UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACION DE UNA RED DE ALTA DISPONIBILIDAD CON SOLUCIONES DE VOZ, VIDEO Y DATOS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

JORGE LUIS ZEGARRA GUARDAMINO

PROMOCIÓN
2001 – I

LIMA – PERÚ
2006

IMPLEMENTACION DE UNA RED DE ALTA DISPONIBILIDAD CON SOLUCIONES DE VOZ, VIDEO Y DATOS

Dedico este trabajo a:

Mis padres, Alvina y Rosendo

inspiración plena de lucha y sacrificio.

SUMARIO

Los avances tecnológicos en materia de Sistemas de Redes de los últimos años y los que se están produciendo, están dando cada vez más posibilidades efectivas y por tanto la oportunidad de jugar un papel preponderante a los contenidos multimedia. En este informe se hace un repaso a las herramientas que hacen posible realizar un comportamiento predecible de las redes con aplicaciones en tiempo real, lo cual es un aspecto importante para todo negocio. Este informe indica la manera de implementar una red con aplicativos en tiempo real haciendo uso de mecanismos de calidad de servicio (QoS).

El escenario donde se implementa esta red, es en una empresa que cuenta con tres sedes, considerando a una de ellas como la sede principal. Este trabajo consiste en unir estas tres sedes mediante enlaces de datos los cuales permitirán hacer uso de aplicaciones de video (videoconferencia, video para vigilancia, etc.), voz (anexos extendidos desde la sede principal) y datos. El uso de estas aplicaciones entre sedes no generará costos adicionales a la empresa, dado que estas aplicaciones están implementadas sobre el enlace de datos que las une.

INDICE

INTRODUCION

El presente informe tiene como objetivo, brindar los alcances necesarios para irmplementar una red de alta disponibilidad con soluciones de voz, video y datos, para PYMES (Pequeña Y Mediana Empresas) que cuentan con más de una sede.

Las empresas de hoy en día, en su gran mayoría, cuentan con sistemas de comunicación de voz, video y datos por separado. Los sistemas de datos en la actualidad cuentan con redes locales basadas en tecnología Ethernet en su gran mayoria, tecnología muy aceptada, por fabricantes, por los estándares establecidos como es el caso de ISO (Organismo de Estándares Internacionales), así como también, por usuarios, por sus bajos costos y buen desempeño, en comparación con otras tecnologías. Bajo esta premisa, nuestro diseño tomará como base que las redes locales cumplen con los estándares de cableado estructurado.

En este informe se realiza la convergencia a una sola red (IP), las redes de voz, video y datos para una empresa con 3 sedes en las cuales cuenta con sus sistemas de datos, comunicación de voz y videoconferencia por separado. Por tanto, esta empresa deberá contar con la instalación de una red LAN de datos y de telefonia que cumplan con los estandares de cableado estructurado.

La red a implementar, considera un enlace de respaldo para cada sede hacia una de las sedes elegida como la principal. Los enlaces de respaldo estan basados en lineas digitales RDSI (Red Digital de Servicios Integrados) los cuales son usados solo cuando se presente problemas en la red del provedor del enlace principal de datos (DDR: Dial on Demand).

Para nuestro diseño se optó por equipos CISCO, debido a su reconocida eficiencia de operación como equipos de redes y al respaldo que brinda el fabricante.

CAPITULO I
FUNDAMENTO TEORICO

1. 1 Calidad de servicio

La gestión de la calidad de servicio en IP con servicios diferenciados se basa en la capacidad de todos los routers de la red para, observando el campo TOS de la cabecera IP u otros campos, ser capaces de clasificar y marcar el tráfico para darle un trato diferenciado Esto ha de ocurrir en todos los nodos, si se desea que esta técnica sea efectiva.

En la red que estamos diseñando, el trato de este octeto de la cabecera IP es crucial para garantizar la calidad de servicio, puesto que nosotros pretendemos aplicar esa gestión a nuestro caso concreto: voz y la videoconferencia sobre IP. Para ello vamos primero a ver sucintamente qué mecanismos tenemos en IP para controlar la QoS, aplicándolo después al caso que nos ocupa.

Nuestro objetivo final va a ser, por tanto, disponer de una red donde el tráfico de voz y video tenga máxima prioridad, garantizando así un servicio de telefonía y de videoconferencia, dejando en un segundo plano el tráfico de datos. Por último, podremos hacer uso del resto de recursos de la red siempre y cuando estos no interfieran con las aplicaciones que estamos considerando como prioridad principal.

1.1.1 Calidad de servicio en IP

Históricamente, la calidad de servicio [1] se define en la cabecera IP en el segundo octeto Fig. 1.1, llamado TOS (Type of Service), según lo convenido en las RFC 791 y RFC 1349. Más adelante se redefinió su significado pasando a llamarse octeto DS (Differentiated

Services) según la RFC 2474, que deja obsoletas a las anteriores. Por tanto, tenemos la opción de utilizar este octeto de una de tres formas posibles:

- Siguiendo las RFC 791 y RFC 1349, que aunque obsoletas, están todavía en uso en muchas aplicaciones actuales.
- Adhiriéndonos a la RFC 2474, asegurando la interoperabilidad con otras redes.
- Definiendo por cuenta propia el significado de este octeto, controlando los parámetros de QoS nosotros.

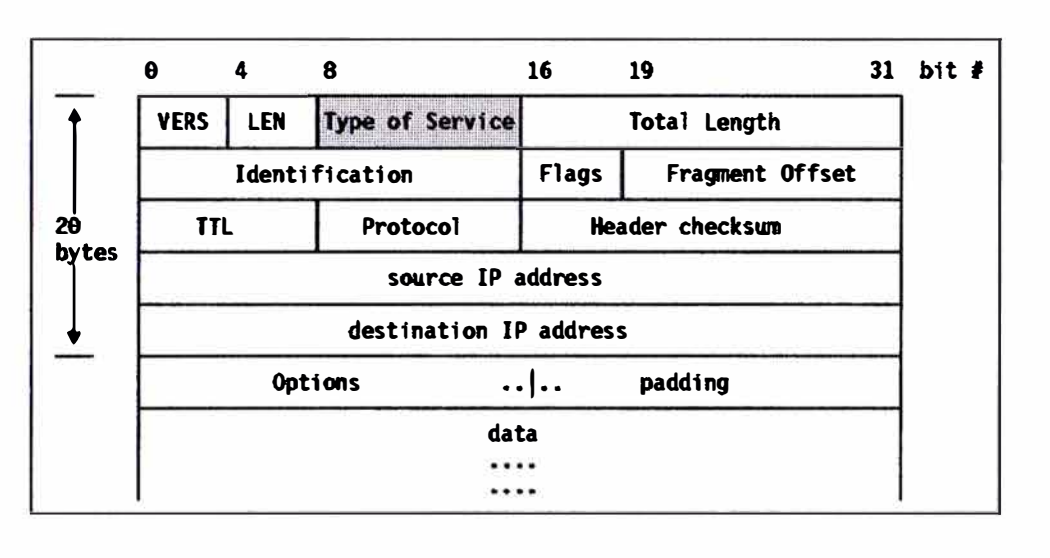

Fig. 1.1 Campo ToS en un paquete Ipv4

Tomemos la opción que tomemos, hemos de saber cómo identificar los paquetes que llegan al nivel IP desde un nivel superior procedentes de una videoconferencia, bien sea sólo audio o bien incluyendo el vídeo. Es decir, al construir el datagrama IP su octeto que define el tipo de servicio (bien según las RFC antiguas, bien según la nueva, o siguiendo un esquema distinto, para el caso que nos ocupa nos es irrelevante) ha de marcarse en función de lo que venga del nivel superior. Para ello vamos a ver qué recibe el nivel IP desde arriba. En cualquier caso, a efectos de este estudio, llamaremos a este octeto de IP "octeto QoS" o "campo QoS", para que quede patente que el marcado de este octeto es independiente del esquema de marcado que se siga.

1.1.2 Aplicación a nuestro caso

Tanto H.323 como SIP, así como el resto de protocolos de videoconferencia mínimamente importantes y eficaces, siguen el mismo esquema: a nivel de aplicación todos usan el protocolo RTP/RTCP para el transporte de audio y/o vídeo. Los paquetes RTP se encapsulan en paquetes de transporte UDP, que son los que le llegan al nivel IP. El problema estriba en que el nivel IP pueda saber que lo que hay en el nivel superior es un paquete de audio o de vídeo, y les asigne la prioridad adecuada. Nos encontramos pues con varias posibilidades:

- La solución trivial, consiste en no hacer nada y esperar que el ancho de banda y la capacidad de procesamiento de la red sean suficientes para bregar con el tráfico de tiempo real.
- IP es consciente del protocolo de nivel superior, TCP ó UDP, por tanto se pueden marcar los paquetes UDP con mayor prioridad. Esto no permite diferenciar entre audio y vídeo y además puede dar prioridad a datagramas que no pertenezcan a una videoconferencia aunque usen UDP.
- Sabiendo que tenemos un paquete UDP entre manos, la tercera opción consiste en intentar averiguar si dentro hay un mensaje RTP/RTCP, o incluso asumir que es así a menos que se demuestre lo contrario. Esto tiene como consecuencia que la interfaz con el nivel IP deba examinar el contenido del paquete UDP, lo que se puede lograr de diversas maneras, y si el contenido es RTP (o asumimos que lo es) se puede deducir, gracias a la existencia del campo fijo PT (Payload Type) de la cabecera RTP, si el contenido es audio o vídeo y marcarlo a tal efecto en el campo de tipo de servicio de IP.
- Otra posible opción, más controvertida, consistiría en hacer la discriminación de los paquetes por puertos, es decir, espiar el contenido de las sesiones H.323 o SIP, averiguar qué puertos se negocian para audio y vídeo, y dar prioridad al tráfico por esos puertos, sería un mecanismo similar al necesario para poder dar servicio H.323 con NAT y/o firewalls. Por último cabe la posibilidad de utilizar un sistema de discriminación de redes privadas, dando prioridad a los paquetes que salgan desde esta la red (mediante listas de acceso).

Teniendo en cuenta todas estas posibilidades básicas, el esquema propuesto consiste en analizar varias de estas posibilidades, siguiendo un orden que permita minimizar el tiempo

de procesado de cada paquete, de forma que al final, con un margen de error mínimo, demos la prioridad deseada a los paquetes de nuestras aplicaciones en tiempo real. El esquema consistiría, pues, a nivel IP en realizar una serie de pasos que nos permitan deducir el contenido del paquete y marcar el campo de QoS de IP de forma consecuente, a continuación se enumeran los mismos, comentando sus pros y sus contras:

1.Las aplicaciones (o terminales hardware) suelen indicar el valor del campo ToS, tal y como el caso de aplicaciones como Netmeeting y el Gnomemeeting. De esta forma sólo hemos de fijarnos en el valor que la aplicación pretende imponer al octeto y deducir inmediatamente si se trata de un paquete de videoconferencia. Hay que hacer notar dos cosas en esta aproximación, primera, que no todas las aplicaciones marcan este octeto y casi todas lo hacen de forma distinta, luego habría que tener en cuenta al desplegar la red qué aplicaciones se pretenden usar, y segunda, tal y como hemos visto no todas las aplicaciones diferencian entre audio y vídeo, con lo cual nuestro análisis en ése caso no terminaría aquí, sino que deberíamos poder distinguir entre ambos. En cuanto a lo segundo, en principio no debería haber problema, ya que podemos entrar a analizar el campo PT de la cabecera RTP, pero en cuanto a lo primero, nos encontramos con que si nos regimos por ello, estaremos haciendo nuestra red hasta cierto punto dependiente de las aplicaciones escogidas, limitándonos a efectos prácticos. Por último, conviene también recordar que otras aplicaciones podrían marcar sus contenidos como urgentes en la misma forma y recibir el mismo trato diferenciado, si no somos cuidadosos.

2.Evidentemente, los paquetes RTP van encapsulados sobre UDP, que a su vez va encapsulado sobre IP. Dado que todos los paquetes de videoconferencia van sobre UDP, nos basta con examinar el paquete IP y ver el campo que indica en su cabecera el tipo de protocolo que va dentro y si es UDP, darle prioridad. El problema con esta aproximación es que puede haber paquetes que lleguen al nivel IP encapsulado en UDP pero que no tengan que ver con la videoconferencia, como por ejemplo relativos a NFS u otras aplicaciones. Aún así, se estima que la proporción de éstos en una red típica es muy pequeña en comparación al número de paquetes de tiempo real pertenecientes a la videoconferencia.

3.Una posibilidad llegados a este punto es, sabiendo que el paquete es UDP, considerar de voz y/o de vídeo los paquetes comprendidos en un cierto rango de tamaños, a determinar tras analizar los distintos codecs posibles, por ejemplo, los paquetes de audio suelen ocupar

entre 40 y 160 bytes, con lo cual paquetes que se salgan de esta escala los podemos descartar del marcado.

4.Combinando las aproximaciones anteriores, y recordando lo que ocurría en el caso del Gnomemeeting, por ejemplo, también sabemos que hay aplicaciones que únicamente utilizan un cierto rango de puertos UDP, con lo que llegados a este punto sabríamos con cuasi total certeza que si, por ejemplo, hay un paquete UDP destinado al puerto 5000 de una cierta máquina, este paquete es de tiempo real. De nuevo el problema que tenemos es que el sistema de diferenciado depende de las aplicaciones usadas.

5.Habiendo comprobado que se trata de un paquete UDP y/o que su puerto de destino se corresponde al utilizado por una aplicación de VoIP, y/o que el paquete está marcado con una cierta prioridad, el siguiente paso consistiría en asumir que se trata de un paquete de tiempo real y tratarlo como tal. Para ello asumimos que se trata de un paquete RTP y realizamos una sencilla comprobación para asegurarnos no de que realmente lo es, sino para descartar aquellos que hayamos marcado como prioritarios hasta ahora erróneamente. Para ello comprobamos los campos fijos y aquellos cuyo valor podemos deducir de la cabecera RTP, y si coinciden con los que deberían ser, asumimos que el paquete es RTP de forma definitiva y examinamos su campo PT, que lleva la codificación del tipo de carga del paquete según lo especificado en la RFC 3551. De esta forma marcamos el paquete con una cierta prioridad para el audio y otra prioridad para el vídeo.

Una posibilidad adicional, no desdeñable a priori, consiste en, viendo que existen soluciones en el mercado que permiten tanto a (algunos) GateKeepers de H.323 y Proxies de SIP actuar de intermediarios enrutando todo el tráfico a su través, incluyendo el de tiempo real, utilizar esos intermediarios para marcar el campo de calidad de servicio de todos los paquetes UDP (recordemos que no podemos hacer una mayor discriminación a nivel IP para ver cuáles son RTP) que sepamos que pertenecen a una videoconferencia. Para saber si es tráfico de videoconferencia una solución muy sencilla consistiría en establecer una interfaz exclusiva con una IP que únicamente se utilice para la aplicación H.323 o SIP, de esta forma, sabemos que todo el tráfico perteneciente a la misma es parte de una videoconferencia, y procederíamos a marcar los paquetes UDP de la misma asumiendo que son RTP según el valor del campo PT de su cabecera, diferenciando entre audio y vídeo. Veamos los principales problemas con los que nos podemos encontrar:

1.Al hacer que el tráfico de tiempo real pase a través de un intermediario, podemos estar añadiendo un retardo adicional significativo, que puede o no estar compensado con la posterior priorización de los paquetes de tiempo real. Es razonable suponer que el retardo es más o menos el mismo para todos los paquetes, no se produciría degradación de la voz por jitter o efectos similares, pero sí se apreciaría un retardo común. Sería necesario determinar empíricamente la validez de esta solución en este sentido.

2.El intermediario tendría una carga mucho mayor de lo habitual, esto se puede solventar teniéndolo en cuenta antes y dimensionando el sistema adecuadamente, por ejemplo añadiendo más GateKeepers y Proxies SIP, y realizando balance de carga entre ellos.

3.Por último, recalcar que estamos priorizando *todo* el tráfico UDP queque pertenece a una red especifica (Según diseño únicamente para equipos de videoconferencia. Afortunadamente, esto redunda en cualquier caso en nuestro beneficio, ya que el hecho de priorizar éste tráfico, aunque sea por error, únicamente ayuda al tránsito en la red de los paquetes asociados a la videoconferencia. Por fin, llegados a este punto deberíamos tener al menos tres tipos de paquetes en la red, los de prioridad normal, los de prioridad máxima, que serían los de voz y de videoconferencia y los de prioridad baja. El siguiente paso consiste, pues, en establecer la política de colas en los routers de la red de forma que prioriticen el audio, luego el vídeo, y luego el resto de paquetes.

Para nuestro diseño se ha considerado tres tipos de tráfico en la red como se muestra en la tabla N° 1.1 que a continuación se muestra:

Tabla N° 1.1 Clasificación de Tráfico de Red

Tipos de Tráfico	Descripción
Prioridad 1 (P5)	Aplicaciones en tiempo real que exijan una baja diferencia de delay (jitter), ejemplo: Multimedia, VoIP, Video Conferencia, Telefonía IP.
Prioridad 2 (P2)	Aplicaciones sensible al retardo (delay) y/o criticas para el negocio, ejemplo: Oracle, SAP, SNA, etc.
Prioridad 3 (P1)	Aplicaciones que no necesita altas exigencias de retardo como por ejemplo http, mail, ftp, etc.

Para el caso de Prioridad 1 (P5) se considera precedencia 5 o dscp cs5 en la Calida de Servicio.

La clasificación de paquetes se realiza usando los bits de DSCP (differentiated Services Code Point), (6 bits) o los de tipo de servicio (3 bits), estos últimos son mapeados en los primeros por compatibilidad, el siguiente cuadro resume el uso de DSCP para la clasificación del tráfico de red en clases de servicios.

