ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ESTUDIO Y DISEÑO DE UNA RED WAN CON CALIDAD DE SERVICIO PARA VOZ SOBRE IP

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

FERNANDO JAVIER CABRERA FAJARDO

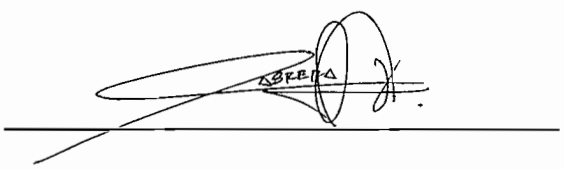
DIRECTOR: ING. PABLO HIDALGO

Quito, Noviembre de 2005

DECLARACIÓN

Yo, Fernando Javier Cabrera Fajardo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.



Fernando Javier Cabrera Fajardo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Fernando Javier Cabrera Fajardo, bajo mi supervisión.

Ing. Pablo Hidalgo

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A Dios, por sus bondades y compañía espiritual que me ha brindado durante toda mi vida, y por esos maravillosos dones como la salud, la felicidad y el amor, que han hecho posible la tranquilidad mental para mis estudios.

A mi familia, por su apoyo fraterno y absoluto, que han hecho posible que haya cumplido con mis objetivos y metas en el transcurso de este proceso educativo.

A mis amigos y compañeros de clase, por su apoyo desinteresado, y que son ahora una parte muy importante en mi vida, y especialmente a Cristina, por su amor y consejos que me han ayudado a crecer como persona.

A mis maestros, porque a más de brindarme ese conocimiento académico, me han preparado como una persona lista para enfrentarse a este mundo competitivo, especialmente un sincero agradecimiento al Ing. Pablo Hidalgo, por sus consejos, y por la paciencia que ha tenido al ayudarme a ser una persona más responsable y dedicada, factores claves para mi desenvolvimiento como profesional y como persona.

A la Escuela Politécnica Nacional, por aceptarme dentro de sus instalaciones, que me han cuidado durante todo este período universitario.

DEDICATORIA

A mis padres, hermanos y amigos que han hecho posible que mis sueños se vuelvan realidad, y que han sido un pilar de apoyo en las buenas y en las malas dentro de mi vida y mis estudios.

CONTENIDO

CAPÍTULO 1

CAPÍTULO 2

PRESENTACIÓN

La idea de implementar una red única, que permita la convergencia entre las redes de voz y datos no es nueva; la continua actualización y mejora de los sistemas de transmisión ha permitido la posibilidad de transmitir las comunicaciones telefónicas por la red de datos. Por tal motivo, la convergencia de redes es ya una realidad. La era de las arquitecturas de redes complejas, distinguidas por el servicio prestado, está finalizando para dar paso a una única red polivalente, más fácil de gestionar, de menores costos y capaz de soportar, con la calidad requerida, todas las necesidades de comunicación de las empresas de forma unificada.

Varias empresas buscan en esta convergencia la posibilidad de tener rentabilidad y de alguna manera, optimizar las fuertes inversiones en infraestructuras de datos; así, la Voz sobre IP (VoIP), protagoniza el primer paso hacia la unificación.

La idea de poder tener una única red homogénea y de calidad, que soporte todo el tráfico, manteniendo bajos costos, empieza a tomar fuerza en el mercado. Éste es sólo el inicio de las comunicaciones convergentes, un nuevo entorno en el que conviven voz y datos sin distinción; una moderna y única infraestructura que soporte todas las comunicaciones abriendo un amplio campo de desarrollo de software para los negocios, los servicios y las aplicaciones.

La implantación de la voz controlada por software sobre estas redes homogéneas que hablan un único idioma, el IP, será sólo el principio del desarrollo de una multitud de servicios de valor añadido basados en software. Pero no hay que olvidar que estos servicios serán viables gracias a tecnologías e infraestructuras instaladas, como la implementación de Calidad de Servicio (QoS), que realiza mecanismos de inteligencia en la red y priorización del tráfico, además la utilización de protocolos de comunicación multimedia como H.323 o SIP, que se han ido sumando para hacer de la convergencia una realidad operativa.

Sin embargo, la situación no es tan optimista cuando el transporte de la voz debe hacerse en un entorno de una red WAN, ya que las capacidades disponibles en muchos casos siguen siendo insuficientes. En este ámbito, los factores críticos a tener presentes son: el ancho de banda, las variaciones de retardo y paquetes perdidos, factores que pueden causar la deficiencia en la calidad de la voz. Para solucionar estos problemas es necesario la implantación de calidad de servicio (QoS), la cual ofrece un rendimiento eficiente de los recursos de la red para el beneficio de los usuarios. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un tipo de tráfico que sigue un conjunto específico de parámetros.

Por tal razón, este proyecto presenta un diseño de una red convergente de voz y datos que se enfatiza en la implementación de Calidad de Servicio, y conjuntamente se realiza un análisis financiero de esta solución con VoIP comparada con la telefonía tradicional.

RESUMEN

En el presente proyecto se analiza la posibilidad de implementar VoIP en una red de datos, con el fin de poder realizar llamadas telefónicas entre agencias de una empresa ficticia que posee sucursales en Guayaquil, Cuenca y su agencia principal en Quito. El diseño se basa en la unificación de las redes de voz y datos en una sola red convergente, aprovechando la infraestructura de red WAN que generalmente tienen ya instaladas las empresas; de esta manera las comunicaciones telefónicas internas de la empresa, que las realizan por medio de la PSTN, se efectuarán a través de esta red WAN para así poder optimizar los recursos y sobre todo ahorrar costos.

El diseño se inicia con el análisis de la voz y su proceso de encapsulación en paquetes IP (VoIP), para poder incluirles como un flujo más dentro de la red de datos y ver la forma de tratarlo de manera preferencial, ya que la VoIP es un protocolo de tiempo real y no debe ser tratada igual que un paquete normal de datos. Adicionalmente se presenta el estudio de los fundamentos de VoIP, protocolos, estándares, y requerimientos que este protocolo tiene para poder ser implementado en una red de datos.

Posteriormente se analiza la manera de tratar los paquetes de VoIP para que este tráfico no represente un problema en el funcionamiento normal de la red. Para esto se realiza un estudio de la implementación de Calidad de Servicio. Por tal razón en el diseño se presentan políticas, herramientas y mecanismos de calidad de servicio que ayudan a la optimización de los recursos en una red. En este sentido se consideran varios criterios según los requerimientos de la red; entre los principales se tienen: la asignación del ancho de banda dependiendo del tipo de codificación que se realice, evitar y/o administrar la congestión en la red, manejar prioridades de acuerdo al tipo de tráfico, modelar el tráfico de la red, etc.

Con todo este marco teórico se realiza el diseño de la red, desde la caracterización de protocolos, topología, esquema de direccionamiento y dimensionamiento de los diferentes enlaces a contratar, donde se incluyen las alternativas de interconexión presentadas en el país, adquisición de equipos y principalmente la implementación de las diferentes técnicas de calidad de servicio para VoIP aplicada al funcionamiento de ellos. Para finalizar, se presenta un estudio financiero de lo que involucra la implementación de VoIP en la red de datos comparado con la utilización de la Red de Telefonía Pública tradicional para las llamadas internas de la empresa.

Conjuntamente al proyecto, se presentan anexos que incluyen: proformas para la contratación de los diferentes enlaces de empresas que ofrecen servicio de portadora (*carriers*), y características técnicas de los *Cisco 2800 Series Integrated Services Routers*.

CAPÍTULO 1

1. FUNDAMENTOS DE VoIP

1.1 INTRODUCCIÓN A VoIP [15]

El aparecimiento del Internet ha dado lugar a un desbordante crecimiento y a una fuerte implantación de redes IP, tanto locales como remotas. Por tal razón los responsables de las comunicaciones de las empresas han tenido en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa.

No obstante, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permiten la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir voz sobre redes IP.

Si se ve la historia, desde hace más de 100 años, las personas cuentan con la PSTN (Red Pública de Telefonía Conmutada) para las comunicaciones de voz. Durante una llamada entre dos sitios remotos, la línea que se está usando, es dedicada exclusivamente a estos dos lugares y otro tipo de información no podría viajar sobre esta línea a pesar de que exista suficiente ancho de banda.

Luego, puesto que las comunicaciones de datos emergieron, las empresas realizan inversiones por sus líneas de datos, para que sus computadores puedan compartir la información, mientras que las comunicaciones de voz y fax, todavía se efectúan sobre la PSTN.

Después de haber constatado que desde un PC con elementos multimedia, como es el caso de NetMeeting de Microsoft o MSN por ejemplo, es posible realizar llamadas telefónicas a través de Internet, se puede pensar que la Voz sobre IP (VoIP) es más que un mito, pues la calidad de voz que se tiene a través de Internet es considerada aceptable.

Si en cierta empresa se dispone de una red de datos con un ancho de banda grande, se puede pensar en la utilización de esta red para el tráfico de voz entre las distintas agencias de la empresa. Los beneficios que se obtendrían al utilizar la misma red para transmitir tanto voz como datos son evidentes:

- Ahorro de costos de comunicaciones, pues las llamadas entre las distintas agencias saldrían relativamente gratis.
- Integración de servicios y unificación de estructura.
- Las redes IP constituyen una red estándar universal para la Internet, Intranets y Extranets.
- Interoperabilidad entre diversos proveedores.
- Administración centralizada y única para todo el sistema convergente.

Realmente la integración de la voz y datos en una misma red es una idea que se la ha estado discutiendo desde hace algunos años. Desde hace tiempo han surgido soluciones de distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes WAN de datos de las empresas (típicamente conexiones punto a punto y *Frame Relay*) para la transmisión del tráfico de voz.

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y el surgimiento de un estándar. La aparición de VoIP junto al abaratamiento de los DSP's (Procesadores Digitales de Señales), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despliegue de estas tecnologías.

Existen dos importantes grupos internacionales que definen el estándar de VoIP:

- *International Telecommunications Union* (ITU) - La ITU ha definido el estándar H.323, el cual abarca VoIP.
- *Internet Engineering Task Force* (IETF) - El IETF ha definido este protocolo desde los siguientes documentos RFC (*Request for Comment*):

- RFC 2543, *the Session Initiation Protocol* (SIP)
- RFC 2705, *the Media Gateway Control Protocol* (MGCP)

1.1.1 ANTECEDENTES DE LA ESPECIFICACIÓN VoIP

Las aplicaciones de VoIP de diferentes vendedores han sido, por algún tiempo, incompatibles, debido a diferencias fundamentales como es el caso de codificación de voz, supresión de silencios, direccionamientos y planes de marcación, administración de llamada, y otras funciones relacionadas, simplemente por la falta de especificaciones de VoIP claramente definidas.

Para solucionar estos problemas, un grupo de corporaciones sin fines de lucro se han unido en los últimos años y han propuestos estándares, y por tal razón la especificación VoIP ha crecido. A ello se añade el IMTC (*International Multimedia Teleconferencing Consortium*), el foro de Voz sobre el Protocolo Internet (VoIP), y el estándar SCSA (*Signal Computing System Architecture*).

IMTC es una corporación sin fines de lucro compuesta por más de 145 miembros y afiliados de Europa, Norte América y Asia. La misión del IMTC es promover, fomentar y facilitar el desarrollo de soluciones de teleconferencia multimedia compatibles, basadas en estándares abiertos internacionales. En este sentido, el IMTC se encuentra actualmente centrado en los estándares para teleconferencia multimedia adoptados por la ITU, concretamente las recomendaciones ITU-T T.120, H.320, H.323 y H.324.

Entre los miembros del IMTC figuran las principales operadoras del mundo y las empresas más significativas en el sector informático y de las telecomunicaciones; entre ellas se puede mencionar a Intel, Microsoft, Apple, Sun, Motorola, Texas Instruments, Alcatel, Siemens, Cisco, Ascend, entre otras.

IMTC mantiene ocho grupos de actividad: conferencias de datos (T.120), interoperabilidad y servicios de red, conferencias en redes de paquetes (H.323), conferencias en redes conmutadas (H.320, H.324), *Forum* de voz sobre IP (VoIP), calidad de servicio, usuarios y aplicaciones, y *marketing*.

El foro de Voz sobre IP es un grupo de vendedores fundado en Mayo de 1996 para garantizar interoperabilidad y alta calidad de servicio para productos de telefonía sobre Internet, definiendo y promoviendo un simple acuerdo de implementación en un foro abierto para discutir la banda de voz sobre una red IP.

En Octubre de 1996 el foro se juntó con IMTC, y desde entonces ha operado como uno de estos grupos activos. A los miembros que fundaron VoIP se incluyen grandes industrias de computación, como es el caso de: 3COM, Microsoft, y U.S. Robotics, así como Telcos Nortel, Octel y Vocaltel, y más recientemente Dialogic y NetSpeak.

La ITU, sede en Génova – Suiza, es una organización internacional con la cual el gobierno y el sector privado coordinan redes y servicios de telecomunicaciones globales; principalmente publica tecnología de telecomunicaciones, información de estándares y regulaciones. Como resultado, existen actualmente, reglas y regulaciones definidas para la especificación de VoIP.

Especialmente los estándares bajo discusión son: ITU-T T.120, H.320, H.323, y el estándar H.324. La recomendación H.323 define protocolos para transmisión de vídeo, voz y datos sobre una red IP; especifica los elementos necesarios para visualizar una llamada incluyendo vídeo, audio, especificación VoIP compartida (T.120), control de llamada, y sistema de control. La norma H.323 fue diseñada específicamente para redes locales, así la variación del ancho de banda y el valor de latencia presentado en Internet elimina la utilidad de algunos de estos elementos.

SCSA, es un conjunto de especificaciones referentes a hardware y software con la especificación de VoIP para el diseño de sistemas escalables de telefonía en

computación. Fue lanzado en 1993 por Dialogic y 70 compañías relacionadas con la telefonía. Para 1997 SCSA tuvo un soporte de más de 300 organizaciones, y más de 100 productos de hardware SCSA han sido anunciados desde ese entonces.

Por lo tanto el fenómeno VoIP ha sido de gran interés para varios fabricantes y para algunos productos de telefonía. La especificación VoIP inicialmente fue definida para las comunicaciones de audio, pero claramente hay un gran mercado potencial para vídeoconferencia vía IP, e IP como un medio de transmisión para la telefonía tradicional.

1.1.2 CONCEPTOS BÁSICOS DE VoIP [4]

La voz sobre datos incluye: Voz sobre IP (VoIP), Voz sobre *Frame Relay* (VoFR), y Voz sobre ATM (VoATM). Cada una de estas tres tecnologías de transporte de voz sobre datos es ligeramente diferente, pero de las tres, VoIP es la más relevante.

Antes que la voz pueda ser escuchada en el otro extremo de una llamada, varias cosas ocurren. Si un usuario levanta el auricular del teléfono y marca, el *router* conectado al teléfono interpreta los dígitos marcados, utiliza una señalización y realiza la llamada de VoIP. Cuando se realiza este tipo de llamadas, primero se digitan los números a marcar, el que realiza la llamada escucha el sonido de tono; en el otro extremo, el teléfono empieza a sonar, se levanta el auricular y la llamada se completa.

Se puede mencionar un ejemplo como el caso de la figura 1-1, donde dos teléfonos están conectados a dos *routers* distantes (R1 y R3), y se desea realizar una llamada entre ellos. Ambos teléfonos se encuentran conectados en puertos analógicos FXS (*Foreign eXchange Station*, ver numeral 1.2.3.1); la extensión 201 directamente a R1 y la extensión 301 por medio de una central PBX a R3. En este caso son los *routers* los que realizan la señalización, por ejemplo se puede hablar de la norma H.323.

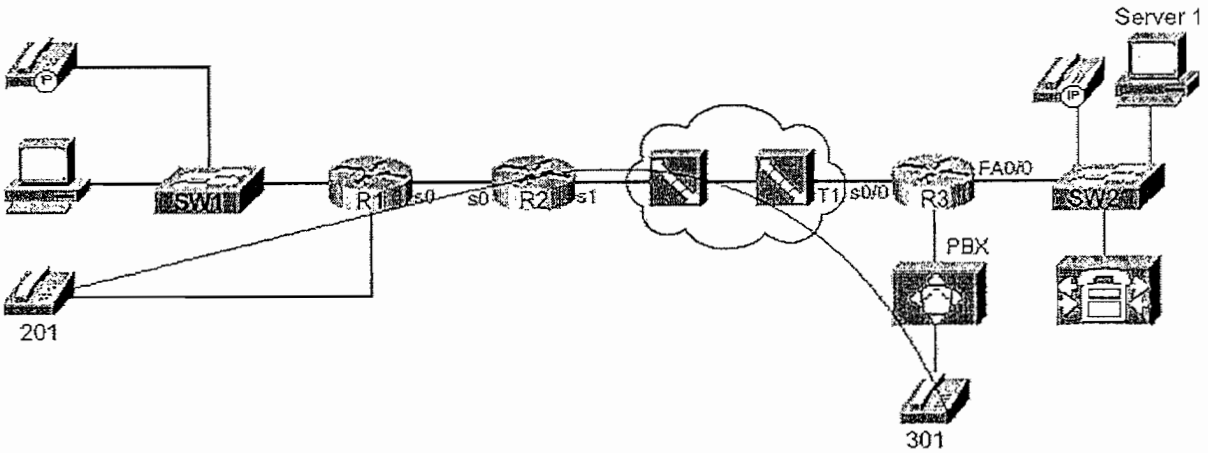


Figura 1-1 Llamada entre teléfonos análogicos en extensiones 301 y 201 [4]

Esta típica llamada utiliza un protocolo de transporte de tiempo real (*Real-Time Transport Protocol*, RTP). En la figura 1-2 se indica el formato de un paquete IP usando RTP.

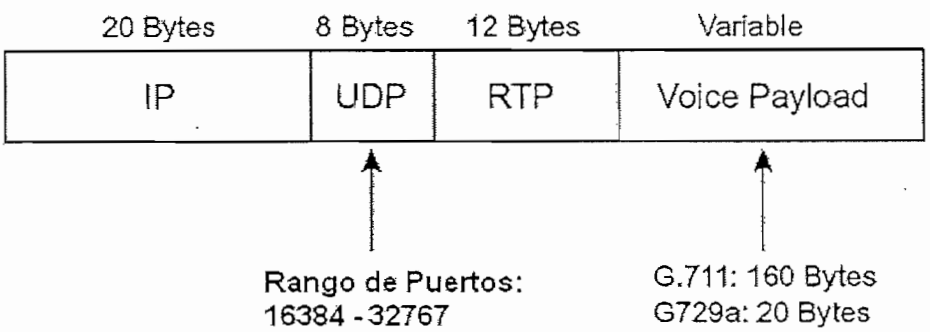


Figura1-2 Formato del paquete IP utilizando RTP [4]

En la llamada entre dos teléfonos analógicos, el *router* recibe señales de voz analógicas, las digitaliza, las codifica utilizando algún tipo de codificador de voz y las sitúa en el campo del *payload* como se muestra en la figura 1-2. Por ejemplo el *router* R1 de la figura 1-1 podría crear un paquete IP como el de la figura 1-2, situar la voz codificada en bits dentro del campo del *payload* de voz y enviar el paquete. La dirección IP fuente podría estar en R1, y la dirección IP destino en la dirección IP de R3. Cuando R3 reciba el paquete, éste revierte el proceso, eventualmente llevando una onda analógica de voz al teléfono analógico.

