="list-style-type: none"> Supports IKE¹², X.509v3 digital certification, and CEP¹³ with certification authorities such as Verisign and Entrust
<p>User authentication</p> <ul style="list-style-type: none"> Supports all leading user-identity verification schemes 	<ul style="list-style-type: none"> Supports PAP/CHAP¹⁴, RADIUS¹⁵, and TACACS+
<p>VPN tunneling</p> <ul style="list-style-type: none"> Offers choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic Allows standards-based IPSec or L2TP¹⁶ client to interoperate with Cisco IOS tunneling technologies Interoperates with public certification authorities and IPSec standards-based products Fits as part of the scalable Cisco end-to-end VPN solution portfolio 	<ul style="list-style-type: none"> Supports IPSec, GRE¹⁷, L2TP, and L2F¹⁸
Business-class DSL	
<ul style="list-style-type: none"> Delivers business-class broadband access Enables voice and video over DSL 	<ul style="list-style-type: none"> Supports ADSL WAN and G.shdsl interface card with following QoS features: <ul style="list-style-type: none"> LLF¹⁹ using MLP²⁰ over ATM LLQ²¹ (also called PQ/CBWFQ) WRED²² CAR²³ Differentiated services (class-based marking)

Table 3 Benefits and Features of Cisco 1760 Modular Access Router

Benefits	Features
QoS	
<ul style="list-style-type: none"> Allocates WAN bandwidth to priority applications for improved performance 	<ul style="list-style-type: none"> CAR Policy routing WFQ²⁴ LLQ (also called PQ/CBWFQ) WRED GTS²⁵ RSVP²⁶ DSCP²⁷ FRE.12²⁸ FRTS²⁹ cRTP³⁰ RSVP + H.323v2 (with fast connect)
Modular architecture	
<ul style="list-style-type: none"> Provides flexibility and investment protection Reduces cost of maintaining inventory Lowers training costs for support personnel Protects investments through reuse on various platforms Simplifies migration to Fast Ethernet performance in the office Enables expansion of hardware-assisted encryption support at T1/E1 speeds 	<ul style="list-style-type: none"> Accepts an array of WICs and VICs Shares WICs with Cisco 1700, 2600, and 3600 routers Offers autosensing 10/100 Fast Ethernet Provides three Ethernet connections (one 10/100 on board and support for two Ethernet WICs 10BASE-T) Provides expansion slot on motherboard
WAN support	
<ul style="list-style-type: none"> Simplifies deployment and reduces Internet access costs Provides easy migration between WAN technologies 	<ul style="list-style-type: none"> Supports Cisco IOS Easy IP Supports asynchronous serial interfaces on serial WICs Supports interface speed up to 115.2 kbps Supports asynchronous serial protocols: PPP³¹ and SLIP³² Supports PPPoE³³ Supports asynchronous/synchronous interfaces Supports ISDN WICs Supports ADSL and G.shdsl WICs Supports ISDN dialup and IDSL³⁴ at 64 and 128 kbps Supports Frame Relay and PPP
LAN support	
<ul style="list-style-type: none"> Enables traffic separation Provides better bandwidth utilization Alleviates scaling issues by logically segmenting the physical LAN infrastructure into different subnets Simplifies deployment 	<ul style="list-style-type: none"> Supports IEEE 802.1Q VLAN Provides DHCP³⁵ server Supports NAT/PAT³⁶

Table 3 Benefits and Features of Cisco 1760 Modular Access Router

Benefits	Features
Traffic management	
<ul style="list-style-type: none"> • Application of QoS features through traffic classification 	<ul style="list-style-type: none"> • Supports NBAR³⁷
Network management	
<ul style="list-style-type: none"> • Simplifies deployment • Reduces deployment time and costs • Allows quick diagnostics and troubleshooting • Allows central monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1760 Router • Reduces management time and costs 	<ul style="list-style-type: none"> • Supports Cisco Configmaker v.2.6 • Provides SETUP configuration utility, AutoInstall, color-coded ports/cables, LED status indicators, graphical LAN/VPN policy configurator, command-line interface, context-sensitive configuration questions, and straightforward cabling • Manageable via SNMP³⁸ • Supports CiscoView and Telnet, and provides console port
Device integration	
<ul style="list-style-type: none"> • Reduces costs and simplifies management 	<ul style="list-style-type: none"> • Offers integrated router, voice gateway, firewall, encryption, VPN tunnel server, DSU/CSU, and NT1 in a single device

1. Open Shortest Path First
2. Enhanced Interior Gateway Routing Protocol
3. Hot Standby Router Protocol
4. Voice over Frame Relay
5. Survivable Remote Site Telephony
6. Session Initiation Protocol
7. Media Gateway Control Protocol
8. Coder/decoder
9. Customer premises equipment
10. Intrusion detection system
11. IP Security
12. Internet Key Exchange
13. Certificate Enrollment Protocol
14. Password Authentication Protocol/Challenge Handshake Authentication Protocol
15. Remote Access Dial-In User Service
16. Layer 2 Tunneling Protocol
17. Generic routing encapsulation
18. Layer 2 Forwarding
19. Link fragmentation and interleaving
20. Multilink PPP
21. Low-latency queuing
22. Weighted Random Early Detection
23. Committed Access Rate
24. Weighted Fair Queuing
25. Generic traffic shaping
26. Resource Reservation Protocol
27. Differentiated services code point
28. Frame Relay fragmentation
29. Frame Relay traffic shaping
30. Compressed Real-Time Transport Protocol
31. Point-to-Point Protocol
32. Serial Line Internet Protocol
33. PPP over Ethernet
34. ISDN leased line
35. Dynamic Host Configuration Protocol
36. Network Address Translation/Port Address Translation
37. Network-based application recognition
38. Simple Network Management Protocol

Figure 4 shows the four modular slots on the front panel view of the Cisco 1760 Modular Access Router. Two slots are for VICs and two slots are either for VICs or for WICs.

Figure 4
Cisco 1760 Modular Access Router Front Panel View

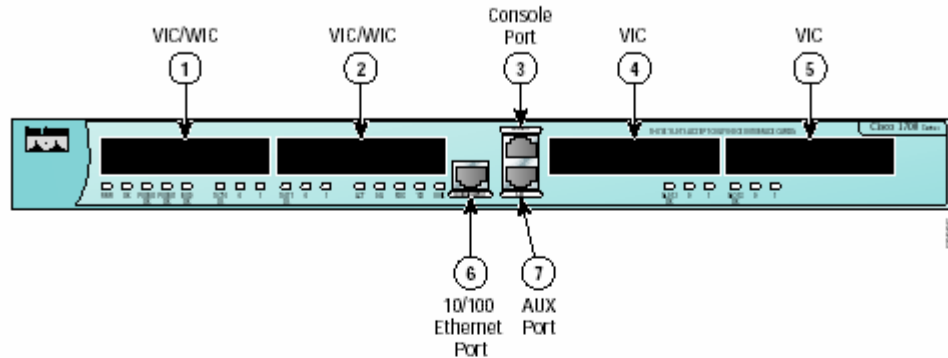


Table 4 Architecture and Physical Interfaces Support

Item	Description
Physical interfaces	
One 10/100BASE-T Fast Ethernet port (RJ-45)	Automatic speed detection; automatic duplex negotiation; VLAN ¹ support
Four slots: <ul style="list-style-type: none"> Two slots can be used for either WICs or VICs or a combination of both Two slots can be used for VICs 	Supports VICs with two ports per card; supports any combination of up to two WICs or VICs
Supports Ethernet WICs	Supports PPPoE; operates in full- and half-duplex modes
One auxiliary (AUX) port	RJ-45 jack with EIA/TIA-232 interface (plug compatible with Cisco 2500 Series AUX port); asynchronous serial DTE ² with full modem controls (CD ³ , DSR ⁴ , RTS ⁵ , CTS ⁶); asynchronous serial data rates up to 115.2 kbps
One console port	RJ-45 jack with EIA/TIA-232 interface (plug compatible with Cisco 1600 and 2500 Series console ports); asynchronous serial DTE; transmit/receive rates up to 115.2 kbps (default 9600 bps, not a network data port); note: no hardware handshaking such as RTS/CTS
One internal expansion slot	Supports hardware-assisted services such as encryption (up to T1/E1)

1. Virtual LAN
2. Data terminal equipment
3. Carrier Detect
4. Data set ready
5. Request to Send
6. Clear to Send

Table 5 WAN Support for the Cisco 1760 Router

Module	Description
WIC-1T	One-port serial, async and sync (T1/E1)
WIC-2T	Two-port serial, async and sync (T1/E1)
WIC-2A/S	Two-port low-speed serial (up to 128 kbps), async and sync
WIC-1B-S/T	One-port ISDN BRI ¹ S/T
WIC-1B-U	One-port ISDN BRI U interface with integrated NT1
WIC-1DSU-56K4	One-port integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU-T1	One-port integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BASE-T Ethernet interface
WIC-1SHDSL	One-port G.shdsl interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-port V.90 analog modem WIC
WIC-1ADSL-IDG	1-port ADSLoISDN Wan Interface Card
WIC-1ADSL-DG	1-port ADSLoPOTS WIC with Dying Gasp
WIC-1B-U-V2	1-Port ISDN BRI NT-1 WIC for 1700, 2600, 3600 and 3700 series

¹ Basic Rate Interface

Table 6 Voice Support for the Cisco 1760 Router

Module	Description
VIC-2E/M	Two-port E&M ¹ voice/fax interface card for voice/fax network module
VIC-2FXO	Two-port FXO ² voice/fax interface card for voice/fax network module
VIC-2FXS	Two-port FXS ³ voice/fax interface card for voice/fax network module
VIC-2FXO-M1	Two-port FXO voice/fax interface card for North America
VIC-2FXO-M2	Two-port FXO voice/fax interface card for Europe
VIC-2FXO-M3	Two-port FXO voice/fax interface card for Australia
VIC-2DID	Two-port analog DID ⁴ voice interface card
VIC-2FXO-EU	Two-port FXO voice/fax interface card for Europe
VIC-2BRI-NT/TE	Two-port network-side ISDN BRI VIC
VIC-4FXS/DID ⁵	Four-port FXS and DID voice/fax interface card
WWIC-1MFT-T1	One-port FJ-48 multiflex trunk - T1

Table 6 Voice Support for the Cisco 1760 Router

Module	Description
VVIC-2MFT-T1	Two-port RJ-48 multiflex trunk - T1
VVIC-2MFT-T1-DI	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VVIC-1MFT-E1	One-port RJ-48 multiflex trunk - E1
VVIC-2MFT-E1	Two-port RJ-48 multiflex trunk - E1
VVIC_2MFT-E1-DI	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VVIC-1MFT-G.703	One-port RJ-48 multiflex trunk - E1 G.703
VVIC-2MFT-G.703	Two-port RJ-48 multiflex trunk - E1 G.703
VIC2-2FXS	Two-port Voice Interface Card - FXS
VIC2-2FXO	Two-port Voice Interface Card - FXO (Universal)
VIC2-4FXO	Four-port Voice Interface Card - FXO (Universal)
VIC2-2E/M	Two-port Voice Interface Card - E and M
VIC2-2BRI-NT/TE	Two-port Voice Interface Card - BRI (NT and TE)

1. Ear and mouth
2. Foreign exchange office
3. Foreign exchange station
4. Direct inward dial
5. The Cisco 1760 can support four VIC-4FXS/DID cards with a maximum of eight port in DID mode

Table 7 Cisco 1760 Router Memory—Defaults and Maximum

Model Number	Flash Memory (in megabytes)		DRAM (in megabytes)	
	Default	Maximum	Default	Maximum
Cisco 1760	32	64	64	128
Cisco 1760-V	32	64	96	128

VPN and Security

The Cisco 1760 router is part of the end-to-end Cisco VPN solution. VPNs create secure connections via the Internet to connect geographically dispersed offices, business partners, and remote users while providing security, traffic prioritization, management, and reliability equal to that of private networks.