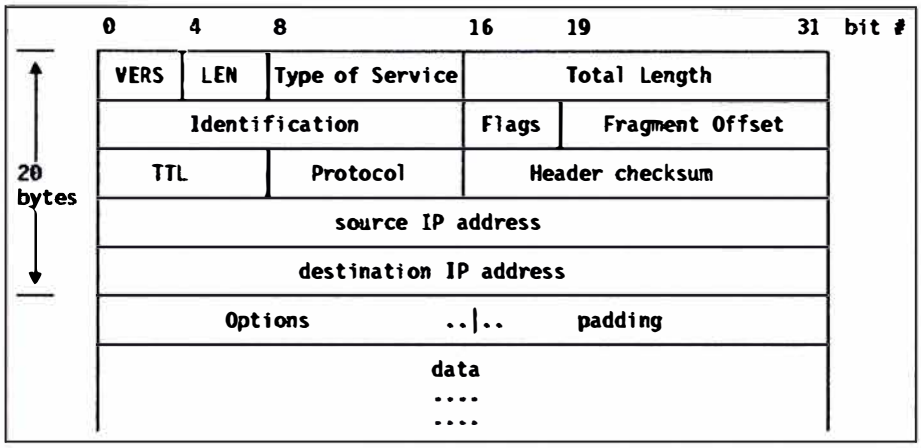

Fig. 1.2 Formato del datagrama IP

Tabla N° 1.2 Clasificación de Tráfico de Red

ToS Byte							
P2	P1	P0	T2	T1	T0	CU0	CU1
Bits Precedecia IP (3bits)			Delay, Throughput and Reliability			No usado	No usado
DiffServ Field							
DS5	DS4	DS3	DS2	DS1	DS0	ESN	ESN
DSCP (6bits)						Para uso futuro	Para uso futuro

En la tabla N° 1.3 se presenta las equivalencias DSCP y Precedencia IP:

Tabla N° 1.3 Equivalencias

TIPO DE TRAFICO	**DSCP**	**PRECEDENCIA IP**
Prioridad 1 (P5)	CS5 (101000)	5 (101)
Prioridad 2 (P2)	CS2 (010000)	2 (010)
Prioridad 3 (P1)	CS1 (001000)	1 (001)

1.2 Manejo de congestión

La característica de manejo de congestión permite controlar la congestión determinando el orden en que se envían los paquetes fuera una interfase basadas en prioridades asignadas a los paquetes. El manejo de congestión trae consigo la creación de colas, la asignación de paquetes a estas colas basadas en clasificación del paquete, y fijando los paquetes en una cola para la transmisión. La dirección de congestión que QoS ofrecen cuatro tipos de protocolos de encolamiento, cada uno de los cuales permiten especificar creación de diferente de colas, ofreciendo, en mayor o menor grado la diferenciación de tráfico, especificando el orden en el cual el tráfico es enviado.

Durante periodos de poca densidad de tráfico, es decir, cuando no exista congestión, los paquetes son enviados fuera de la interfase de manera inmediata luego de su arrivo a dicha interfase. Durante periodos de congestión a la salida de una determinada interfase, son generadas cuando los paquetes arriban más rápidamente a la interfase, a la que estas pueden ser enviadas. Sí hacemos uso de las características de manejo de congestión, se generan colas de paquetes; entonces estas son enviadas según su prioridad asignada y de acuerdo al mecanismo de encolamiento asignado para la interfase. El router determina el orden de transmisión del paquete controlando, qué paquetes se ponen en cola y cómo estas colas son atendidas respecto de nosotras.

Algunas de las características de manejo de congestión están dadas por:

1.2.1 FIFO

Las colas FIFO son bien conocidas por los ingenieros y los programadores. Su nombre viene de First Input - First Output y son colas simples, sin clases, que liberan los paquetes en la salida en el mismo orden en que entran. Normalmente nos interesa asociar una longitud en paquetes, y no en bytes, a una cola FIFO, que sería el número de paquetes que se pueden encolar.

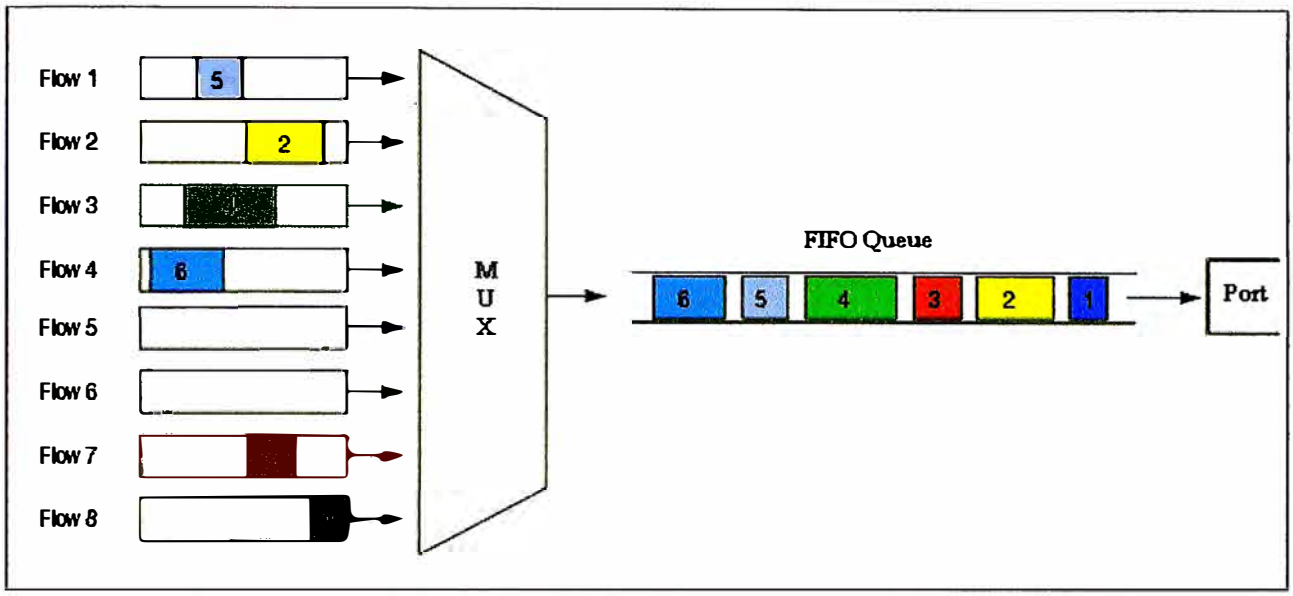

Fig. 1.3 Disciplina FIFO

La clasificación por lo tanto es simple y llanamente basada en el orden de llegada. Las colas FIFO no sirven en sí mismas para establecer prioridades, pero las usaremos como elementos constructivos de disciplinas de colas más complejas para encolar el tráfico derivado a las subclases.

1.2.2 WFQ (Weighted Fair Queueing)

WFQ ofrece colas de paquetes dinámicas e imparciales que divide el ancho de banda por las colas de tráfico basado en los pesos. (WFQ asegura que todo el tráfico se trata justamente, dado su peso.

Dado este manejo, WFQ asegura tiempos de respuestas satisfactorios a las aplicaciones críticas, como aplicaciones interactivas, aplicaciones basadas en transacciones que son intolerante de degradación de tiempos de respuesta. Cuando ninguna otra estrategia de encolamiento se configura, todas las interfaces de un router usan FIFO por defecto.

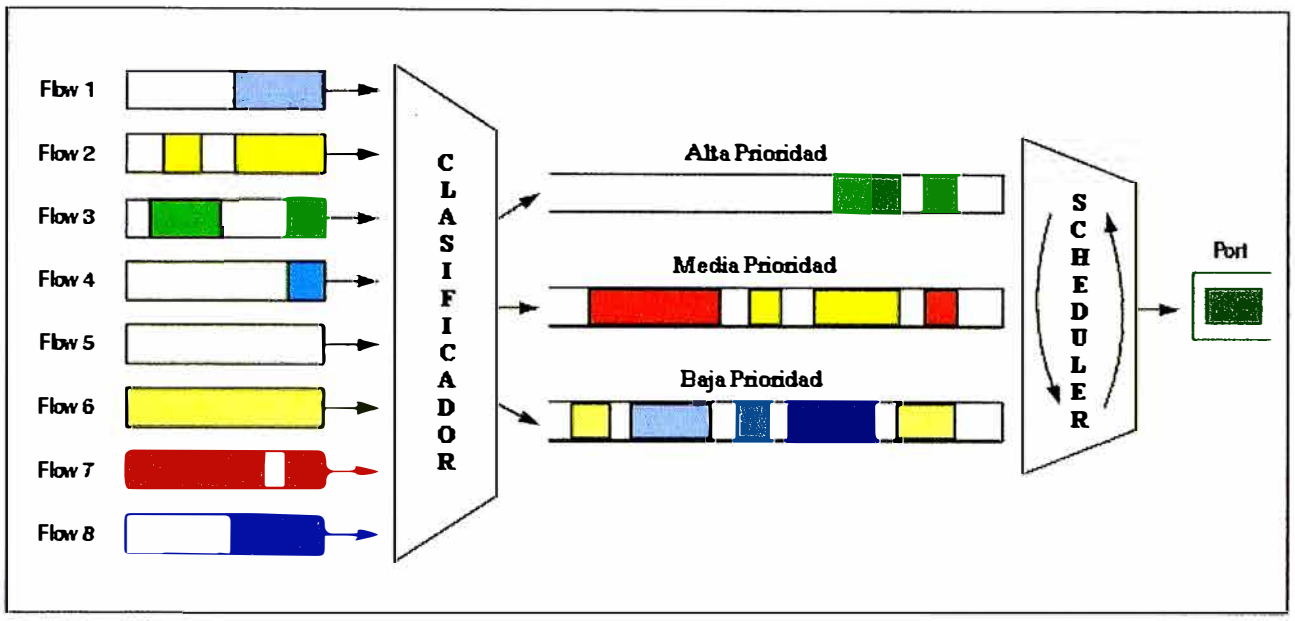

Fig. 1.4 Encolamiento de tráfico con prioridades

1.2.3 RED (Random Early Detection)

Las distintas disciplinas de colas vistas comparten dos problemas cuando se llega a una situación de congestión:

Se puede dar que unos pocos flujos mantengan las colas permanentemente saturadas y los demás no puedan directamente obtener servicio

Se pueden producir oscilaciones porque, si la cola está llena y llegan casi simultáneamente paquetes de varios flujos, y estos se descartan, todos ellos reaccionan disminuyendo su tasa de envío, y al reducirse drásticamente el tráfico se produce una situación de desocupación que tiene el efecto exactamente inverso.

RED realiza un descarte preventivo de paquetes antes de que se llene la cola. De esa forma el descarte de paquetes es consciente y no forzado y se puede escoger qué se descarta y a qué ritmo. Cuando la carga de tráfico es baja, no se descargan paquetes; cuando se llega a cierta carga se empiezan a descartar los paquetes con probabilidad 'p', y a partir de cierto otro nivel superior que se considera muy próximo a la congestión total se descartan todos los paquetes. De esa forma se obtiene un comportamiento como el que indica la línea roja de la figura.

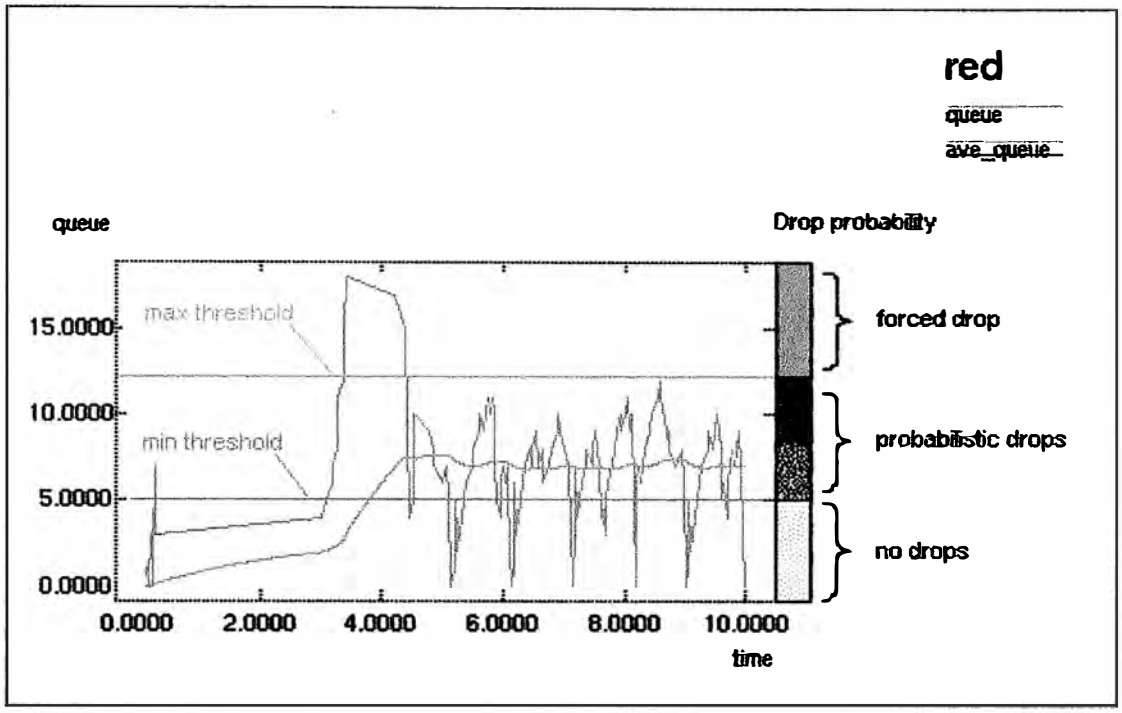

Fig. 1.5 Disciplina RED

1.3 Voz sobre IP

Vamos a analizar cómo se encuentra actualmente el mundo de la VoIP, a todos los niveles. Actualmente existen dos estándares prominentes en el mundo de la voz sobre IP: H.323 y SIP. Pasamos a continuación a verlos en detalle, analizando sus ventajas e inconvenientes, sobre todo en su relación con la red de VoIP que se pretende desplegar.

Nuestro objetivo fundamental es diseñar una red IP con la capacidad y funcionalidad suficiente como para proporcionar un servicio de VoIP al usuario garantizando la calidad de servicio. Para ello se pretende analizar el funcionamiento de las soluciones de VoIP más comunes y extrapolar las medidas a tomar para diseñar una red que sea capaz de dar la prioridad adecuada a los paquetes de voz y de vídeo pertenecientes a una videoconferencia.

1.3.1 Arquitectura de redes VoIP

En general un sistema de voz sobre IP (Voice over IP, VoIP) consiste en establecer una conferencia de audio entre dos terminales conectados a una red. En su forma más básica, todo lo que requiere es que sea bidireccional, que el retardo sea prácticamente constante y muy bajo, y que la calidad subjetiva de audio sea suficientemente buena para entender al interlocutor. El problema principal de encargar este cometido a una red IP consiste en que

estas redes son de tipo best-effort, y no proporcionan por tanto calidad de servicio, necesaria para garantizar que los paquetes de voz llegan en el orden adecuado y con retardo mínimo y común a todos ellos.

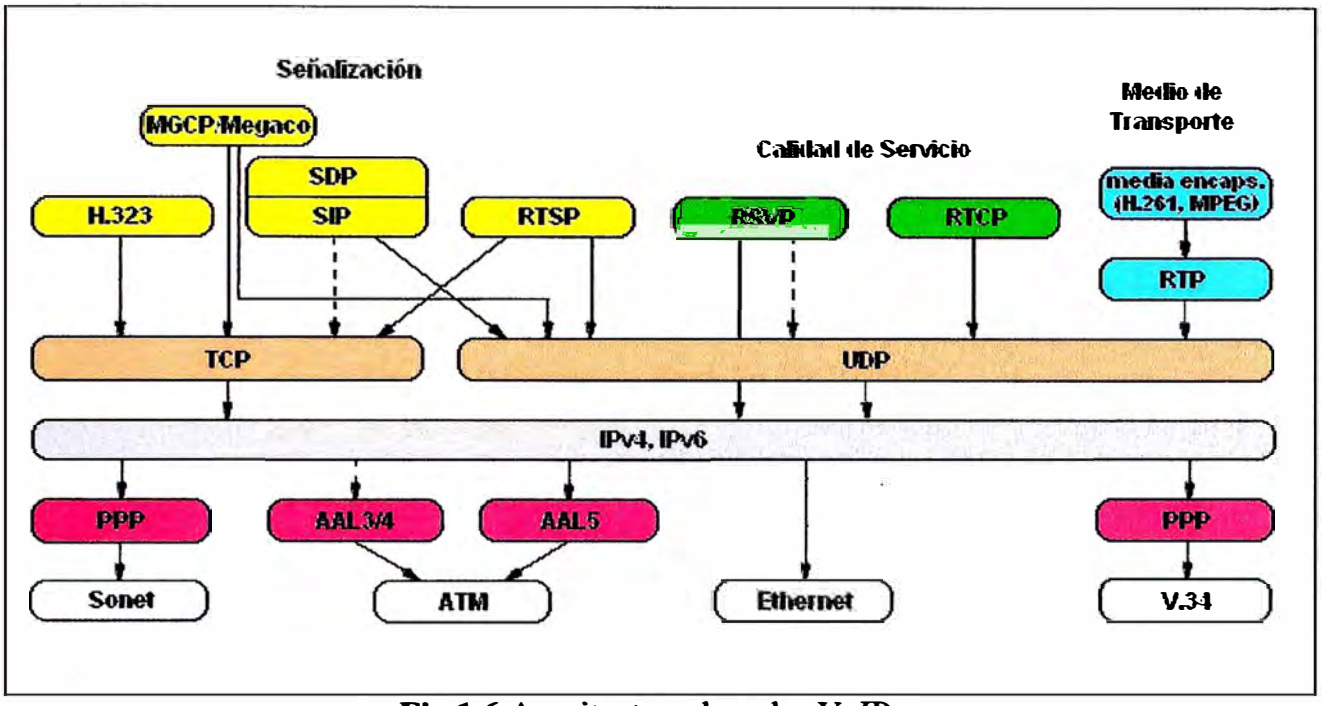

Fig 1.6 Arquitectura de redes VoIP

1.3.2 Protocolos RTP/RTCP

Para aplicaciones como la Voz sobre IP, con flujos de datos en tiempo real, se desarrollaron los protocolos RTP/RTCP (Real Time Protocol/Real Time Control Protocol) , definidos en la RFC 1889. Son capaces de proporcionar calidad relativamente aceptable a los flujos de datos de tiempo real mediante mecanismos como control de datagramas descartados en la red, o control del correcto orden de reensamblaje de los mensajes, por citar dos de los más comunes. Son protocolos de nivel de aplicación y, evidentemente, por sus necesidades de tiempo real, los mensajes RTP/RTCP van encapsulados sobre datagramas UDP, lo que garantiza que los procesados de protocolos de nivel inferior añaden el mínimo retardo, amén de no necesitar establecer una conexión, como ocurriría si se utilizara TCP, por ejemplo.