Un teléfono IP podría experimentar un proceso similar, en concepto, a pesar de que algunos detalles difieren. En el proceso de señalización se debe incluir un Protocolo de Control de Llamada, el cual fluye hacia cada uno de los teléfonos IP y una central IP. Después de que la señalización haya sido completada, un paquete RTP va a circular entre los dos teléfonos. La Central IP no influye completamente en la llamada, sino básicamente en el inicio y finalización de la sesión. En este caso los *routers* no realizan la creación del paquete RTP, porque los teléfonos IP lo crean.

Finalmente el administrador de la red puede escoger el tipo de codificador a utilizar. Cada codificador tiene varias características, pero la más significativa es la del requerimiento mínimo de ancho de banda para enviar el *payload* de voz creado por el codificador.

La tabla 1.1 muestra una lista de codificadores comunes y su requerimiento de capacidad.

Tabla 1.1 Codificadores de voz y requerimiento de capacidad para el *payload* [4]

Codificador	**Bit Rate por *payload** (Kbps)**	**Tamaño del *payload***
G. 711 (PCM[1])	64	160 bytes
G. 726 (ADPCM[2])	32	80 bytes
G.729	8	20 bytes
G. 723.1 (ACELP[3])	5.3	20 bytes

* El *payload* contiene la voz digitalizada, pero no incluye los *headers y trailers* utilizados para enviar tráfico de voz.

[1] ***Pulse Code Modulation***: Convierte una señal analógica (sonido, voz) en digital para que pueda ser procesada por un dispositivo digital.

[2] ***Adaptive Digital Pulse Code Modulation***: Proceso en el cual las muestras de la onda analógica son codificadas dentro de señales digitales comprimidas.

[3] ***Algebraic Code Excited Linear Prediction***: Proceso por el cual las muestras de las onda analógica de voz es codificada en señales digitales de alta calidad.

1.2 SERVICIOS E IMPLEMENTACIONES COMUNES DE VoIP [5]

La PSTN existente está basada en transmisión de señales analógicas sobre circuitos conmutados; en contraste, una red VoIP envía voz digitalizada sobre un paquete en una red IP. Como bien se ha visto, las redes VoIP ofrecen diferentes tipos de servicios de telefonía.

1.2.1 FUSIÓN DE LA VOZ CON LA RED DE DATOS

Hoy en día varias compañías poseen redes separadas tanto para voz como para datos. Imagine la fusión de estas redes dentro de una sola infraestructura de red que pueda llevar ambos servicios.

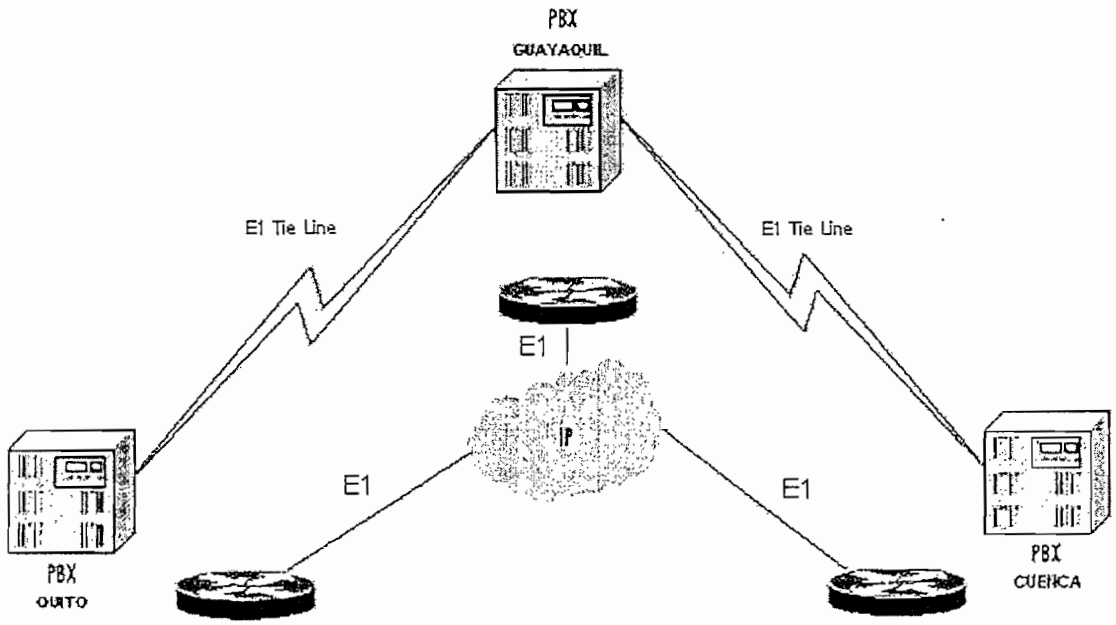


Figura 1-3 Red transmitiendo servicios separados de Voz y Datos entre las oficinas [5]

En algunas ocasiones se ha escuchado la frase "llamadas gratis", y se sabe que nada en esta vida es gratis, pero lo que sí se puede asegurar es que si se utiliza una fusión de voz y datos en una sola red, los costos disminuirán notablemente.

Cuando se menciona esto, seguramente se está refiriendo al caso de que muchas compañías ya poseen líneas de datos funcionando paralelamente con las líneas de

voz. Como se indica en la figura 1-3, la red posee enlaces E1[4] para transmitir datos, y otros enlaces E1[4] troncalizados para trasmitir voz, por lo que se puede observar que se está pagando por dos costosas redes.

La red de datos puede soportar varias funciones tales como *e-mail*, Internet, y archivos compartidos por ejemplo. Con un apropiado monitoreo de red, algún administrador podría saber cuál es la carga en este circuito de datos. Dependiendo de la aplicación, existe una buena oportunidad de unificar los servicios de voz y de datos, si se toman algunos criterios de calidad de servicio para que la red se siga manteniendo óptima.

1.2.1.1 Convergencia

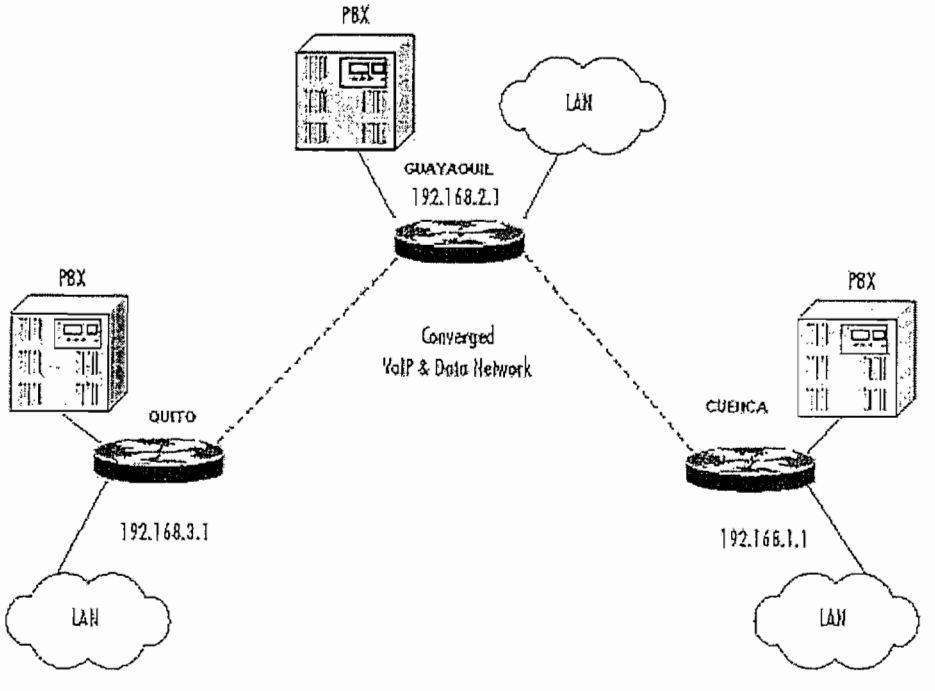


Figura 1-4 Red Convergente de Voz y Datos [5]

[4] Esquema de transmisión digital de área extendida usada internacionalmente excepto en Norte América y Japón, y su velocidad de transmisión es a 2.048 Mbps.

Se debe considerar el costo que se ahorraría si se eliminan los enlaces troncalizados para la transmisión de voz; incluso si al circuito de datos se tendría que incrementar un poco el ancho de banda, este costo sería menor que instalar completamente circuitos separados. Esto permitiría realizar llamadas directamente entre Quito y Cuenca, a través de Guayaquil (figura 1-4) por ejemplo.

1.2.1.2 La PSTN como respaldo

Para proveer redundancia en redes VoIP, algunas compañías ofrecen el uso de la PSTN como respaldo. Ciertos *Gateways* pueden proveer esta redundancia. Cuando la red VoIP determina que la interfaz de la WAN que está llevando tráfico de voz se encuentra abajo, el *gateway* convierte el paquete de voz digitalizada a un flujo de voz analógica, y transmite la llamada a través de la PSTN.

1.2.2 *TOLL BYPASS*

Relativo al Internet, la PSTN ofrece servicios de voz con cargos o impuestos (*Toll*) elevados. *Toll bypass* es la evasión de cargos pero usando la red de datos, como el Internet, para llevar las conversaciones de voz.

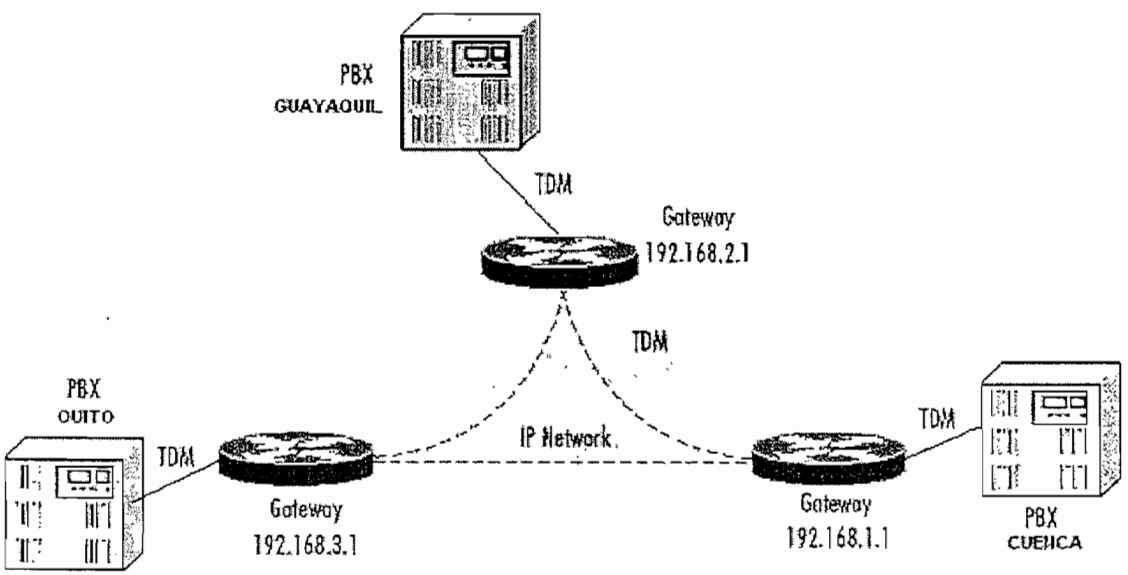


Figura 1-5 *Toll Bypass* con *Gateways Routers* [5]

En la figura 1-5 se muestra un ejemplo de *toll baypass* usando *gateways,* que son capaces de proveer una interfaz entre una red IP y una tradicional PBX.

Este sistema es legal si las llamadas telefónicas se utilizan únicamente para la empresa. La ilegalidad existe cuando se maneja este sistema como un servicio público.

Actualmente en el Ecuador no está autorizada ninguna otra forma de prestar servicios públicos de comunicación de voz que no sea el servicio que ofrecen las empresas autorizadas por el CONATEL (Consejo Nacional de Telecomunicaciones), por lo que se limitan a servicios de telefonía tradicional.

Si bien en cierto la prestación de servicios de acceso a Internet está regulada por el reglamento para la prestación de Servicios de Valor Agregado (Resolución No. 35-13-CONATEL-96). En dicho reglamento se definen los Servicios de Valor Agregado (SVA), que comprenden el acceso a Internet y sus derivados. Pero en el mismo reglamento se especifica que si los Servicios de Valor Agregado tienen como finalidad transmitir voz en tiempo real, violan los reglamentos de exclusividad que poseen las Empresas Telefónicas autorizadas por el CONATEL.

Sin embargo este tipo de aplicaciones y otras más que impliquen utilización de tecnologías Informáticas (*Hardware* y/o *Software*) sí están permitidas para enlaces de comunicaciones de uso privado, siempre y cuando su uso o aplicación no exceda de la Infraestructura del Abonado, según lo indica el Reglamento a la Ley Especial de Telecomunicaciones en el Capítulo 7.

1.2.2.1 VoFR (Voz sobre *Frame Relay*)

En Voz sobre *Frame Relay* (VoFR) se utiliza una infraestructura *Frame Relay* para poder llevar paquetes que contienen voz digitalizada. Teléfonos IP, conmutadores o *routers* capaces de soportar tráfico de voz, podrían engancharse a una red *Frame*

Relay para digitalizar señales de voz y estas señales situarlas dentro de un paquetes IP. Este paquete IP puede ser llevado a diferentes destinos sobre la red *Frame Relay*.

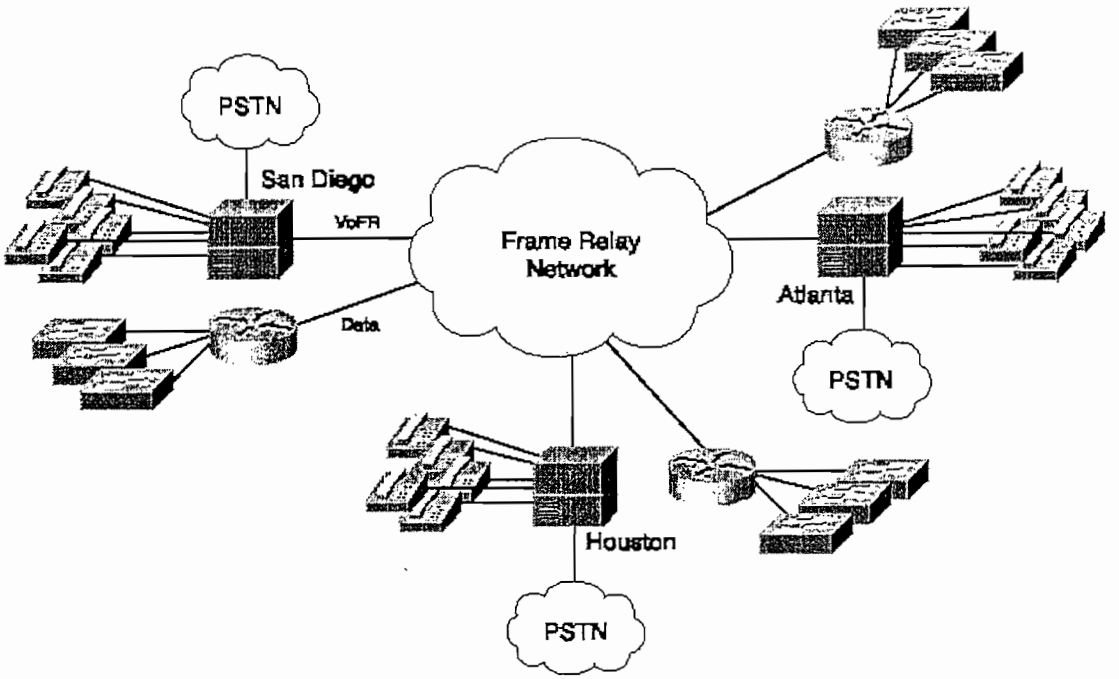


Figura 1-6 Conexión entre PBXs utilizando VoFR [3]

Algunos vendedores de PBX proveen tarjetas VoFR para sus conmutadores, de esta manera poder distribuir llamadas sobre una red *Frame Relay*. En la figura 1-6 se muestra un ejemplo de tres PBXs conectadas entre ellas usando VoFR. La PSTN es utilizada como respaldo si los circuitos de la red *Frame Relay* llegan a fallar.

Un estándar para VoFR es ***Frame Relay Forum (FRF) 11.1***. Esta norma establece especificaciones para el inicio de una llamada, tipos de codificadores, y formatos de paquetes para el servicio de VoFR.

Construyendo una red privada se puede llevar voz y datos pudiendo no ser financieramente posible para algunas compañías. Una compañía puede escoger en

rentar servicios *Frame Relay* en lugar de construir su propia red privada. Un proveedor podría ofrecer un servicio de línea dedicada a la compañía que tenga oficinas en diferentes localizaciones. Las líneas se encuentran enlazadas por medio de *switches Frame Relay* para proveer relativamente un servicio de red a bajo costo.

1.2.2.2 VoATM (Voz sobre ATM)

Voz sobre Modo de Transferencia Asincrónica (VoATM) es el uso de una red ATM para llevar paquetes de voz digitalizada. En lugar de llevar tramas de longitudes variables, una red ATM lleva tramas de pequeñas dimensiones llamadas ***celdas***.

Cada una de estas celdas tiene una longitud de 53 bytes, conteniendo una cabecera (*header*) de 5 bytes y una carga (*payload*) de 48 bytes. En una red ATM, los paquetes de VoIP son segmentados y localizados en estas celdas. La pequeña celda ATM ofrece varias ventajas.

Este pequeño tamaño significa que la latencia o retardo que se produce cuando la celda pasa por los *switch*es ATM es muy corta. En contraste, el retardo que se produce en el almacenamiento y envío de un paquete IP a través de un *router* es más largo, porque el último bit del paquete debe ser recibido antes de que el primer bit pueda ser transmitido.

Los *switch*es ATM son extremadamente rápidos, y la calidad de servicio que se ofrece en estas redes puede ser muy alta. Adicionalmente a esto, ATM ofrece varias opciones de clase de servicio (CoS), tal como tasa de bits constante (*Constant Bit Rate,* CBR) que fue diseñada específicamente para transportar voz y otros protocolos de tiempo real. CBR provee la mejor calidad de servicio pero minimizando las variaciones de tiempo en la transición de la celda de voz, fenómeno conocido como ***Jitter***.

1.2.2.3 Enlaces Punto a Punto

El uso de enlaces punto a punto para interconectar las oficinas de una compañía, permite a ésta construir y administrar su propia red privada. Usando VoIP sobre enlaces punto a punto se puede operar ambos servicios de transmisión, datos y voz.

Los protocolos comunes de capa enlace usados por enlaces punto a punto son: *High-Level Data Link Control* (HDLC) y *Point-to-Point Protocol* (PPP).

1.2.3 COMPONENTES PARA PUERTOS DE VoIP GENERALMENTE UTILIZADOS

En este punto se analizarán algunos componentes que generalmente se utilizan para la implementación de soluciones VoIP. Como ya se conoce, en el mercado existen varios ambientes en los que se podría implementar VoIP, pudiendo ser el caso de pequeñas, medianas y grandes oficinas.

Diferentes tipos de aplicaciones requieren tipos específicos de puertos o interfaces. En algunas ocasiones el tipo de puerto depende del tipo de dispositivo que se encuentre conectado a la red.

Ciertas compañías podrían actualizar sus equipos de redes de datos para poder soportar tráfico de voz en su misma red, e inclusive existen marcas de equipos que únicamente con el cambio de una tarjeta, mas no todo el equipo, podrían migrar a una solución de VoIP.