By supporting industry standards IPsec, L2TP, and DES and 3DES, the Cisco 1760 router delivers robust VPN solutions to ensure data privacy, integrity, and authenticity.

The optional Cisco VPN Hardware Encryption Module for the Cisco 1760 router further optimizes VPN encryption performance. By offloading encryption tasks to the VPN module, the router processor is freed up to handle other operations. The VPN module accelerates the rate at which encryption occurs, speeding the process of transmitting secure data—a critical factor when using 3DES encryption.

The Cisco 1760 router offers integrated security features, including stateful inspection firewall functionality and IDS as an optional Cisco IOS Software feature. By deploying Cisco IOS Software firewall functionality, customers do not need to purchase or manage multiple devices, thus simplifying network management and reducing capital costs. Additionally, remote management applications, such as Cisco Security Device Manager (SDM), make it easier than ever to deploy and monitor VPN and Cisco IOS Firewall on your Cisco 1760 router.

Cisco IOS Software firewall security features include access control lists (ACLs) and user authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS). These security features provide the optimal level of firewall protection to customers.

Voice Implementation

The Cisco 1760 Modular Access Router supports FXO, FXS, E&M, ISDN BRI VICs, and T1/E1 multiflex V/WICs.

The FXO interface allows an analog connection to the central office of the Public Switched Telephone Network (PSTN). The FXS interface connects basic telephone service phones (home phones), fax machines, key sets, and PBXs through ring voltage and dial tone. The E&M interface allows connection for PBX trunk lines (tie lines). The ISDN-BRI NT/TE VIC is used to connect to the PSTN or a PBX/KTS, whereas the T1/E1 multiflex V/WIC (multiflex V/WIC) supports both data and voice services.

The multiservice-ready Cisco 1760-V router version includes all the features needed for immediate integration of data and voice services:

- One DSP—support for up to two voice channels
- 32-MB Flash memory
- 96-MB DRAM
- Cisco IOS IP/Voice Plus feature set

VICs and WICs are available separately.

The Cisco 1760 and Cisco 1760-V routers have two DSP module slots on the motherboard, each of which supports a DSP module with up to five DSPs to allow additional voice-channel support. A maximum of ten DSPs are supported.

DSP Requirements

Cisco 1760 series routers support 3 types of DSP images: high complexity (HC), medium complexity (MC) and Flexi-6. HC and MC are used for analog¹ VICs; Flexi-6 is used for T1/E1 V/WICs² and BRI VIC. MC is introduced in Cisco 1760 series starting from Cisco IOS 12.2(8)YN release, which will merge into 12.3(2)T. Therefore, please make sure to use Cisco 12.2(8) YN or later releases when using MC. In addition, starting from 12.2(8)YN release, the default DSP image for BRI VIC is changed from HC to Flexi-6. BRI VIC cannot be configured to HC or MC through CLI, however. If any DSP resources used for analog are left, BRI VIC can automatically take use of those resources by using HC or MC. Table 8 lists the default images for each type of VICs; Table 9 lists IOS support for each DSP image. Table 10 lists the number of channels supported by one DSP (PVDM-256K-4) for each codec type.

Please use the following rules for calculating DSP requirements on the Cisco 1760 series routers:

1. Analog VICs include VIC-2FXS, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2FXO-EU, VIC-2E/M, VIC-2DID, VIC-4FXS/DID

2. T1/E1 V/WICs include V/WIC-1MFT-T1, V/WIC-2MFT-T1, V/WIC-2MFT-T1-DL, V/WIC-1MFT-E1, V/WIC-2MFT-E1, V/WIC-2MFT-E1-DL, V/WIC-1MFT-G703, V/WIC-2MFT-G703

1. For 12.2T releases:
 - a. Each 2-port analog VIC requires 1 DSP (PVDM-256K-4)
 - b. Each VIC-2BRI-NT/TE requires 2 DSPs (PVDM-256K-8)
 - c. For VWICs, refer to Table 10. For example, 12 G.711 digital T1/E1 voice calls require two DSPs; 12 G.729 calls require four DSPs
 - d. Total DSP requirement is the sum of a, b and c. The DSP resources can not be shared between analog VICs and VWICs
2. For the Early Deployment (ED) releases: Cisco IOS 12.2(8)YN or later (Note: not include 12.2(11)YT) or 12.3T train releases or later, please always refer to the DSP Calculator in the following link:

http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

The DSP calculator optimizes the DSP resources for your configuration and suggests CLI configurations.

Table 8 DSP Firmware for each type of VICs

VIC Type	Firmware Support
2-port Analog VICs	HC (default), MC (starting from 12.2(8)YN)
4-port Analog VIC	HC, MC (default, starting from 12.2(8)YN)
VIC-2BRI-NT/TE	HC (default for ED releases prior to 12.2(8)YN or T train releases prior to 12.3(2)T); Flexi-6 (default for ED releases 12.2(8)YN or later or T train releases 12.3(2)T or later)
T1/E1 VWICs	Flexi-6 (default)

Table 9 Cisco IOS Support for DSP firmware

Firmware Support	IOS Release Support
HC	In all orderable IOS Releases
MC	ED Releases: Cisco IOS 12.2(8)YN or later ¹ T Train Releases: Cisco IOS 12.3(2)T or later
Flexi-6	For T1/E1 VWICs: <ul style="list-style-type: none"> • ED Releases: Cisco IOS 12.2(4)YB or later² • T Train Releases: 6th releases of 12.2(15)T or later For VIC-2BRI-NT/TE: <ul style="list-style-type: none"> • ED Releases: Cisco IOS 12.2(8)YN or later³ • T Train Releases: Cisco IOS 12.3(2)T or later

1. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support MC.

2. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.

3. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.

Table 10 The number of channels supported by one DSP (PVDM-256K-4) per codec type

Codec	Firmware		
	HC (for analog)	MC (for analog)	Flexi 6 (for VWICs & BRI VIC ¹)
G.711	2	4	6
G.729 ² /G.729a	2	4	3
G.726	2	4	3
G.723	2	-	2
G.728	2	-	2
Fax Relay	2	4	3

1. BRI VIC support in Flexi-6 starts from 12.2(8)YK or 12.3(2)T.

2. G.729 and G.729a is not supported in MC or Flexi-6 images

Table 11 DSP Modules Available on Cisco 1760

Modules	DSPs
PVDM-256K-4	1 DSP Module
PVDM-256K-8	2 DSP Modules
PVDM-256K-12	3 DSP Modules
PVDM-256K-16HD	4 DSP Modules
PVDM-256K-20HD	5 DSP Modules

Table 12 Cisco 1760 Router Voice Call Support

Maximum Number of Voice Calls Supported	
Analog Calls	Digital Calls
• 12 calls (with three 4-port FXS/DID Voice Interface Cards leaving one slot for WAN access)	• 30 calls (for example with one VWIC-1MTF-E1)

Cisco IOS Technology

The Cisco 1760 Modular Access Router benefits from the power of Cisco IOS Software. For example, through Cisco IOS Software, the Cisco 1760 router delivers QoS capabilities, including RSVP, WFQ, CAR, and DSCP Precedence.

These features enable businesses to prioritize traffic on their networks by user, application, traffic type, and other parameters to ensure that business-critical data and delay-sensitive voice are appropriately prioritized.

Further, for businesses that are increasingly accessing the Internet via DSL, QoS features are necessary to ensure highest voice quality. For DSL services with QoS features, the Cisco 1760 router can be deployed with the ADSL or the G.shdsl WAN Interface Card.

The advanced DSL QoS features include the following:

- LFI using MLP over ATM

- Low-latency queuing (also called PQ/CBWFQ)
- Weighted Random Early Detection (WRED)
- Committed Access Rate (CAR)
- Differentiated services (DiffServ) (class-based marking)

Cisco IOS Software Feature Sets

The Cisco 1760 router supports a choice of Cisco IOS Software feature sets with rich data features as well as a combined data and voice feature set. Tables 10 and 11 list these feature sets, including the memory requirements.

The Cisco 1760 router was first released on the Cisco IOS 12.2(2)XK release. The Cisco 1760 router will be supported on the 12.2T release in Q3 2002.

Table 13 Cisco 1760 Router Cisco IOS Data Software Feature Sets and Memory Requirements

Cisco 1760 Data Software Feature Sets for Cisco IOS Release 12.2(2)XK				
Software Product Description	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1700 Cisco IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 56	c1700-bk8no3r2sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	c1700-bk9no3r2sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL/IPX/AT/IBM PLUS	c1700-bnr2sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/IPX/AT/IBM	c1700-bnr2y-mz	8	32	RAM
Cisco 1700 Cisco IOS IP/ADSL/FW/IDS PLUS IPSEC 56	c1700-k8o3sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL PLUS IPSEC 56	c1700-k8sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL PLUS IPSEC 3DES	c1700-k9sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/ADSL/IPX/FW/IDS PLUS	c1700-no3sy7-mz	16	48	RAM
Cisco 1700 Cisco IOS IP/IPX	c1700-ny-mz	8	24	RAM
Cisco 1700 Cisco IOS IP/FW/IDS	c1700-o3y-mz	8	24	RAM
Cisco 1700 Cisco IOS IP/ADSL PLUS	c1700-sy7-mz	8	32	RAM
Cisco 1700 Cisco IOS IP/ADSL	c1700-y7-mz	8	24	RAM
Cisco 1700 Cisco IOS IP	c1700-y-mz	8	24	RAM

Table 14 Cisco 1760 Router Cisco IOS Data & Voice Software Feature Sets and Memory Requirements

Cisco 1760 Data and Voice Software Feature Sets for Cisco IOS Release 12.2(2)XX					
Cisco 1700	Cisco IOS IP/ADSL/IPX/AT/IBM/VOICE/FWIDS PLUS IPSEC 56	c1700-bk9no3r2sv3y7-mz	32	64	RAM
Cisco 1700	Cisco IOS IP/ADSL/IPX/AT/IBM/VOICE/FWIDS PLUS IPSEC 3DES	c1700-bk9no3r2sv3y7-mz	32	64	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE/FWIDS PLUS IPSEC 56	c1700-k8o3sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE PLUS IPSEC 56	c1700-k8sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE/FWIDS PLUS IPSEC 3DES	c1700-k9o3sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE PLUS IPSEC 3DES	c1700-k9sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/IPX/VOICE/FW/IDS PLUS	c1700-no3sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE/FWIDS PLUS	c1700-o3sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/ADSL/VOICE PLUS	c1700-sv3y7-mz	16	48	RAM
Cisco 1700	Cisco IOS IP/VOICE PLUS	c1700-sv3y-mz	16	48	RAM

Cisco IOS IP base feature sets include NAT, OSPF, RADIUS, and Next Hop Resolution Protocol (NHRP).