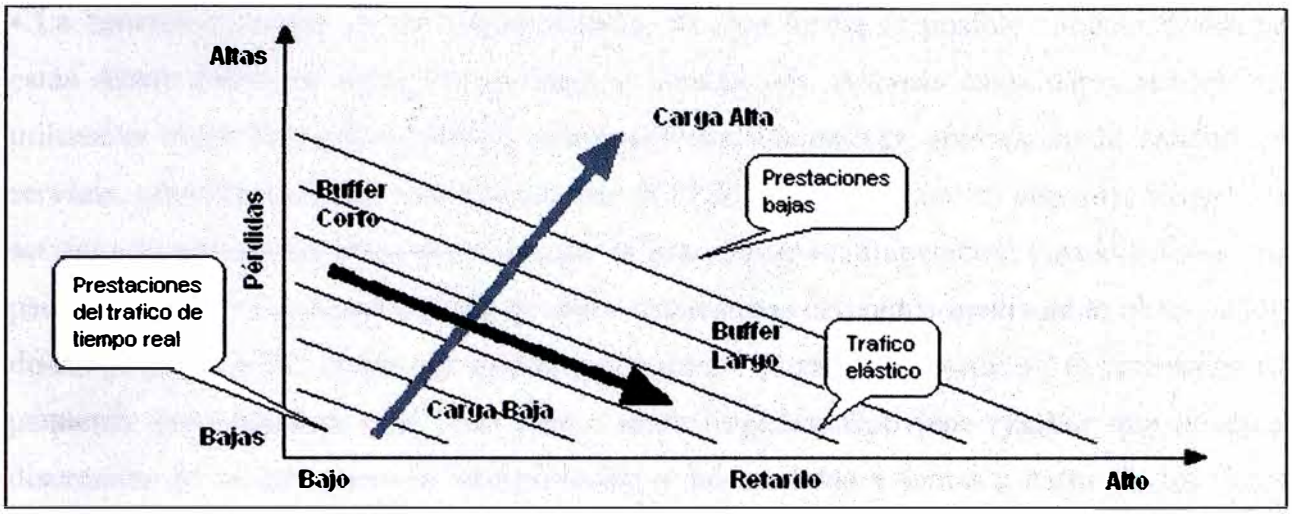

Fig. 1.7 Relación de Perdidas Vs Retardo

En este sentido, el protocolo RTP proporciona una serie de mecanismos para cumplir su función:

- Proporciona un campo Payload Type que permite identificar el formato del tipo de datos incluido en el paquete de datos de RTP, bien asociando nosotros mismos los valores del PT a ciertos formatos, o bien siguiendo la RFC 3551, donde se proporciona una lista de formatos y sus valores asociados, de forma análoga a como ocurre con los well-known ports de TCP.
- Marca los paquetes de datos con un número de secuencia, teniendo en cuenta que éstos viajan sobre UDP y que pueden llegar desordenados o incluso no llegar, esto proporciona un mecanismo que permite ordenar los paquetes en el destino y saber cuáles y cuántos faltan.
- Implementa una marca de tiempo (timestamp) a partir del reloj de muestreo del emisor, que permite al receptor detectar error de jitter (variación de la latencia) y tomar las medidas adecuadas.
- Tiene campos en su cabecera para identificar cada una de las fuentes dentro de una misma sesión RTP, y para identificar qué fuentes han contribuido en la carga del paquete de datos.
- Al ir encapsulados sobre UDP, los paquetes RTP aprovechan las capacidades del mismo con respecto a la detección de errores (checksum) y multiplexación.

Por su parte, el protocolo RTCP se encarga del control y monitorización del flujo de datos RTP, mediante la transmisión de paquetes de control periódicamente a todos los participantes. Éstos tienen las siguientes funciones:

• La función principal es de realimentación, de esta forma es posible conocer dónde se están dando fallos, si éstos son globales o locales, etc. Además estos datos pueden ser utilizados como base para realizar codificaciones adaptativas, mejorando la calidad de servicio ofrecida (aunque recordemos que RTP/RTCP no garantiza ninguna calidad de servicio determinada). Para poder ejercer la función de realimentación correctamente, los paquetes RTCP se generan a partir de datos estadísticos obtenidos mediante la observación de los paquetes RTP, como por ejemplo, el número de paquetes perdidos, el porcentaje de paquetes desordenados, o el jitter medio entre llegadas. Conviene resaltar que queda a discreción de la aplicación la interpretación y las medidas a tomar a partir de los datos recolectados mediante RTCP.

• Más funciones de RTCP incluyen dar nombres canónicos a los usuarios por si cambian su identificador de fuente, controlar el flujo de paquetes RTCP en función de el número de usuarios de la sesión (por motivos de escalabilidad), y por último, proporcionar información de control sobre la sesión, por ejemplo sobre qué usuarios hay presentes, para uso de las aplicaciones involucradas.

1.4 CODEC's

Los paquetes de voz (y en su caso de vídeo) son transportados por RTP codificados de alguna manera [2]. Esta codificación determina el ancho de banda utilizado y la calidad de la comunicación. Generalmente se requiere que los interlocutores negocien el mismo códec para poder comunicarse, lo que tiene consecuencias en la interoperabilidad de los terminales. Veamos a continuación los códecs más conocidos y utilizados, con sus características más relevantes.

1.4.1 Audio

La gran mayoría de las aplicaciones de telefonía de VoIP, implementan la recomendación G.711 del CCITT de 1984, diseñada para transportar telefonía digital en canales de 64 Kbps, codificando muestras independientemente (Pulse-Coded Modulation o PCM) de forma no lineal (leyes A y μ). Recomendada para redes con ancho de banda suficiente, suele usarse como referencia de calidad para otros métodos que comprimen las muestras basándose en su historia. Se describe la características de cada CODEC en la tabla N° 1.4.

G.726 es una codificación adaptativa diferencial (ADPCM) a diferentes tasas de bit. Su rendimiento y calidad a 40 Kbps son comparables a G.711. A tasas de error altas, puede tener una calidad subjetiva mayor, tanto a 40 Kbps como a 32 Kbps. Antecesor suyo es G.721, que sólo funciona a 32 kbps. Este códec lo implementa Gnomemeeting, y algunas aplicaciones más, sin embargo, su difusión es más limitada que la del G.711.

G.728 comprime según una Low-Delay Code Excited Linear Prediction (LD-CELP), usándose a 16 Kbps. Comparado con G.721, G.728 tiende a ser objetivamente peor, pero es mejor en pruebas subjetivas. Tiende a funcionar peor en presencia de ruido.

G.723.1 provee de dos tasas distintas (5.3 y 6.4 Kbps). Además la velocidad en cada sentido no tiene porqué ser la misma y puede variar entre tramas. Con respecto a los códecs G.729/G.729A, ofrece tonos DTMF (los tonos utilizados por la marcación telefónica digital) con menor distorsión, lo cual permite mayor fiabilidad al acceder a servicios de red inteligente en telefonía, por ejemplo.

G.729 es un códec compresor de tipo Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP). El G.729 es una versión de complejidad reducida. Se desarrolló para usarse en situaciones de multimedia con voz y datos. Una versión mejorada de este codec es el G729r8 que además de utilizar compresión CELP (Code-Excited Linear Prediction) codificando la voz en tramas de 8 kbps.

Tabla N° 1.4 Tabla de codecs de audio

Nombre	Tasa binaria (kbps)	Tamaño de paquete (octetos sin cabeceras)	Duración de un paquete (ms)	Puntuación MOS
G.711	64	160	20	4.1
G.723.1	5.3/6.4	24	30	3.65/3.9
G.726	16/24/32/40	80	20	3.85 para 32 kbps
G.728	16	60	30	3.61
G.729	8	20	20	3.9

1.4.2 Vídeo

H.261 es un estándar de vídeo publicado por la ITU (International Telecom Union) en 1990. Fue diseñado para tasas de bit múltiplos de 64. Se diseñó con líneas RDSI en mente, de ahí este valor. Es un híbrido de predicción entre tramas, codificación transformada y compensación de movimiento. Funciona entre 40 kbps y 2 Mbps. Soporta dos resoluciones distintas, QCIF (Quarter Common Interchange format, 176x144) y CIF (Common Interchange format, 352x288).

H.263 es una versión mejorada de H.261. Fue diseñado para bajas velocidades, pero se amplió a grandes rangos de tasas de bit. Se supone que reemplazará a H.261 en muchas aplicaciones. Soporta cinco resoluciones distintas, QCIF, CIF, SQCIF (mitad de resolución que QCIF), 4CIF y 16CIF (cuatro y dieciséis veces la resolución de CIF, respectivamente). Estas altas resoluciones implican que puede incluso competir con los estándares MPEG.

Ambos algoritmos son los más utilizados (de hecho, son casi los únicos que se utilizan) en las aplicaciones que requieren vídeo, hay que hacer notar que el uso de H.263 a resolución CIF o superior implica que un terminal H.323 ha de ser capaz de proporcionar H.261 CIF. En otras palabras, si un terminal H.323 implementa el códec H.263 ha de implementar al menos el códec H.261 a la misma resolución, por razones de compatibilidad.

Tabla N° 1.5 Tabla de códecs de vídeo

Nombre	Tasa binaria (kbps)	Imagen por segundo	Resoluciones soportadas
H.261	P * 64 (P=1..30) (Valor típico 384)	29.97/mpi, (mpi=1..4)	CIF (352x288), QCIF (176x144)
H.263	P * 0.1 (P=1..192)	29.97/mpi, (mpi=1..32)	CIF (352x288), QCIF (176x144), SQCIF (128x96), 4CIF (704x576), 16CIF (1408x1152)

Tasa binaria: P es sencillamente un factor de escala, la tasa de estos códecs es múltiplo de 64 kbps.

Imágenes por segundo: mpi (minimum picture interval) es el mínimo intervalo entre fotogramas, evidentemente, cuanto menor sea mayor será la tasa de imágenes por segundo.

1.5 Norma H.323

La norma H.323 [3] fue creada por el ITU-T, y en realidad es una norma paraguas, es decir, no es un protocolo en sí mismo, sino una familia de protocolos que interactúan entre sí para proveer un servicio, en este caso telefonía o servicios de videoconferencia IP. Como tal no nos vamos a centrar en desglosar los distintos protocolos que la componen, sino que a medida que éstos nos resulten relevantes en nuestro estudio, los iremos incluyendo proporcionando los detalles necesarios para entenderlos.

1.5.1 Red básica H.323

En su forma más sencilla, una red H.323 consta únicamente de terminales (al menos dos), entendiéndose por terminal un cliente que implementa el protocolo H.323, bien de forma hardware (el caso de un teléfono IP, por ejemplo), bien como aplicación de software (también llamados softphones). Cada cliente ha de implementar parte de la familia de protocolos H.323, en concreto los siguientes protocolos son necesarios:

- El protocolo H.225.0, variante evolucionada del Q.931, que se encarga del establecimiento y señalización de la llamada. Es de notar que, inicialmente, las implementaciones H.323 utilizaban el protocolo Q.931 directamente para esta tarea; con el tiempo y atendiendo a las necesidades específicas de VoIP, se modificó para ajustarse a las nuevas necesidades, dando como resultado el H.225.0, que es compatible en sus funciones más básicas con el anterior, aunque por supuesto se recomienda que las nuevas implementaciones utilicen el más moderno de los dos.
- Mención especial merece el protocolo RAS (Registration/Admission/Status), que se utiliza para la comunicación de un terminal H.323 con otro elemento, llamado GateKeeper, que será introducido en la siguiente sección. Baste por ahora con saber que es una entidad encargada entre otras cosas de gestionar a un cierto número de terminales. Dicho protocolo es parte de H.225.0, y ha de implementarse obligatoriamente en un cliente, dado que si existe un GateKeeper en la red, hay obligación de usarlo.
- El protocolo H.245, que se encarga del control de uso del canal y de la negociación de capacidades entre los terminales.

• Por supuesto, también ha de implementar la pareja de protocolos RTP/RTCP, para el envío de información (vídeo y audio) en tiempo real.

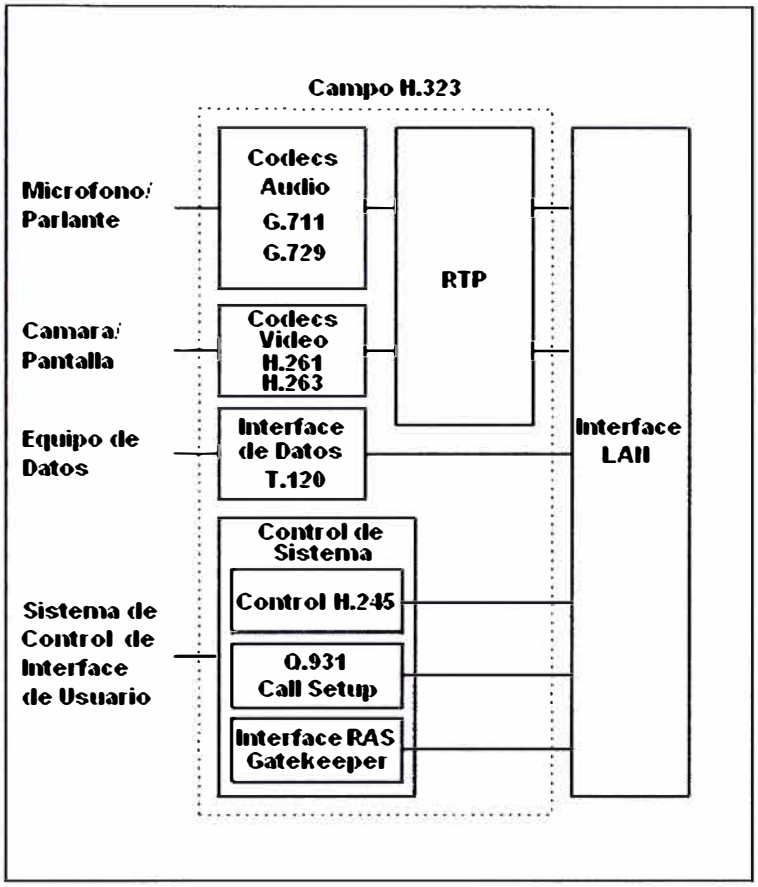

Fig. 1.8 Terminal H.323

Además de todas estas condiciones, un cliente puede también implementar otras capacidades, como el envío de datos mediante el protocolo T.120 u otras, como soporte para multiconferencia, por ejemplo.

Centrémonos, pues, en las capacidades que ha de tener la red subyacente para proveer de un servicio H.323. En este sencillo escenario, en el que sólo intervienen los terminales, el único requisito que se pide al nivel de transporte es poder enviar y recibir datagramas UDP, no habiendo ningún requisito especial en el nivel de red. No obstante, más adelante tendremos en cuenta el uso de proxies, firewalls, y/o sistemas de NAT/PAT (Network y Port Address Translation), elementos no transparentes a la red, que pueden impedir la comunicación H.323 entre extremos, por los motivos que en su momento veremos.

Cabe destacar a este respecto lo ya mencionado: se trata de una red best-effort, por tanto no se garantiza la calidad de servicio, aunque la familia de protocolos H.323 y los protocolos RTP/RTCP intenten maximizar los recursos de la misma y dar el mejor servicio posible.

Pasemos entonces a analizar una comunicación H.323. Esto nos va a servir entre otras cosas, además de profundizar en el funcionamiento del protocolo, para detectar con qué elementos podemos jugar a la hora de intentar garantizar una cierta calidad de servicio, objetivo último de la red que se pretende desplegar.