Numerosos componentes relacionados con voz son adquiridos para completar una solución VoIP, pero el objetivo es examinar los componentes más necesarios tales como: módulos de voz (VNM) e interfaces de voz (VIC) que ciertos equipos los necesitan para soportar este tipo de tráfico.

Por lo tanto se analizará el hardware que básicamente se utiliza para poder implementar VoIP y mas que todo poder interconectar a la tradicional PSTN. Para la interconexión con la PSTN se van a analizar los tipos de enlaces troncales de voz analógicos.

Estos enlaces troncales se utilizan cuando el *switch* telefónico no soporta conexiones digitales, o cuando se necesitan pocos canales de voz. Hay tres tipos comunes de enlace troncal analógico: Inicio de Bucle (*loop-start*), Inicio de tierra (*ground-start*), E&M.

1.2.3.1 Inicio de Bucle (*loop-Start*)

Los sistemas de telefonía residencial de todo el mundo utilizan señalización *loop-start*. Debido a que los enlaces troncales se conectan entre los *switches* telefónicos y las líneas conectan un *switch* telefónico a un teléfono, las facilidades particulares se llaman líneas *loop-start*. Un circuito entre una CO (Oficina Central) y un PBX se puede llamar enlace troncal desde la perspectiva del cliente, o línea desde la perspectiva del vendedor del circuito.

La señalización analógica *loop-start* utiliza sólo un par de cables entre el *switch* telefónico en una CO y el teléfono o *switch* telefónico conocido como CPE (Equipo terminal del abonado). En la figura 1-7 se muestra un circuito libre *loop-start* sin llamadas activas.

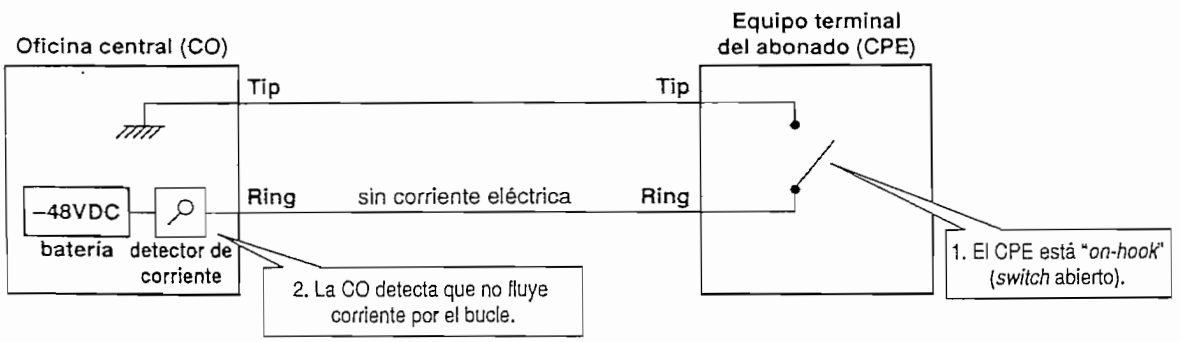


Figura 1-7 Circuito *loop-start* en un estado libre [7]

La CO proporciona una batería de corriente continua (DC) de -48 V, que genera corriente eléctrica a través del bucle del circuito. Los teléfonos particulares no necesitan fuentes de potencia separadas por esta razón. La CO también proporciona un generador de tono de marcación y un generador de *ringing* de corriente alterna (AC) para señalar al CPE. La corriente eléctrica fluye desde la batería en la CO al CPE mediante el cable *RING*, y vuelve a través del CPE a la CO a tierra mediante el cable *TIP*.

Cuando el CPE está en el estado *on-hook* (es decir, el teléfono está colgado), hay un *switch* eléctrico abierto que evita que la electricidad fluya a través del bucle del circuito. Cuando el CPE inicia una llamada cambiando al estado *off-hook* (teléfono descolgado), el *switch* se cierra y la correinte fluye a través del bucle del circuito. Cuando la corriente fluye por el bucle, la CO detecta la condición *off-hook* del CPE. La CO responde transmitiendo un tono de marcación en el bucle, el cual informa al CPE de que la CO está preparada para recibir dígitos del número telefónico del destino (figura 1-8).

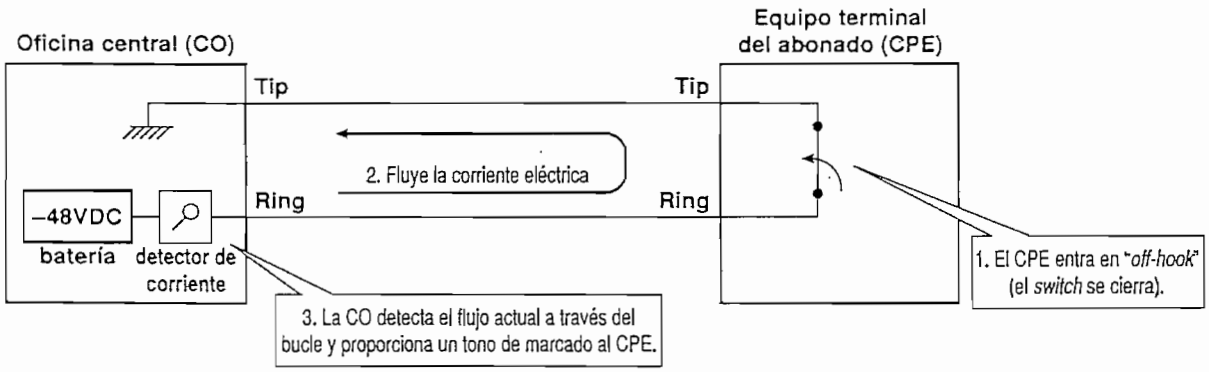


Figura 1-8 El CPE inicia una conexión en un enlace troncal *loop-start* [7]

Cuando la parte distante responde a la llamada la CO local transmite la señal de supervisión de respuesta con una inversión de polaridad en los cables *tip* y *ring.* En otras palabras, las conexiones *tip* y *ring* a tierra y a la batería se invierten en la CO durante la llamada (figura 1-9).

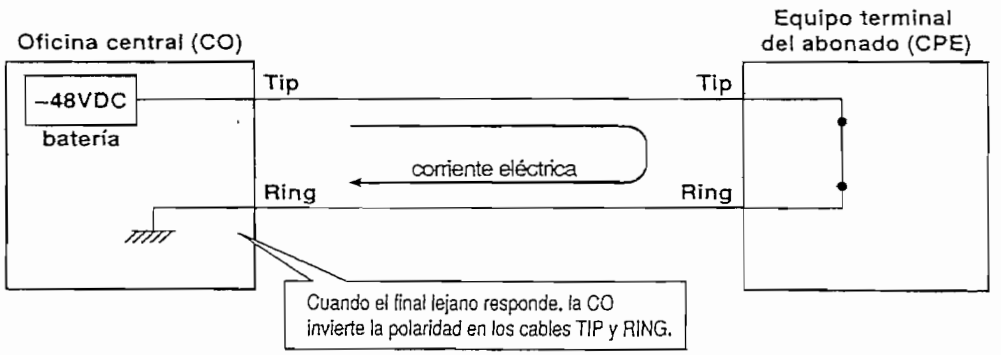


Figura 1-9 Inversión de polaridad de *TIP* y *RING* [7]

1.2.3.2 Inicio de Tierra (*Ground-Start*)

Este tipo de enlaces también utilizan dos cables entre la CO y el CPE. Estos enlaces no funcionan correctamente a menos que los cables *tip* y *ring* se conecten con la polaridad correcta (es decir, *tip* a tierra, *ring* a -48 VDC). En la figura 1-10 se muestra un circuito *ground-start* en estado desocupado.

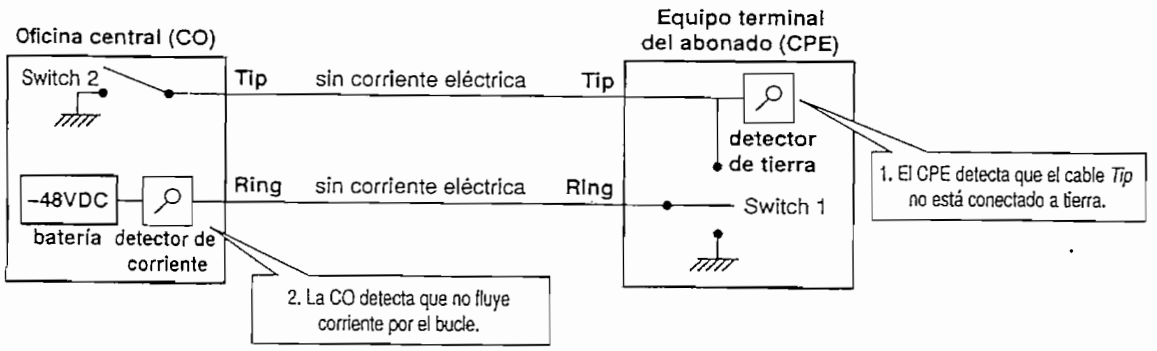


Figura 1-10 Enlace troncal *ground-start* en un estado desocupado [7]

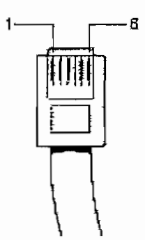
Los enlaces troncales *ground-start* son más difíciles de suministrar a la capa física que los enlaces troncales *loop-start*. Mientras que los enlaces troncales *loop-start* no son afectados por la polaridad *tip/ring*, los enlaces *ground-start* dependen de la polaridad apropiada. Esto significa que los cables cruzados en una regleta telefónica no afectará a un enlace troncal *ground-start*. Sin embargo puede ser el origen de fallo para un enlace *ground-start*, el potencial eléctrico de tierra debe ser el mismo en

ambas localizaciones. En la práctica, la única forma de conseguir este requisito es asegurar que los sistemas eléctricos de ambas localizaciones estén bien conectados a tierra.

Como ya se había mencionado, en su mayoría, los sistemas telefónicos analógicos utilizan enlaces *loop-start*, o ciertos equipos permiten escoger entre ambas señalizaciones. Los componentes más comunes que utilizan este tipo de señalizaciones son: FXS y FXO.

1.2.3.2.1 Interfaz FXS (Foreign eXchange Station)

El puerto FXS se emplea para conectar a un dispositivo de red, como un *router,* un teléfono analógico común o un fax. El puerto FXS puede surninistrar voltajes de timbrado, tonos *dial*, y otras señalizaciones básicas que requieren los teléfonos comunes. El puerto FXS es configurado con un estándar de conexión RJ-11 (figura 1-11).



Pin	Señal
1	-
2	-
3	Ring
4	Tip
5	-
6	-

Figura 1-11 Configuración de pines de un RJ-11 para conectores FXS y FXO [9]

Para la realización de llamadas internas, la señalización de una llamada entre dos teléfonos remotos que se encuentren en una red local, la hacen los *routers*; en este caso, en nada interviene la PSTN, y los teléfonos analógicos estarían conectados a las interfaces FXS de los *routers* como indica la figura 1-12.

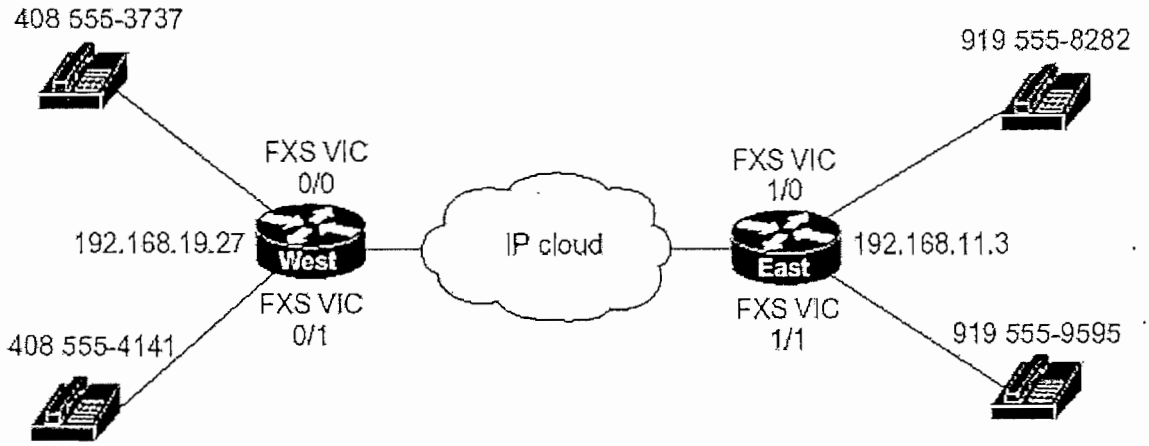


Figura 1-12 Conexión IP entre *routers* en una red privada [9]

1.2.3.2.2 Interfaz FXO (Foreign eXchange Office)

El puerto FXO al igual que el FXS es configurado con un conector RJ-11 (figura 1-11). Sin embargo en lugar de proporcionar la señalización y el voltaje, necesita de un equipo básico de telefonía; los puertos FXO son usados para conectar la red IP a la tradicional PSTN, o a una línea de una central PBX.

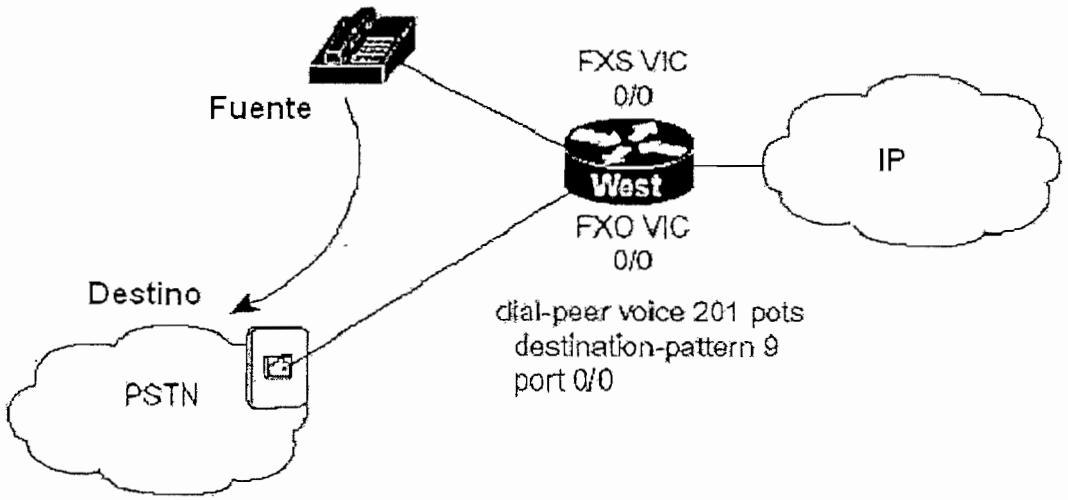


Figura 1-13 Conexión entre una Red IP y la PSTN [9]

Por lo tanto las interfaces FXO proveen de un *gateway* para la conexión entre una red de VoIP y la analógica PSTN (figura 1-13) o una PBX que no soporte señalización E&M.

1.2.3.3 E&M (*Ear and Mouth/Earth and Magneto*)

Los diagramas de circuito E&M tienen cables que se nombran con E y M, de modo que el nombre es relevante en cualquier caso.

En los enlaces troncales *loop-start* y *ground-start* se utilizaba el mismo par de cables tanto para la ruta de audio como para las funciones de señalización, en los enlaces troncales E&M se aislan estas funciones en par de cables distintos.

Dependiendo de la configuración del circuito E&M, las señales de enlace troncal y la ruta de audio pueden necesitar uno o dos pares de cables, para un total de cuatro a ocho cables. La figura 1-14 identifica la configuración de pines que se utiliza en este tipo de interfaces con su respectiva descripción.

Pin	Cable	Nombre	Descripción
1	SB	Señal de batería	Forma un bucle con el cable M a través del que la corriente puede fluir en configuraciones de aislamiento de tierra
2	M	Boca (*Mount*) o Magneto	La boca del PBX habla a la CO por este cable. El estado de la señal es: 1) flujo de corriente; o 2) no hay flujo de corriente.
3	R	*Ring*	Proporciona audio entrante a la PBX en circuitos E&M de 4 cables
4	R o R1	*Ring*	Audio saliente o audio en dos sentidos (input/output) en circuitos de 2 cables
5	T o T1	*Tip*	Audio saliente o audio en dos sentidos (input/output) en circuitos de 2 cables
6	T	*Tip*	Proporciona audio entrante a la PBX en circuitos E&M de 4 cables
7	E	Oído (*Ear*) o Tierra (*Earth*)	El oído del PBX oye las señales desde la CO en este cable. El estado de la señal es: 1) flujo de corriente; o 2) no hay flujo de corriente
8	SG	Señal a tierra	Forma un bucle con el cable E a través del que la corriente puede fluir en configuraciones de aislamiento de tierra

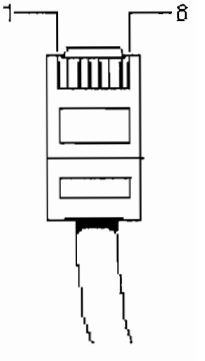


Figura 1-14 Conector RJ-48 y configuración de pines [9]

Esta interfaz se realiza a través de un conector de tipo RJ-48S (figura 1-14) que permite conexiones especialmente para interconexión entre PBX (generalmente conocidas como *tie-line* y *trunk connection*).

Si se tiene más que unos pocos usuarios de voz por oficina, podría ser eficiente usar un PBX en cada localización para conmutar el tráfico local y direccionar las llamadas entrantes.

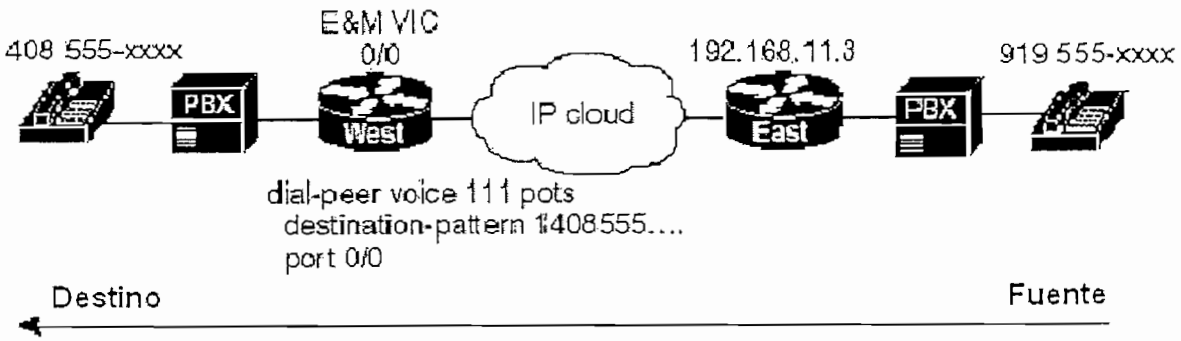


Figura 1-15 Enlace entre centrales PBX, por medio de una red IP [9]

Un enlace troncal E&M analógico puede operar en el modo E&M de dos cables o en el modo E&M de cuatro cables.

Los circuitos E&M de dos cables alojan las direcciones de transmisión y recepción de la ruta de audio sobre un solo par de cables.

Los circuitos E&M de cuatro cables utilizan un par de cables para la dirección de transmisión y otro par de cables para la dirección de recepción de la ruta de audio.