Cisco IOS IP Plus feature sets contain L2TP, L2F, the Border Gateway Protocol (BGP), IP Multicast, Frame Relay switched virtual circuit (SVC), RSVP, the NetWare Link Services Protocol (NLSP), AppleTalk Simple Multicast Routing Protocol (SMRP), the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP).

Encryption is offered in special encryption feature sets (Plus IPsec 56, and Plus IPsec 3DES). The VPN encryption module requires a Cisco IOS IP Plus IPsec image.

DSL is supported in the base IP/DSL Cisco IOS image. In addition, the Cisco IOS IP Plus feature sets support DSL.

Network Management and Ease-of-Installation Tools

The Cisco 1760 router supports a range of network-management and ease-of-installation tools.

Cisco Security Device Manager (SDM) is an intuitive, web-based device management tool embedded within the Cisco IOS access routers. SDM simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI). For more information visit <http://www.Cisco.com/go/sdm>.

Cisco ConfigMaker is a Microsoft Windows wizard-based tool designed to configure a small network of Cisco routers, switches, hubs, and other network devices from a single PC. This tool makes it easy to configure value-add security features such as the Cisco IOS Firewall feature set, IPsec encryption, Network Address Translation (NAT), the Dynamic-Host-Configuration-Protocol (DHCP) server, and to establish VPN policies (including QoS and security).

Cisco ConfigMaker 2.6 is supported on the Cisco 1760 Modular Access Router.

CiscoView, a member of the CiscoWorks2000 Family, is a Web-based device-management application that provides dynamic status, monitoring, and configuration information for the broad range of Cisco Internetworking products. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow comprehensive changes to devices, given that requisite security privileges are granted.

Additional features include:

- Real-time monitoring of key information that relates to device performance, traffic, and usage, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators
- The ability to change device configurations such as IP route, VLAN, and duplex settings
- On-demand access to Cisco.com, Cisco's Web site, for new and updated device support
- A Web-based application that allows multuser access to a single CiscoView server

CiscoView is supported on the Cisco 1760 router.

CiscoWorks 2000 Resource Manager Essentials, a member of the CiscoWorks2000 family of network management products, is a powerful suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers. The Resource Manager Essentials browser interface allows easy access to information critical to network uptime and simplifies time-consuming administrative tasks. The Management Connection feature in Resource Manager Essentials adds Web-level integration of other management tools from Cisco and partner companies, thereby enabling utilization of these tools and applications to create a seamless, central point of network administration. Comprising six applications and optional add-on packages such as CiscoWorks for Switched Internetworks Campus, Resource Manager Essentials includes:

- Inventory Manager
- Change Audit
- Device Configuration Manager
- Software Image Manager
- Availability Manager
- Syslog Analyzer
- Cisco Management Connection

CiscoWorks2000 Resource Manager Essentials version 3.3 is supported on the Cisco 1760 router.

Device Fault Manager (DFM) provides real-time fault analysis for devices and alerts network managers of critical conditions within the network. DFM provides:

- Real-time fault analysis for Cisco devices
- Intelligent Cisco trap generation for integration with enterprise management systems
- No rules to write—ever

Device Fault Manager support on the Cisco 1760 router is targeted for Q3CY2002.

Service and Support

Technical Support Services

Technical Support Services for the Cisco 1760 router are available through Cisco SMARTnet™ and SMARTnet Onsite service programs. Cisco SMARTnet support augments the resources of your operations staff; it provides them access to a wealth of expertise, both on line and via telephone, the ability to refresh their system software at will, and a range of hardware Advance Replacement options. Table 12 details the features and benefits of Cisco SMARTnet offerings.

Cisco SMARTnet Onsite provides all SMARTnet services and complements the hardware Advance-Replace ment feature by adding the services of a field engineer, offering support that can be critical for those locations where staffing is insufficient or unavailable to perform parts-replacement activities.

Table 15 Cisco SMARTnet Features and Benefits

Technical Support Services	Benefits	Features
Cisco SMARTnet Support Cisco SMARTnet Onsite Support	<ul style="list-style-type: none">• Enables proactive or expedited issue resolution• Lowers cost of ownership by utilizing Cisco expertise and knowledge• Minimizes network downtime	<ul style="list-style-type: none">• Access 24 x 7 to software updates• Web access to technical repositories• Telephone support through the Technical Assistance Center (TAC)• Advance Replacement of hardware parts

Technical Support Services Delivery

Cisco SMARTnet support is available to customers from both Cisco directly and through Cisco's channel partners. Partners purchasing directly from Cisco may offer Cisco Branded Resale of Cisco SMARTnet Software. Partners purchasing through distribution may offer Packaged Cisco SMARTnet Software.

For partners supporting the Cisco 1760 router with their own service and support infrastructure, Cisco System Integrator Support 98 (SIS98) is available.

Contact your Cisco account manager for appropriate delivery options.

Technical Specifications

Dimensions

- Dimensions (H x W x D): 1.7 x 17.5 x 12.8 in. (4.32 x 44.5 x 32.5 cm)
- Weight (maximum): 9.4 lb (4.3 kg) fully loaded with WAN/voice interface cards, PVDMs, DRAM module, VPN module, single in-line memory module (SIMM)
- Weight (minimum): 8.2 lb (3.7 kg)

Power

The Cisco 1760 router has one universal internal power supply (applicable to all countries) and no external power brick. It has no locking connector on the power cord.

- AC Input Voltage: 100 to 240 V
- Frequency: 50-60 Hz

- AC Input Current: 1.5A maximum
- Power Output: 50W maximum
- No redundant power supply option

Environmental

- Operating Temperature: 32 to 104 F (0 to 40 C)
- Nonoperating Temperature: -4 to 149 F (-20 to 65 C)
- Relative Humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating

Regulatory Approvals (Safety, EMC, and Telecom Compliance)

Safety

- UL 60950, 3rd Edition (includes Czech Republic)
- CSA 22.2 No 60950, 3rd Edition
- EN60950, 3rd Edition
- TS001-1997
- AS/NZS 3260 with A1 through A4
- IEC 60950, 3rd Edition and all country deviations
- ETSI 300-047 GOST-R

EMC

- EN55022 (CISPR22) Class A
 - EN55022/EN50082
- CFR47 part 15 Class A
- ICES 003, issue 2 Class A
- VCCI Class A
- AS/NZS 3548: Class A
- EN55024 (CISPR24) Immunity:
 - a) EN61000-4-2 ESD
 - b) EN61000-4-3 Radiated immunity
 - c) EN61000-4-4 Electrical fast transients
 - d) EN61000-4-5 Surge
 - e) EN61000-4-6 Conducted RF immunity
 - f) EN61000-4-11 AC dips and sags
 - g) EN61000-3-2 AC harmonics and flicker
- GOST-R

Telecom

- Europe: CTR2, CTR3, TBR21
- Canada: CS-03 Part I, II, VI, VIII
- United States: TIA-IS-968

- Japan: JATE
- Australia/New Zealand: TS002, TS003, TS006, S.043, TS031
- Brazil: Anatel
- China: GB-514-92, YD-514-92; Hong Kong: HKTA 2011, 2014, 2015, 2017
- Hungary ETR328 (T)
- Mexico: CFT
- Singapore: IDA
- Poland PB-TE rev. 2 (T)
- South Africa: ICASA
- South Korea: MIC

Product Numbers and Descriptions

For ordering information, Table 13 lists the product part numbers with the respective part descriptions for the two versions, Cisco 1760 and Cisco 1760-V routers, the memory options, the DSP modules, the VPN module and bundled offerings.

This is not a comprehensive list. For further information, please contact your Cisco account manager or your local sales office.

Table 16 Cisco 1760 Router Product Numbers and Descriptions

Product Number	Description
CISCO1760	10/100 Modular Access Router with 2WIC/2VIC, 2VIC slots, 19-inch chassis
CISCO1760-V	10/100 Modular Router with Voice, IP/VOICE Plus, 19-inch chassis
Memory and Memory Upgrades	
MEM1700-64U128D	Cisco 1700 64 MB to 128 MB DRAM Factory Upgrade
MEM1700-64U96D	Cisco 1700 64 MB to 96 MB DRAM Factory Upgrade
MEM1700-32U64MFS	Cisco 1760 32 MB to 64 MB Flash SIMM Factory Upgrade
MEM1700-8MFS=	Cisco 1760 8 MB Flash SIMM-Spare
MEM1700-16MFS=	Cisco 1760 16 MB Flash SIMM-Spare
MEM1700-32MFS=	Cisco 1760 32 MB Flash SIMM-Spare
MEM1700-64MFS=	Cisco 1760 64 MB Flash SIMM-Spare
MEM1700-16D=	Cisco 1700 16 MB DRAM DIMM-Spare
MEM1700-32D=	Cisco 1700 32 MB DRAM DIMM-Spare
MEM1700-64D=	Cisco 1700 64 MB DRAM DIMM-Spare
DSP Modules and Upgrades	
PVDM-256K-4U8	Cisco 1760-V 4 Channel to 8 Channel PVDM Factory Upgrade
PVDM-256K-4U12	Cisco 1760-V 4 Channel to 12 Channel PVDM Factory Upgrade