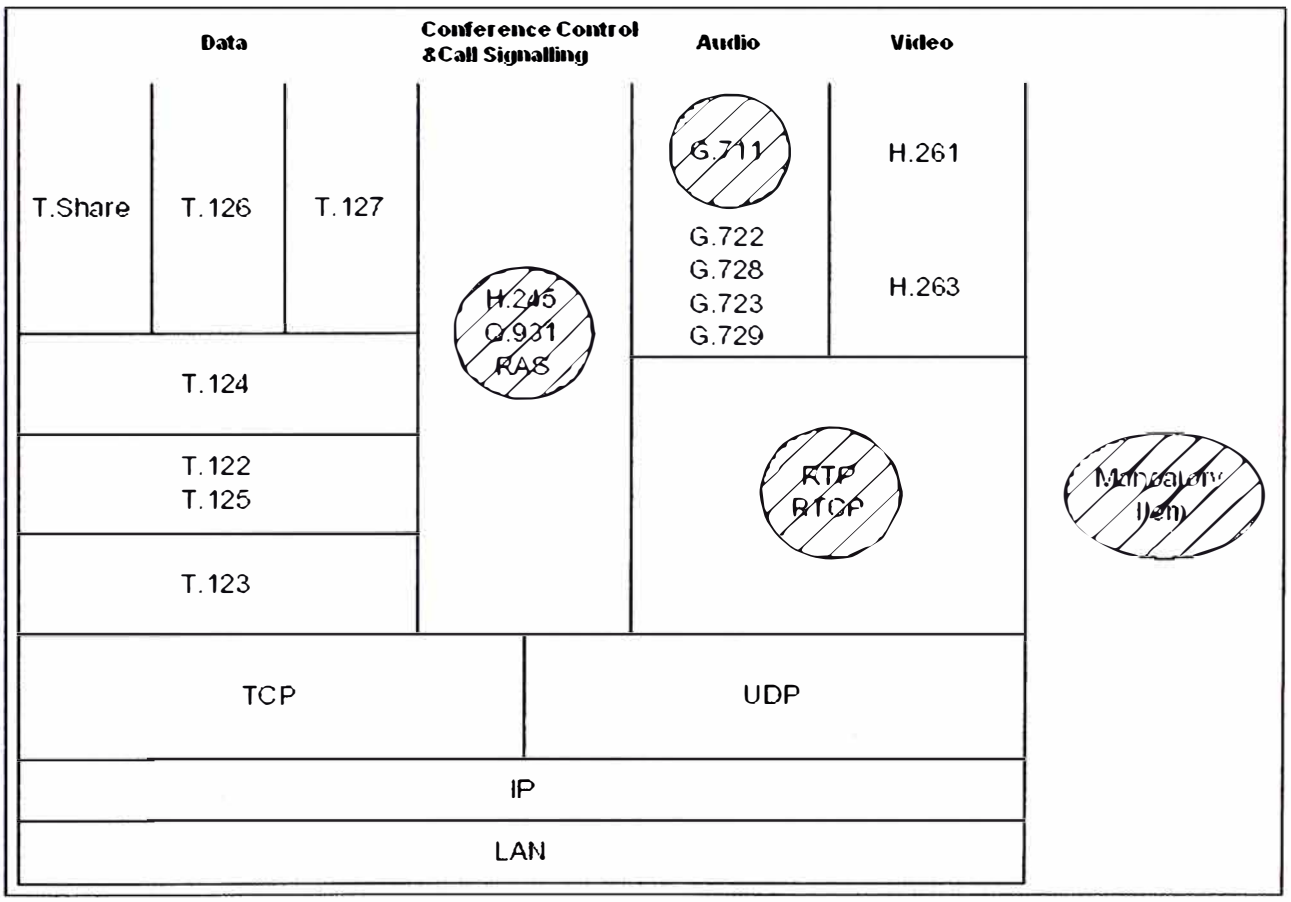

Fig. 1.9 Torre de protocolos

Para iniciar una comunicación H.323, se establece una conexión de control, la que lleva los mensajes de establecimiento y señalización H.225.0. Lo habitual para esto es utilizar el puerto TCP 1720, aunque a continuación veremos algunas variantes. Se seleccionan entonces dinámicamente los puertos a usar, escogidos de entre el rango de 1024-65535, por un lado el canal de control, con el protocolo H.245, en un puerto TCP, y por otro los

canales de audio y/o vídeo, asignando los puertos necesarios para RTP y RTCP, pero éstos son UDP (se necesitan una pareja de puertos en cada sentido, para cada flujo de datos, siendo x el puerto RTP, par, y x+1 su correspondiente RTCP, impar).

Alternativamente, existe la opción de encapsular los mensajes del protocolo H.245 sobre el canal H.225.0, ahorrando de esta forma el establecimiento de una conexión más. Y si además se utiliza un puerto UDP en vez de establecer una conexión TCP para el canal H.225.0, tenemos lo que se conoce como procedimiento Fast-Connect, que es el método más rápido que existe para establecer una conexión H.323, igualando en velocidad de establecimiento al protocolo SIP.

Resumiendo, no es necesario hacer nada en especial para habilitar las conferencias H.323 sobre una red TCP/IP, salvo disponer de los terminales preparados para efectuar y recibir llamadas. Sólo en el caso de tener elementos no transparentes habrá que tomar medidas para que éstos no sean un obstáculo. Eso sí, la calidad de servicio no está ni mucho menos garantizada, aunque H.323 apoyándose en RTP/RTCP permite adaptar el uso del canal al ancho de banda disponible, mediante la renegociación de códecs, por ejemplo.

1.5.2 Red H.323 con Gatekeeper

Un GateKeeper es una entidad H.323 que se encarga, necesariamente, de las siguientes funciones:

- Traducción de direcciones: de aliases H.323 a sus correspondientes direcciones reales.

H.323 soporta numerosas formas de identificación de usuario, soporta varios tipos de direccionamiento (DNS, ENUM, TRIP), de forma que un usuario se puede registrar en el GateKeeper dejando como identificador un nombre escogido por él (o por el GateKeeper) con su número de teléfono, por ejemplo, y otro puede hacerlo dejando un URL similar a una dirección de correo electrónico. El GateKeeper se encarga pues de la función de traducir el nombre del usuario que un llamante quiere localizar a su correspondiente dirección real.

- Control de admisión: permite o no registrarse a los clientes de la LAN en función de varios criterios.

En principio H.323 fue diseñado con redes de área local en mente, extendiéndose su ámbito más adelante a redes de área extensa. Aún así, la idea original de situar un

GateKeeper en cada LAN persiste, aunque no sea necesariamente así. Un cliente puede registrarse en cualquier GateKeeper que se lo permita, éste mantiene un directorio con la dirección real del cliente y el alias H.323 que éste está utilizando. Los criterios de admisión pueden ser desde permitir registrarse a cierto tipo de direcciones hasta por ejemplo admitir un número máximo de clientes registrados.

- Control de ancho de banda: para la gestión del ancho de banda disponible.

El GateKeeper puede denegar a un cliente el establecer una conferencia si estima que todo el ancho de banda de una conexión está siendo utilizado, por ejemplo, esto puede servir para ayudar a mantener una cierta calidad de servicio.

- Gestión de zona: el GateKeeper ofrece sus servicios a los elementos H.323 que se hayan registrado en su zona de control.

La zona de un GateKeeper se define sin más como el conjunto de entidades H.323 que se hayan registrado en el mismo. Aunque teóricamente hay uno por zona, como se desprende de la propia definición de zona, se pueden establecer GateKeepers alternativos para mayor robustez frente a fallos y balance de carga.

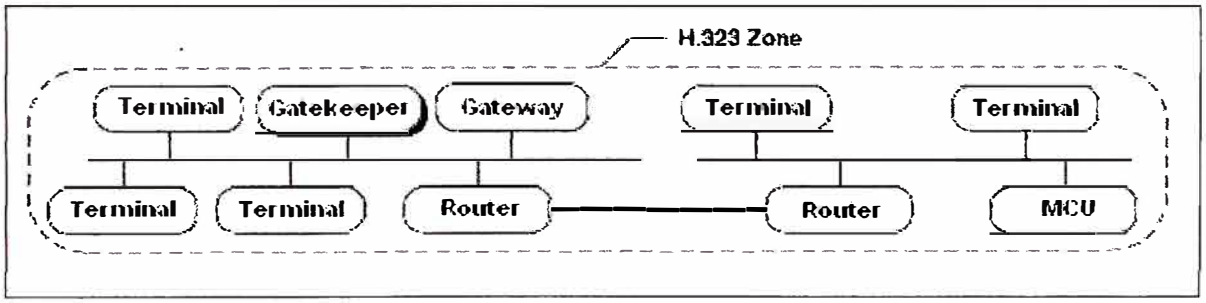

Fig. 1.10 Zona de un GateKeeper

El uso de un Gatekeeper en la red H.323 es opcional, pero si hay uno, ha de ser utilizado. Es decir, cuando un cliente H.323 se pone en funcionamiento, automáticamente busca un GateKeeper. Si no lo encuentra, no se registra con él y además de no recibir ninguno de los servicios asociados al mismo, ha de proporcionar direcciones reales para la red donde está ubicado.

1.6 RDSI

RDSI permite que las señales digitales se transmitan a través del cableado telefónico existente. Esto se hizo posible cuando se actualizaron los switches de la compañía telefónica para que manejaran señales digitales. RDSI generalmente se considera como una alternativa para las líneas arrendadas, que se pueden utilizar para el trabajo a distancia y conectar mediante networking oficinas pequeñas y remotas en las LAN como se muestra en la figura 1.11.

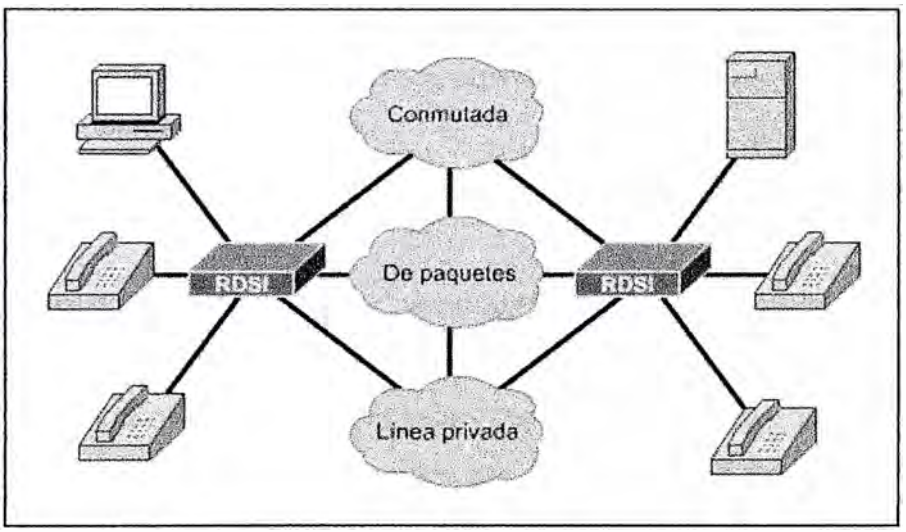

Fig. 1.11 Descripción General de la RDSI.

Las compañías telefónicas desarrollaron RDSI como parte del esfuerzo por estandarizar los servicios para los abonados. Esto incluía la interfaz de red de usuario (UNI), que es la vista de la pantalla cuando el usuario marca a la red y las capacidades de red. La estandarización de los servicios para el abonado hace que sea posible asegurar la compatibilidad internacional. Los estándares RDSI definen los esquemas de hardware y de configuración de llamadas para la conectividad digital de extremo a extremo, que ayudan a cumplir con el objetivo de lograr conectividad a nivel mundial al asegurar que las redes RDSI se puedan comunicar fácilmente entre sí. Básicamente, la función de digitalización se realiza en el sitio del usuario en lugar de realizarse en la compañía telefónica.

La aptitud de RDSI para otorgar conectividad digital a los sitios locales tiene muchas ventajas, incluyendo las siguientes:

* RDSI puede transportar una gran variedad de señales de tráfico de usuario. RDSI permite acceder a servicios de vídeo digital, de datos conmutados por circuito y los servicios de la red telefónica utilizando la red telefónica normal, que es conmutada por circuito.
* RDSI ofrece una configuración de llamada mucho más rápida que las conexiones de módem porque utiliza señalización fuera de banda (canal D, o de datos). Por ejemplo, algunas llamadas RDSI se pueden establecer en menos de un segundo.
* RDSI suministra una velocidad de transferencia de datos mucho más rápida que la de los módems al utilizar el canal principal (canal B de 64Kbps). Con múltiples canales B, RDSI brinda a los usuarios más ancho de banda en las WAN que algunas líneas arrendadas. Por ejemplo, si fuera a utilizar dos canales B, la capacidad de ancho de banda es de 128Kbps, ya que cada canal B administra 64Kbps.
* RDSI puede suministrar una ruta de datos limpia a través de la que se pueden negociar los enlaces PPP.

Sin embargo, en la fase de diseño debe asegurarse de que el equipo seleccionado cuente con un conjunto de funciones que aproveche la flexibilidad de RDSI. Además, debe tener en cuenta las siguientes cuestiones relacionadas con el diseño RDSI:

* Temas de seguridad: Como en la actualidad los dispositivos de red se pueden conectar a través de la Red pública de telefonía conmutada (PSTN), es fundamental diseñar y confirmar un modelo de seguridad sólido para proteger la red.
* Temas de costo y contención: Uno de los objetivos principales de la selección de RDSI para la red es evitar el costo de los servicios de datos de tiempo completo (como las líneas arrendadas o Frame Relay). Por lo tanto, es sumamente importante evaluar los perfiles de tráfico de datos y monitorear los modelos de uso de RDSI para asegurarse de que los costos de WAN estén controlados.

1.6.1 Componentes básicos de RDSI

Los componentes de RDSI incluyen terminales, adaptadores de terminal (TA), dispositivos de terminación de red (NT), equipo de terminación de línea y equipo de terminación de central telefónica. La tabla N°1.6 suministra un resumen de los componentes de RDSI. Las terminales RDSI vienen en dos tipos, Tipo 1 o Tipo 2, como se indica en la figura 1.12.

Tabla N°1.6 Componentes de RDSI

COMPONENTE	DESCRIPCION
Equipo Terminal Tipo 1 (TE1)	Designa un dispositivo que es compatible con la red RDSI. Un TE1 conecta a una terminación de red de tipo 1 o tipo 2.
Equipo Terminal Tipo 2 (TE2)	Designa un dispositivo que no es compatible con RDSI y requiere un adaptador de Terminal.
Adaptador de Terminal (TA)	Convierte señales eléctricas estándar a la forma utilizada por RDSI, de manera que los dispositivos que no son de RDSI se puedan conectar a la red RDSI.
Terminación de Red Tipo 1 (NT1)	Conecta el cableado de suscriptor de RDSI de cuatro cables a la instalación convencional de dos cables de loop local.
Terminacion de Red Tipo 2 (NT2)	Dirige el tráfico desde y hacia diferentes dispositivos de suscriptor y NT1. La NT2 es un dispositivo inteligente que realiza conmutación y concentración.

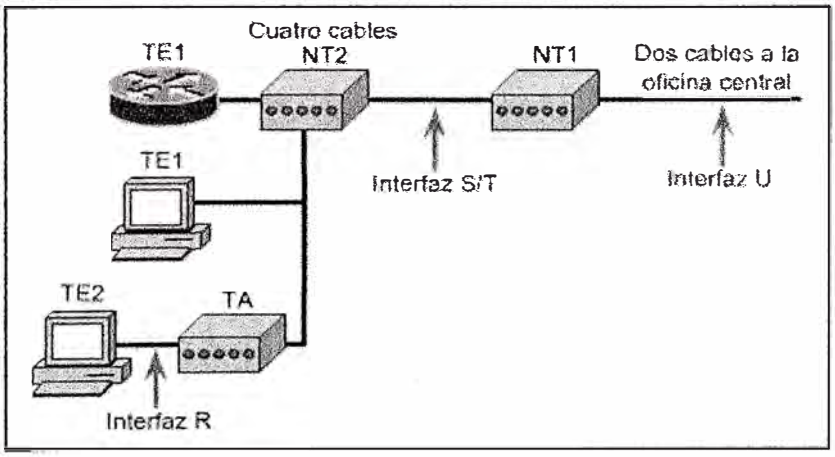

Fig. 1.12 Red Digital de Extremo a Extremo para Datos, Fax, Voz y Video.

RDSI cuenta con cuatro puntos de referencia:

* Punto de referencia R, referencia la conexión entre un dispositivo no compatible con RDSI y un TA.
* Punto de referencia S, referencia los puntos que se conectan a NT2 o dispositivo de conmutación del cliente, es la interfase que habilita las llamadas entre las diferentes partes del CPE.
* Punto de referencia T, eléctricamente idéntica a la interfase S, una interfase T referencia la conexión saliente desde la NT2 a la red RDSI o NT1.
* Punto de referencia U, referencia la conexión entre la NT1 y la red RDSI de propiedad de la compañía telefónica, este punto es relevante solo en América del Norte donde la función NT1 no es suministrada por el proveedor del servicio.

Las terminales especializadas RDSI se denominan equipo de Terminal de tipo 1 (TE1). Las terminales que no son RDSI, como el equipo Terminal de datos (DTE), más antiguos que los estándares RDSI, se denominan equipo de Terminal de tipo 2 (TE2). Los TE1 se conectan a la red RDSI a través de un enlace digital de par trenzado de cuatro hilos. Los TE2 se conectan a la red RDSI a través de un TA. El TA RDSI puede ser un dispositivo autónomo o una placa dentro del TE2. Si el TE2 se implementa como un dispositivo autónomo, se conecta al TA a través de una interfaz estándar de la capa física.

Más allá de los dispositivos TE1 y TE2, el siguiente punto de conexión en la red RDSI es el dispositivo de terminación de red de tipo 1 (NT1) o de terminación de red de tipo 2 (NT2) Estos son dispositivos de terminación de red que conectan el cableado de cuatro hilos del abonado con el loop local de dos hilos convencional. En Estados Unidos, NT1 es un dispositivo del equipo Terminal del abonado (CPE). En la mayoría de los países del mundo, además de Estados Unidos, NT1 forma parte de la red suministrada por la portadora. NT2 es un dispositivo más complicado, que habitualmente se encuentra en las centrales telefónicas privadas (PBX) digitales, que ejecutan servicios de protocolo de Capa 2 y Capa 3. También hay un dispositivo NT1/2, que es un dispositivo único que combina las funciones de NT1 y NT2.

1.6.2 Servicios RDSI: BRI y PRI

Hay dos servicios RDSI: BRI y PRI El servicio BRI RDSI ofrece dos canales B de 8 bits y un canal D de 2 bits, que a menudo se denominan 2B+D, como se indica en la figura. La BRI RDSI suministra un ancho de banda total de una línea de 144 kbps en tres canales

individuales (8000 tramas por segundo*(2*canales B de 8 bits+canal D de 2 bits)=8000*18 = 144kbps). El servicio del canal B de BRI opera a 64 kbps (8000 tramas por segundo*canal B de 8 bits) y está diseñado para transportar datos de usuario y tráfico de voz.