Hay cinco configuraciones primarias de circuitos E&M, las cuales se distinguen por el grado de aislamiento eléctrico a tierra y la capacidad de operar en una configuración *back-to-back.* Estas configuraciones son los tipos de circuitos E&M.

1.2.3.3.1 ***E&M, Tipo I***

La figura 1-16 ilustra la configuración del circuito para enlaces troncales E&M tipo I. La CO señaliza un estado libre *on-hook* a la PBX dejando el *switch* 1 en posición abierta. La PBX detecta la señal en ausencia de un flujo de corriente a través del cable E.

La CO señaliza un estado *off-hook* a la PBX cerrando el *switch* 1, lo que provoca que la corriente fluya a través del cable E. La PBX detecta corriente en el cable E durante la señal *off-hook* desde la CO.

La PBX señala un estado libre *on-hook* a la CO dejando el *switch* 2 en la posición a tierra, que lleva a tierra el cable M. No hay corriente en el cable M en esta condición, porque cada extremo del cable está conectado a tierra. La CO detecta la ausencia de corriente en el cable M durante la señal *on-hook* desde la PBX.

La PBX señala un estado *off-hook* a la CO conectando el cable M a una batería, lo que hace que la corriente fluya a través del cable M. La CO detecta el flujo de corriente en el cable M durante la señal *off-hook* desde la PBX.

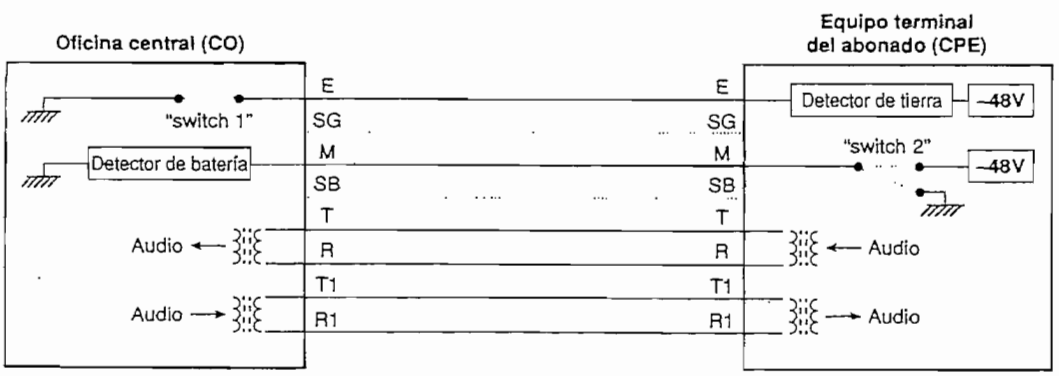


Figura 1-16 Circuito E&M tipo I [7]

Se puede deducir que los enlaces E&M tipo I no proporcionan aislamiento a tierra, porque la corriente fluye desde una batería en la PBX a tierra en la CO.

1.2.3.3.2 ***E&M, Tipo II***

La figura 1-17 muestra la configuración de un circuito E&M tipo II. Exactamente como en la señalización E&M tipo I, la CO señala un estado libre *on-hook* a la PBX dejando el switch 1 en la posición abierta.

La CO señaliza un estado *off-hook* cerrando el *switch* 1, lo que hace que la corriente fluya por el cable E (y el cable SG), donde se detecta por la PBX. La PBX señaliza un estado libre *on-hook* a la CO dejando el *switch* 2 en la posición abierta, que hace que no fluya corriente a través del cable M.

La PBX señaliza un estado *off-hook* cerrando el *switch* 2, lo que permite que la corriente fluya desde la batería de la CO a través del cable SB, y se vuelva por el cable M al detector de corriente en la CO.

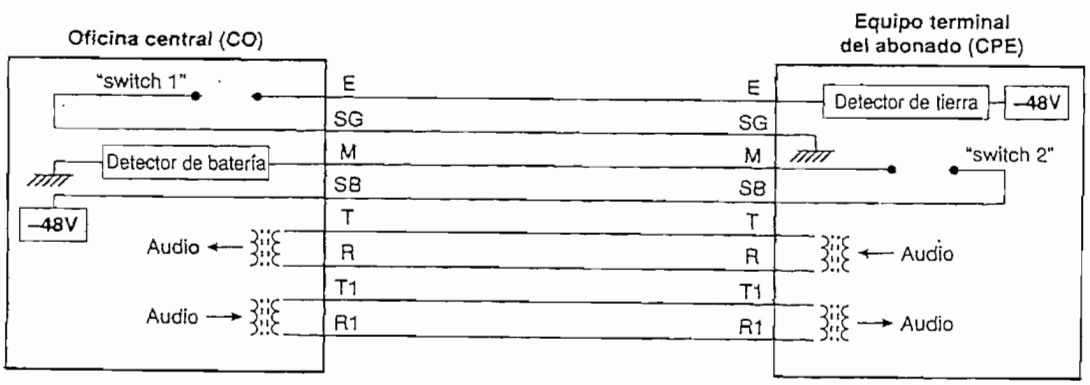


Figura 1-17 Circuito E&M tipo II [7]

Los circuitos E&M tipo II operan de la misma manera que los tipo I, con la adición de un elemento de aislamiento a tierra. En lugar de situar la toma a tierra por el cable E en los terminales de la CO, el cable SG actúa como un cable de extensión para llevar corriente de vuelta a la toma de tierra en la PBX.

En lugar de situar la batería por el cable M en la PBX, el cable SG actúa como un cable de extensión para llevar la corriente desde una batería a la CO.

1.2.3.3.3 E&M, Tipo III

La figura 1-18 muestra la configuración del circuito E&M tipo III. Un elemento interesante de este tipo de circuito es que las señales procedentes del CPE a la CO necesitan tres cables (M/SG/SB), mientras que las señales desde la CO al CPE sólo necesitan de un cable. Esta simetría permite al lado CPE operar normalmente en ausencia de una buena referencia a tierra.

La CO controla qué señal se envía al CPE mediante el cable E exactamente como en el circuito tipo I. El CPE controla qué señal se envía desde la CO mediante el cable M configurando el *switch* 2 de modo que M se conecta a SB o a SG. El CPE conecta M a SB para señalar un estado *off-hook*, y conecta M a SG para señalar un estado *on-hook*. En ambos casos, la tierra o la batería en el cable M se originan desde el lado de la CO.

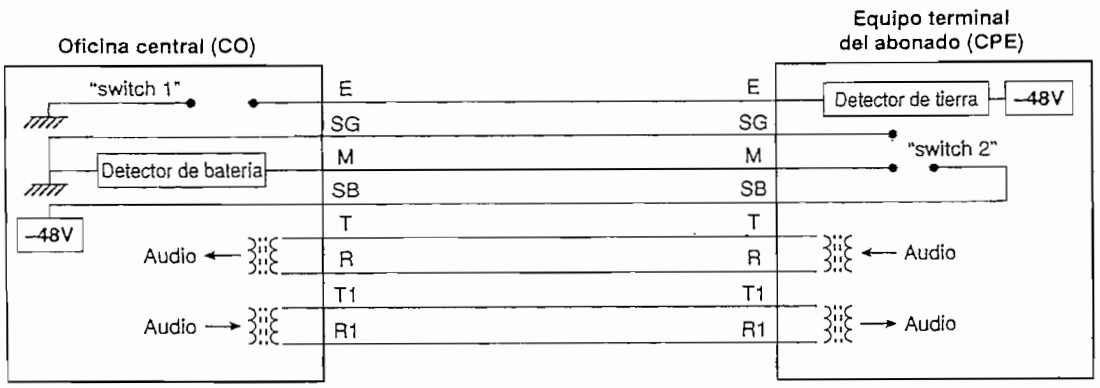


Figura 1-18 Circuito E&M tipo III [7]

1.2.3.3.4 E&M, Tipo IV

La figura 1-19 muestra la configuración del circuito E&M tipo IV. Este tipo de circuitos son casi idénticos a los circuitos tipo II. El bucle de circuito formado por los cables E y SG funciona igual que en un circuito tipo II. El bucle formado por los cables M y SB es ligeramente diferente, ya que las posiciones de la batería y tierra están combinadas y la polaridad de la corriente está invertida. Los *swtiches* realizan las funciones que el E&M tipo II (el switch abierto es *on-hook*, y el switch cerrado es *off-*

hook). Sin embargo, un estado *off-hook* desde la PBX da un voltaje de nivel a tierra en le cable M y en el cable SB, en oposición al voltaje de nivel de la batería en el caso del circuito E&M tipo II.

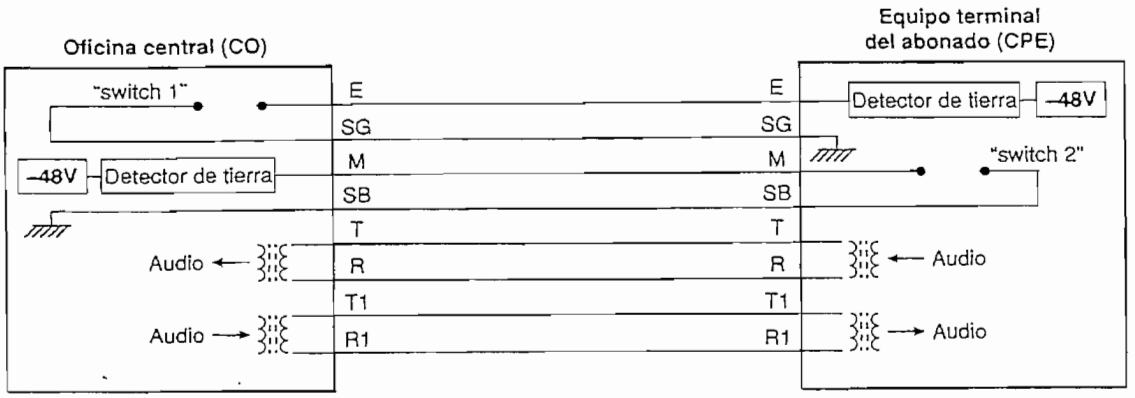


Figura 1-19 Circuito E&M tipo IV [7]

1.2.3.3.5 E&M, Tipo V

Este tipo combina la simplicidad del cableado E&M tipo I, con los beneficios del aislamiento de tierra, exactamente no existe aislamiento a tierra, sin embargo, trata el problema de la fuga de corriente.

La figura 1-20 muestra la configuración del circuito E&M tipo V. Los switches 1 y 2 están abiertos cuando la PBX y la CO están enviando un estado *on-hook* desocupado. El switch 1 se cierra cuando la CO señala un *off-hook* a la PBX, y el switch 2 se cierra cuando la PBX señala un *off-hook* a la CO.

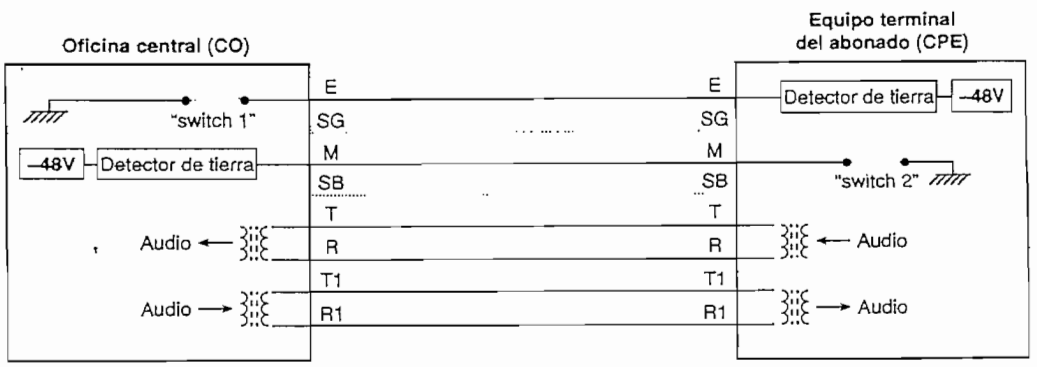


Figura 1-20 Circuito E&M tipo V [7]

1.2.3.4 Telefonía IP

La telefonía IP se refiere a servicios de comunicaciones como, voz, fax, aplicaciones de mensajes de voz, etc. que son transportados a través de una red IP. La infraestructura de telefonía IP está caracterizada por 4 componentes, éstos son:

1.2.3.4.1 Infraestructura

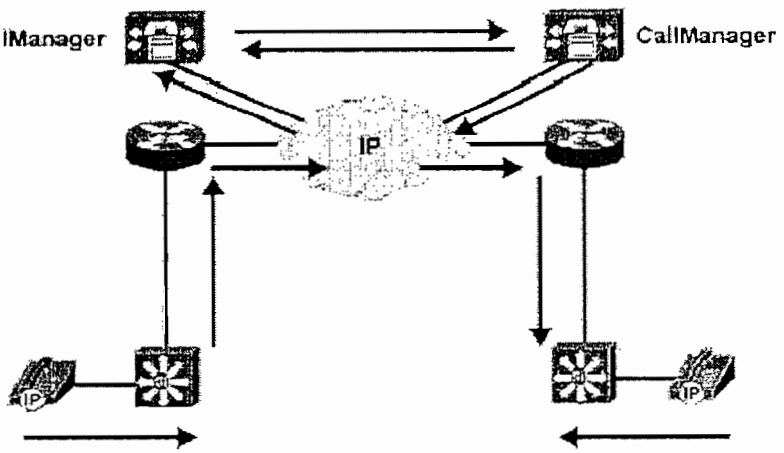


Figura 1-21 Sistema de Telefonía IP [7]

La infraestructura está basada en conmutación de capa 2 y capa 3, y un *gateway* que sirve para la interconexión con la PSTN. La señalización es manejada por un administrador de llamadas o Central IP (*CallManager*; figura 1-21).

Los dispositivos finales son conectados a puertos Ethernet 10/100 de *switches* comunes.

1.2.3.4.2 Administrador de Llamadas

El administrador de llamadas puede ser un equipo o un software que administra el procesamiento de la llamada. Este administrador posee funciones similares a las centrales PBX comunes como por ejemplo:

- Registro de dispositivos telefónicos IP
- Procesamiento de llamadas
- Administración de planes de digitalización y planes de ruteo
- Administración de recursos

1.2.3.4.3 Aplicaciones

Las aplicaciones de un sistema de telefonía IP añaden nuevas características a un sistema analógico tradicional como por ejemplo: *Voice mail*, *Interactive Voice Response* (IVR), centro de contactos, contestación automática, grabación y monitoreo de llamadas, etc.

Las aplicaciones de un sistema de telefonía IP generalmente son de código abierto y puede ser desarrollado dependiendo de las necesidades y requerimientos de las compañías.

1.2.3.4.4 Dispositivos Clientes

Los dispositivos clientes son teléfonos IP y aplicaciones de software que permiten comunicación a través de una red IP. Los teléfonos IP son capaces de digitalizar las señales de voz, ya que poseen procesadores digitales de señales (DSPs) para desempeñar esta función. Estos dispositivos contienen interfaces Ethernet y FastEthernet para la conexión con la LAN, y deben registrarse en algún tipo de administrador de llamadas.

También existen aplicaciones de software, que son teléfonos virtuales corriendo en un computador. El computador donde se implemente este software debe poseer micrófono y altavoces para poder operar igual que un teléfono.

Adicionalmente este software digitaliza las señales de voz y las envía por medio de paquetes IP a través de la red de datos.

1.3 CARACTERÍSTICAS DE TRÁFICO DE VOZ [4]

La red tradicional de telefonía fue originalmente diseñada para transportar tráfico de voz. La tecnología de diseño de circuitos conmutados provee garantía en el camino y en el retardo entre la fuente y destino.

Una red IP fue originalmente diseñada para llevar datos. La red de datos no fue diseñada para llevar tráfico de voz a pesar de que el tráfico de datos es un tráfico del mejor esfuerzo. Para transportar señales de voz requiere que se implemente calidad de servicio. En ausencia de parámetros de calidad de servicio un paquete de voz es tratado de igual manera que un paquete de datos. El usuario debe tener una red administrada, de extremo a extremo, que permita "correr" aplicaciones sensitivas al retardo tal como VoIP.

Diferentes tipos de tráfico requieren distintas características de desempeño en una red. Una aplicación de transferencia de archivos simplemente podría necesitar un *throughput* fijo por ejemplo, pero a este tipo de tráfico no le interesa el retardo de los paquetes. Otro tipo de aplicaciones como las interactivas, deberían tener tiempos de respuestas consistentes. Las llamadas de voz necesitan niveles bajos de retardo.

Existen problemas en asociar tráfico de voz en tiempo real en una red IP que es del mejor esfuerzo, porque se conoce que una red IP es no orientada a conexión y la información tiene varios caminos para llegar a su destino.

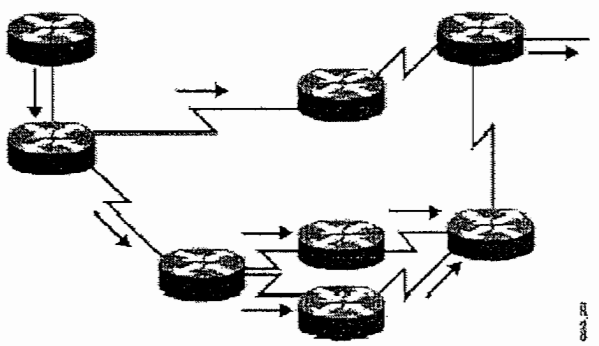


Figura 1-22 Red IP [7]

Por este tipo de razones, muchos usuarios suelen tener inconvenientes con el desempeño de su red, por lo que ellos deben tener en cuenta el tipo de tráfico que va a estar circulando por la red y ver la manera de cómo controlarlo. Los problemas que se podrían generar son:

- Lentitud en la aplicación.
- Aplicaciones de vídeo se quedan quietas por momentos.
- La comunicación telefónica posee mucho retardo y se mezclan las conversaciones.
- Se pierden las llamadas, entre otros.

En redes IP como la de la figura 1-22, los paquetes de voz que entran a la red tienen una tasa constante que puede alcanzar a su destino a través de varios *routers*. Cada uno de éstos podría tener diferentes características de retardo, y el arribo de los datos puede variar; a esta condición se la llama *Jitter*.

Otro efecto de tener varios *routers* es que los paquetes de voz pueden llegar en desorden. La transmisión en una red de datos añade ruido, retardos, ecos, *jitter*, y pérdida de paquetes. VoIP es susceptible a estos problemas, los cuales degradan las aplicaciones de voz.

Si una red VoIP provee la misma calidad que la red tradicional de telefonía, entonces la red podría garantizar que el retardo en transmitir los paquetes de voz a través de la red, esto es el *jitter* que se puede presentar, no exceda los límites específicos. En estos casos para poder eliminar estos problemas se debería implementar características de Calidad de Servicio. La Calidad de Servicio procura resolver problemas de tráfico de red. Desafortunadamente mejorando una característica de Calidad de Servicio, se podría degradar otra.

El ancho de banda define la capacidad de transmisión del medio. Herramientas de compresión reducen la cantidad de ancho de banda necesaria para enviar todos los

paquetes, pero el proceso de compresión añade algunos retardos por paquetes y consume ciclos de CPU.

El *Jitter* es una variación del retardo entre paquetes consecutivos. Un *router* puede reducir *Jitter* para cierto tipo de tráfico, pero esto suele generar retardos y *Jitter* para otro tipo de tráfico.