Table 16 Cisco 1760 Router Product Numbers and Descriptions

Product Number	Description
PVDM-256K-4U16	Cisco 1760-V 4 Channel to 16 Channel PVDM Factory Upgrade
PVDM-256K-4U20	Cisco 1760-V 4 Channel to 20 Channel PVDM Factory Upgrade
PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module
PVDM-256K-8	8-Channel Packet Voice/Fax DSP Module
PVDM-256K-12	12-Channel Packet Voice/Fax DSP Module
PVDM-256K-16	16-Channel Packet Voice/Fax DSP Module
PVDM-256K-20	20-Channel Packet Voice/Fax DSP Module
VPN Module	
MOD1700-VPN	Cisco 1700 Series VPN Module
Bundle Offering	
CISCO1760-ADSL	1760 bundle with ADSLoPOTS WIC, IP/ADSL, 32MB FL/64MB DR
CISCO1760-SHDSL	1760 bundle with WIC-1SHDSL, IP/ADSL, 32MB FL/64MB DR
CISCO1760-VPN/K9	1760 VPN bundle with VPN module, 96MB DRAM, 32MB Flash, IP Plus/FW/3DES
CISCO1760-VPN/K9-A	1760 VPN bundle with ADSL WIC, VPN Module, 96MB DR, 32MB FL, IP+/FW/3DES
CISCO1760-V-SRST	Cisco 1760-V with 24-user SRST Feature License, 32F/128D



Corporate Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (6387)
 Fax: 408 526-4100

European Headquarters
 Cisco Systems International BV
 Haarderbergpark
 Haarderbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www.europe.cisco.com
 Tel: 31 0 20 357 1000
 Fax: 31 0 20 357 1100

Americas Headquarters
 Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-7660
 Fax: 408 527-0883

Asia Pacific Headquarters
 Cisco Systems, Inc.
 Capital Tower
 168 Robinson Road
 #22-01 to #29-01
 Singapore 068912
www.cisco.com
 Tel: +65 6317 7777
 Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
 Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
 Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
 Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
 Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2010 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco ICS, the Cisco ICS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IPTV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PD, Post-Routing, Pre-Routing, RouteMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StackWise Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
 (031048) ETMG 203078-MS 1/03

ANEXO E

Polycom Serie VSX 7000



La serie de productos Polycom VSX 7000 ofrece flexibilidad, confiabilidad y una arquitectura robusta para casi cualquier salón de reuniones, salón de clases o ambientes de grupos pequeños. Con un sistema de sonido integrado único, la serie VSX 7000 de Polycom eleva los límites de calidad para obtener un audio estéreo sin igual Siren™ 14 de Polycom, con patente en trámite. Durante una video conferencia, las voces de los participantes ubicados del otro lado del salón se proyectan en estéreo. Con bocinas y micrófonos duales, escuchará cada una de las voces claramente, podrá descifrar múltiples conversaciones simultáneas con facilidad y escuchará un sonido puro y rico.

Además, cada producto de la serie VSX 7000 ofrece un video verdaderamente excepcional con H.264 y Pro-Motion con calidad tipo televisión, una interfaz de usuario hecha a la medida y fácil de usar, codificación criptográfica de software con norma AES, capacidades de integración con pantallas touch-screen y capacidades para añadir llamadas de voz.

Para integrar aplicaciones especiales, cualquiera de los productos de la serie VSX 7000 puede añadirse al Polycom Media Center para obtener una solución completa de rack y monitor.

El VSX 7800 es la solución de primera línea para video conferencias set-top. Con el VSX 7800, tiene todo lo que necesita para empezar a colaborar. Esta solución incluye un kit de bocinas de alta fidelidad para acomodar el audio estéreo Siren 14, conectividad para una segunda pantalla, función de People+Content™ para información compartida de alta resolución y una función multipunto integrada para expandir fácilmente su conferencia a ubicaciones múltiples.

Seleccione el VSX 7400 para obtener la solución óptima de colaboración. Las capacidades incluyen soporte para People+Content de alta resolución, un servicio de Web Streaming para grabar y ver conferencias posteriormente y subtítulo para participantes con problemas de audición. Adicionalmente, el modelo VSX 7400 está disponible en un paquete integrado junto con el SoundStation VTX 1000, el primer teléfono de conferencias de banda ancha en el mundo. Únalos y utilice el VTX 1000 para añadir participantes de audio o video a una conferencia y para que sirva como micrófono para llamadas tanto de audio como de video. Si ya tiene un VSX 7000 y un teléfono de conferencias SoundStation VTX 1000, puede combinarlos en una sola solución con nuestro kit de actualización.

El VSX 7000 es ideal para video conferencias de alta calidad con todo lo necesario para tener comunicaciones productivas de vanguardia. Este modelo base proporciona flexibilidad y capacidad de expansión al ofrecer a los usuarios la opción de añadir pantallas adicionales, micrófonos, un kit de bocinas, módulos de red, funciones de multipunto y más.

Funciones aumentadas – AES integrado para llamadas seguras, enlace adicional de audio para participantes de voz y vistas de presencia continua en llamadas de video de multipunto.

Video sobresaliente – Video de excelente calidad en cualquier ancho de banda con estándares basados en H.264 y video Pro-Motion™ de alta resolución.

ESPECIFICACIONES

Cumple con ITU H.323 y H.320

Certificado por Cisco AVVID

Ancho de Banda

- Tasa Máxima de Datos IP y Serie/V.35: Hasta 2 Mbps
- Tasa Máxima de Datos ISDN: Hasta 2 Mbps

Estándares y Protocolos de Video

- H.261, Anexo D
- H.263+ Anexos: F, I, J, L, N, T
- H.263++ Anexos: W
- H.264
- ITU 60-fps pantalla completa – Pro-Motion™

Tasa de Cuadros (Punto a Punto)

- De forma inteligente selecciona la tasa de cuadros para el mejor rendimiento de video
- 30 fps a 56 kbps hasta 2 Mbps
- 60 campos por segundo hasta 2 Mbps
- Entradas de Video: Cámara Principal + 2 Entradas
- Cámara principal integrada
- 1 x S-Video; 4-pin mini DIN (Cámara de documentos, VCR o segunda cámara)
- 1 x Composite; RCA/Phono (Cámara de documentos, VCR o segunda cámara)

Puerto de Datos RS-232: 1 Conector

- 1 x 8-pin mini DIN
- Puerto de control para integración a la medida con dispositivos remotos tales como los sistemas de control Crestron y AMX
- Conectividad para dispositivo de teletipo cerrado con subtítulos o control PTZ para una PowerCam™ auxiliar.
- Puerto de comunicación para la transmisión de información en serie (por ejemplo, dispositivos médicos) sobre llamadas ISDN

Salidas de Video (5 salidas)

- 1 x S-Video; 4-pin mini DIN (Monitor principal)
- 1 x Composite; RCA/Phono (Monitor principal)
- 1 x S-Video (Segundo monitor)
- 1 x Composite; RCA/Phono (Segundo monitor)
- 1 x VGA (Segunda pantalla de gráfica)

Formatos de Video

- NTSC/PAL
- Gráfica: XGA, SVGA, VGA

Cámara Principal Integrada

- Ultra-silenciosa, acción ultra-rápida pan/tilt/zoom (PTZ)
- Campo de visión de 65°
- Tilt Range: +/- 25° (Arriba/Abajo)
- Pan Range: +/- 100° (Izquierdo/Derecho)
- Campo Total de Visión: 265°
- 12x Zoom; f-4.2 to 42mm
- F=1.85 a 2.9 mm
- Enfoque Automático

- Balance de blancos automático
- Posiciones pre-establecidas de cámara – locales y de extremo (hasta 99)
- Control de cámara remota basada en estándares (FECC)

Resolución de Video de Personas

- Video Pro-Motion entrelazado 60/50 campos en pantalla completa para NTSC/PAL
- 4SIF (704 x 480)
- 4CIF (704 x 576)
- SIF (352 x 240)
- CIF (352 x 288)
- Opción de relación de 4:3 ó 16:9 de aspecto de la pantalla
- Pantalla de personas en segundo monitor VGA

Resolución de Video de Contenido

- XGA (1024 x 768), SVGA (800 x 600), VGA (640 x 480) para pantallas gráficas
- Soporte a pantalla para personas en 4CIF y SIF en la segunda pantalla VGA
- Hasta 4CIF para pantallas NTSC/PAL

Estándares y Protocolos de Audio

- Listo para estéreo Siren 14 de Polycom
- Ancho de banda de 14 kHz con audio de Siren 14 de Polycom en llamadas mixtas IP, ISDN, e IP/ISDN
- Ancho de banda de 7 kHz con G.722, G.722.1
- Ancho de banda de 3.4 kHz con G.711, G.728, G.729^a

Funciones de Audio

- Enlace adicional de audio sobre el teléfono de conferencias SoundStation VTX 1000TM
- Enlace adicional de audio sobre ISDN

- Audio digital full duplex
- Cancelación de eco de adaptación instantánea
- Control automático de amplificación (AGC) – activado mediante la voz
- Supresión automática de ruidos (ANS)
- Mezclador de audio (Micrófono, VCR, entrada de línea)
- Prueba de tonos de bocinas incluida
- Medidor del nivel de audio en tiempo real para micrófonos locales y remotos
- Mezcla de audio del micrófono y VCR entrante
- Capacidad de hablar sobre el audio del VCR
- Capacidad de cancelación de eco cuando se utiliza equipo externo de audio

Entradas de Audio (3 entradas)

- 1 x link de conferencia
- Hasta tres conjuntos de micrófonos
- Posibilidad de conectar el SoundStation VTX 1000TM
- Entrada 1 x RCA para estéreo o entrada mono de VCR
- Entrada 1 x RCA para estéreo o entrada mono de mezclador externo

Salidas de Audio (2 salidas)

2 x RCA para grabación de VCR estéreo (o estéreo para bocinas auxiliares o productos Instalados de Voz Vortex)

Micrófono Digital Polycom para mesa

- Captación de voz de 360°, con menos de 4.8 dB en reverberancia que el micrófono omnidireccional.
- Tres elementos cardioide por micrófono
- Base de flotación que reduce la transmisión del ruido sobre la mesa
- Botón integrado de silencio
- Puede fijarse en el techo o pared

Bocina y Subwoofer Integrado

- Respuesta de frecuencia: de 80Hz a 22kHz
- Frecuencia de cruce al subwoofer: 216 Hz
- Energía Total de Salida: 20 Watts (RMS)
- Individualiza el audio para el entorno del usuario
- Control del volumen principal
- Bocinas de alcance mediano y de subwoofer ON/OFF
- Nivel ajustable de subwoofer
- Controles de agudos y bajos ecualizados por el usuario