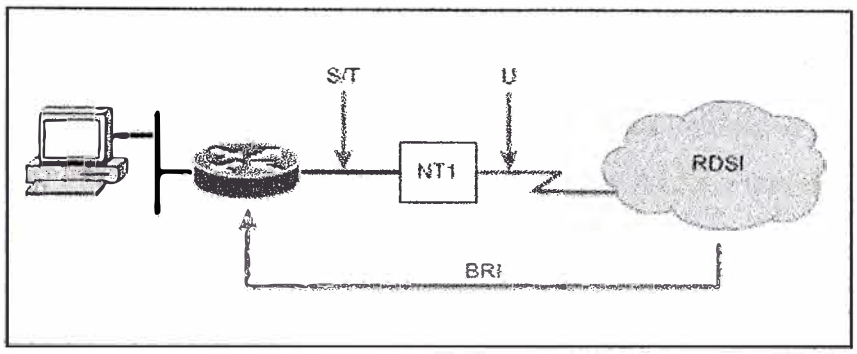

Fig. 1.13 Establecimiento de conectividad BRI

RDSI suministra más flexibilidad al diseñador de la red dada su capacidad para utilizar cada uno de los canales B para aplicaciones individuales de voz y/o datos. Por ejemplo, un documento de gran tamaño se puede descargar desde la red corporativa a través de un canal B de 64 kbps RDSI, mientras que el otro canal B se utiliza para conectarse y visitar una página Web.

El tercer canal, denominado canal D (de datos), es un canal de señalización de 16 kbps (8000 tramas por segundo *canal D de 2 bits) que se utiliza para transportar instrucciones que le indican a la red telefónica cómo debe administrar cada uno de los canales B. El servicio del canal D de BRI opera a 16 kbps y está diseñado para transportar información de control y señalización, aunque en determinados casos puede soportar la transmisión de datos de usuario. El protocolo de señalización del canal D se produce en las Capas 1 a 3 del modelo de referencia OSI.

Las terminales no pueden transmitir al canal D a menos que antes detecten una cantidad específica de unos (que indica que no hay señal) correspondiente a una prioridad preestablecida. Si el TE detecta un bit en el canal de eco (E) que es diferente de los bits D, debe dejar de transmitir inmediatamente. Esta técnica sencilla asegura que solamente una terminal pueda transmitir su mensaje D por vez. Esta técnica es similar y tiene el mismo efecto que la detección de colisiones en las LAN Ethernet. Después de que la transmisión del mensaje D se realiza con éxito, la prioridad de la terminal se reduce ya que se requiere que detecte una mayor cantidad de unos continuos antes de realizar la transmisión. Las

terminales no pueden elevar su prioridad hasta que todos los demás dispositivos en la misma línea hayan tenido oportunidad de enviar un mensaje D. Las conexiones telefónicas tienen mayor prioridad que todos los demás servicios, y la información de señalización tiene mayor prioridad que la información que no corresponde a la señalización.

El servicio de PRI RDSI ofrece 23 canales de 8 bits y 1 canal D de 8 bits más 1 bit de entramado en América del Norte y Japón, lo que significa una velocidad binaria total de 1,544 Mbps (8000 tramas por segundo * (23 * canales B de 8 bits + canal D de 8 bits + 1 bit de entramado) = 8000*8*24,125 = 1,544 Mbps) (el canal D de PRI funciona a 64 kbps). PRI RDSI en Europa, Australia y otras partes del mundo suministran 30 canales B de 8 bits más un canal D de 8 bits más un canal de entramado de 8 bits, lo que otorga una velocidad total de interfaz de 2,048 Mbps (8000 tramas por segundo* (30*canales B de 8 bits + canal D de 8 bits + canal de entramado de 8 bits) = 8000*8*32 =2,048 Mbps).

En T1/E1 y en las tramas de velocidad de datos superiores los canales B se mueven en línea como los furgones en un tren de carga. Al igual que los furgones en un patio de maniobras, los canales B se reacomodan y se desplazan a otras tramas a medida que atraviesan la Red pública de telefonía conmutada (PSTN) hasta que llegan a su destino. Esta ruta a través de la matriz del switch establece un enlace síncrono entre los dos extremos finales. Esto permite comunicaciones de voz continuas sin pausas, datos descartados o degradación. RDSI saca provecho de esta estructura de transmisión digital para la transferencia de datos digitales.

CAPITULO II
ESCENARIOS

El diseño de una red de alta disponibilidad es lo ideal para cualquier empresa donde la información es fundamental para su crecimiento, tal sea el caso de cadenas de tiendas como supermercados, ferreterías, boticas, etc. El propósito del diseño de esta red es mantener el intercambio de información de datos de manera permanente entre sedes. El escenario para nuestra red es como se muestra en la Fig. 2.1:

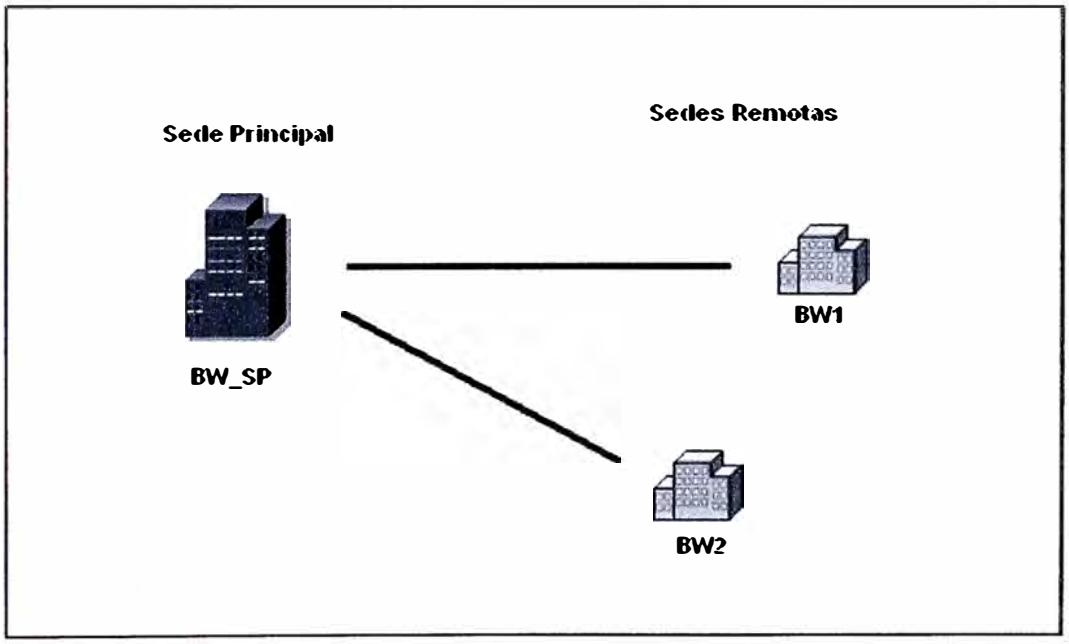

Fig. 2.1 Escenario de Red

Las sedes remotas se comunicaran a través de la sede principal.
En condiciones normales, la relación de ancho de banda entre sedes es:

$$BW\_SP = BW(a) + BW(b) \quad \text{.....(3.1)}$$

Donde:

BW_SP: Es el ancho de banda a contratar para la sede principal.
BW(a): Es el ancho de banda a contratar para la sede A.
BW(b): Es el ancho de banda a contratar para la sede B.

2.1 Tecnologías de red.

El empleo de contenidos multimedia ha obligado a que las infraestructuras de red cada vez hayan ido ofreciendo un mayor ancho de banda que facilitase la transmisión de este tipo de contenidos sin saturar los enlaces. Es por esto que cada vez han ido apareciendo tecnologías que consiguen un mayor ancho de banda tanto en entornos de red de área local como de área extensa, por tanto el proveedor de los enlaces a arrendar deberá contar con una infraestructura de red basadas en una de las siguientes tecnologías para nuestra red **WAN** (Wide Area Network):

RDSI (Red Digital de Servicios Integrados)
SDH (Sincronous Digital Hierarchy)
Frame Relay
ATM (Asynchronous Transfer Mode)
MPLS (Multiprotocol Label Switching)

Para las redes de área local (LAN) en cada sede, estas deberán estar implementadas en tecnología Ethernet.

CAPITULO III
REQUERIMIENTOS

3.1 Principales requerimientos

1. Integrar sus sedes a través de una red IP para el transporte de voz, video y datos.

2. Centralizar consumos de telefonía (voz) a través de una sede central.
Para esto se implementará una solución completa de VoIP que integre:
2.1 Habilitar 4 puertos de Voz FXO en el router de la sede principal.
2.2 Distribuir las 4 líneas analógicas de la sede principal en las sedes remotas de acuerdo a la demanda de estas líneas.

La aplicación de comunicación de voz tiene presente el desarrollo y crecimiento de la empresa, dado que el hardware ha implementar tiene una capacidad de escalabilidad muy importante.

3. Implementar aplicaciones de Videoconferencia de oficina en cada sede, reservando un ancho de banda de 256kbps para esta aplicación, de acuerdo al requerimiento promedio del fabricante de equipos de videoconferencia Polycom V500, para cada sede remota.

4. Aplicar Calidad de Servicio a través de políticas de calidad priorizando las aplicaciones en tiempo real como es el caso para el tráfico de voz y de video para garantizar un servicio sin problemas de calidad en las comunicaciones entre sedes.

Para esto se usa DSCP (Diferenciated Services Code Point) en la configuración de los equipos router Cisco en la implementación de estas policitas de Calidad de Servicio (QoS)

5. Se requiere que el proveedor de los enlaces privados maneje su Backbone con tecnología ATM (Asynchronous Transfer Mode), o en su defecó una red MPLS (Multiprotocol Label Switching) debido a que estas tecnologías permiten implementar soluciones propuestas en este informe de manera eficiente.

CAPITULO IV
IMPLEMENTACION DEL PROYECTO

A continuación detallamos los procesos realizados para la implementación del proyecto. Empezaremos con el diagrama general de la Red de Datos y la configuración de los puertos de voz (VoIP) en cada sede, la distribución de sus sedes, y luego iremos definiendo los diferentes aspectos que son importantes como el plan de numeración IP para la red de Datos, para finalmente llegar a la prueba de los servicios.

4.1 Diagrama del proyecto final

4.1.1 Diagrama de la red de datos

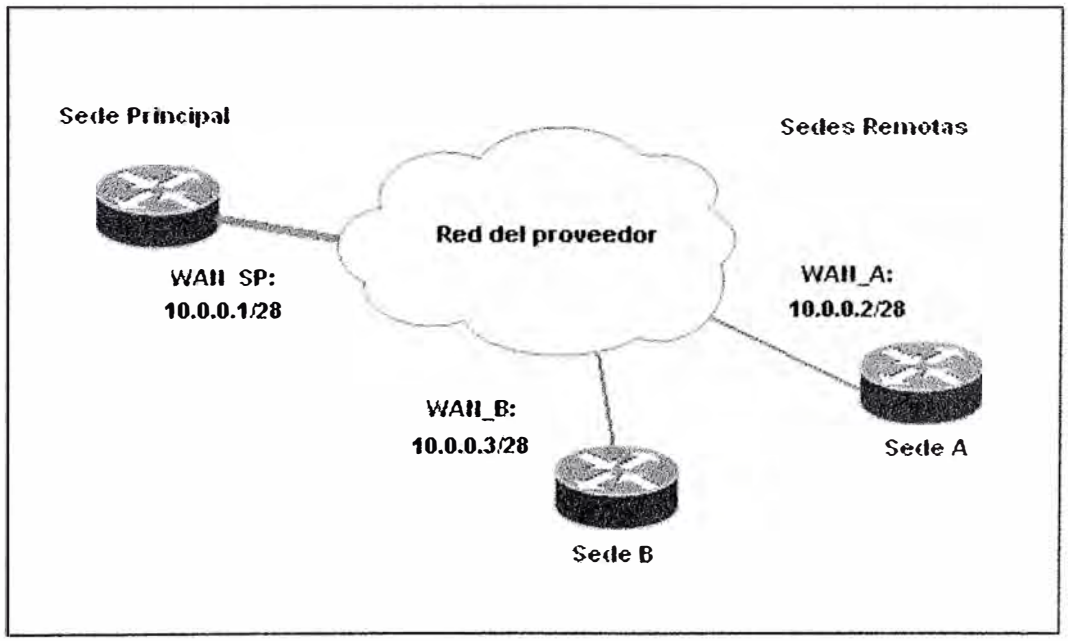

Fig. 4.1 Escenario de la red de datos

4.1.2 Diagrama de la red LAN en cada sede

En el escenario de la red local, se concentrará nuestros equipos de red, como servidores y computadoras personales de empleados de la empresa, y equipos de video, que para el esquema de red es transparente, puesto que es un equipo terminal mas, pero que sin embargo es fundamental el tratamiento de su trafico.

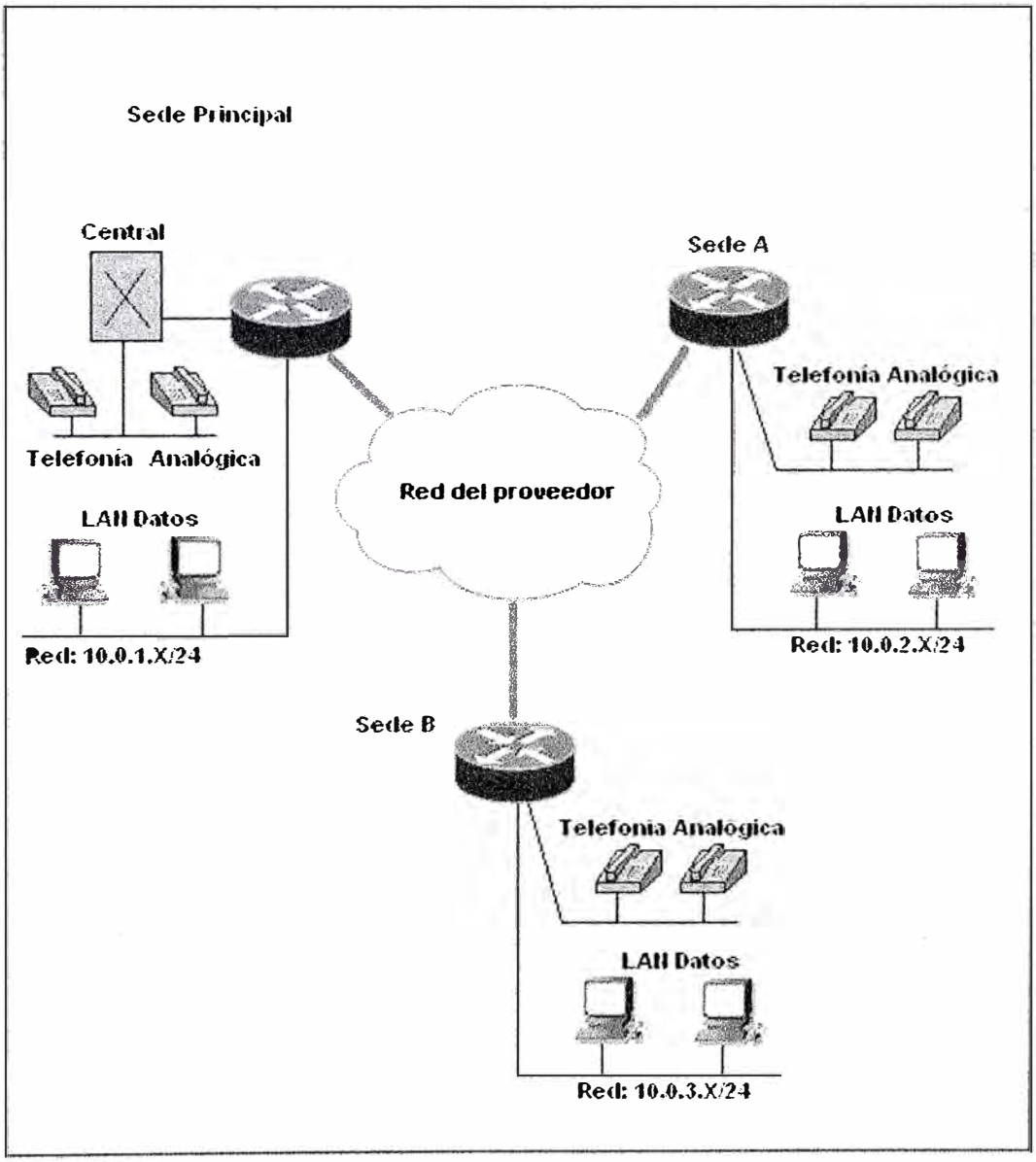

Fig. 4.2 Escenario de la red LAN

4.1.3 Diagrama de la red de contingencia RDSI

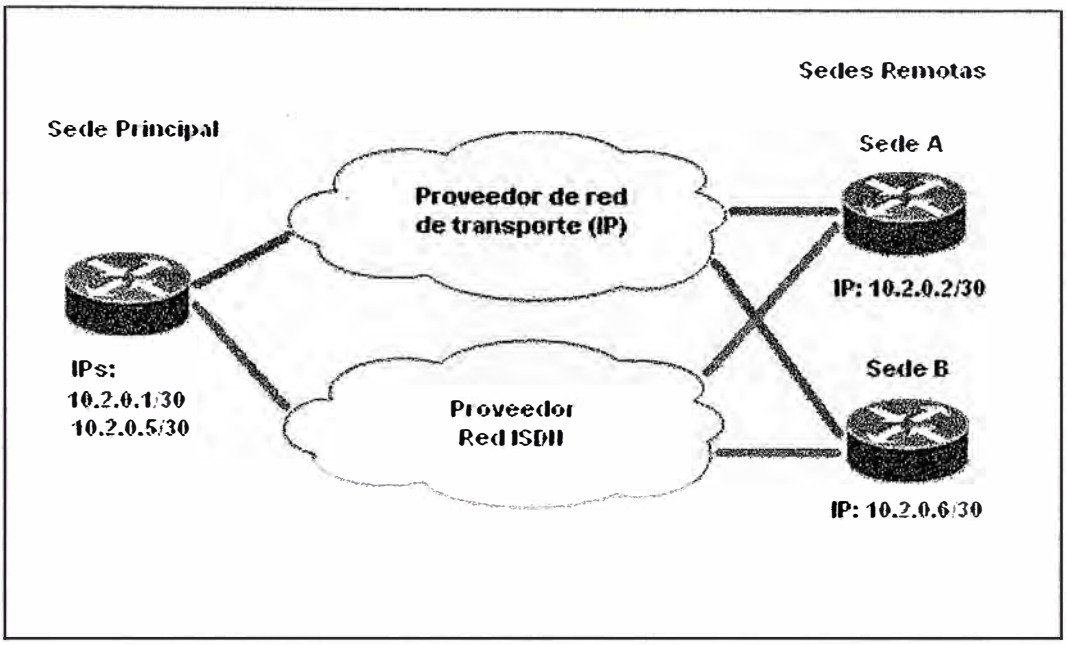

Fig. 4.3 Escenario de la red de contingencia RDSI

4.1.4 Topología de la red de datos

El sistema de VoIP debe ser implementada en la Sede Principal con los siguientes equipos: un router Cisco 2611XM como concentrador de las líneas telefónicas, las cuales se distribuirán en las 3 sedes remotas a través del enlace de datos.