1.3.1 CONSIDERACIONES DE ANCHO DE BANDA PARA TRÁFICO DE VOZ

Las llamadas de voz crean un flujo con una tasa de datos fija, con igual número de bits entre cada paquete. El flujo de voz puede ser descrito como *isochronous* que significa "caracterizado por u ocurrido en igual intervalo de tiempo." Considere la figura 1-23, donde la llamada puede ser entre teléfonos analógicos con las extensiones 201 y 301 [4].

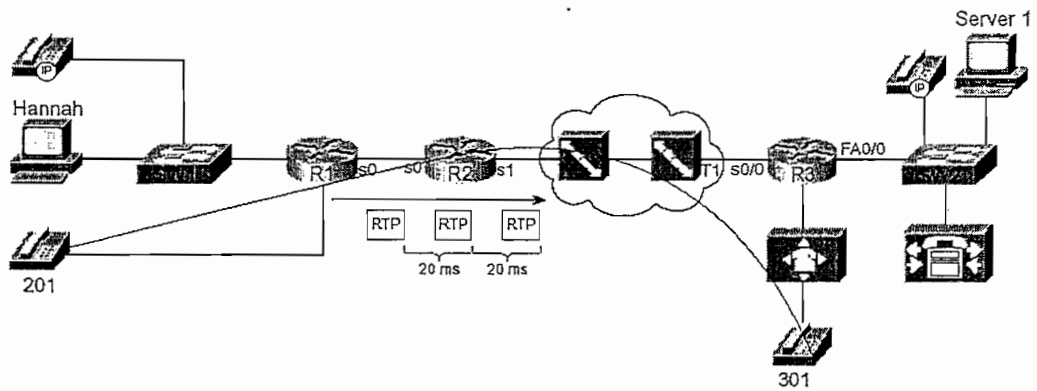


Figura 1-23 Flujo *isochronous* de paquetes para una llamada de voz [4]

El *router* R1 crea los paquetes de voz IP/UDP/RTP y los envía, por defecto, cada 20 ms (tiempo que tarda en codificar cada paquete y enviarlo), pero se debe conocer cuánto ancho de banda es realmente necesario para esta llamada de voz. El ancho de banda depende de algunos factores:

- *Codec*
- Sobrecarga del paquete (*Overhead*, IP/UDP/RTP)
- Fragmentación (*Data link framing*, que depende del tipo de enlace utilizado)
- Compresión

Tabla 1.2 Requerimientos de capacidades para varios tipos de tecnologías de capa enlace [4]

Tipo de *header* de (capa 2)	Tamaño del *header* (capa2)	Tamaño del *header* (IP/UDP/RTP)	Codec	Capacidad del *payload*	Capacidad Total requerida**
Ethernet	14 bytes	40 bytes	G.711	64 Kbps	85.6 Kbps
MLPPP/FR*	6 bytes	40 bytes	G.711	64 Kbps	82.4 Kbps
Ethernet	14 bytes	40 bytes	G.729	8 Kbps	29.6 Kbps
MLPPP/FR	6 bytes	40 bytes	G.729	8 Kbps	26.4 Kbps

* *MLPPP/FR: MultiLink PPP/Frame Relay*

** *Datos obtenidos por medio del proceso de la sección 3.4.2*

Las llamadas que usan G.711 poseen 64 Kbps (tabla 1.2), o usan G.729 que tiene 8 Kbps. Estas capacidades o velocidades de transmisión consideran solo el *payload*, ignorando capa de enlace, y cabeceras de IP, UDP, y RTP.

En la tabla 1.2 se observan los requerimientos de capacidades para varios tipos de llamadas de voz.

El requerimiento de ancho de banda, si se utiliza compresión en las cabeceras del paquete RTP, varía dramáticamente basado en el efecto del *codec* y la compresión. *Compressed* RTP (cRTP) actualmente comprime las cabeceras IP/UDP/RTP, con sustancial reducción en ancho de banda, y usa codificadores de menos tasa de bits.

En la tabla 1.3 se presentan los requerimientos de capacidades para diferentes tipos de enlaces.

Tabla 1.3 Requerimientos de capacidades para varios tipos de enlaces [4]

Carga (incluye overhead de L2)	802,1Q Ethernet (32 bytes de overhead de L2)	PPP (9 bytes de overhead de L2)	MLP (13 bytes de overhead de L2)	Frame Relay (8 bytes de overhead de L2)
G.711 en 50 pps	93 Kbps	84 Kbps	86 Kbps	84 Kbps
G.711 en 33 pps	83 Kbps	77 Kbps	78 Kbps	77 Kbps
G.729A en 50 pps	37 Kbps	28 Kbps	30 Kbps	28 Kbps
G.729A en 33 pps	27 Kbps	21 Kbps	22 Kbps	21 Kbps

* pps = paquetes por segundo

1.3.2 CONSIDERACIONES DE RETARDO EN TRÁFICO DE VOZ

La calidad de una llamada de voz se deteriora cuando ocurre demasiado retardo. El tráfico de voz experimenta retardos como cualquier otro paquete; el retardo puede originarse debido a varias fuentes. En la tabla 1.4 se pueden observar algunos componentes de retardo.

Tabla 1.4 Componentes de Retardo [4]

Componentes de Retardo	Definición	Donde ocurre
Retardo de serialización	Tiempo que toma en llevar todos los bits de una trama al medio físico. Es de acuerdo al tamaño de la trama y a la velocidad del enlace.	Típicamente en la salida de cada interfaz.
Retardo de Propagación	El tiempo que toma a un bit en trasladarse por el medio físico de un lugar a otro.	En cada enlace físico. Es ligeramente despreciable en el enlace de la LAN y en enlaces de cortas distancias de una WAN.
Retardo por encolamiento	Tiempo gastado en una cola de espera hasta la oportunidad de ser enviado.	Generalmente en las salidas de la interfaz.
Retardo por envío y procesamiento	Tiempo requerido en recibir una trama hasta que la trama/paquete haya sido encolada para transmitir.	En algunas piezas de equipos de conmutación, incluyendo *routers*, *switches* LAN, *switches Frame Relay*, y *switches* ATM.
Retardo modelado (*Shaping Delay*)	Retardo formado en la transmisión paquetes (es configurado). Se utiliza para evitar paquetes perdidos en medio de una nube *Frame Relay* o ATM.	Este retardo se lo configura en el *router* cuando se envía paquetes a redes *Frame Relay* o ATM.
Retardo de la red	Retardo que se produce por componentes de los *carriers*, cuando se usa un servicio.	Dentro de la red del proveedor del servicio.

En la figura 1-24 se muestra un ejemplo del concepto de retardo, con simples valores de retardo; cuando el retardo es despreciable su valor se presenta en cero.

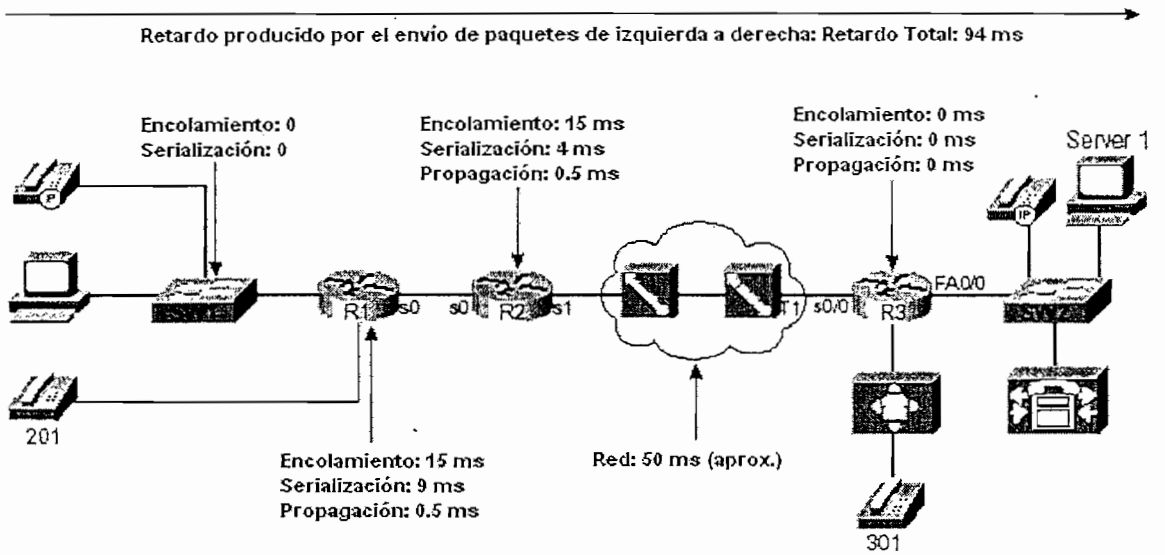


Figura 1-24 Ejemplo de una red con varios componentes de retardo con el flujo de izquierda a derecha [4]

Los valores de retardo que se presentan en la figura 1-24 son básicos y reales [4]:

- El ***retardo de envío*** (*Forwarding*) es típicamente medido en milisegundos, y por lo tanto despreciable.
- *El* ***retardo de propagación*** de R1 a R2 es calculado en base a un enlace de 100 Km (figura 1-15).
- Los ***retardos de serialización*** son calculados en base a un paquete codificado por G.729, sin compresión, en un enlace PPP [forma de calcular en sección 3.3.1.3].
- El ***retardo de encolamiento*** (*queuing*) varía gradualmente. El ejemplo de la figura 1-15 da un valor de 15 ms en un enlace de 56 Kbps que está en el *router* R1, el cual se basó asumiendo que una simple trama de 105 bytes fue puesta en cola delante del paquete cuyo retardo se está rastreando.
- El ***retardo de la red*** de 50 ms fue aproximado de acuerdo al proveedor de servicios.
- El ***retardo total*** es únicamente **94 ms**, lo que se asume que es aceptable.

Cuando el retardo es mínimo, la llamada de voz puede ser tolerable. La ITU define algunos estándares que dan límites aceptables de retardo (ver tabla 1.5).

Tabla 1-5 Tiempos de retardo aceptables otorgados por la recomendación ITU G.114 [4]

Retardo en una sola vía (en ms)	Descripción
0-150	Rango aceptable por la Recomendación ITU G.114
150-400	Rango de servicio degradado (ITU G.114)
+ 400	Rango no aceptado en ningún caso (ITU G.114)

Con el ejemplo dado en la figura 1-24, el retardo de la llamada de voz está en los límites aceptados por la recomendación G.114, sin embargo el tráfico de voz introduce pequeños componentes de retardo adicionales a los factores de retardo que todo paquete de datos experimenta:

- Retardo por el Codec
- Retardo de paquetización
- Retardo en el *buffer* De-*jitter* (Retardo inicial en el *payload*)

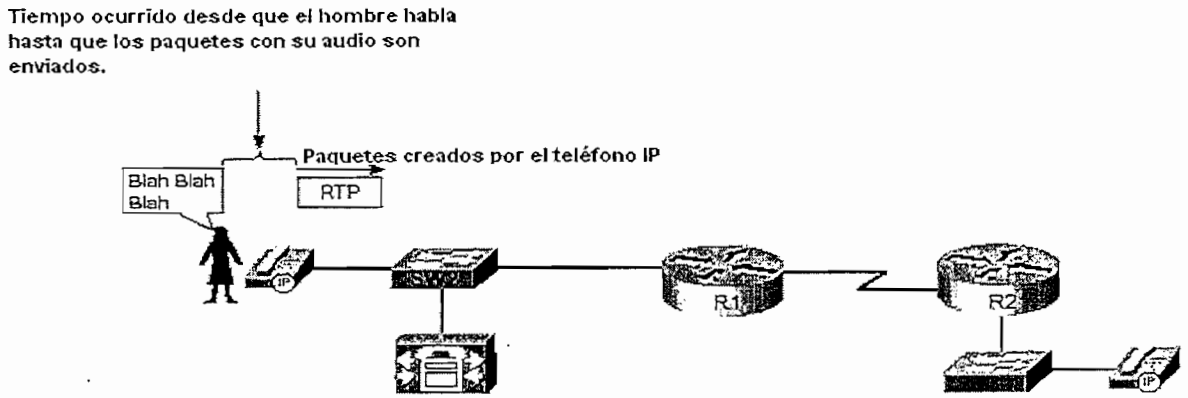


Figura 1-25 Retardo de Codec y Paquetización [4]

El retardo del Codec, y el retardo de paquetización coinciden entre sí. Para explicar mejor este tipo de retardos, se puede ver la figura 1-25 y tomar en cuenta cuándo una persona habla y cuándo el paquete IP es enviado.

Hay que considerar qué tiene que suceder en un teléfono IP antes de que un paquete pueda ser enviado. Primero se digita el número y la llamada se realiza. Cuando la llamada comienza, el teléfono IP envía paquetes RTP. Cuando estos paquetes inician, son enviados cada 20 ms (por defecto), en otras palabras, cada paquete tiene 20 ms para que la voz pueda introducirse dentro del *payload* del paquete.

Otro punto importante es el tiempo que transcurre desde que la persona empieza a generar el sonido, hasta cuando el primer paquete con estas ondas de sonido digitalizadas y paquetizadas sean enviadas. Este tiempo puede generar retardos, a este tipo de retardos se los llama: retardo de paquetización y retardo de *Codec*

El retardo de *Codec* tiene 2 componentes:

- El tiempo requerido para procesar una señal analógica y convertirla en señal digital.
- Una característica llamada *look-ahead* (causado por el algoritmo).

El primer componente de retardo de *codec* es válido para todos los *codecs*. El algoritmo utilizado por el *codec* puede causar un retardo adicional, al cual se lo llama *look-ahead*. Este componente ocurre cuando el *codec* es predictivo[5].

Consideraciones del efecto de retardos por paquetización y por *Codec*:

Se deben considerar los retardos de paquetización y de codec juntos, porque entre ellos se sobrelapan. Por ejemplo, el retardo de paquetización toma 20 ms, mientras espera los 20 ms para que la voz se produzca. Pero qué sucede en los primeros 20 ms?

[5] Codificador que toma muestras basadas en muestras anteriormente tomadas.

La tabla 1.6 muestra lo que sucede en los primeros segundos desde que se produce la voz.

Tabla 1.6 Proceso del retardo de paquetización y Codec – G.729 [4]

Cronograma	Acción	Retardo de *Codec*	Retardo de paquetización
T=0	Empieza a colectar las señales de voz para la conversión A/D.	No empieza todavía.	Comienza.
T=10	Colecta completamente los 10 ms de muestreo, el cual va a ser codificado con G.729.	Empieza.	Hasta ahora 10 ms, continúa el retardo de paquetización.
T=15	Colecta los primeros 5 ms de los segundos 10 milisegundos de muestreo.	5 ms hasta ahora, G.729 tiene ahora 5 ms que aparecen delante del algoritmo necesario para codificar los primeros 10 ms de muestreo.	Hasta ahora 15 ms, continúa el retardo de paquetización.
T=20	Colecta los primeros 5 ms de los terceros 10 milisegundos de muestreo.	Ahora 5 ms de retardo en los segundos 10 ms de muestreo, 15 ms en total, G.729 tiene ahora 5 ms que aparecen delante del algoritmo necesario para codificar los segundos 10 ms de muestreo.	Finaliza con el retardo de paquetización, 20 ms de voz han sido recibidos.
T=30	Finaliza colectando el tercer muestreo de 10 ms.	20 ms en total para el retardo de *codec*, RTP y el *payload* están listos para ser enviados.	Finaliza. 20 ms en total.
Total de retardos en el primer paquete.		20 ms	20 ms

Se nota que los retardos de paquetización y *codec* se sobrelapan. Aunque cada uno toma 20 ms, porque hay sobrelapamiento, el paquete experimenta cerca de 30 ms de retardo total, en lugar de un total de 40 ms.

1.3.3 CONSIDERACIONES DE *JITTER* EN TRÁFICO DE VOZ

Jitter es la variación entre el arribo esperado de un paquete y cuando éste es realmente recibido. Los puntos extremos de VoIP usan *buffer de_jitter* para retornar las variaciones de retardo dentro de un valor constante, para que la voz pueda tratarse fácilmente.

El *jitter* causa una especie de titubeo en la persona que habla y pierde sonidos; si el *jitter* se incrementa rápidamente se degrada la comunicación. Por ejemplo considérese la figura 1-26 donde los paquetes 3 y 4 experimentan *jitter*.

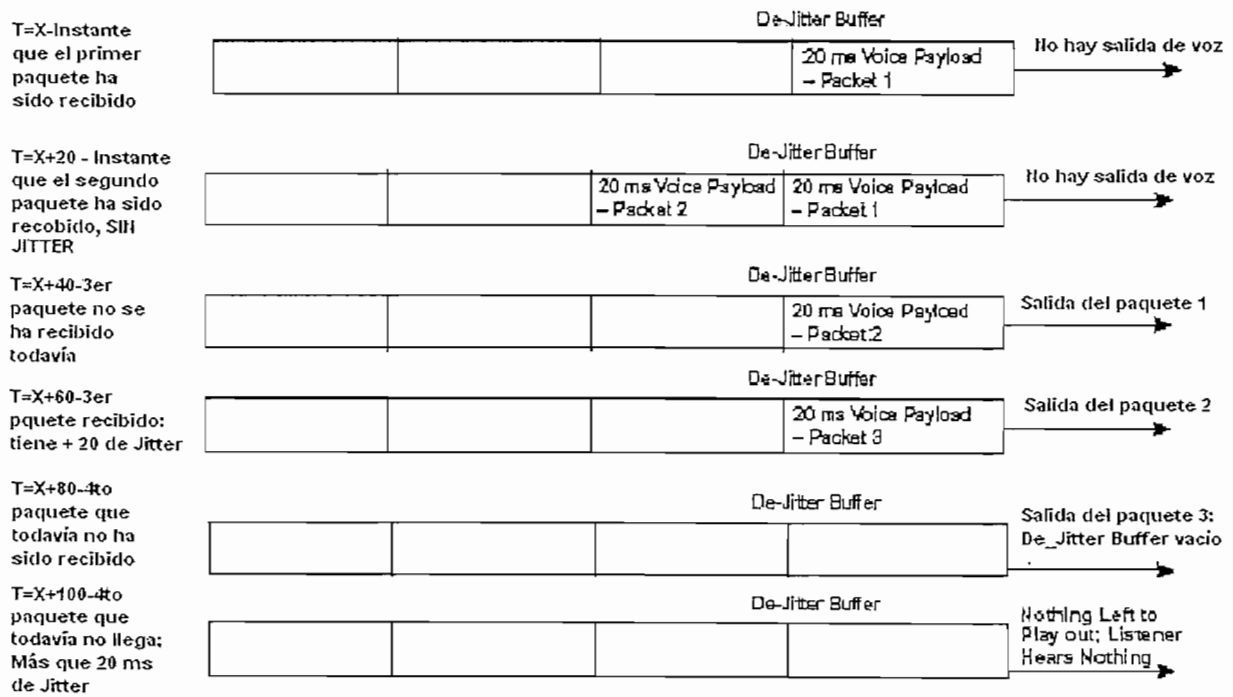


Figura 1.26 Ejemplo de *jitter* en tráfico de VoIP [4]

En la figura se observa que el segundo paquete experimenta el mismo retardo que el primero. Se puede saber porque el teléfono IP envía paquetes cada 20 ms; si ellos llegan cada 20 ms, el retardo de cada paquete es el mismo, esto significa que no hay *jitter*. Sin embargo el paquete 3 arriba 40 ms después del paquete 2, lo que significa que el paquete 3 experimenta 20 ms de *jitter*. El paquete 4 no arriba hasta 45 ms después que el paquete 3; porque el paquete 4 fue enviado 20 ms después del paquete 3, el paquete 4 experimenta 25 ms de *jitter*. Como resultado, el *buffer* de *jitter* se vacía, y existe un período de silencio. En efecto, después de que el paquete 4 aparece, el que lo reciba, lo descarta.