Otros Estándares ITU Soportados

- Comunicaciones H.221
- Control de la cámara remota H.224/H.281
- Soporta estándar anexo Q para FECC en llamadas H.323 H.225, H.245, H.239, H.241
- Llamadas multipunto H.231
- Contraseña de H.243 MCU
- Estándares de codificación criptográfica H.233, H.234, H.235V3
- Bonding, Modo 1
- Interfaz de Red
- IP (LAN, DSL, cable módem)
- Puerto Ethernet 10/100 (10 Mbps/100Mbps/Auto)
- Módulo Opcional ISDN QBRI (Interfaz de Tasa Básica)
- Módulo Opcional ISDN PRI (Interfaz de TasaPrimaria) T1/E1
- Módulo de Serie Opcional (V.35/RS-530/RS-449 con marcación RS-366)
- Soporte opcional inalámbrico LAN vía puerto Ethernet

Funciones de la Red

- Integración con CallManager Versión 4.0 de Cisco Systems
- Llamadas Automáticas IP/ISDN
- Marcación sobre IP e ISDN

- Ocultación de Errores de audio & video sobre IP, ISDN y llamadas mixtas
- Aviso de conflicto de dirección IP
- Conexión Rápida IP para conexiones veloces de video
- Cronometrador digital de máxima duración de llamada
- Detección Automática SPID y configuración de número de línea
- Función de Click & View™ MGCTM para diseños individuales de pantalla
- Sistema de manejo de llamadas inteligentes OneDial™ de Polycom que intenta preferencia de llamadas en la red (IP o ISDN) y automáticamente se traslada a una red secundaria de ser necesario Soporte a Polycom PathNavigator para fácil colocación de llamadas y optimización de costo de la red TCP/IP, DNS, WINS, DHCP, ARP, HTTP, FTP, TelnetImplementación de SIP* (Protocolo de Inicio de Sesión)básico.
- Control director mediante comandos de API o Interfaz
- Integrada de Web
- Inverse Multiplexer actualizable por software
- Funciones Internas de Multipunto (Opcional)
- Marcación mixta de protocolo que conecta un total de cuatro terminales (IP/ISDN/Serie) a través de la MCU interna
- Llamadas de marcación de Entrada/Salida (IP/ISDN/Serie)
- Protección de contraseña para llamadas recibidas
- Soporta teléfonos IP
- Marcación automática en IP/ISDN
- Soporta People+Content™ desde cualquier terminal (no sólo el sitio anfitrión)
- Conmutador de voz activada – ver locutor actual
- Presencia continua – ver todas las ubicaciones
- Presentación automática – cambio entre los modos de
- Presentador y presencia continua
- Instalación de clave MP durante la llamada

- Enlace adicional de audio sobre ISDN
- Conexión en cascada hasta para 10 participantes a la conferencia(mezcla de IP/ISDN/Video en Serie y Audio ISDN)
- Conferencia en Demanda
- Inicia llamadas no programadas en el MGC
- Utiliza Polycom Office™ (PathNavigator y MGC)
- Auto selecciona el multipunto interno o externo
- Marca simultáneamente el número telefónico de todos los participantes
- Seguridad
- Pruebas COMSEC realizadas por Titan Systems, División de Sistemas de Seguridad en la Información y validadas de manera independiente para operar con tecnologías en codificación criptográfica aprobada por el gobierno
- Apoyo de codificación criptográfica KG-194/KIV-7 con marcación en pantalla y libreta de direcciones
- Integración avanzada para dispositivos clasificados de codificación criptográfica, certificados independientemente
- Entrada del número de validación de la cuenta
- Aviso de colector SNMP de todos los intentos fracasados de conexión desde HTTP, FTP o Telnet
- Autenticación segura de la contraseña
- Contraseñas automáticas creadas individualmente por la fábrica
- Contraseña del administrador
- Contraseña para marcación telefónica en las reuniones
- Contraseña con codificación criptográfica para acceso VSX Web
- Capacidad de desactivar interfases remotas (FTP, Telnet, HTTP, SNMP)
- Capacidad de desactivar llamadas multipunto de protocolo mixto
- Auto-Respuesta (ON/OFF)
- Permite acceso a la configuración de los usuarios (ON/OFF)

Codificación Criptográfica Incorporada

- Norma de Codificación Criptográfica Avanzada (AES)
- FIPS validado por la agencia certificada del Instituto Nacional de Normas y Tecnología (NIST)
- Longitud clave de 128-bits
- Codificación criptográfica del software AES en ISDN, IP y Serie/V.35 hasta 2 Mbps
- Basado en la norma H.235V3 (IP)
- Basado en la norma H.233/H.234 (ISDN/Serie)
- Generación e intercambio automático de clave
- Soporta People-Content™
- Soporte a llamadas punto a punto, multipunto, IP & ISDN & mixtas Interfaz del Usuario

VSX 7800 Incluye

- Sistema VSX 7000
- Licencia de Software Interna de Multipuntos
- Kit de Adaptador de Pantalla Adicional
- (2) Micrófonos Digitales para colocar encima de la mesa
- Visual Concert™ VSX
- Kit de Bocinas Estéreo VSX 7400 Incluye
- Sistema VSX 7000
- Kit de Adaptador de Pantalla Adicional
- Visual Concert™ VSX Capacidad Eléctrica
- Suministro de energía auto sensitiva
- Energía/voltaje operacional: 90-260 VAC, 47-63 Hz/80 vatios

Especificaciones Ambientales

- Temperatura Operacional: 0-40° C
- Humedad Operacional: 15-80%

- Temperatura No-Operacional: -40-70° C
- Humedad No-Operacional (No-condensada): 10-90% Características Físicas
- Unidad Base de Video (W/H/D):
11.82"/5.83"/9.63"300.3mm/148mm/244.5mm
- Peso de la Unidad Base de Video: 6.0 lbs/2.8 kg
- Subwoofer (W/H/D): 6.9"/10.72"/8.67" 175.2mm/272.4mm/220mm
- Peso del Subwoofer: 9.0 lbs/4.08 kg

Garantía

- Un año de garantía en piezas y mano de obra
- Un año de actualizaciones y upgrades de software
- Las extensiones de video SIP están en el proceso de
- ratificación de normas

ANEXO F

Sistema Tandberg 880 MXP IP

Las características más importantes de un sistema de la videoconferencia son el empleo fácil, la confiabilidad y las facilidades y servicios que ofrezca el equipo. Es por esto que nuestros sistemas de Videoconferencia enfocan especial atención en el uso sencillo del mando a distancia para conseguir rápidamente cualquiera de las prestaciones que brinde el sistema para que usted y sus colaboradores se sientan más cómodos y sin temores de utilizar el sistema, logrando rápidamente el retorno de la inversión, así como un gran número de facilidades que aportan en el apoyo de la videoconferencia y la confiabilidad de esta.

El número de personas que participan normalmente en una videoconferencia en cualquier momento dado y el tamaño de la sala de reuniones, así como las ayudas audiovisuales con que esta cuenta, determina, en un mayor o menor grado, los requisitos del sistema.

Nuestros sistemas de Videoconferencia han sido constantemente los primeros en imponer el estado de arte de la tecnología, trabajando muy de cerca con los clientes basados en sus experiencias para poder así ofrecer las características y realces que mejoran la videoconferencia. Algunas de las características más únicas se incluyen en la facilidad NPP (Natural Presence Package), una suite de facilidades al usuario que mejoran las características de la presentación de la videoconferencia. Dos de las otras características más populares son Multi-Sitio y Encriptación. Los sistemas de videoconferencia permiten reunir fácilmente múltiples participantes en una conferencia y al mismo tiempo proteger el contenido de las llamadas y de la seguridad de la red video.

LA SOLUCION DE VIDEOCONFERENCIA

Cada producto está diseñado para un manejo simple, alta calidad y tecnología y una gama de valores agregados en funciones y servicios.



Nuestra línea de productos del alto rendimiento ofrece una gama completa de soluciones para tratar todas sus necesidades de comunicación de video. La solución de Telenorma consiste en los sistemas y software siguientes que se pueden adquirir individualmente y de manera escalonada, que trabajan de manera conjunta para una solución total de videoconferencia:

θ Línea de Productos de Sistemas de Videoconferencia

Una alta gama de productos desde el sistema básico, como por ejemplo el T1000 el cual es un sistema compacto totalmente integrado ideal para la oficina de los altos ejecutivos, hasta el elegante y sofisticado T8000, así como sistemas portátiles y codecs para aquellas salas de reunión que disponen de toda la infraestructura audiovisual. **Todos con la posibilidad de transmisión vía RDSI (ISDN) y/o IP de manera simultánea.**

θ MCU (Multipoint Control Unit)

Es el sistema que permite atender las necesidades corporativas de aquellos empresarios que requieren reunir más de cuatro sedes en una conferencia, donde se cuenta con soluciones de hasta 16 sedes y la posibilidad de incluir adicionalmente 16 audio conferencias.

θ Software TMS (Management Suite)

Para las corporaciones que disponen de varios sistemas de videoconferencia, el software TMS basado en WEB es la solución perfecta para los administradores para el manejo y monitoreo centralizado de la red de video, permitiendo incluir además equipos de video de otras marcas, y hasta controlar los costos de llamadas de acuerdo con el centro de costos correspondiente.

θ Scheduler.

Es la herramienta de software basada en WEB, ideal para simplificar a los usuarios de los sistemas de videoconferencia dentro de la organización, el horario de sus conferencias. La herramienta no solo informa sobre las posibilidades de realizarla, sino además realiza la reservación de la sala, cita a los conferencistas y coordina el calendario con Outlook de los participantes, teniendo en cuenta el ajuste en tiempo de acuerdo con la zona horaria.

LA LINEA DE PRODUCTOS DE VIDEOCONFERENCIA



La gama de productos atiende los requerimientos no solo en cuanto a la aplicación y dimensión de la sala de conferencias, sino además aquellos requerimientos específicos como por ejemplo el ancho de banda disponible de la red de comunicación RDSI (ISDN) y/o IP, las facilidades y servicios, los recursos de apoyo en las conferencias como DUO Video, Streaming, etc., sin olvidar las posibilidades de Wireless LAN y los recursos audiovisuales que disponga la oficina del ejecutivo o la sala de conferencias, en cuyo caso se podrá hacer uso de la gama de Codecs, diseñados específicamente para la interconexión de los equipos sofisticados de audio y video que se hayan adquirido para este tipo de salas, minimizando el costo de la inversión.



Adicionalmente se dispone de equipos portátiles para aquellas corporaciones que necesitan realizar videoconferencias eventuales y que por lo tanto no requieren adquirir sistemas de manera definitiva.

Para aquellos empresarios que requieren la participación de más de cuatro sedes, igualmente se dispone de la solución de cascada hasta 10 sitios o del sistema multipunto MCU, permitiendo así lograr capacidades de hasta 16 videoconferencias más 16 participantes en audio.

De esta manera, suministramos soluciones de videoconferencia innovativas, de alta calidad que son confiables, fácil de usar y generan un valor agregado a nuestros clientes.