Para esta finalidad el equipo router de la sede principal contará con 4 puertos de voz FXO, los cuales se recibirán las 4 líneas de la central telefónica, por este router central saldrían las llamadas a través de la central telefónica a la red pública (PSTN), implementándose también los números directos asignados a cada anexo interno en la Sede Principal como en las Sedes Remotas.

La red de Datos y la Red de VoIP, son manejadas por el router principal. La interfase WAN y LAN en este router principal es proporcionada por interfaces *FastEthernet.* Para la red de VoIP, se deberá habilitar una interfase Loopback para manejar el uso de políticas de calidad.

4.2 Distribución de las sedes

En este caso la relación de las sedes remotas con la sede principal esta dada por el ancho de banda que requiera cada sede, por tanto el ancho de banda a contratar para cada sede esta determinado por las aplicaciones que compartirá cada sede remota con la sede principal.

4.2.1 Calculo de ancho de banda para cada sede remotas

Para determinar el ancho de banda a contratar al proveedor, el cálculo se basará, considerando el ancho de banda de aplicaciones en tiempo real tal como la comunicación de Voz y aplicativos de video conferencia así como también trafico de datos. Por tanto el ancho de banda para cada sede remota por tipo de aplicación será:

$$BWr = X + Y + Z \text{ (kbps)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (4.2.1.1)$$

Donde:

X: Ancho de banda para la voz sobre IP (VoIP).

Y: Ancho de banda para aplicación de video conferencia.

Z: Ancho de banda para trafico de datos.

El ancho de banda reservado para el tráfico de VoIP, estará determinado por el número de canales (líneas) asi como también el tipo de CODEC a usar, y el tamaño de paquete de voz (payload). CISCO implementa diferentes tipos de CODECs de los cuales el que cuenta con la mejor relación calidad / compresión es el G729r8 trabajado con un payload de 40 bytes, dado que hace uso de 22kbps por canal de voz:

Tabla N° 4.1 Ancho de banda usado por el CODEC G729r8

Canales de Voz Telefonía	CODEC	Ancho de Banda usado por el CODEC G.729r8	Ancho de Banda
X	G729r8	22Kbps	X*22Kbps

El Ancho de banda para el aplicativo de Videoconferencia estará dado por el tipo de hardware y la inversión que el cliente desee usar, en el mercado existe aplicaciones de este

tipo que usan desde 56kbps a más, ancho de banda, sin embargo el ancho de banda determina la calidad de este tipo de aplicativo.

Para el tráfico de datos podremos separar en dos tipos:

$Z = Z1 + Z2$

Donde:

Z1: Trafico de aplicación de administración de la empresa.

Z2: Otro tipo de Trafico de datos como el de Internet (best effort)

4.2.2 Priorizacion de tráfico por tipo de aplicación

Asignando prioridades a cada tipo de tráfico:

Prioridad 1: P1 aplicativos de tiempo real.

Prioridad 2: P2 aplicativos críticos de la empresa como por ejemplo una aplicativo de Base de Datos.

Prioridad 3: P3 otros tipos de trafico como FTP, HTTP, etc.

Entonces tendremos:

P1 = X + Y

P2 = Z1

P3 = Z2

Por tanto el ancho de banda para una sede remota también esta dada por:

BWr = P1 + P2 + P3.

a. Ancho de banda para la aplicación de voip.

X = 2 * 22 kbps (2 canales de Voz)

X = 44 kbps

b. Ancho de banda para la aplicación de videoconferencia:

En este caso el valor del ancho de banda a usar, varia de acuerdo al tipo del aplicativo a usar, puesto que existe 3 tipos de aplicativos de videoconferencia: Desktop, Oficina y de Sala.

Para nuestro diseño, el tráfico reservado para la aplicación de video conferencia asignado será de 256 kbps.

Este ancho de banda permite correr una aplicación de videoconferencia de oficina de buena calidad (Polycom V500).

Entonces:

$$Y = 256 \text{ kbps.}$$

Por lo tanto el tráfico para aplicaciones en tiempo real será:

$$P1 = 256 + 44 \text{ (kbps)}$$

$$\mathbf{P1 = 300 \text{ kbps.}}$$

c. Ancho de banda para tráfico de datos:

Como comentamos anteriormente este tráfico se divide en dos tipos:

Z1: Trafico de datos críticos para la empresa, como una aplicación de BD.

Z2: Trafico de datos no críticos para la empresa Ej: FTP, HTTP, etc.

El administrador de red puede determinar el ancho de banda para el tráfico a reservar para Z1, mediante un analizador de red como el *Ethereal.*

Sí reservamos un ancho de banda de 128kbps, valor típico para este tipo de aplicaciones.

Entonces el valor de P2 es:

$$\mathbf{P2 = 128kbps.}$$

Por tanto el tráfico de datos del tipo Z2 es el tráfico con prioridad por defecto o P3, por tanto, es el que resta del ancho de banda contratado para cada sede. Entonces, en el caso que se contrate 512kbps en cada sede remota el tráfico Z2 con P3 es:

$$BWr = P1 + P2 + P3 \text{ (kbps)}$$

$$512 = 300 + 128 + P3 \text{ (kbps)}$$

$$\mathbf{P3 = 84 \text{ kbps}}$$

En la sede Principal:

Por defecto en la sede principal se hará uso de la relación de ancho de bandas con las demás sedes (ref. formula 2.1)

$$\mathbf{BW\_SP = BW(a) + BW(b)}$$

En la sede principal contaremos con un ancho de banda contratado de BW_SP, aplicando la relación descrita en la formula 4.2.1.1 tendremos:

BW_SP = BW(a) + BW(b)

BW SP = 2BW

BW_SP = 1024 kbps

De igual manera los tráficos priorizados están dados por:

P(i) = 2 * P(i)r

Donde P(i)r es el tipo de tráfico priorizado de la sede remota (A y B):

Entonces:

P1= 2 P1r

P1 = 2 * 300 kbps

P1 = 600 kbps

P2 = 2 P2r

P2 = 2 * 128 kbps

P2 = 256 kbps

P3 = 2 P3r

P3 = 2 * 84 kbps

P3 = 168 kbps

La calidad en las comunicaciones de Voz se dará, siempre y cuando se apliquen políticas de calidad para el tráfico de Voz, pues de no considerarlas, en caso de saturación del ancho de banda contratado, la calidad de las comunicaciones de voz se verán afectadas, estas se manifiestan como ruido y entrecortes en las comunicaciones establecidas.

4.3 Diseño de la red IP

En esta sección se asignará la Red IP para la WAN, red LAN, red de VoIP y la red RDSI para cada sede.

4.3.1 Asignamiento de las direcciones IP´s de la red WAN

Tabla N° 4.2 Direcciones IP de la red WAN

ÍTM	SEDE	IP WAN PRINC.	MASCARA
1	Principal	10.0.0.1	255.255.255.240
2	Sede A	10.0.0.2	255.255.255.240
3	Sede B	10.0.0.3	255.255.255.240

4.3.2 Asignamiento de las direcciones IP´s de la red LAN de datos

Tabla N° 4.3 Direcciones IP de la red WAN de datos (Enlace Principal)

ÍTM	SEDE	RED IP LAN	IP DG	MASCARA
1	Principal	10.0.1.X	10.0.1.1	255.255.255.0
2	Sede A	10.0.2.X	10.0.2.1	255.255.255.0
3	Sede B	10.0.3.X	10.0.3.1	255.255.255.0

Tabla N° 4.4 Direcciones IP de La red de video

ÍTM	SEDE	RED IP LAN	IP DG	MASCARA
1	Principal	10.0.20.X	10.0.20.1	255.255.255.0
2	Sede A	10.0.30.X	10.0.30.1	255.255.255.0
3	Sede B	10.0.40.X	10.0.40.1	255.255.255.0

4.3.3 Asignamiento de las IP´s para la red de VoIP

Tabla N° 4.5 Direcciones IP para la red de VoIP

ÍTM	SEDE	IP Loopback	MASCARA
1	Principal	10.0.10.1	255.255.255.255
2	Sede A	10.0.10.2	255.255.255.255
3	Sede B	10.0.10.3	255.255.255.255

4.3.4 Asignamiento de las IP´s para la red de respaldo (RDSI)

Tabla N° 4.6 Direcciones IP para la red de respaldo RDSI

ITM	SEDE	IP WAN PRINC.	IP WAN SEDE	MASCARA
1	Sede A	10.2.0.1	10.2.0.2	255.255.255.252
2	Sede B	10.2.0.5	10.2.0.6	255.255.255.252

4.3.5 Plan de numeración de anexos telefónicos

Tabla N° 4.7 Dirección de los anexos extendidos

ITM	SEDE	Anexo 1	Anexo 2	Anexo 3	Anexo 4
1	Principal	101	102	103	104
2	Sede A	201	202	-	-
3	Sede B	301	302	-	-

4.5 Requerimientos de equipos

Para la implementación de nuestro escenario de red se requiere de equipos con interfaces de tecnología ethernet e interfaces de voz, para lo cual en el mercado existe gran variedad de productos, sin embargo por el reconocido respaldo del fabricante y la mayor capacidad para integrar soluciones tecnológicas dando una utilidad a largo plazo se ha elegido a *Cisco System.*

En el Siguiente grafico Fig. 4. 4 se muestra una escala de Hardware con integración de voz/Datos en equipos Cisco:

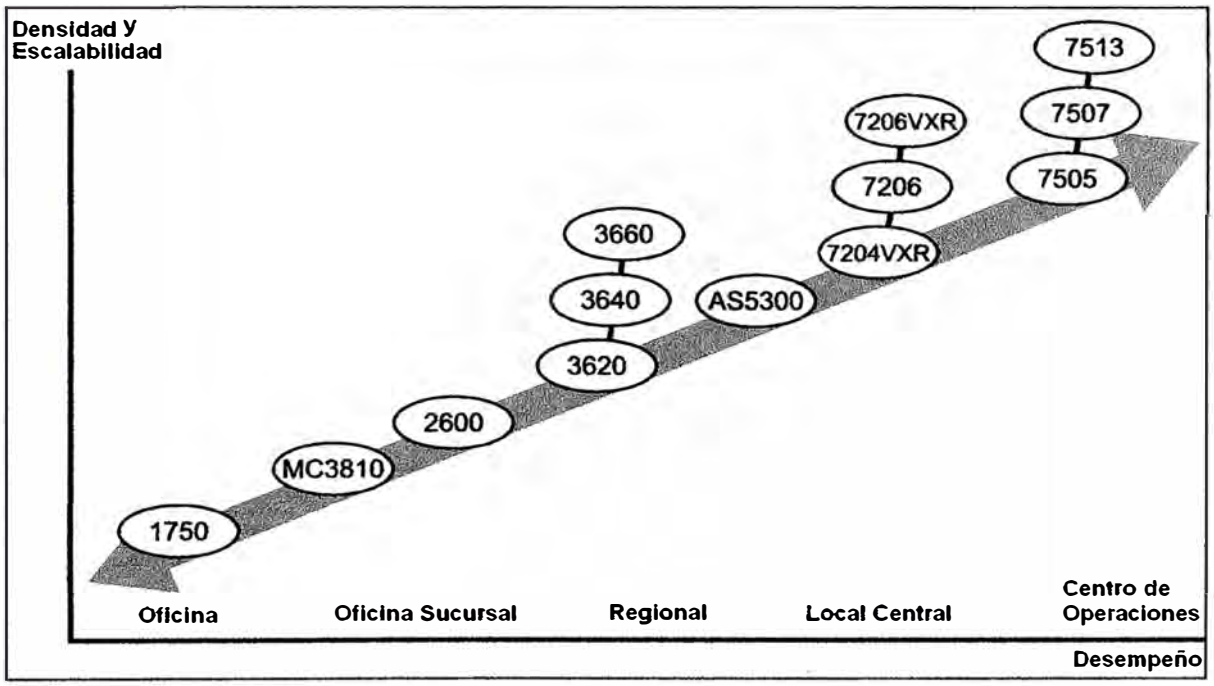

Fig. 4.4 Escala de Hardware con integración de voz/Datos en equipos Cisco:

Esta gama de hardware permite la integración de voz y datos, comenzando por un router 1750 modular que ofrece 3 slots en la cual uno de ellos es dedicado a interfaces de Voz, y la dos restantes pueden tomarse para interfaces Ethernets, RDSI y de voz también.

Hasta un router 7200 el cual cuenta con múltiples interfaces como puertos de Voz, interfaces controladoras E1/T1, interfaces Ethernet fastEthernet, Token Ring, serial, ISDN, ATM y POS (Packets Over Sonet).

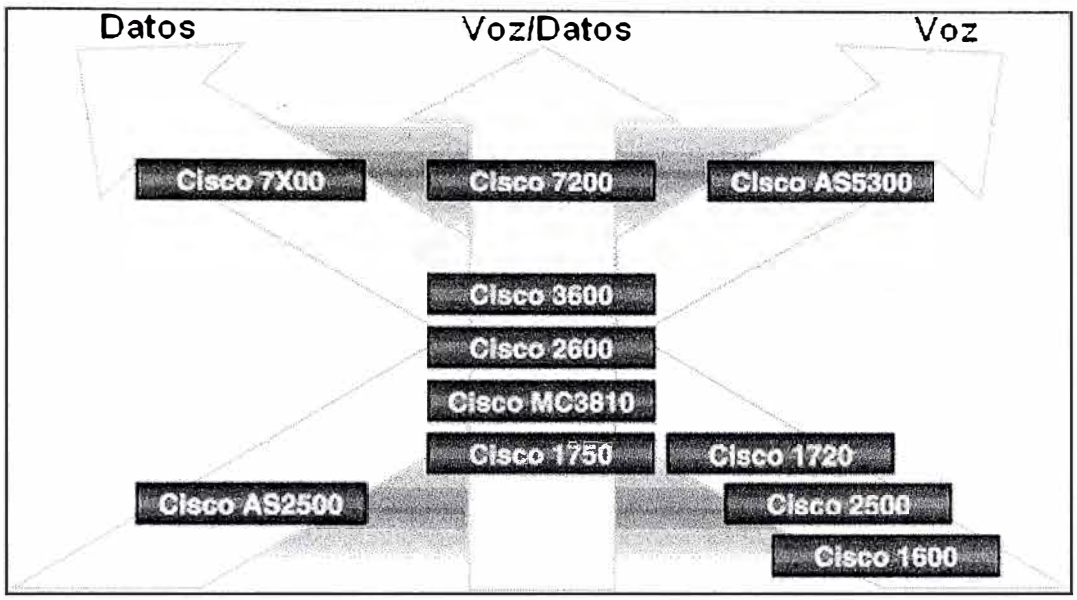

Fig. 4.5 Escala de productos cisco por tipo de aplicación

Nuestro escenario de red es como se muestra en la Fig. 4.6:

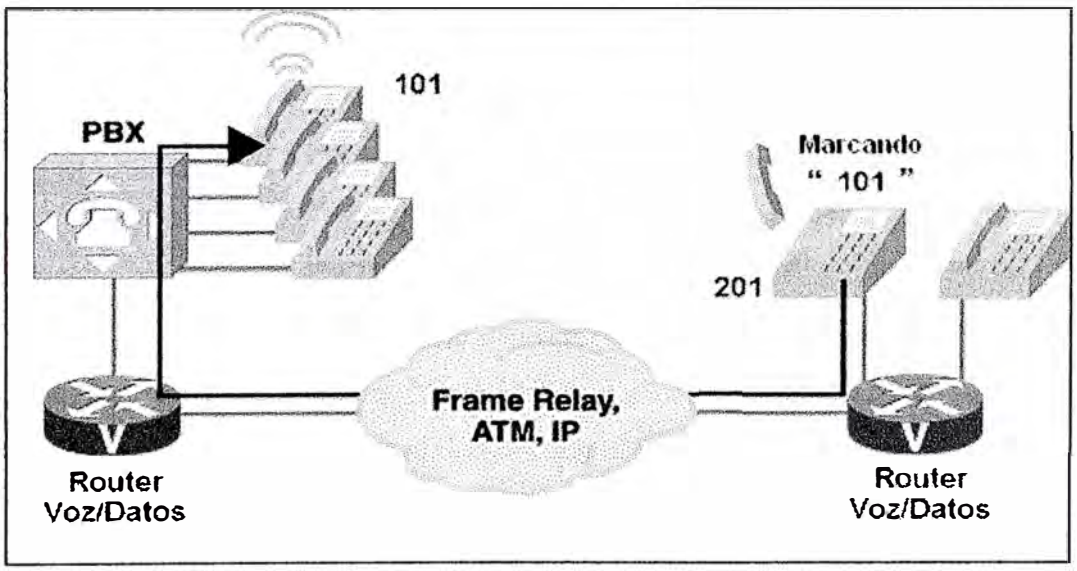

Fig. 4.6 Escenario para la aplicación de VoIP

El cual se implementara con routers Cisco 2611XM para todas las sedes.