Pero en definitiva que causa el *Jitter*? Sus respuestas son los componentes de retardo variables. Los dos más notorios componentes de retardo variables son el encolamiento y el retardo de red. El retardo de encolamiento puede reducirse y estabilizarse por un paquete de voz, usando métodos de encolamiento que sirve al paquete de voz en cuanto sea posible.

Se podría usar fragmentación en los paquetes de datos, permitiendo a los paquetes de voz intercalarse entre estos paquetes de datos fragmentados; de esta manera se puede reducir retardos y *jitter* en redes *Frame Relay* y ATM. Herramientas de calidad de servicio, particularmente herramientas de encolamiento y fragmentación pueden ayudar a reducir el *jitter* lo suficiente para que la red trabaje efectivamente.

1.3.4 CONSIDERACIONES DE PÉRDIDA DE PAQUETES EN TRÁFICO DE VOZ

Los paquetes perdidos usualmente ocurren cuando en los *routers* se "corre" fuera del espacio del *buffer* para una interfaz particular (encolamiento de salida). La figura 1-27 ilustra un *buffer* de salida de una interfaz llena, el cual causa que los paquetes sean desechados. El término usado en estos casos de descarte es "*output drop*" o "*tail drop*" (paquetes descartados del encolamiento). El *tail drop* ocurre cuando el encolamiento de salida se encuentra lleno. Existe descartación común de paquetes cuando hay mucha congestión en el enlace.

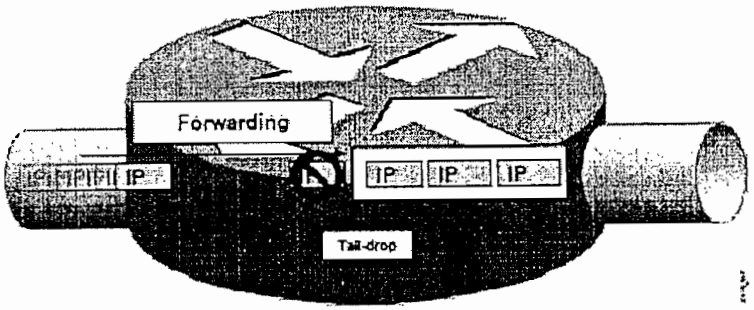


Figura 1-27 Paquete perdido en la cola del *buffer* de una interfaz [7]

Los *routers* descartan paquetes por varias razones, las dos más grandes son:

- Bits errados
- Falta de espacio en la cola

La calidad de servicio no puede ayudar mucho con los bits errados, sin embargo, la calidad de servicio puede ayudar bastante tratándose del espacio de encolamiento. La figura 1-28 contrasta un encolamiento FIFO (una cola) con un simple método de encolamiento: con una cola para el *payload* de voz, y otra para todos los demás.

Imagínese por un instante que cuatro paquetes arriban casi instantáneamente, numerados del 1 al 4, siendo el paquete 1 el primero en arribar. En el esquema FIFO, el *router* sitúa los paquetes dentro de un encolamiento de salida, en el mismo orden que arribaron. ¿Qué sucede cuando el encolamiento de salida tiene espacio únicamente para tres paquetes, como indica la figura 1-28?. El cuarto paquete es desechado de la cola.

Ahora supóngase que el cuarto paquete es de voz, y los dos sistemas de encolamientos están siendo usados. Cada cola tiene espacio para tres paquetes. En estos casos el *router* no desecha el paquete de voz (paquete 4). En efecto el *router* saca la cola de voz para que cualquier paquete siempre consiga ser enviado, por tanto, este *router* reduce el retardo para un paquete de voz.

Con el ejemplo de la figura 1-28, el *router* no desecha el paquete de voz; sin embargo, el poder real de estos dos sistemas de encolamiento para evitar paquetes de voz perdidos brilla a través de un examen un poco más minucioso.

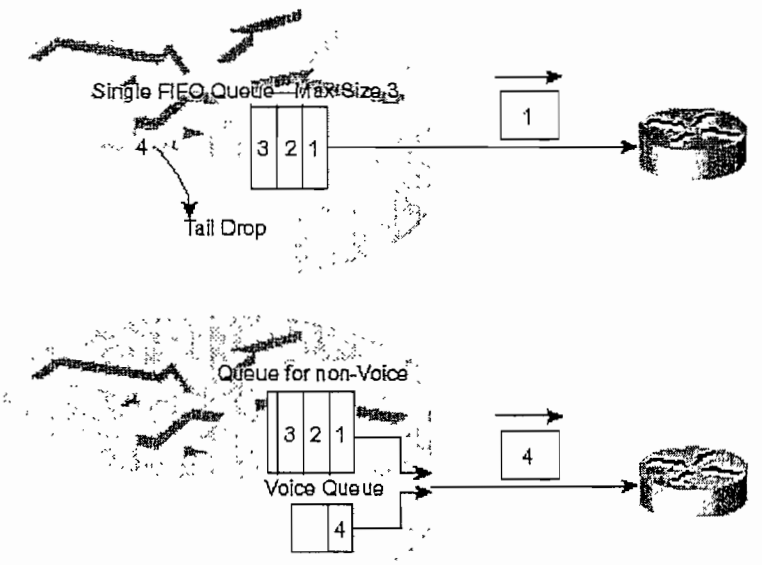


Figura 1-28 Encolamiento FIFO vs. Sistema imaginario de dos colas (una cola para voz y otra para cualquier cosa) [4]

Considérese que un CAC (Control de admisión de llamadas) permite únicamente dos llamadas concurrentes G.729a a través de este *router*, y supóngase que este *router* no usa cRTP. La capacidad de canal requerida sería de 26.4 Kbps para cada llamada, o un total de 52.8 Kbps. Ahora imagínese que el método de encolamiento siempre envía paquetes de voz en la siguiente oportunidad cuando un paquete de voz arriba, únicamente esperando por el envío actual del paquete de finalización. También imagínese que el método de encolamiento garantiza al menos 60 Kbps de los 128 Kbps del enlace para el encolamiento de la voz.

Con todas estas características la cola de voz nunca podría ponerse muy larga (asumiendo los siguientes parámetros):

- La correcta opción para la longitud máxima de encolamiento.
- Encolamiento que siempre toma los paquetes de voz como primera oportunidad.
- Control de acceso de llamadas que previenen muchas llamadas de voz
- La cola de voz nunca podría llenarse y el paquete no podría ser desechado de la cola en esta interfaz.

Otro tipo de herramienta de calidad de servicio es el control de admisión de llamadas que provee muy importantes componentes para prevenir los paquetes perdidos, y poder mejorar la calidad de la voz.

1.4 SEÑALIZACIÓN DE VoIP Y PROTOCOLOS DE TRANSPORTE DE VOZ [5]

Para proveer comunicación sobre una red IP, con protocolos de transporte en tiempo real (RTP) se deben crear sesiones. Estas sesiones son dinámicamente creadas y habilitadas por uno de los diferentes procedimientos de control de llamadas.

Típicamente, estos procedimientos incluyen también mecanismos para señalizar eventos durante llamadas de voz y para administrar y recolectar estadísticas acerca de las llamadas de voz.

Este modelo enfoca tres protocolos que ofrecen control de llamadas para VoIP: H.323, Protocolo de inicialización de llamada (*Session Initiation Protocol* - SIP), y Protocolo *gateway* de Control de Medios (*Media Gateway Control Protocol* - MGCP).

1.4.1 SEÑALIZACIÓN ENTRE *ROUTERs* Y PBXs

La conexión entre la PBX y el *router* se muestra como una línea troncal a la PBX. Una vez que se tenga esta línea troncal, la PBX envía los números digitados por el usuario al *router* de la misma manera que se envían estos números marcados a una compañía común de teléfonos o a otra PBX (figura 1-29).

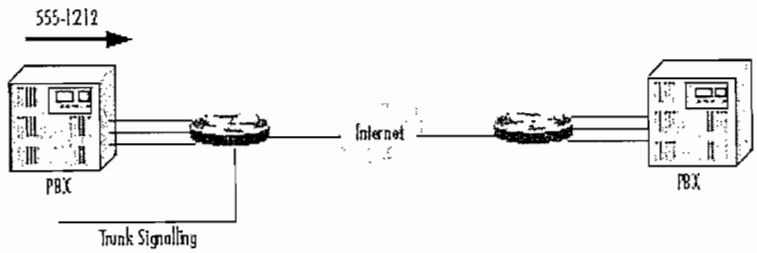


Figura 1-29 Señalización del PBX al *Router* [5]

La interfaz que se utiliza para enviar la señalización de la PBX al *router* puede ser las interfaces comúnmente utilizadas como FXS, FXO, E&M o T1/E1.

Como se puede observar en la figura 1-30, se establece la llamada por medio del protocolo Q.931 para hacer la petición al *router* y poder convalidar los números telefónicos con las direcciones IP. Mientras tanto este canal de control se usa para estructurar los *streams* de audio RTP.

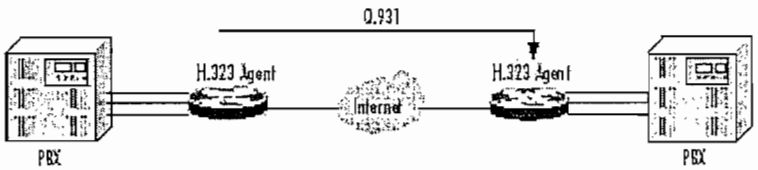


Figura 1-30 Señalización de *Router* a *Router* [5]

Cuando el *router* remoto reciba la petición de la llamada Q.931, éste señala una línea para la conexión a la PBX. Después de reconocer esta línea de conexión, el *router* remoto envía los números marcados a la PBX y realiza un reconocimiento de llamada al *router* original como se muestra en la figura 1-31.

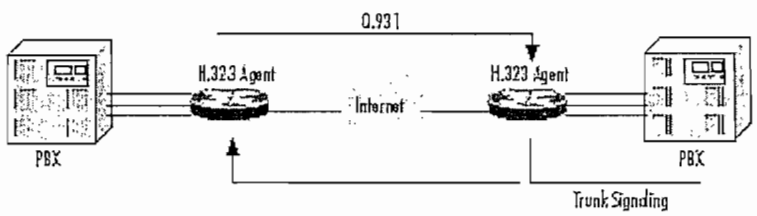


Figura 1-31 Señalización de *Router* a PBX [5]

1.4.2 SEÑALIZACIÓN DE VoIP

En arquitecturas de redes no orientadas a conexión tal como redes IP, la responsabilidad para establecer sesiones y tener señalización es de las estaciones finales. Para emular servicios de voz a través de una red IP, es necesario mejorar estas señalizaciones. Por ejemplo, un agente H.323 se añade al *router* para soportar este tipo de estándar para el audio y el flujo de señales. El protocolo Q.931 se usa para establecer y finalizar llamadas entre el agente H.323 o las estaciones finales. H.225 es esencialmente lo mismo que Q.931.

El Protocolo de Control en Tiempo Real (RTCP) provee una transferencia de información confiable una vez que el *stream* de audio ha sido establecido. Un protocolo confiable y orientado a conexión tal como TCP se desarrolla entre las estaciones finales para llevar los canales de señalización.

RTP, el cual es construido sobre UDP, se usa para transportar el *stream* de audio en tiempo real. RTP usa UDP como mecanismo de transporte, porque éste tiene menor retardo que TCP y, porque el tráfico de voz real es diferente al tráfico o señales de datos, tolera bajos niveles de pérdidas y no podría efectivamente tener retransmisiones. La señalización de control H.245 se emplea para negociar canales que se encuentran en uso y que poseen suficiente capacidad, como los canales de audio. La tabla 1.7 muestra la relación entre el modelo OSI y protocolos utilizados en agentes de voz IP.

Tabla 1.7 Modelo OSI y el estándar H.323 [5]

Capas del modelo OSI	**Estándar**
Presentación	G.711, G.729, G.729a, etc.
Sesión	H.323, H.245, H.225, RTCP
Transporte	RTP, UDP
Red	IP, RSVP, WFQ
Enlace	RFC 1717 (PPP/ML), Frame Realy, ATM, etc.

1.4.2.1 Protocolo H.323

H.323 es probablemente el estándar más importante que soporta tecnología de voz paquetizada. Es una recomendación de la ITU que establece el estándar que define los componentes, protocolos y procedimientos necesarios para proveer comunicaciones multimedia (audio, vídeo y datos), sobre una red IP.

- **Audio:** Los algoritmo de compresión de H.323 para audio, son los que se encuentran en la recomendación ITU (G.711, G.722, G.723, G.728 y G.729). Audio es el mínimo servicio provisto por el estándar H.323.
- **Vídeo:** Las capacidades de vídeo por H.323 son opcionales (H.261, H. 263).
- **Datos:** Para datos H.323 se refiere a la especificación T.120 para conferencia de datos.

La figura 1-32 muestra los roles e interoperabilidad de varios protocolos de H.323.

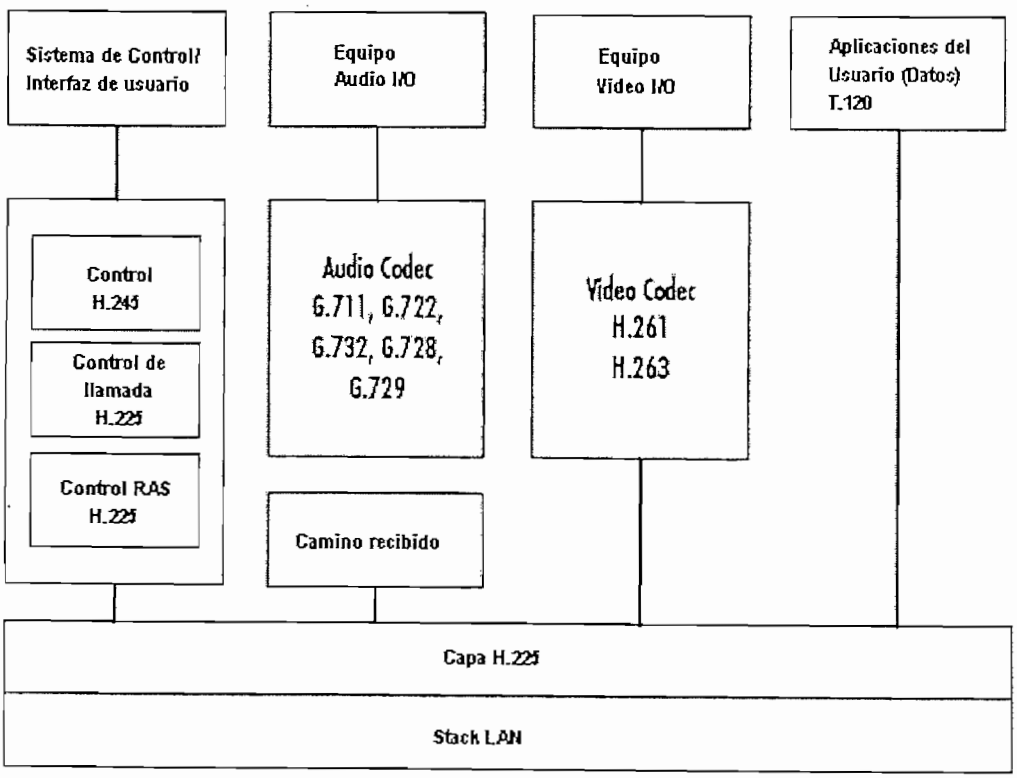


Figura 1-32 Interoperabilidad del protocolo H.323 [5]

1.4.2.1.1 Componentes de H.323

El protocolo H.323 se utiliza para numerosas aplicaciones tales como VoIP, vídeoconferencia y similares; todos los dispositivos que caen dentro del *stack* de protocolos H.323 pueden ser categorizados en uno de los cuatro tipos de dispositivos. Estos dispositivos son:

- **Terminales**: Se refieren a los puntos extremos. En el caso de voz, el terminal H.323 es generalmente un teléfono IP. En el caso de vídeo, el terminal H.323 es un terminal de videoconferencia. H.323 es también desarrollado en PC's. Una aplicación común del protocolo H.323 puede ser encontrado en software, como por ejemplo Microsoft NetMeeting que permite usar transmisiones de voz y vídeo en una PC normal.

- ***Gateways***: Trabajan como un traductor de todas las comunicaciones entre entidades H.323 y no H.323 (por ejemplo entre terminales H.323 y teléfonos de la PSTN o sistemas PBX). Los *Gateways* proveen algunas funciones:

  - **Protocolos de traslación:** El *gateway* actúa como un intérprete; permitiendo a la PSTN y la red H.323 "hablar" entre ellas.
  - **Formatos de conversión de información:** Varias redes codifican su información de diferentes maneras. El *gateway* convierte esta información para que ambas redes puedan intercambiar esta información libremente como un discurso o vídeo.
  - **Transferencia de información:** El *gateway* es el responsable de transferir información entre diferentes redes, tal como la PSTN y el Internet.

- ***Gatekeeper***: Proveen funciones de control de llamadas tal como traslación de direcciones y administración de ancho de banda.
- **MCUs (Unidades de Control multipunto):** Proveen facilidades de conferencia para usuarios que desean conferencias entre tres o más puntos.

1.4.2.1.2 Stack de Protocolos H.323

Así como con el *stack* de protocolos TCP/IP, el protocolo H.323 es una colección de protocolos que trabajan juntos para proveer funcionalidad extremo a extremo en una red convergente. Sin embargo el protocolo H.323 también tiene relación con los protocolos de TCP, IP, y UDP así como RTP. Los protocolos que fueron creados con H.323 son: Registro, Admisión y Estatus (RAS), H.245, y H.225.

a) Protocolo Internet (IP)

Como con otras redes que usan TCP/IP, el protocolo IP provee un esquema de direccionamiento jerárquico para H.323. Cada terminal, *gateway*, *gatekeeper*, y MCU tienen una única y válida dirección IP. IP provee a cada nodo H.323 una dirección y un mecanismo de ruteo de paquetes H.323 a través de la red.

b) Protocolo de Control de Transmisión (TCP)

Como ya se conoce, TCP es el responsable de proveer una transmisión confiable sobre una red no confiable incorporando mecanismos de secuenciamiento, *windowing*, y reensamblado de paquetes. En H.323, TCP se usa para proveer la conexión inicial entre terminales H.323 y *gateways* o *gatekeeper*.

c) User Datagram Protocol (UDP)

UDP ofrece una comunicación no confiable, sin secuenciamiento. Es un protocolo no orientado a conexión que sacrifica confiabilidad por velocidad. UDP confía en los protocolos de capas superiores para proveer secuenciamiento y confiabilidad y, como tal, provee un protocolo más rápido de transporte que TCP. Por esta razón UDP se usa para el transporte de llamadas VoIP.

d) H.225

H.225 provee la inicialización y control de la llamada, con toda la señalización necesaria para establecer una conexión entre dos terminales H.323. La ITU Q.931 provee un recurso para establecer, mantener y terminar las conexiones de redes a

través de la ISDN. Ésta es definida como un protocolo básico de inicialización de llamada en ISDN.

e) Registro, Admisión y Estatus

RAS es un protocolo utilizado entre dispositivos finales (terminales y *gateways*) y *gatekeeper*. Éste se usa para el manejo del registro, control de admisión, cambios en el ancho de banda, y el estatus del sistema. RAS usa el puerto UDP 1719.

f) Protocolo de Transporte de tiempo Real (RTP)

RTP provee funciones de transporte en la red de extremo a extremo apropiado para aplicaciones de transmisión en tiempo real tal como audio, vídeo, o simulación de datos, sobre redes *multicast* o *unicast*. RTP se usa para transportar datos vía UDP, no garantiza calidad de servicio para aplicaciones de tiempo real. RTCP provee un control de transporte para RTP. RTCP provee una regeneración en la distribución de la calidad de los datos y lleva un nivel de identificación para una fuente RTP usada por receptores de sincronización de audio y vídeo.

g) CODECS

Los codificadores y decodificadores se utilizan, no únicamente por el protocolo H.323, sino por todos los protocolos de VoIP para definir el grado de compresión y descompresión de los algoritmos que se emplean cuando se transporta voz y vídeo a través de una red convergente. Entre estos estándares se tiene:

- Serie G.7XX de la ITU: *codecs* de audio (G.711, G.723, G.729).
- Serie H.26X de la ITU: *codecs* de vídeo (H.261, H.263). la Serie H.26X describe *streams* de vídeo para transporte usando RTP.