BENEFICIOS

Los beneficios generales de la videoconferencia son principalmente:

- θ Productividad

El tiempo de espera en los aeropuertos y el desplazamiento, entre otros, son factores que reducen la productividad de los altos ejecutivos de la compañía y por lo tanto la productividad en general de la compañía, sin tener en cuenta la pérdida de la disponibilidad del ejecutivo en su sitio de trabajo.

- Reducción de costos

La videoconferencia es hoy por hoy la pieza fundamental para la reducción de costos en la gran mayoría de las empresas a nivel mundial. La tendencia a nivel mundial es la de reducir cada vez más el número de viajes, viáticos y costos hoteleros dentro de todos los niveles de la compañía.

- Mejoramiento de la gestión empresarial

Aumento del control de las sucursales y el contacto con la casa matriz, al intensificar la cantidad de reuniones, permitiendo un mejoramiento en la toma rápida y acertada de las decisiones, mejoramiento del flujo de información y logro de una comunicación más efectiva. El disponer de la videoconferencia permite la comunicación cara a cara para así atender problemas, sin necesidad de moverse del puesto de trabajo.

De acuerdo con el modelo, los sistemas ofrecen además beneficios exclusivos como:

- θ Nuestros sistemas son los únicos que permiten una conectividad total gracias a la conexión simultánea IP e ISDN en una multiconferencia, sin necesidad de añadir equipos externos (gateways) costosos.

- θ Las multiconferencias no necesariamente deben ser preestablecidas con anterioridad, la facultad dial in / dial out permite que cada uno de las sedes pueda integrarse a la conferencia en el momento que se requiera, ahorrando costos de conexión.

- θ Facilidad de conexión y manejo: todos los equipos están diseñados con sentido de usuario, su instalación, puesta en marcha y operación es extremadamente sencilla y todos los modelos son manejados con un único control remoto.
 - La facilidad de vídeo dual permite no solo la transmisión simultánea de presentador y presentación (power point, excel, etc.) sino también la transmisión de dos videos simultáneos en total movimiento, presentador y filmación, sin la degradación de la calidad de imagen.

- θ Los equipos debido a su avanzado desarrollo permiten la transmisión de 30 fps (imágenes por segundo) con tan solo una velocidad de 168 kbps, lo que representa una excelente calidad de imagen con un ahorro de costos sustantivo y un mejor aprovechamiento del ancho de banda en conexiones IP a nivel nacional.

- θ Los equipos son actualizables por software lo que protege la inversión en el tiempo y garantiza un equipo siempre moderno con todos los avances tecnológicos.

- θ Telenorma ofrece a sus clientes el programa de gestión global **GPP** el cual brinda suministro, asistencia técnica, soporte y entrenamiento en cualquier parte del mundo.

- θ Contar con recomendaciones basadas en las mejores prácticas en Videoconferencia.

- θ Disponer de personal profesional altamente especializado en RDSI, IP y Vídeo Conferencia.
- θ Soporte a Nivel Nacional e Internacional.
- θ Contar con herramientas de clase mundial como solución de Videoconferencia.
- θ Contar con soporte certificado para el acceso a Internet.

FACILIDADES Y SERVICIOS

θ NATURAL PRESENTER PACKAGE - NPP

Los equipos combinan la presentación y los datos desde un PC con una alta calidad e imagen completa en dos pantallas a la vez. Con Natural Presenter Package (NPP), compartir ideas es mucho más fácil y utilizado por ejemplo en las siguientes situaciones:

- En una videoconferencia cuando desea ver una presentación en vivo desde el PC y al presentador simultáneamente.
- En una conferencia cuando desea ver al conferencista y al auditorio al mismo tiempo.
- Durante una presentación, cuando desea ver al conferencista haciendo la presentación y el producto al mismo tiempo.
- En una reunión, cuando desea ver el conferencista y el documento al mismo tiempo.

Los cuatro componentes que conforman el Natural Presenter Package, Duo Video, PC Presenter, PC Soft Presenter y Digital Clarity trabajan juntos para asegurar una presentación real en un ambiente de reunión interactiva.

θ Duo Video



Duo Video significa que el sistema de videoconferencia puede enviar y recibir dos imágenes al mismo tiempo; una imagen en un monitor y la otra imagen sobre el otro monitor.

Con dos imágenes de increíble calidad de audio y video, las personas se sienten en un ambiente de reunión natural y real.

Dentro de las aplicaciones de la segunda imagen se cuenta por ejemplo con: la presentación a realizar desde un PC, una segunda cámara de video, una cámara de documentos, VCR, DVD, Tablero Digital, etc.

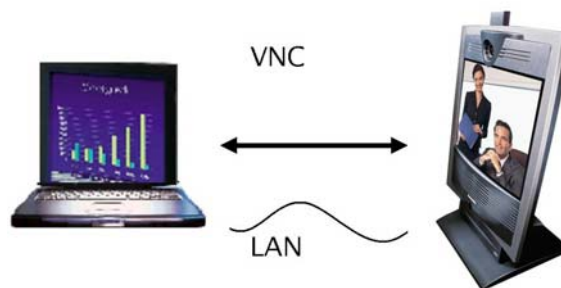
θ PC Presenter Package



Con PC Presenter, es posible realizar presentaciones de manera fácil de la información (remota y local) en un PC en vivo en el sistema de videoconferencia: solo conecte (entrada XGA) y realice la presentación tal como lo haría con un video proyector.

PC Presenter soporta todo tipo de archivos en un PC incluyendo Word, Power Point y Excel. Cuando no se dispone de sistemas Duo Video, es posible cambiar fácilmente al presentador por una gráfica, o un texto solo con un botón del control remoto.

θ PC SoftPresenter



Al igual que PC Presenter ^{TF}, PC SoftPresenter ^{TF} permite realizar presentaciones en vivo de un PC en el sistema de videoconferencia: en lugar de conectar la

entrada XGA, el PC se conecta a la red virtual usando la tecnología VNC sobre la red LAN.

Solamente es necesario bajar un programa en su PC, el cual estará conectado a la red LAN, al igual que el sistema de videoconferencia, teniendo imágenes de alta calidad en formato PC.

θ **Digital Clarity**

Digital clarity asegura que la imagen que usted observa en la videoconferencia sea clara y de colores brillantes, transmitiendo imágenes de cámaras de documentos con cuatro veces la resolución de video estándar (4CIF), así como imágenes de PC con resolución nativa (XGA).

θ **HIGH RESOLUTION**

La calidad de imagen es una función de la tasa de muestreo y de la resolución. Con la facilidad de “Natural Video” y “Native Resolutions” se logra los más altos niveles en estos elementos.

θ **Natural Video**

La tecnología de Televisión y la tecnología de Videoconferencia no son lo mismo por cuanto la calidad de imagen obtenida en Televisión no es la misma que en video. Cuando se usa Natural Video puede olvidar las diferencias y observar la imagen con una calidad de señal de televisión sobre el sistema de videoconferencia.

Natural Video envía y recibe hasta 60 cuadros por segundo (iCIF/iSIF) “true interlaced video”. Esta facilidad es iniciada automáticamente por el sistema de

videoconferencia para asegurar un excepcional movimiento suave de las imágenes y resolución de la más alta calidad.

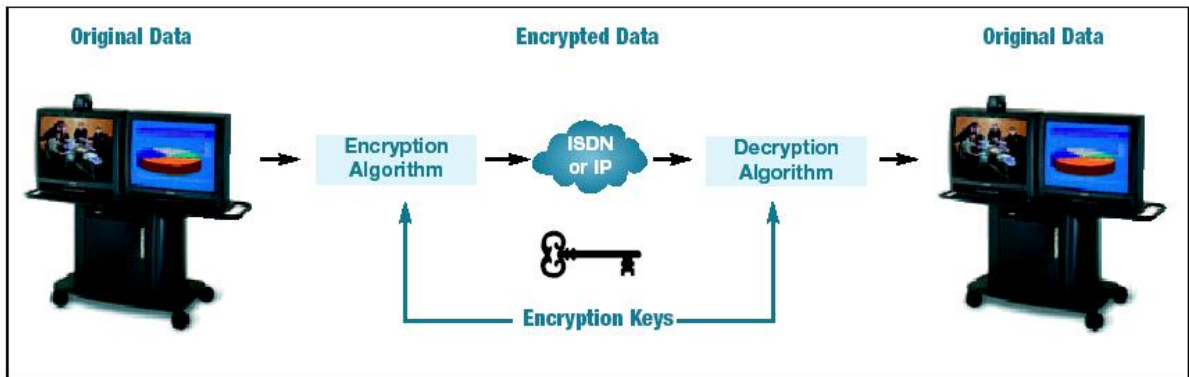
θ **Native Resolution**



Native Resolution es una nueva facilidad avanzada de videoconferencia que aprovecha los ajustes de formato de video para evitar degradación de la imagen cuando se visualiza múltiples sedes. El resultado es una imagen lo más clara posible. El sistema dialoga con los otros sistemas y selecciona la resolución más óptima para llenar las necesidades de las diferentes fuentes de video que pueden ser usadas durante una reunión.

θ **CONFIDENCIALIDAD DE LAS LLAMADAS Y DE LA INFORMACION**

Las llamadas punto a punto o multipunto entre los sistemas de videoconferencia son encriptadas automáticamente sin la intervención del usuario, para asegurar una confidencialidad completa durante las conferencias. Esta facilidad es soportada por todos los sistemas.



Un sistema se encarga de codificar tanto la información de vídeo y audio como de datos y el otro decodificará la información una vez recibida, de manera automática, según los estándares internacionales, sin degradación de la calidad o de demora. Esta función también puede ser deshabilitada manualmente o de manera automática cuando se conecta con otros sistemas que no disponen de dicha aplicación. El protocolo de encriptación utilizado corresponde a DES o AES.

θ SOPORTE DE MULTIPLES REDES - SOFTMUX

El sistema ofrecido permite la conexión simultánea sobre redes IP e ISDN (RDSI) en una multiconferencia sin necesidad de añadir equipos adicionales. El sistema detectará automáticamente si la llamada se realiza por IP o por ISDN eliminando la necesidad de técnicos especializados en redes de comunicación.

- **STREAMING**



Esta facilidad permite enviar la información de la videoconferencia sobre la red LAN y ser visualizada sobre los terminales de usuario de la red autorizados, tanto de audio como de video (broadcasts).

A su vez los usuarios de la red pueden participar activamente en la conferencia, desde su computador mediante chat, siendo una ayuda adicional para enviar información a una mayor audiencia, traducciones simultáneas en vivo, aclaración de temas.

Adicionalmente también es utilizado para presentar información, resultados, nuevos modelos, instrucciones o procesos a muchos empleados a la vez, compartir un debate o una discusión sin necesidad de tener a todos presentes en el mismo sitio, etc.