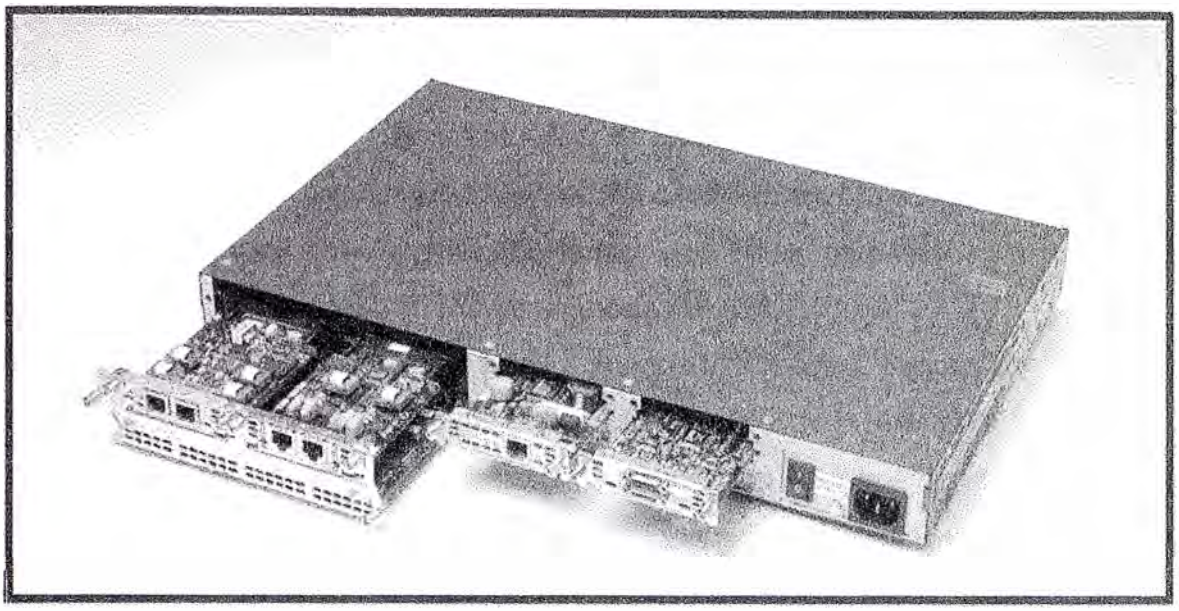

Fig. 4.7 Router Cisco 2611XM

Tabla 4.8 Características del Router Cisco 2611XM

Componente	Características
Base Chasis	♦ Capacidad para manejar desde 2 hasta 30 puertos de voz. ♦ Puertos Auxiliares y de Consola ♦ Sistema opcional de energía redundante. ♦ Integra tecnología Ethernet con Token Ring opcional.
Modulo de Red	♦ Compatible con routers Cisco serie 3600. ♦ Integración de Voz y Datos, Modems, tecnología RDSI y BRI, serial, LAN y opcional ATM.
Tarjetas	♦ Compatible con routers Cisco serie 1600, 1700 y 3600. ♦ Cualquier combinación de 2 tarjetas con interfaces WAN. ♦ Opcionales serial, RDSI PRI.

Los componentes requeridos para el router Cisco 2611XM [4] son:

1.- El Chasis del router Cisco 2611XM, el cual tiene integrado 2 puertos FastEthernet deberá contar con el sistema operativo (IOS) ***c2600-is-mz.123-17b.bin*** el cual requiere de 128 Mb de memoria DRAM y 32 Mb de memoria Flash, para cada sede remota, y para el router de la sede principal 256 Mb de memoria DRAM.
2.- 1 Modulo NM-HDA (Permite hasta 8 puertos FXO) con 2 Tarjetas de Voz de 2 puertos FXO (Foreign Exchange Office) cada una para el router de la sede principal.
3.- 1 Modulo NM-HDV2 (permite hasta 4 puertos) con 1 tarjetas de voz con 2 puertos FXS (Foreign Exchange Station) para los routers de las sedes remotas (Sede A y B)
4.- 1 Tarjeta WAN con 1 interfase ISDN.

4.6 Aplicación de políticas de calidad

Estas políticas de calidad se realizara en la configuración de cada equipo router a través de los comando de línea del equipo router Cisco, el cual consiste en los siguientes pasos:

a. Paso 1. Creación de una clase de tráfico

Crear una clase de tráfico consiste en agrupar un tipo de tráfico de la red bajo un mismo concepto, de tal manera que los paquetes agrupados en esa clase pueden tener un mismo tratamiento cuando llegan al router.
Se utiliza con el comando class-map, y para eliminar la clase de tráfico, se hace con no class-map.

```
class-map match-any qos5
 match ip dscp cs5

class-map match-any qos2
 match ip dscp cs2
```

Class Map: *Se define la clase que identifica el tipo de trafico hacia la sede remota, esto, mediante un marcado de paquetes con determinada precedencia (por tipo de aplicaciones) en la red cliente, no es necesario hacer referencia a redes en listas de acceso, sino solamente a la precedencia de paquetes.*

b. Paso 2. Crear una Política de tráfico

Para configurar una política de tráfico, se usa el comando policy-map, en el que se especifica en nombre de la política, y a la que se asocian clases de tráfico, definidas previamente.

Todo el tráfico que no se equipara con los criterios de las clases, pertenecen a la clase de tráfico por defecto. Esta también se puede configurar por el usuario, pero no eliminar.

policy-map ***qos***
 class qos5
  priority *BWqos5*
 police *BWqos5* [*20%*BWqos5*] [*40%*BWqos5*] conform-action transmit exceed-action drop
 class qos2
  priority BWqos2
 police BWqos2 (20%*BWqos2) (40%*BWqos2) conform-action transmit exceed-action set-dscp-transmit 1
 class class-default
  set ip dscp cs1
  fair-queue
  random-detect

Policy-map: ***qos*** , *Se define la política hija de nombre* ***qos*** *que identifica el tráfico clasificado hacia la sede remota, aplicando los anchos de banda reservado para cada tipo de trafico.Tener en cuenta que en el comandode linea "priority BWqos5" el valor de "Bwqos5" esta expresado en kbps, y en el comando de linea "police" los valores estan expresado en bps.*

policy-map ***wan***
 class class-default
  shape average BWtotal
  service-policy qos

Policy-map: ***wan,*** Se define la política principal o padre de nombre **WAN** donde se especifica el trafico total para la sede y la asignación de trafico para la política hija **qos**.

c. Paso 3. Asociar una política a una Interfaz

Para asociar una política de tráfico a una interfaz, y especificar la dirección en la cual debe especificarse la política (paquetes entrantes o paquetes salientes), se utiliza el comando service-policy.

```
interface FastEthernet0/0
 service-policy output wan
```

Marcado de paquetes en las interfaces VoIP se realizará agregando 2 líneas de comando:

```
dial-peer voice [# interface] voip
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
```

CONCLUSIONES

1.- Se recomienda como CODEC para compresión de voz al G.729r8 debido a su alto MOS de 4.9 de 5 (Mean Opinion Score), bajo retardo y alta capacidad de compresión.

2.- Con la finalidad de hacer más eficiente el envío de la voz en cada paquete, se recomienda utilizar el tamaño de payload a 40bytes por defecto, debido a que al aumentar el payload se degrada la calidad de servicio en un medio de saturación.

3.- La aplicación de estas políticas en simultáneo no afecta de manera significativa el consumo de memoria ni CPU de los routers.
La expansión a enlaces con varios puntos remotos se hace sencillo, ya que la aplicación de las herramientas de calidad de servicio son las mismas para cada sede, claro esta cumpliendo la formula 4.2.1.1.

4.- Se recomienda que el proveedor de los enlaces sea por una red ATM , quien deberá configurar el parámetro CDVT (Cell Delay Variation Tolerance) en los PVCs a 10000 por la notable mejora en la calidad de servicio a diferencia del valor configurado por default (250000).

5.- La empresa tiene la capacidad de crecer en su red hasta 4 líneas analógicas en cada sede remota y 8 en la sede principal.

6.- Para el router 2611XM se recomienda trabajar hasta un máximo de 2 Mbps de ancho de banda, en WAN de la sede principal, por tanto nuestro diseño permite que se puede crecer hasta 4 sedes remotas.

7.- Las líneas RDSI a contratar por la Empresa, debe considerar que estas solo son usadas cuando se presenten problemas con los enlaces principales de las interfaces WAN de cada sede, por tanto, cuando esto suceda solo el trafico de la base de datos podrá hacer uso de la contingencia.

8.- Solicitar al proveedor la asignación de interfaces FastEthernet para la WAN de cada router, esto debido a una mejor forma de resolución de problemas.

9.- La configuración de los equipos mostrados en el anexo A, pertenecen a la Guías Operativas de una empresa de telecomunicaciones las cuales funcionan correctamente en la actualidad en equipos de redes de empresas clientes del mercado local. Para el caso de estudio de Calidad de Servicio implementadas en equipos CISCO, se recomienda el emulador *The Boson NetSim for CCNP V.6.00*, programa aplicativo de ordenador de escritorio, el cual permite realizar practicas de configuración por comandos de líneas a equipos router, switchs, etc. De tal manera que permite emular el comportamiento de una red integrada por routers, swtichs y estaciones de trabajo (PCs) teniendo en cuenta el manejo de los tipos de tráficos por clases de servicio.

ANEXO A

CONFIGURACION DE EQUIPOS

La configuración de los equipos router CISCO 2611XM permitirá la conectividad entre las redes LAN de las sedes. Para tal fin la configuración en los equipos seria como sigue:

Router Principal

```
version 12.3

hostname Sede_Principal

isdn switch-type basic-net3
isdn voice-call-failure 0

username rprincipal
ip cef

interface Loopback0
 description IP para VoIP
 ip address 10.0.10.1 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.1

interface FastEthernet0/0
 description ENLACE WAN SEDE PRINCIPAL
 ip address 10.0.0.1 255.255.255.240
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE PRINCIPAL
 ip address 10.0.1.1 255.255.255.0
 ip address 10.0.20.1 255.255.255.0 secondary
 speed auto
 full-duplex

Router eigrp 10
 network 10.0.0.0
 network 10.0.10.0
```

```
network 10.0.20.0
 network 10.0.1.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.2 255.255.255.252
 ip address 10.2.0.6 255.255.255.252 secondary
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.1 name sede_A broadcast 2830990     (Numero BRI1 2830990)
 dialer map ip 10.2.0.5 name sede_B broadcast 2830991     (Numero BRI2 2830991)
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.1.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 10.0.10.2 255.255.255.255 10.2.0.1 200
ip route 10.0.0.2 255.255.255.255 10.2.0.1 200
ip route 10.0.10.3 255.255.255.255 10.2.0.5 200
ip route 10.0.0.3 255.255.255.255 10.2.0.5 200

voice-port 1/0/0
 connection plar 201
 timeouts call-disconnect 0

voice-port 1/0/1
 connection plar 202
 timeouts call-disconnect 0

voice-port 1/0/2
 connection plar 301
 timeouts call-disconnect 0

voice-port 1/0/3
 connection plar 302
 timeouts call-disconnect 0

mgcp profile default

dial-peer cor custom

dial-peer voice 1 pots
```

```
 destination-pattern 101
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 102
 port 1/0/1

dial-peer voice 3 pots
 destination-pattern 103
 port 1/0/2

dial-peer voice 4 pots
 destination-pattern 104
 port 1/0/3

dial-peer voice 10 voip
 destination-pattern 20.
 incoming called-number 10.
 session target ipv4:10.0.10.2
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 30.
 session target ipv4:10.0.10.3
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 cisco
line aux 0
line vty 0 4
 password 7 cisco

end
```

Router A

```
version 12.3

hostname Sede  A

interface Loopback0
 description IP parato VoIP
 ip address 10.0.10.2 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.2

interface FastEthernet0/0
 description ENLACE WAN SEDE A
 ip address 10.0.0.2 255.255.255.240
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE A
 ip address 10.0.2.1 255.255.255.0
 ip address 10.0.30.1 255.255.255.0 secondary
 speed auto
 full-duplex

router eigrp 10
 network 10.0.0.0
 network 10.0.10.0
 network 10.0.30.0
 network 10.0.2.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.1 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.2 name Sede_Principal broadcast
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.2.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 0.0.0.0 0.0.0.0 10.2.0.2 200
```

```
voice-port 1/0/0
 connection plar 101
 timeouts call-disconnect 0
 timeouts ringing 30

voice-port 1/0/1
 connection plar 102
 timeouts call-disconnect 0
 timeouts ringing 30

dial-peer voice 1 pots
 destination-pattern 201
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 202
 port 1/0/1

dial-peer voice 10 voip
 destination-pattern 10.
 incoming called-number 20.
 session target ipv4:10.0.10.1
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 30.
 session target ipv4:10.0.10.3
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 00321A12051D051300374D01
line aux 0
line vty 0 4
 password 7 097A471D18431907041A0565

end
```

Router B

```
version 12.3

hostname Sede  B
```

```
interface Loopback0
 description IP parato VoIP
 ip address 10.0.10.3 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.3

interface FastEthernet0/0
 description ENLACE WAN SEDE B
 ip address 10.0.0.3 255.255.255.240
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE B
 ip address 10.0.3.1 255.255.255.0
 ip address 10.0.40.1 255.255.255.0 secondary
 speed auto
 full-duplex

Router eigrp 10
 network 10.0.0.0
 network 10.0.10.0
 network 10.0.40.0
 network 10.0.3.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.5 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.6 name Sede_Principal broadcast
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.3.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 0.0.0.0 0.0.0.0 10.2.0.6 200

voice-port 1/0/0
 connection plar 103

 timeouts call-disconnect 0
 timeouts ringing 30
```

```
voice-port 1/0/1
 connection plar 104
 timeouts call-disconnect 0
 timeouts ringing 30

dial-peer voice 1 pots
 destination-pattern 301
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 302
 port 1/0/1

dial-peer voice 10 voip
 destination-pattern 10.
 incoming called-number 30.
 dtmf-relay h245-alphanumeric
 session target ipv4:10.0.10.1
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 20.
 session target ipv4:10.0.10.2
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 00321A12051D051300374D01
line aux 0
line vty 0 4
 password 7 097A471D18431907041A0565

end
```

En las configuraciones mostradas, los equipos ruteadores están listos para ser puestos en producción. Sin embargo la calidad de los servicios no podrá ser predecible con este tipo de configuración, puesto que el tráfico de datos de las empresas podría presentar picos de saturación de manera esporádica en cualquier momento, lo cual afectaría al tráfico sensible como por ejemplo el tráfico generado por aplicaciones en tiempo real como es el caso de la VoIP, y de videoconferencia, generando problemas de calidad en la comunicación como entrecorte de las llamadas, ruido, o simplemente las llamadas no podrán realizarse debido a falta de ancho de banda.