La figura 1-33 muestra la interrelación de los protocolos H.323.

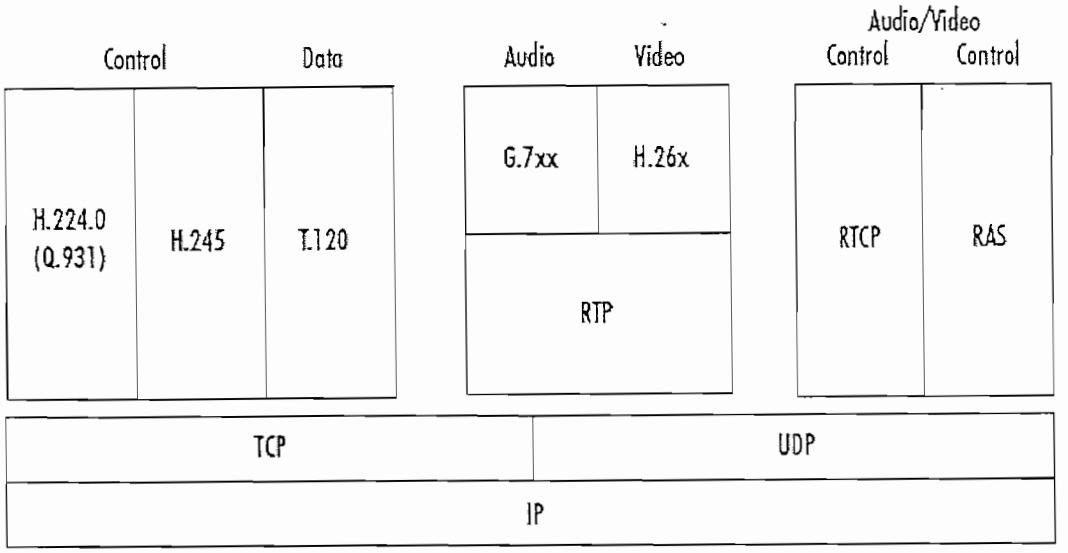


Figura 1-33 *Stack* del protocolo H.323 [5]

1.4.2.2 Protocolo SIP (*Session Initiation Protocol*)

SIP es un protocolo de señalización que se utiliza para conferencias en Internet y Telefonía. SIP está definido en el RFC 2543, y se basa en SMTP y HTTP. SIP fue desarrollado por un grupo de trabajo de la IETF (MMUSIC).

SIP especifica procedimientos para conferencias de telefonía y multimedia sobre el Internet. SIP es un protocolo independiente de la capa aplicación. SIP se basa en una arquitectura Cliente/Servidor en la cual los clientes inician las llamadas y los servidores contestan las llamadas.

Debido a que es un protocolo de fuente abierta, es independiente del tipo de vendedor o implementación.

SIP es un protocolo más actualizado que H.323 y actualmente no es muy nombrado ni desarrollado por el mercado. Sin embargo por la simplicidad, escalabilidad, modularidad, y facilidad de integrarse con otras aplicaciones, es un protocolo más

atractivo para usar en una arquitectura de voz paquetizada. Algunas de las características que SIP ofrece son:

- Resolución de direcciones, mapeo de nombres, y redireccionamiento de llamadas.
- Descubrimiento dinámico de medios que usan SIP.
- Administración entre el *host* y los puntos extremos.

Componentes de SIP:

El sistema SIP contiene dos componentes: agente usuario (*user agent*) y servidor de red. Un *user agent* UA, es un componente de punto extremo de SIP, el cual realiza y recibe llamadas.

El cliente es llamado *user agent client (UAC)* y se usa para inicializar peticiones. El servidor se llama *user agent server (UAS),* recibe las peticiones del UAC y retorna las respuestas al usuario.

El Cliente SIP incluye:

- Teléfonos IP, ellos pueden actuar como UAC o UAS
- *Gateways*

Hay 3 tipos de servidores SIP:

- ***Proxy Server***: Decide a qué servidor la petición debe remitirse y enviar la petición. La petición puede cruzarse entre varios servidores SIP antes de alcanzar su destino. La respuesta entonces atraviesa en el mismo orden pero de reversa. Un *proxy server* puede actuar de cliente o servidor dependiendo de si es petición o respuesta.

- ***Redirect server***: Es diferente al *proxy server*, él no envía peticiones a otros servidores, en lugar de eso notifica dónde se inició la llamada y la localización del destino.

- ***Registrer server***: Provee servicio de registro para los UAC y sus localizaciones.

La figura 1-34 indica un ejemplo de los componentes de SIP.

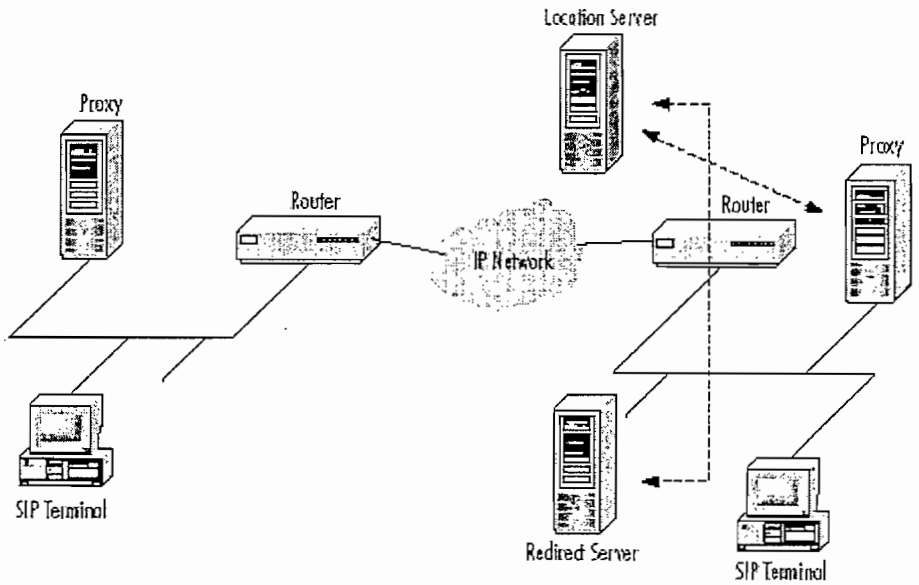


Figura 1-34 Componentes de SIP [5]

CAPÍTULO 2

2. CALIDAD DE SERVICIO PARA VoIP

2.1 CONSIDERACIONES DE CALIDAD DE SERVICIO [5] [7]

QoS (Quality of Service) es un conjunto de herramientas disponibles, para que el administrador de la red tenga la certeza de que se pueda ejecutar de manera segura varios niveles de servicios para diferentes clases de tráfico.

Muchos protocolos y aplicaciones no son sensibles a la congestión en la red, FTP por ejemplo, tiene gran tolerancia al retardo en la red y a la limitación en el ancho de banda. Pero por lo contrario, aplicaciones como voz y vídeo son particularmente sensibles al retardo en la red. Si a los paquetes de voz les toma mucho tiempo en llegar a su destino, el resultado es un sonido distorsionado. La QoS puede ser utilizada para dar ciertos niveles de servicio a cada una de estas aplicaciones.

Una red podría tener una o varias tecnologías de capa enlace, en las cuales se puede habilitar Calidad de Servicio; estas tecnologías son:

- *Frame Relay*
- Ethernet
- Token Ring
- *Point to Point Protocol*
- HDLC
- ATM

Cada una de estas tecnologías tiene diferentes características que necesitan ser consideradas para implementar QoS. Se puede implementar QoS en algunas situaciones de congestión. La administración de congestión es una técnica utilizada para administrar y priorizar tráfico en una red, donde las aplicaciones requieren más ancho de banda del que la red está dispuesta a ofrecer.

Implementar QoS puede ser una tarea complicada para el administrador de la red, pero si se lo realiza se puede llegar a altos niveles de flexibilidad en el control de los flujos y acciones que ocurran en el tráfico de la red.

Aplicaciones de tiempo real, como las aplicaciones de voz, tienen diferentes características y requerimientos que una aplicación de datos tradicional.

Las aplicaciones de voz toleran pequeñas variaciones de retardo (*jitter*), estas variaciones de retardo afectan a la calidad de los paquetes de voz. Los paquetes perdidos y el *jitter* degradan la calidad de la voz como muestra la figura 2-1.

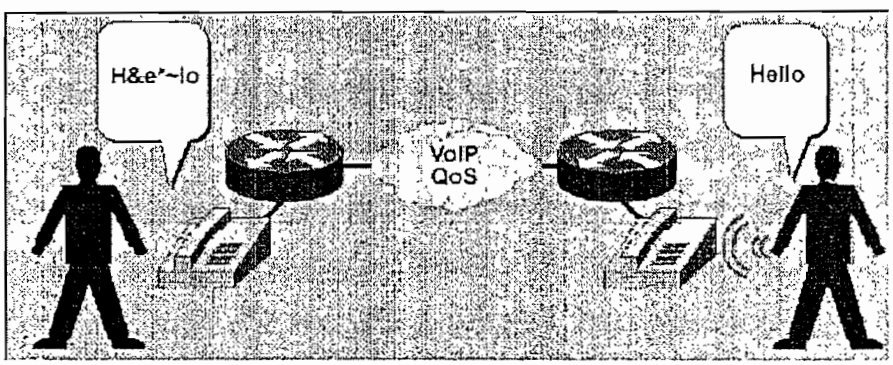


Figura 2-1 Calidad de voz degradada [7]

VoIP garantiza una buena calidad en la transmisión de voz; los paquetes de señalización y de audio son los únicos que tienen prioridad sobre otros tipos de tráficos en la red. Para implementar VoIP se debe proporcionar un nivel aceptable de calidad de voz, pero VoIP posee problemas con parámetros relacionados con el ancho de banda, latencia y *jitter*. Por lo tanto implementar QoS ayuda a solucionar entre otros problemas, los siguientes:

- **La voz debería competir con los datos:** La demanda de tráfico de voz en una WAN es típicamente uniforme; cada llamada de voz consume una determinada cantidad de ancho de banda por la duración de la llamada. Por otro lado el tráfico de datos es variado, dependiendo de las aplicaciones del usuario. El ancho de

banda total que se debería proveer debe tener la capacidad de llevar todos estos tipos de tráfico.

- **La voz es dada en tiempo real y debería ser enviada primero:** Como la voz es una aplicación en tiempo real y los paquetes retardados tienen un severo impacto en el rendimiento, se debe priorizar la carga de voz ante el tráfico de datos que no es un tráfico en tiempo real.

- **La sobrecarga debería ser minimizada**: La voz es enviada usando UDP. Desafortunadamente este requerimiento añade una significativa carga en el tamaño del paquete.

- **Los paquetes de datos grandes tardan más que los paquetes pequeños de voz**: En algunas aplicaciones tal como la transferencia de archivos y *web browsing,* los paquetes de datos que compiten con los de voz podrían ser relativamente grandes. Los paquetes de voz son forzados a esperar hasta que el paquete de datos grande sea enviado. Utilizando fragmentación, el paquete de datos se haría más pequeño, y su tamaño sería más manejable, esto ayudaría a reducir el retardo que experimentarían los paquetes de voz.

- **Las variaciones de retardo en la WAN deben ser minimizadas**: El comportamiento natural de tecnologías WAN tales como *Frame Relay*, ATM y PPP poseen altas variaciones de retardo, dando como resultado un pobre desempeño en la calidad de voz. Pero usando herramientas que reduzcan las variaciones de retardo en estas tecnologías WAN, se puede añadir un significativo desempeño a las aplicaciones de voz.

- **La WAN no debería ser sobresuscrita**: Si se realizan varias llamadas de voz por la WAN, el ancho de banda necesario, que es requerido para las aplicaciones de datos podría ser "asfixiado". Se debe tener cuidado en asegurar que los datos

todavía tengan el suficiente de ancho de banda. Las excesivas llamadas de voz podrían tener un impacto en la red.

Hay tres niveles de QoS:

- **Mejor esfuerzo**: Ocurre cuando la red intenta deliberadamente enviar como sea posible un paquete a su destino. Este tipo de servicio no tiene la garantía de que un paquete alcance su destino. Aplicaciones como FTP o HTTP pueden soportar el servicio del mejor esfuerzo sin que haya algún problema crítico. Pero en aplicaciones que son sensibles al retardo o a las fluctuaciones del ancho de banda este servicio no debe ser considerado.

- **Servicios Integrados:** Provee a ciertas aplicaciones la garantía de un nivel de servicio para negociar parámetros de la red de extremo a extremo, y confiar en un mecanismo de calidad de servicio para reservar los recursos necesarios de la red antes de que la aplicación empiece a transmitir. Es importante notar que la aplicación no enviará tráfico hasta que reciba una señal de la red asegurando los recursos de la misma. Para asegurar esto, se utiliza un proceso llamado control de admisión. El control de admisión es un mecanismo que previene que la red sea sobrecargada. La red envía una señal a la aplicación para que se empiece a transmitir los datos. Cuando la aplicación empieza a transmitir sus datos, la red reserva recursos para esta aplicación. La red realiza esta tarea de mantenimiento por: estado de flujo, clasificación, políticas, y encolamiento inteligente por paquete, parámetros que se los encuentra al implementar QoS.

- **Servicios Diferenciados**: Incluyen un conjunto de herramientas de clasificación o mecanismos de encolamiento que poseen ciertos protocolos o aplicaciones para que tengan cierta prioridad sobre otros tipos de tráfico en la red. El tráfico en la red puede ser clasificado por: direccionamiento IP, protocolos y puertos.

2.2 ADMINISTRACIÓN DE CONGESTIÓN [5]

La demanda para más ancho de banda y tiempos de respuesta cortos se ha ido incrementando de acuerdo a las aplicaciones que han ido apareciendo y necesitando cada vez más de estos parámetros.

La administración de congestión es un término genérico que comprende varios tipos de estrategias de encolamiento, usadas para administrar situaciones en las cuales las demandas de ancho de banda exceden el ancho de banda total que las redes pueden proveer.

La administración de congestión, no controla la congestión antes de que ésta ocurra, controla la inyección de tráfico dentro de la red para que ciertos flujos de la red tengan prioridad sobre otros.

Se examinarán algunas técnicas de QoS como:

- cRTP
- *Queuing* (Formación de colas)
  - Encolamiento común (CQ)
  - Prioridad en el encolamiento (PQ)
  - *Weighted Fair Queuing* (WFQ) - Encolamiento de peso justo
  - Clases basadas en WFQ (CBWFQ)
- Clasificación de Paquetes
- IP *precedence*
- Protocolo de reservación de recursos (RSVP)
- Control de Admisión de llamada (CAC)

Implementar y configurar prioridades así como encolamientos comunes en *routers* requiere que el administrador de la red premedite algunos planteamientos básicos.

2.2.1 PROTOCOLO DE TRANSPORTE DE TIEMPO REAL COMPRIMIDO (CRTP)

Este protocolo provee un mecanismo por el cual se puede reducir el *header* para el tráfico RTP por medio de eliminación de información redundante entre paquetes.

RTP, definido en el RFC 1889, se usa en redes IP para manipular la compresión de audio en paquetes IP. RTP corre sobre UDP, el cual tiene menos retardo que TCP. El tráfico de tiempo real es llevado sobre los puertos UDP que van desde el puerto 16384 hasta el puerto 16624.

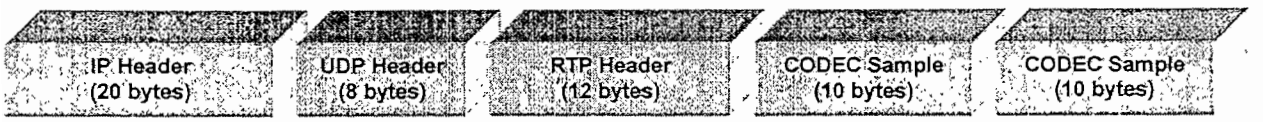


Figura 2-2 *Headers* IP, UDP y RTP de un paquete VoIP [4]

El protocolo RTCP (Protocolo de Control para RTP, ver numeral 1.4.2) también es definido en el RFC 1889. RTCP es un protocolo de capa de sesión que monitorea los datos y provee funciones de control e identificación. La figura 2-2 muestra un paquete de VoIP con *headers* IP, UDP y RTP.

RTP provee servicios como secuenciamiento que permiten identificar los paquetes perdidos. En general las funciones de RTP son:

- Proveer funciones de transporte de extremo a extremo para audio y vídeo sobre servicios *unicast* y *multicast*.
- Soportar conferencias de grupos en tiempo real.
- Sincronizar *streams* de audio y vídeo.

Los paquetes de VoIP están compuestos de *frames* encapsulados en 40 bytes de *headers* IP/UDP/RTP. Estos 40 bytes representan una sobrecarga, considerando que

el *payload* de voz es generalmente de 20 bytes (figura 2-2). Por esta razón, se creó la compresión del *header* (cRTP) y se encuentra definida en el RFC 2508.

Comprimiendo los *headers* de IP/UDP/RTP en un paquete RTP, se puede efectivamente reducir la cantidad de ancho de banda requerida en una red VoIP. Los resultados de comprimir pueden ser grandiosos, tomando el tamaño del *header* de 40 bytes y disminuyéndolo a 2 bytes sin *checksums* y 4 bytes con *checksums* (figura 2-3).

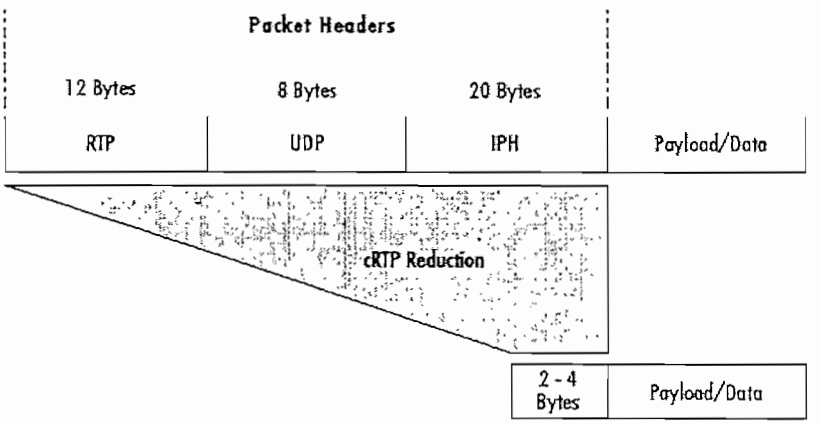


Figura 2-3 Compresión de los *headers* RTP/UDP/IP [5]

En la figura 2-4 se puede ver el proceso de compresión del *header* RTP. La formación de la cola ocurre antes del proceso de compresión. El equipo determina un tráfico RTP, y solo los paquetes RTP son comprimidos. Todos los paquetes que no sean RTP y cRTP pasan a la interfaz.