Toma solo unos segundos iniciar la sesión de streaming. Para observar una sesión se requiere:

- Instalar un media player estándar en el PC.
- Entrar a la videoconferencia mediante una dirección IP (puede ser habilitado un password).
- Ver y escuchar una conferencia en vivo mediante un web-browser estandarizado.

- Participar en la videoconferencia mediante “chat” de texto.

θ MULTISITIO Y MULTIAUDIO.



Es la posibilidad de establecer una videoconferencia con diferentes sitios, los cuales pueden ser incorporados a medida que se requiera sin necesidad de hardware adicional. Además permite la incorporación de llamadas telefónicas convencionales.

Con la función Multisitio tiene más vías para involucrar a los participantes en la reunión de forma fácil y efectiva.

Se dispone de una calidad de audio y video excelente para todos los participantes, con funcionalidad de dial-in y dial-out para recibir llamadas entrantes o para contactar a un colega e involucrarlos a la conferencia.

Se cuenta con la facilidad de Presencia Continua o Modo de Conmutación de Voz, con el fin de determinar si se observan a todos simultáneamente o bien solo la persona que habla aparece en toda la pantalla.

θ **MULTIMEDIA.**

Los sistemas permiten la conexión de múltiples equipos, para soporte de la reunión como PC's, cámaras adicionales, cámaras de documentos, DVD, VHS, equipos de audio, micrófonos inalámbricos, etc.

θ **IMAGEN Y VÍDEO.**

La calidad de la imagen se logra mediante nuestra funcionalidad de Natural Vídeo (60 Campos por segundo) y Digital Clarity que permite una mejor resolución de la presentación. Natural Audio reproduce un sonido natural eliminando los factores externos a la voz con cancelación de ecos y control automático de volumen.

θ **DOWNSPEEDING**

Durante una videoconferencia, las líneas ISDN (RDSI) que transmiten el audio y el video, pueden presentar fallas o errores. Las consecuencias son que sin la facilidad de Downspeeding, la calidad de la imagen y el sonido se reducen o desconexión de la llamada.

Con esta facilidad, el riesgo de errores en la red que afectan la videoconferencia son ampliamente reducidos. El sistema automáticamente se ajusta sin tener que realizar ningún procedimiento manual por parte del usuario.

- Mantiene la conexión si la red es interrumpida durante una llamada
- Mantiene la llamada hasta con un mínimo de un canal
- No hay pérdida de tiempo en el restablecimiento de la comunicación

θ **SUPERVISIÓN Y ADMINISTRACIÓN**

Con el software TMS las funciones de supervisión, mantenimiento, monitoreo y control de costos de llamadas se podrá realizar desde una consola, desde cualquier parte del mundo, sobre el total de los sistemas instalados.

The screenshot displays the TANDERBERG Management Suite interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL <http://localhost:8061/>. The interface includes a navigation menu with tabs for System Management, Monitoring, Scheduling, and Administrative Tools. The main content area is titled "Graphical Call Monitor - Statistics - Event Notification" and features a network diagram with nodes labeled with site names such as EDUCAL, SALES, LONDON, SINGAPORE, and OTLO. A sidebar on the left contains a "Control Panel" with various settings like "Credit Point", "Zoom", "Animation Speed", and checkboxes for "In call", "Calls", "No response", and "All". Below the network diagram, there is a section for "System Information | Directory | Call Status | Settings | Send Message To Codec | Statistics | Web | Tcbnet | ERP". The "Call Status" section displays a table with the following data:

ID	Remote Site	Type	Direction	Channels	Audio	Video	Video Res	Duo Res	Enc.	Duration	Disconnect
1	8776	bonding	incoming	bonding-30/bonding-30	g722.1/g722.1	H263/263	of/of		off/off	01:32:09	Disconnect
2	15e										
3	15e										
4	15e										

Below the table, there are input fields for "Number to call:" and "Call Quality:" (set to "auto"), along with a "Refresh Page" button and a "Call" button. The TANDERBERG logo is visible in the bottom left corner of the interface.

ANEXO G

ACCESO Y VERIFICACIÓN DE PUERTOS EN ROUTER CISCO

- Ingreso por Telnet

Si ingresamos por telnet lo primero que aparecerá será:

```
User Access Verification
```

```
Password:
```

Una vez ingresada la password aparece el *prompt* del router (*):

```
Router>
```

Para poder efectuar cualquier tipo de cambio que afecte el funcionamiento se debe acceder al modo privilegiado o *enable*:

```
Router>enable
```

```
Password:
```

Una vez ingresada esta 2a. password estaremos en modo enable:

```
Router#
```

El símbolo del prompt (">" o "#") es el que indica en qué modo uno se encuentra. Si queremos acceder al modo de configuración ingresar:

```
Router#configure terminal
```

Aparece el prompt que nos confirma que estamos en modo de configuración global:

```
Router(config)#
```

Ingreso por el port de consola mediante una notebook

Se utiliza un cable especial provisto por Cisco cuyos dos terminales son RJ-45. Típicamente es de color celeste. Mediante un adaptador a DB-9 (también provisto por Cisco) este cable se conecta a la interface serial de la PC.

Se debe utilizar cualquier programa de emulación de terminal, como por ejemplo HyperTerminal, que deberá estar configurado en 9600, N,8,1.

Dando <enter> el router debe responder con el prompt. En este punto se accede directamente al nivel arriba indicado con *:

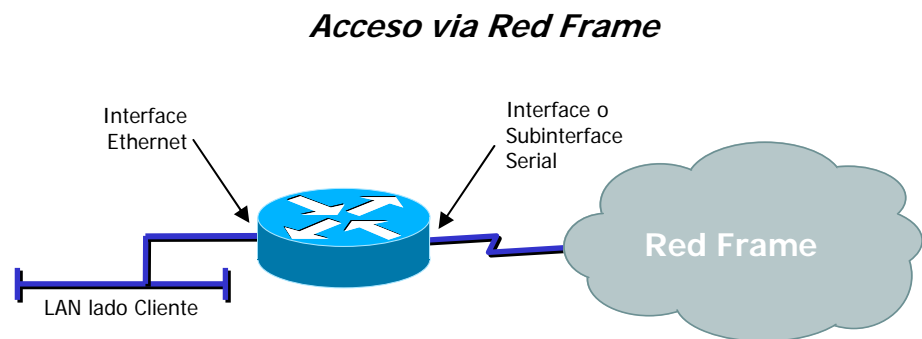
Router>

De aquí en adelante la operación del router es idéntica a la mostrada más arriba.

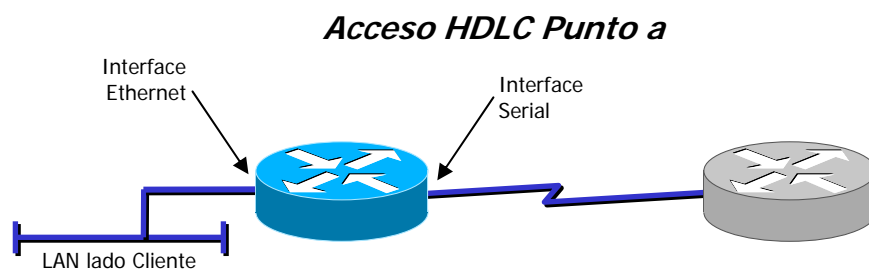
Interfaces Seriales

Se diferencian en dos servicios:

- 1) Acceso Frame Relay



- 2) Acceso HDLC Punto a Punto



Para la verificación del estado de las interfaces y subinterfaces, se pueden utilizar los siguientes comandos:

show interfaces serial [número de interface o subinterface]

show controllers serial [número de interface]

Ejemplo 1a (Acceso Frame Relay, diagnóstico de **interface**):

```
Router#sh int ser 1
Serial1 is up, line protocol is up
Hardware is HD64570
Description: A Telepuerto
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
Keepalive set (10 sec)
LMI enq sent 3, LMI stat recvd 3, LMI upd recvd 0, DTE LMI up
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 1/0, interface broadcasts
1
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 00:00:34
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/2/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 1 packets/sec
5 minute output rate 3000 bits/sec, 1 packets/sec
68 packets input, 2965 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
93 packets output, 36416 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Nivel 1 Identificador y número de interface

Nivel 2

Descripción de la interface

Encapsulación

Promedio de tráfico de los últimos 5'

Estadísticas tráfico entrante

Estadísticas tráfico saliente

Transiciones de portadora

Estado físico de las señales de la interface

Ejemplo 1b (Acceso Frame Relay, diagnóstico de **subinterface**):

```
Router#sh int ser 1.1
Serial1.1 is up, line protocol is up
Hardware is HD64570
Description: Monitoreo
Internet address is 192.168.255.78/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY
```

Nivel 1 Identificador y número de

Nivel 2

Descripción de la subinterface

Dirección IP de la subinterface

Encapsulación

Ejemplo 2 (Acceso HDLC Punto a Punto, diagnóstico de **interface**):

```

Router#sh int ser 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Description: Enlace Cliente X
  Internet address is 10.40.5.2/30
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:01, output hang never
  Last clearing of "show interface" counters 2w6d
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queuing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/2/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    294555 packets input, 34242746 bytes, 0 no buffer
    Received 239405 broadcasts, 0 runts, 0 giants, 0 throttles
    78 input errors, 78 CRC, 59 frame, 0 overrun, 0 ignored, 10 abort
    264063 packets output, 18141069 bytes, 0 underruns
    0 output errors, 0 collisions, 11 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
  
```

Nivel 1 Identificador y número de interface

Nivel 2

Descripción de la interface

Dirección IP de la interface

Encapsulación

Promedio de tráfico de los últimos 5'

Estadísticas tráfico entrante

Estadísticas tráfico saliente

Transiciones de portadora

Estado físico de las señales de la interface

Ejemplo 3 (para los dos tipos de servicio):