Para esto proponemos la siguiente plantilla de configuración en cada sede, donde se aplican calidad de servicio (QoS):

APLICACION DE POLÍTICAS DE CALIDAD

Por tanto, la configuración de los equipos con QoS será:

Router Principal

```
version 12.3

hostname Sede_Principal

isdn switch-type basic-net3
isdn voice-call-failure 0

username rprincipal
ip cef

class-map match-any qos5
 match ip dscp cs5
 match access-group name video


class-map match-any qos2
 match ip dscp cs2

policy-map qos
 class qos5
  priority 600
 police 600000 120000 240000 conform-action transmit  exceed-action drop
 class qos2
  bandwidth 256
 police 256000 51200 102400 conform-action transmit  exceed-action set-dscp-transmit 1
 class class-default
  set ip dscp cs1
  fair-queue
  random-detect

policy-map wan
 class class-default
  shape average 1024000
```

```
 service-policy qos

interface Loopback0
 description IP para VoIP
 ip address 10.0.10.1 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.1

interface FastEthernet0/0
 description ENLACE WAN SEDE PRINCIPAL
 ip address 10.0.0.1 255.255.255.240
 service-policy output wan
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE PRINCIPAL
 ip address 10.0.1.1 255.255.255.0
 ip address 10.0.20.1 255.255.255.0 secondary
 speed auto
 full-duplex

Router eigrp 10
 network 10.0.0.0
 network 10.0.10.0
network 10.0.20.0
 network 10.0.1.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.2 255.255.255.252
 ip address 10.2.0.6 255.255.255.252 secondary
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.1 name sede_A broadcast 2830990     (Numero BRI1 2830990)
 dialer map ip 10.2.0.5 name sede_B broadcast 2830991     (Numero BRI2 2830991)
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.1.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 10.0.10.2 255.255.255.255 10.2.0.1 200
ip route 10.0.0.2 255.255.255.255 10.2.0.1 200
```

```
ip route 10.0.10.3 255.255.255.255 10.2.0.5 200
ip route 10.0.0.3 255.255.255.255 10.2.0.5 200

ip access-list extended video
 permit ip host 10.0.20.5  any                    (Direccion IP del host  Videoconferencia)

voice-port 1/0/0
 connection plar 201
 timeouts call-disconnect 0

voice-port 1/0/1
 connection plar 202
 timeouts call-disconnect 0

voice-port 1/0/2
 connection plar 301
 timeouts call-disconnect 0

voice-port 1/0/3
 connection plar 302
 timeouts call-disconnect 0

mgcp profile default

dial-peer cor custom

dial-peer voice 1 pots
 destination-pattern 101
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 102
 port 1/0/1

dial-peer voice 3 pots
 destination-pattern 103
 port 1/0/2

dial-peer voice 4 pots
 destination-pattern 104
 port 1/0/3

dial-peer voice 10 voip
 destination-pattern 20.
 incoming called-number 10.
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 session target ipv4:10.0.10.2
 dtmf-relay h245-alphanumeric
```

```
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 30.
 session target ipv4:10.0.10.3
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 00321A12051D051300374D01
line aux 0
line vty 0 4
 password 7 097A471D18431907041A0565

end
```

Router A

```
version 12.3

hostname Sede  A
ip cef

class-map match-any qos5
 match ip dscp cs5
 match access-group name video

class-map match-any qos2
 match ip dscp cs2

policy-map qos
 class qos5
  priority 256
 police 256000 51200 102400 conform-action transmit  exceed-action drop
 class qos2
  bandwidth 128
 police 128000 25600 51200 conform-action transmit  exceed-action set-dscp-transmit 1
 class class-default
  set ip dscp cs1
  fair-queue
  random-detect

policy-map wan
 class class-default
  shape average 512000
```

```
 service-policy qos

interface Loopback0
 description IP parato VoIP
 ip address 10.0.10.2 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.2

interface FastEthernet0/0
 description ENLACE WAN SEDE A
 ip address 10.0.0.2 255.255.255.240
 service-policy output wan
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE A
 ip address 10.0.2.1 255.255.255.0
 ip address 10.0.30.1 255.255.255.0 secondary

 speed auto
 full-duplex

router eigrp 10
 network 10.0.0.0
 network 10.0.10.0
 network 10.0.30.0
 network 10.0.2.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.1 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.2 name Sede_Principal broadcast
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.2.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 0.0.0.0 0.0.0.0 10.2.0.2 200

ip access-list extended video
```

```
 permit ip host 10.0.30.5  any                (Direccion IP del host  Videoconferencia)

voice-port 1/0/0
 connection plar 101
 timeouts call-disconnect 0
 timeouts ringing 30

voice-port 1/0/1
 connection plar 102
 timeouts call-disconnect 0
 timeouts ringing 30

dial-peer voice 1 pots
 destination-pattern 201
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 202
 port 1/0/1

dial-peer voice 10 voip
 destination-pattern 10.
 incoming called-number 20.
 session target ipv4:10.0.10.1
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 30.
 session target ipv4:10.0.10.3
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 00321A12051D051300374D01
line aux 0
line vty 0 4
 password 7 097A471D18431907041A0565
end
Router B


version 12.3
```

```
hostname Sede  B
ip cef

class-map match-any qos5
 match ip dscp cs5
 match access-group name video

class-map match-any qos2
 match ip dscp cs2

policy-map qos
 class qos5
  priority 256
 police 256000 51200 102400 conform-action transmit  exceed-action drop
 class qos2
  bandwidth 128
 police 128000 25600 51200 conform-action transmit  exceed-action set-dscp-transmit 1
 class class-default
  set ip dscp cs1
  fair-queue
  random-detect

policy-map wan
 class class-default
  shape average 512000
  service-policy qos

interface Loopback0
 description IP parato VoIP
 ip address 10.0.10.3 255.255.255.255
 h323-gateway voip bind srcaddr 10.0.10.3

interface FastEthernet0/0
 description ENLACE WAN SEDE B
 ip address 10.0.0.3 255.255.255.240
 service-policy output wan
 speed auto
 full-duplex

interface FastEthernet0/1
 description ENLACE LAN SEDE B
 ip address 10.0.3.1 255.255.255.0
 ip address 10.0.40.1 255.255.255.0 secondary
 speed auto
 full-duplex

Router eigrp 10
 network 10.0.0.0
```

```
 network 10.0.10.0
 network 10.0.40.0
 network 10.0.3.0
 passive-interface BRI0/0

interface BRI0/0
 ip address 10.2.0.5 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 180
 dialer map ip 10.2.0.6 name Sede_Principal broadcast
 dialer-group 1
 isdn switch-type basic-net3
 ppp authentication chap

access-list 101 deny eigrp any any
access-list 101 permit ip 10.0.3.0 255.255.255.0 any

dialer-list 1 protocol ip list 101

ip route 0.0.0.0 0.0.0.0 10.2.0.6 200


ip access-list extended video
 permit ip host 10.0.40.5  any                (Dirección IP del host  Videoconferencia)

voice-port 1/0/0
 connection plar 103

 timeouts call-disconnect 0
 timeouts ringing 30

voice-port 1/0/1
 connection plar 104
 timeouts call-disconnect 0
 timeouts ringing 30

dial-peer voice 1 pots
 destination-pattern 301
 port 1/0/0

dial-peer voice 2 pots
 destination-pattern 302
 port 1/0/1

dial-peer voice 10 voip
 destination-pattern 10.
```

```
 incoming called-number 30.
 dtmf-relay h245-alphanumeric
 session target ipv4:10.0.10.1
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 codec g729r8 bytes 80
 no vad

dial-peer voice 20 voip
 destination-pattern 20.
 session target ipv4:10.0.10.2
 ipqos dscp cs5 media
 ipqos dscp cs5 signaling
 dtmf-relay h245-alphanumeric
 codec g729r8 bytes 80
 no vad

line con 0
 password 7 00321A12051D051300374D01
line aux 0
line vty 0 4
 password 7 097A471D18431907041A0565

end
```

VERIFICACIÓN DE LAS POLÍTICAS DE QOS

Para verificar y mostrar la información referente a una política o una clase, se pueden usar el siguiente comando:

```
rprincipal#show policy-map interface
 FastEthernet0/0

  Service-policy output: wan

    Class-map: qos5 (match-any)
      12337402 packets, 3942233891 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: access-group name TotalCID38650
        12337403 packets, 3942233984 bytes
        5 minute rate 4000 bps
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess   Interval  Increment
             Rate           Limit  bits/int  bits/int (ms)     (bytes)
          1536000/1536000   9600   38400     38400    25       4800

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                        Delayed   Delayed   Active
```

```
      0        12337145  3941893166 1016934   1057054960 no

Service-policy : qos5

  Class-map: qos5 (match-any)
    6485134 packets, 509035939 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: access-group name qos5
      6485134 packets, 509035939 bytes
      5 minute rate 0 bps
    Queueing
      Strict Priority
      Output Queue: Conversation 72
      Bandwidth 484 (kbps) Burst 12100 (Bytes)
      (pkts matched/bytes matched) 168677/13263195
      (total drops/bytes drops) 0/0

  Class-map: class-default (match-any)
    5852269 packets, 3433198045 bytes
    5 minute offered rate 4000 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 64
  (total queued/total drops/no-buffer drops) 0/258/0
```

Con el comando "show policy-map interfase" nos permite mostrar las estadísticas de todas las entradas y salidas de las políticas asociadas a la interfase a la cual se han aplicado, en nuestro caso es la salida de la Interfase WAN, la FastEthernet 0/0

En la Política QOS5 por ejemplo, no debe presentarse perdidas (drops) de paquetes para el trafico priorizado, en cambio, en la política de ultima prioridad o "trafico por default" esta si podría presentar perdida de paquetes.

ANEXO B

GLOSARIO

ADPCM (Adaptive Differential Pulse Code Modulation)
Código de modulación diferencial adaptativo de pulsos o pulsaciones, una forma de código de modulación de pulsaciones que produce una señal digital con un bit rate más bajo que el estándar.

ATM (Asynchronous Transfer Mode)
Tecnología de comunicación en red basada en la transferencia de datos por celdas o paquetes de un tamaño fijo

BRI (Basic Rate Interface)
Interfaz de Acceso Básico. Interfaz RDSI compuesta por dos canales B y un canal D para la comunicación por conmutación de circuito de voz, vídeo y datos.

CISCO SYSTEM
Empresa de comunicación computarizada mundial, que produce canales de comunicación para el Internet (situada en San José, California, EEUU).

CCITT
Comité Consultativo Internacional Telefónico y telegráfico, organización que determina los estándares de comunicación internacional

CHECKSUM (SUMmation CHECK)
Suma de chequeo: esquema simple de detección de errores, donde cada mensaje transmitido es acompañado con un valor numérico basado en el número de grupo de bits del mensaje.

CODEC (Codificador-Decodificador)

Describe una especificación implementada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (stream) o una señal. Los códecs pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones. Los códecs son usados a menudo en videoconferencias y emisiones de medios de comunicación.

CPE (Customer Premises Equipment)
El CPE es el equipo de telecomunicaciones usado en casa u oficina (u otra instalación) para originar, encaminar o terminar una telecomunicación.

DATAGRAMA
Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el ordenador receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ordenador destino.

DIFFSERV (DIFFerentiated SERVices)
Propone que diferentes clases de tráfico puedan ser distinguidas en cada nodo, recibiendo un trato más o menos prioritario a partir de esa diferenciación. Los nodos periféricos a la red se encargan de clasificar cada paquete entrante en una de las clases definidas para que los encaminadores que recorra le den el tratamiento apropiado; se produce por lo tanto una agregación de flujos. De esta forma, ante el caso de que la red se encuentre congestionada, se llega a obtener un resultado preferente para el tráfico prioritario frente a los demás.

DSCP (DiffServ Code Point)
Campo en la cabecera de un paquete IP, para propósitos de clasificación de dicho paquete.

DNS (Domain Name Service)
Servicio de nombres de dominios, servicio del Internet que traduce los nombres de los dominios (gov, edu, net, etc.) en direcciones IP (direcciones numéricas).

ETHERNET

Es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.

ETHEREAL

Es un analizador de protocolos, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos. La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque soporta algunas otras) estableciendo la configuración en modo promiscuo.

FIREWALL

Sistema diseñado para prevenir el acceso ilegal a/o desde una red privada conectada a Internet.

FRAME RELAY

Transmisión de cuadro (inform.), estándar rápido para la transmisión de datos digitales en las redes de comunicación local o regional

FXO (Foreign Exchange Office)

Las tarjetas FXO son dispositivo de computador que permite conectar éste a la RTB (Red Telefónica Conmutada), y mediante un software especial, realizar y recibir llamadas de teléfono. Sirve sobre todo para implementar centralitas telefónicas con un ordenador. Las tarjetas para conectar un teléfono a un ordenador son las llamadas FXS.

FXS (Foreign Exchange Station)

Las tarjetas FXS sirven para conectar teléfonos analógicos normales a un computador, y mediante un software especial, realizar y recibir llamadas hacia el exterior, o hacia otros interfaces FXS. Las tarjetas para conectar un ordenador a la RTB son las FXO.

GNOMEMEETING

Ahora llamado Ekiga, es una aplicación de software libre para realizar videoconferencias y telefonía por IP para GNOME. Usa el hardware o software compatible con H.323 (como Microsoft Netmeeting) y se libera bajo licencia GPL. Permite todas las características modernas de una videoconferencia como soporte de proveedor inteligente o llamadas de telefonía desde el ordenador a un teléfono.

IP (Internet Protocol - Protocolo de Internet)

Estándar o formato para conexiones de ordenadores con la red del Internet

ITU (International Telecommunication Union)

Unión de telecomunicación Internacional.

IETF (Internet Engineering Task Force)

Principal organización de estándares en transmisión de información de la Internet.

LAN (Local Area Network)

Red de área local, un grupo de dos o más ordenadores conectados entre sí por medio de cables.

LOOPBACK

Interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. Se utiliza en tareas de diagnóstico de conectividad y validez del protocolo de comunicación.

MULTIPLEXACIÓN

Es la combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación.

MPLS (Multiprotocol Label Switching)
Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

NAT ((Network Address Translation - Traducción de Dirección de Red)
Estándar creado por la Internet Engineering Task Force (IETF) el cual utiliza una o más direcciones IP para conectar varios computadores a otra red (normalmente a Internet), los cuales tiene una dirección IP completamente distinta (normalmente una IP no válida de Internet definida por el RFC 1918). Por lo tanto, se puede utilizar para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

NETMEETING
Reunión en conferencia virtual, programa de Microsoft que incluye al Explorer y permite la conversación en conferencia en la red del Internet.

NFS (Network File System)
s. sistema de ficheros de red, sistema operativo abierto que permite a los usuarios de una red de acceder a ficheros compartidos (almacenados en ordenadores de diferente tipo)

PCM (Pulse Code Modulation)
Modulación del Código de Pulsos, método usado para transmitir una señal de audio como información digital.

POLYCOM V500
Es un dispositivo de llamada de video sencillo y económico para empresas pequeñas, oficinas remotas y profesionales que quieran comunicarse cara a cara. El V500 es suficientemente sencillo para usuarios de video nuevos, lo suficientemente pequeño para

caber en cualquier espacio reducido y sin embargo, ofrece la calidad de audio y video requeridos en comunicaciones de negocios.

PSTN (Public Switched Telephone Network)
Sistema telefónico basado en alambres de cobre que transportan señales de voz análogas.

PPP (Point to Point Protocol)
Protocolo de punto a punto, protocolo que se utiliza para la conexión de ordenadores al Internet a través de líneas de teléfono.

QoS (Quality of Services - Calidad de Servicio)
Garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput). Una de las grandes ventajas de ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) respecto de técnicas como el Frame Relay y Fast Ethernet, es que soporta niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que la latencia de extremo a extremo no excederá un nivel específico de tiempo. Además que en los servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

RFC (Request For Comments)
Serie de notas sobre el Internet, documentos que contienen proposiciones, comentarios y los estándares relacionados a la tecnología del Internet, propuesta por el IETF.

ROUTER (encaminador)
Dispositivo que conecta dos redes de área local.

RTP (Real-time Transport Protocol)
Es un protocolo de nivel de aplicación (no de nivel de transporte, como su nombre podría hacer pensar) utilizado para la transmisión de información en tiempo real, como por ejemplo audio y video en una video-conferencia.

RTCP (Real time control protocol)

Protocolo hijo de RTP. Este protocolo se encuentra definido en el RFC 3550.

SDH (Synchronous Digital Hierarchy - Jerarquía Digital Síncrona)
Se puede considerar como la evolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transmisión, así como de la necesidad de sistemas más flexibles y que soporten anchos de banda elevados. La jerarquía SDH se desarrolló en EEUU bajo el nombre de SONET y posteriormente el CCITT en 1989 publicó una serie de recomendaciones donde quedaba definida con el nombre de SDH.
Uno de los objetivos de esta jerarquía estaba en el proceso de adaptación del sistema PDH (Plesiochronous Digital Hierarchy), ya que el nuevo sistema jerárquico se implantaría paulatinamente y debía convivir con la jerarquía plesiócrona instalada. Esta es la razón por la que la ITU-T normalizó el proceso de transportar las antiguas tramas en la nueva. La trama básica de SDH es el STM-1 (Synchronous Transport Module level 1), con una velocidad de 155 Mbps.
Cada trama va encapsulada en un tipo especial de estructura denominado contenedor. Una vez se ha encapsulado se añaden cabeceras de control que identifican el contenido de la estructura y el conjunto, después de un proceso de multiplexación, se integra dentro de la estructura STM-1.
Los niveles superiores se forman a partir de multiplexar a nivel de Byte varias estructuras STM-1, dando lugar a los niveles STM-4, STM-16 y STM-64.

SIP (Session Initiation Protocol - Protocolo de Inicialización de Sesiones)
Protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual. En Noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP (Generation Partnership Project) y elemento permanente de la arquitectura IMS (IP Multimedia Subsystem). SIP es uno de los protocolos de señalización para voz sobre IP, acompañado por H.323.

TCP (transmission control protocol)
Protocolo de control de transmisión, protocolo para la transmisión de datos en red y en especial en el Internet, protocolo orientado a la conexión.

TIMESTAMP
Marca de tiempo, fecha y hora.

ToS (Type of Services - Tipo de Servicio)
El tipo de servicio es una indicación de la calidad del servicio solicitado en el campo de 8 bit de un datagrama IP.

UDP (User Datagram Protocol)
Protocolo del datagrama del usuario, protocolo falto de conexión (que no demanda conexión directa entre el remitente y el destinatario), permite el envío de paquetes de datos por medio del Internet

URL (Uniform Resource Locator)
Dirección global de documentos y otras fuentes en el Internet.

VoIP (Voice Over Internet Protocol - Voz sobre IP)
Sistema de enrutamiento de conversaciones de voz mediante paquetes basados en IP por la red de Internet.

WAN (Wide Area Network)
Red de comunicación extendida, red de comunicaciones que conecta ordenadores dispersos en una amplia área geográfica (conectados por líneas telefónicas u ondas de radio).

BIBLIOGRAFIA

[1] Calidad de Servicio
http://www.cisco.com\en\US\customer\products\sw\iosswrel\ps1831\products_configuration_guide_book09186a008007ff1d.html
Fecha de consulta: Junio del 2005.

[2] RTP Profile for Audio and Video Conferences with Minimal Control, Stephen L. Casner, Trabajo en desarrollo, bajo el nombre draft-ietf-avt-profile-new-12.txt. Válido hasta Mayo de 2002.
http://tools.ietf.org/html/draft-ietf-avt-profile-new-12
Fecha de consulta: Junio del 2005.

[3] Basic Architecture of H.323, C. Schlatter, 2003,
http://www.switch.ch/vconf/ws2003/h323_basics_handout.pdf
Fecha de consulta: Abril del 2006.

[4] Hardware Cisco 2611XM
http://www.cisco.com\univercd\cc\td\doc\product\access\acs_mod\cis2600\index.htm
Fecha de consulta: Junio del 2005.

[5] Internetwork Design Guide
http://www.cisco.com\univercd\cc\td\doc\cisintwk\idg4\index.htm
Fecha de consulta: Junio del 2005.