```

Router#sh controllers ser 0
HD unit 0, idb = 0x12ABAC, driver structure at 0x130A80
buffer size 1524 HD unit 0, V.35 DTE cable
cpb = 0x61, eda = 0x4940, cda = 0x4800
RX ring with 16 entries at 0x614800
00 bd_ptr=0x4800 pak=0x131F3C ds=0x6187C4 status=80 pak_size=88
01 bd_ptr=0x4814 pak=0x13443C ds=0x61F384 status=80 pak_size=450
02 bd_ptr=0x4828 pak=0x134B2C ds=0x6207B8 status=80 pak_size=447
03 bd_ptr=0x483C pak=0x133AFC ds=0x61D894 status=80 pak_size=24
04 bd_ptr=0x4850 pak=0x13184C ds=0x617390 status=80 pak_size=88
05 bd_ptr=0x4864 pak=0x132ACC ds=0x61A970 status=80 pak_size=88
06 bd_ptr=0x4878 pak=0x132D1C ds=0x61B02C status=80 pak_size=24
07 bd_ptr=0x488C pak=0x132F6C ds=0x61B6E8 status=80 pak_size=88
08 bd_ptr=0x48A0 pak=0x1341EC ds=0x61ECC8 status=80 pak_size=88
09 bd_ptr=0x48B4 pak=0x13340C ds=0x61C460 status=80 pak_size=24
10 bd_ptr=0x48C8 pak=0x1323DC ds=0x61953C status=80 pak_size=88
11 bd_ptr=0x48DC pak=0x133D4C ds=0x61DF50 status=80 pak_size=88
12 bd_ptr=0x48F0 pak=0x13365C ds=0x61CB1C status=80 pak_size=24
13 bd_ptr=0x4904 pak=0x13287C ds=0x61A2B4 status=80 pak_size=88
  
```

Identificador y número de interface

Debe detectar correctamente el tipo de cable conectado

```

14 bd_ptr=0x4918 pak=0x13262C ds=0x619BF8 status=80 pak_size=88
15 bd_ptr=0x492C pak=0x1331BC ds=0x61BDA4 status=80 pak_size=88
16 bd_ptr=0x4940 pak=0x131A9C ds=0x617A4C status=80 pak_size=24
cpb = 0x61, eda = 0x5000, cda = 0x5000
TX ring with 1 entries at 0x615000
00 bd_ptr=0x5000 pak=0x000000 ds=0x630D08 status=80 pak_size=88
01 bd_ptr=0x5014 pak=0x000000 ds=0x630D08 status=80 pak_size=22
1725438 missed datagrams, 238143 overruns
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
123443 residual bit errors

```

Router#

Para casos de servicios via Red Frame Relay, el estado de los PVCs y de las subinterfaces con sus correspondientes DLCIs puede verificarse con los comandos:

```

show frame-relay pvc interface serial [número de
interface]
show frame-relay map

```

Ejemplo 4:

Router#**sh frame-relay pvc int ser 1**

PVC Statistics for interface **Serial1 (Frame Relay DTE)**

Interface y tipo (FR)

	Active	Inactive	Deleted	Static
Local	1	0	0	0
Switched	0	0	0	0
Unused	0	1	0	0

DLCI = 0, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE = Serial1

```

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0        in FECN pkts 0
in BECN pkts 0      out FECN pkts 0      out BECN pkts 0
in DE pkts 0        out DE pkts 0
out bcast pkts 0    out bcast bytes 0    Num Pkts
Switched 0

```

Estado del PVC

pvc create time 3w3d, last time pvc status changed 3w3d

DLCI

```

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1.1

```

```

input pkts 465        output pkts 414        in bytes 20973
out bytes 67321      dropped pkts 0         in FECN pkts 0
in BECN pkts 0      out FECN pkts 0       out BECN pkts 0
in DE pkts 0        out DE pkts 0
out bcast pkts 0    out bcast bytes 0

```

Subinterface correspondiente

```

pvc create time 02:44:25, last time pvc status changed 02:41:12

```

```
Router#
```

Tiempo desde último cambio de estado del PVC

Tiempo desde que fue creado el PVC

Ejemplo 5:

```
Router#sh frame-relay map
Serial1.2 (up): ip 10.200.10.2 dlci 101(0x65,0x1850), dynamic,
                broadcast,, status defined, active
Serial1.1 (up): ip 192.168.255.77 dlci 100(0x64,0x1840), dynamic,
                broadcast,, status defined, active
Router#
```

Dirección IP remota (mapeo)

Subinterface y estado

Estado

Interfaces Ethernet/FastEthernet

Para verificar que la conexión de una interface Ethernet o FastEthernet a la red LAN local sea correcta, se utiliza el comando:

```
show interfaces ethernet [número de interface]
show interfaces fastethernet [número de interface]
```

Ejemplo 6:

```
Router#sh int eth 0
Ethernet0 is up, line protocol is up
Hardware is AmdP2, address is 0030.94d8.f6c0 (bia 0030.94d8.f6c0)
Internet address is 10.0.50.41/27
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 1/75, 966130 drops
5 minute input rate 24000 bits/sec, 5 packets/sec
5 minute output rate 2000 bits/sec, 4 packets/sec
34587887 packets input, 2174837174 bytes, 89133 no buffer
Received 10834854 broadcasts, 0 runts, 0 giants, 0 throttles
71310 input errors, 0 CRC, 0 frame, 0 overrun, 71310 ignored
0 input packets with dribble condition detected
22946314 packets output, 302905751 bytes, 0 underruns
312 output errors, 48817 collisions, 2 interface resets
0 babbles, 0 late collision, 138811 deferred
0 lost carrier, 0 no carrier
```

Nivel 1 Identificador y número de interface

Nivel 2

Dirección IP de la interface

Promedio de tráfico de los últimos 5'

Estadísticas tráfico entrante

```
0 output buffer failures, 0 output buffers swapped out
Router#
```

Estadísticas tráfico saliente

Procedimiento para configuración de routers

- a) El área de Integración, responsable de levantar los nuevos servicios, proveerá para los dos tipos de acceso (Frame Relay y/o HDLC) un modelo o *template* de configuración del router ya "customizado", o sea prearmado con los parámetros particulares del cliente (nombres, passwords, direcciones IP, etc.).
- b) Este modelo de configuración será recibido en forma de un archivo de texto plano para que sea copiado y pegado en la consola del router (desde modo de configuración global).

Por ejemplo, la siguiente es una configuración para un cliente que tendrá un acceso HDLC Punto a Punto.

```
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname Cliente_Z
!
enable secret impsat
!
ip subnet-zero
no ip domain-lookup
!
interface Ethernet0
!
interface Serial0
  no shut
  ip address 192.168.25.1 255.255.255.252
!
ip classless
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
  transport input all
line vty 0 4
  exec-timeout 180 0
  password impsat
!
end
```

Funcionamiento y grabado de la configuración

- Funcionamiento básico

Los routers Cisco tienen **2 configuraciones**:

1. La primera de **inicio o "startup"** ubicada en memoria no volátil (NVRAM);
2. Y la otra **activa o "running"** ubicada en memoria RAM.

Cuando el router es encendido, parte del proceso de booteo consiste en leer la configuración de inicio y copiarla en RAM. Esta copia pasa a ser la configuración activa.

A partir de allí, todos los cambios que se efectúan son asentados sobre la configuración activa, o sea que cada comando es ejecutado y entra en acción **inmediatamente** después de ingresado.

Esto significa que se debe tener cuidado cuando se ingresan comandos "peligrosos", como por ejemplo cambio de dirección IP o deshabilitación de una interface, ya que se puede correr el riesgo de perder visibilidad del router sobre el que se está trabajando. En caso de que esto suceda, generalmente no hay otra solución que hacer resetear el router (apagarlo y encenderlo) para que vuelva a levantar con la última configuración que tenía grabada.

- Visualización

1. Para ver la configuración de **inicio o "startup"** se debe ejecutar el comando:

```
Router#show startup-config
```

2. Para ver la configuración **activa o "running"** se debe ejecutar el comando:

```
Router#show running-config
```

- Grabado de la configuración en memoria no volátil (NVRAM)

Dado que la **configuración activa corre desde RAM**, en caso de corte de energía o reseteo del router esta configuración **se pierde**.

Entonces, luego de configurar exitosamente un router, o de efectuar cualquier cambio que tenga que quedar operativo, **se debe salvar la configuración** en memoria no volátil para que en caso de reseteo del router éste levante con la configuración correcta.

Esto se logra ejecutando cualquiera de los siguientes comandos desde modo enable:

```
Router#copy running-config startup-config  
Router#write memory
```

Ejemplo 7:

```
Router_X#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
Router_X#
```

Verificaciones y pruebas finales

En todos los casos (interfaces/subinterfaces seriales o de LAN), deben efectuarse pruebas de conectividad, de manera de verificar que estén operativas.

- Ping

Permite verificar que los paquetes están siendo ruteados e informa también el tiempo en que tardan los paquetes llegar a destino y volver.

```
ping [dirección IP remota]
```

Ejemplo 8:

```
Router#ping 10.40.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.40.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
Router#
```

Dirección IP remota

Tiempo de respuesta

Resultado de la prueba

Interpretación del resultado del Ping:

! = OK
. = No hubo respuesta (timeout)
U = Destination Unreachable

- Ping extendido

Permite especificar la cantidad de paquetes a enviar, su tamaño, tiempo de espera y la dirección origen desde la que se hace el ping. De no especificarse este último parámetro, será enviado con la dirección de la interface por la que el ping sale del router.

Para poder ejecutar ping extendido se debe hacer desde modo *enable*.

```
ping
```

Ejemplo 9:

```

Router#ping
Protocol [ip]:
Target IP address: 10.50.50.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 200.41.63.74
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.50.50.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 464/470/480
ms
Router#

```

Diagram annotations for the ping command:

- Dirección IP remota: 10.50.50.1
- Acceso a comandos extendidos: y
- Dirección IP origen: 200.41.63.74
- Tiempo de respuesta: = 464/470/480 ms
- Resultado de la prueba: Success rate is 100 percent (5/5), round-trip min/avg/max = 464/470/480 ms

- Traceroute

Esta herramienta es similar al ping, pero provee un detalle de los lugares por los que pasa.

Para abortar el comando presionar Control-Shift-6 x.

```

traceroute [dirección IP remota]

```

Ejemplo 10:

```

Router>trace 10.70.6.74
Type escape sequence to abort.
Tracing the route to 10.70.6.74
  0 10.70.248.1 [528 msec 528 msec 528 msec]
  1 10.70.6.245 [564 msec 536 msec 536 msec]
  2 10.70.6.74 [536 msec 536 msec 536 msec]
Router>

```

Diagram annotations for the traceroute command:

- Dirección IP remota: 10.70.6.74
- Número de saltos: 1, 2, 3
- Direcciones IP intermedias: 10.70.248.1, 10.70.6.245, 10.70.6.74
- Tiempos de respuesta: 528 msec, 564 msec, 536 msec

- Traceroute extendido

En forma similar al ping extendido, permite especificar la dirección origen. También se debe ejecutar desde modo *enable*.

```

traceroute

```

Ejemplo 11:

```
Router#trace
Protocol [ip]:
Target IP address: 10.70.6.74
Source address: 10.10.0.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.70.6.74
```

	Número de saltos				
1	10.70.248.1	528 msec	528 msec	528 msec	
2	10.70.6.245	536 msec	528 msec	536 msec	
3	10.70.6.74	536 msec	564 msec	536 msec	

Router#

Direcciones IP intermedias

Tiempos de respuesta