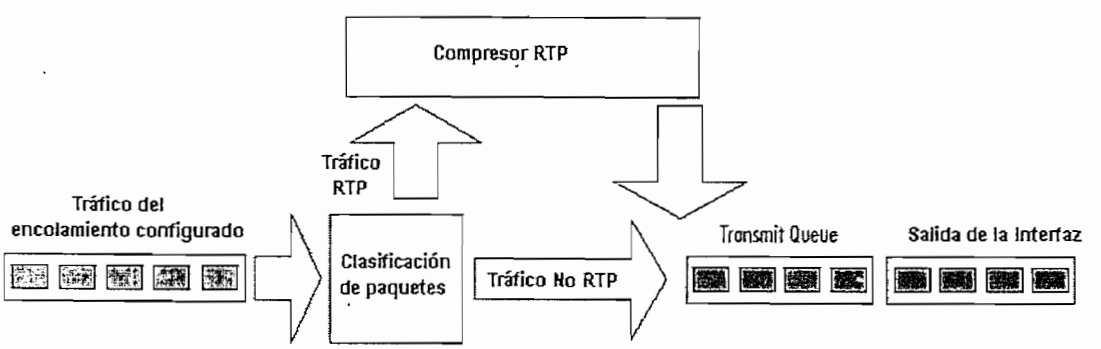


Figura 2-4 Proceso de compresión del *header* RTP [5]

cRTP es soportado en líneas seriales usando encapsulaciones *Frame Relay*, HDLC, o PPP; cRTP también es utilizado en interfaces ISDN.

2.2.2 FORMACIÓN DE COLAS (*QUEUING*)

Es importante entender los procesos básicos de encolamientos. En un *router* las colas actúan como un área de sostenimiento. Las colas sostienen paquetes hasta que los recursos estén disponibles para enviar los paquetes fuera del puerto. Los paquetes serán enviados inmediatamente, con tal que no haya congestión en el *router.* Las colas en las redes se usan para manipular el tráfico que llega más rápidamente en relación a la velocidad de salida que el interfaz pueda manipular.

Por ejemplo un *router* con una interfaz LAN *FastEthernet* y una WAN T1, generalmente se ve que el tráfico que llega a la interfaz LAN es más rápido, en comparación a la velocidad que el *router* lo envía por el puerto de la WAN. Ésta es una operación normal que no necesariamente indica un problema de congestión. Varios tipos de encolamiento podrían beneficiar a una red VoIP. Se analizarán algunos tipos de encolamiento que ayudarán a mejorar el tráfico de VoIP.

2.2.2.1 Encolamiento personalizado (CQ)

Este tipo de encolamiento (*Custom Queuing*) trabaja permitiendo una configuración personalizada, para que un número específico de bytes se envíen de una cola cada vez que ésta haya sido abastecida. Un número máximo de paquetes por cola también pueden ser especificados.

CQ abastece las colas circulando a través de ellas, enviando la porción de datos asignados para cada cola antes de moverse a la siguiente cola. Cuando el *router* descubre una cola vacía, envía paquetes de la siguiente cola que están listos para ser enviados. Cuando una cola en particular es procesada, se envían los paquetes hasta que el número de bytes enviados excedan la cuenta de bytes de la cola o la

cola esté vacía. El ancho de banda usado por una cola es detallado por la cuenta de bytes de la cola o su longitud. La figura 2-5 muestra como CQ trabaja.

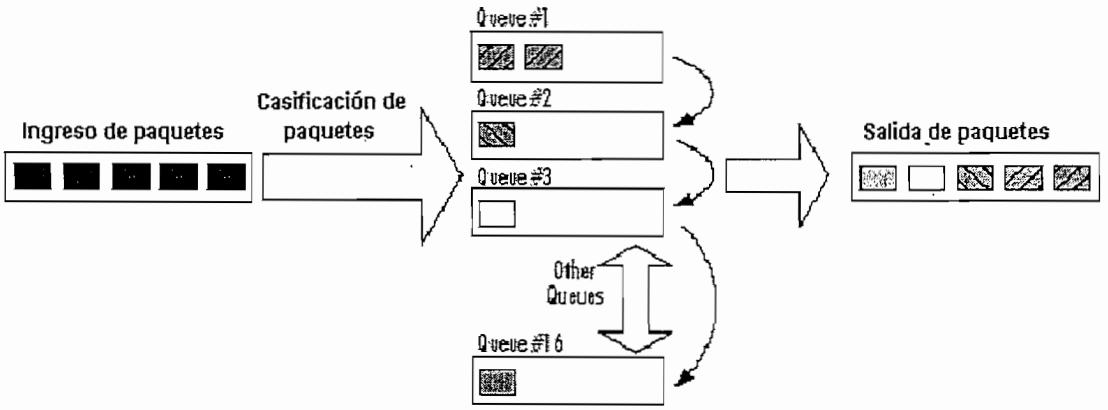


Figura 2-5 Encolamiento Común [5]

La configuración de CQ no es dinámica, lo que no debería alterar las condiciones existentes de la red.

2.2.2.2 Encolamiento con prioridad (PQ)

Este encolamiento (*Priority Queuing*) permite definir cómo el tráfico es priorizado en la red.

El *router* sitúa el tráfico en estas colas basado en filtros que son predefinidos. La cola con alta prioridad es atendida primero hasta que ésta esté vacía, y así se atienden en secuencia hasta la de menor prioridad.

Existen cuatro niveles de prioridad:

- Alta
- Mediana
- Normal
- Baja

Los paquetes que no sean clasificados en alguno de estos tipos de prioridad caen dentro de un encolamiento normal. La figura 2-6 muestra cómo trabaja PQ.

Figura 2-6 Encolamiento con prioridad [5]

Este encolamiento en una interfaz es escaneada por paquetes en orden descendente de prioridades, empezando con la prioridad más alta.

2.2.2.3 Encolamiento de Peso Justo (WFQ)

WFQ (*Weighted Fair Queuing*) es un método de planificación que provee un ancho de banda exacto para el tráfico de toda la red. WFQ aplica pesos a los paquetes para determinar cuánto de ancho de banda se permite a cada conversación en relación a otras conversaciones.

WFQ provee administración de prioridad de tráfico que dinámicamente clasifica el tráfico en mensajes que constituyen una conversación. WFQ separa la serie de paquetes dentro de una conversación garantizando que el ancho de banda sea compartido justamente entre conversaciones individuales y que el bajo volumen de tráfico sea transferido de manera oportuna.

WFQ clasifica el tráfico interno en diferentes flujos basados en direccionamiento de cabeceras, incluyendo características como: la dirección fuente y destino, los puertos fuente y destino, y el valor del tipo de servicio. Existen dos categorías de flujos:

- Sesiones de gran ancho de banda
- Sesiones de poco ancho de banda

Las sesiones de poco ancho de banda tienen prioridad sobre las de gran ancho de banda, y el tráfico de gran ancho de banda comparte el servicio de transmisión de acuerdo a los pesos asignados.

El flujo de tráfico correspondiente al de poco ancho de banda, el cual es una composición de la mayoría del tráfico, recibe un servicio preferencial, permitiendo enviar las cargas ofrecidas completas en un tiempo oportuno. El gran volumen de flujo de tráfico comparte la capacidad restante proporcionalmente entre ellos.

WFQ difiere de PQ y CQ en varias maneras. Una diferencia importante es que WFQ no permite que las opciones de clasificación sean configuradas. WFQ clasifica los paquetes basados en flujos. Un flujo consiste de todos los paquetes que tienen una misma dirección IP fuente y destino y mismos números de puertos fuente y destino.

El flujo basado en WFQ se usa por definición en la mayoría de interfaces seriales configuradas para soportar velocidades menores a un E1 (2,048 Mbps).

WFQ ofrece soluciones dependiendo de la situación en la cual se desee proveer tiempos de respuesta consistentes a usuarios de redes pesadas y livianas sin añadir un excesivo ancho de banda. WFQ automáticamente se adapta a los cambios de las condiciones del tráfico.

WFQ trabaja pobremente para tráfico de voz y vídeo, porque ambos requieren de un *mínimo* de retardo y *jitter*. WFQ no provee una cola con prioridad para minimizar estos parámetros. Además el retardo puede ser incrementado cuando ocurren varios flujos concurrentemente, dando un ancho de banda justo para cada flujo, por lo que puede ocurrir que los flujos de voz y vídeo no consigan suficiente ancho de banda.

2.2.2.4 Clases Basadas en WFQ (CBWFQ)

CBWFQ extiende el estándar WFQ, para proveer soporte a usuarios definidos en clases de tráfico. Para CBWFQ, el usuario define las clases de tráfico basado en criterios que coinciden con: protocolos, listas de control de acceso (ACL), y entradas de interfaces. Una cola se reserva para cada clase, y el tráfico perteneciente a una clase se direcciona a la cola para esa clase.

Una vez que una clase haya sido definida de acuerdo a ciertos criterios, se pueden asignar determinadas características. Caracterizar una clase, es asignar ancho de banda, peso y un límite máximo de paquetes. El ancho de banda asignado a una clase es un ancho de banda garantizado que la clase entrega durante una congestión.

Al caracterizar una clase se puede también especificar el límite de encolamiento para esa clase, el cual es el máximo número de paquetes permitidos para acumularse en la cola para la clase. Los paquetes pertenecientes a una clase están sujetos al ancho de banda y al límite de encolamiento que caracteriza la clase.

Después de que una cola haya alcanzado su configuración de encolamiento límite, el encolamiento de los paquetes adicionales a la clase causa que los paquetes de la cola sean eliminados (*tail drop*), dependiendo de cómo la política de la clase sea configurada. ***Tail drop*** se usa por clases CBWFQ a menos que se emplee una política de configuración explícita para una clase que use *Weighted Random Early Detect* (WRED) (Descubrimiento del peso al azar) para eliminar los paquetes como una medida de eliminar la congestión.

Hay que notar que si se utiliza la eliminación de paquetes por medio de WRED en lugar de *tail drop* para una o más clases, configuradas como una política, se debería asegurar que WRED no esté configurado para una interfaz en la cual se ataque esa política de servicio.

Si una clase por defecto se configura con una política para el ancho de banda, todo tráfico no clasificado se coloca en una sola cola y se trata de acuerdo a la configuración del ancho de banda. Si una clase es configurada con encolamiento justo o exacto, todo tráfico no clasificado se trata como el método del mejor esfuerzo.

El flujo de clasificación es un tratamiento normal WFQ. Esto es, paquetes con igual dirección fuente, dirección destino; puertos TCP o UDP fuentes o destino son clasificados como pertenecientes al mismo flujo. WFQ localiza un ancho de banda equivalente para cada flujo.

Para CBWFQ, el cual extiende el concepto de encolamiento justo (WFQ), el peso especificado para la clase llega a ser el peso para cada paquete que reúne el criterio de la clase. El paquete que llega a la salida de una interfaz se clasifica de acuerdo a los criterios de filtros que se definieron, por lo tanto a cada uno se asigna un peso apropiado. El peso para un paquete que pertenece a una clase específica es deducido del ancho de banda que se asignó a la clase cuando se la configuró; en este sentido el peso para una clase es configurado por el usuario.

Después de que se asigna el peso para un paquete, éste es encolado en una apropiada clase de encolamiento. CBWFQ usa los pesos asignados a los paquetes encolados para asegurar que la clase de encolamiento sea atendida imparcialmente.

2.2.3 CLASIFICACIÓN DE PAQUETES

Algunas veces, en una red se necesita clasificar el tráfico. La razón para clasificar el tráfico depende del tipo de red. Se puede ir marcando paquetes con una "bandera" para así hacer relativamente a los paquetes más o menos importantes en la red e identificar también los paquetes que serán descartados.

A estas banderas se las puede marcar de diferentes maneras, y los niveles de clasificación dependerán del método a utilizarse. El uso de esquemas de priorización

tal como RED (*Random Early Detection*) y ABR (*Adaptive Bit Rate*) obliga al *router* a analizar los *streams* de datos y las características de congestión y así aplicar controles de congestión a los *streams* de datos.

2.2.4 IP *PRECEDENCE*

IP *Precedence* es un parámetro definible en ciertas interfaces que da un valor de prioridad en la red. Es manualmente asignado a una interfaz particular en las configuraciones de VoIP.

Este comando se debería usar para dar a los paquetes IP más prioridad en relación a otros paquetes cuando ellos comparten el mismo ancho de banda.

Existen ventajas y desventajas al usar métodos de QoS para VoIP. Uno de los más importantes factores es identificar qué tipo de calidad de servicio se va a ofrecer a la red. Hay que entender los siguientes puntos cuando se está decidiendo el algoritmo a utilizar:

- **IP *precedence*** es controlado por el administrador de la red. Se puede escoger niveles de precedencia que están disponibles para el tráfico que se use en QoS. Esto no puede ser controlado dinámicamente, se configura manualmente en cada interfaz.

- **RSVP (Protocolo de Reservación de Recursos)** es más difícil de implementar inicialmente, ya que los niveles de tráfico necesitan ser analizados y ajustados en cada puerto físico. RSVP es poderoso en enlaces que tengan alta congestión y enlaces WAN lentos. Éste es un beneficio extra si se requiere controlar el sistema dinámicamente.

2.2.5 PROTOCOLO DE RESERVACIÓN DE RECURSOS (RSVP)

El modelo de servicios integrados (*Intserv*) se crea para aplicaciones o estaciones finales que reservan recursos a través de la red y garantizan ciertos niveles de servicio.

RSVP es un protocolo de señalización que hace reservación de recursos para aplicaciones, y así garantizar QoS. Es considerado un protocolo de señalización porque las reservaciones son negociadas por comunicación entre las estaciones finales. También es llamado protocolo de señalización fuera de banda (*out-of-band*) debido a que los paquetes RSVP no son utilizados para transmitir flujos de datos; ellos coexisten en la red con otros paquetes y son usados para reservar recursos para un típico paquete IP.

RSVP hace reservación de recursos para el flujo de datos a través de la red. Estos flujos reservados son referidos a sesiones.

Una sesión es definida como paquetes teniendo la misma dirección destino (*unicast* o *multicast*), ID del protocolo IP, y puerto destino. Los recursos pueden ser: ancho de banda, ciclos del CPU, o prioridad de encolamiento. Los clientes usan RSVP para pedir una garantía de QoS a través de la red. Los *routers* participan con RSVP situando los recursos en flujos particulares, o denegando recursos si no están disponibles, y enviando la información de RSVP a los otros *routers*.

RSVP es un protocolo de control para el Internet que reside en capa 4 del modelo OSI (capa de transporte). Este protocolo es similar a otros protocolos de control; como ICMP (*Internet Control Message Protocol*) e IGMP (*Internet Group Management Protocol*). RSVP no es un protocolo de ruteo, el camino que toma a través de la red es el mismo que los paquetes IP, y está determinado bajo los lineamientos de los protocolos de enrutamiento (OSPF, EIGRP, BGP).

2.2.5.1 Ventajas de RSVP

- **Control de Admisión**: RSVP ayuda a otras aplicaciones a no trasmitir cuando la red se encuentra ocupada.
- **Independencia en la red o flexibilidad**: RSVP no es dependiente de alguna arquitectura de red en particular.
- **Interoperabilidad**: RSVP trabaja con protocolos existentes y con mecanismos de calidad de servicio.

2.2.5.2 Desventajas de RSVP

- **Selección de la ruta y estabilidad:** El camino más corto podría no tener disponibilidad de recursos, y el camino activo podría desactivarse (*down*).
- **Tiempo de espera:** Una aplicación no podría empezar a transmitir hasta que la reservación haya sido completada.

2.2.6 CONTROL DE ADMISIÓN DE LLAMADAS (CAC)

El control de admisión de llamadas es un término genérico para describir el método en el cual un nodo puede prevenir sobresuscripción de recursos de la red, para de esta manera conservar la calidad en las transmisiones existentes.

Generalmente se usa en aplicaciones de voz o vídeoconferencia. CAC rechaza una petición para recursos de la red si la aplicación de la petición requiere de mayor ancho de banda del que esté disponible. Por ejemplo, si una interfaz es configurada para 128 kbps, y 5 llamadas de VoIP que requieren 24 kbps cada una están en progreso, CAC va a prevenir que una sexta llamada se complete, porque esta llamada adicional degradaría la calidad de las seis llamadas concurrentes.

Este sistema asegura que toda una conexión existente mantenga el ancho de banda que se necesite. Cuando una conexión se rechaza, el nodo original, dependiendo de

la configuración de la red, buscará un camino alternativo o proveerá un tono de ocupado.

Hay diferentes métodos de implementar CAC, pero para el propósito de VoIP, el más comúnmente usado es RSVP y un *gateway* H.323.

2.3 CARACTERÍSTICAS Y CLASIFICACIÓN DE TRÁFICO [4]

La calidad de servicio es la disponibilidad de proveer niveles de tratamiento a clases específicas de tráfico. Antes de que alguna aplicación o mecanismo de QoS pueda ser aplicado, el tráfico debe ser identificado y clasificado en diferentes clases.

Las herramientas de QoS para clasificación, categorizan los paquetes examinando el contenido de los *frames*, celdas y cabeceras de paquetes, por cuanto las herramientas de marcación permiten cambiar los bits de las cabeceras de los paquetes para facilitar la clasificación.

Varias herramientas de clasificación de tráfico permiten a ciertas clases de tráfico recibir un nivel de tratamiento diferente a otras clases de tráfico. Se usa este método para priorizar un tráfico de otro.

En lugar de dar encolamientos preferenciales, descartación de paquetes, conformación de tráfico y políticas de control, las herramientas de clasificación y marcado cambian los bits de la cabecera del paquete IP.

2.3.1 CLASIFICACIÓN DE TRÁFICO

La clasificación es el proceso de identificar el tráfico y categorizarlo en diferentes clases. La clasificación de paquetes usa un descriptor de tráfico para categorizar un paquete dentro de un grupo específico. Típicamente el descriptor incluye: el ingreso en las interfaces, IP *precedence*, servicios diferenciados con código de punto

(DSCP), direcciones fuente y destino, y aplicación. Después de que un paquete haya sido definido (es decir clasificado), el paquete está accesible a ser manipulado por la QoS en la red.

Usando la clasificación de paquetes el administrador de la red puede particionar el tráfico en varios niveles de prioridad o clases de servicio. Cuando el descriptor de tráfico se usa para clasificar el tráfico, la fuente se pone de acuerdo en adherir las condiciones acordadas que la red promete en QoS. La clasificación debe estar en los extremos de la red, típicamente en los teléfonos o dispositivos de red.

2.3.2 MARCACIÓN DE TRÁFICO

La marcación es relativa a la clasificación. Permite a los dispositivos de red clasificar un paquete o *frame* basado en un descriptor de tráfico específico. Típicamente este descriptor de tráfico incluye: clase de servicio (CoS), DSCP, IP *precedence*, QoS *group*, y MPLS (*Multiprotocol Label Switching*). La marcación puede hacerse en la información del *header* de capa 2 y/o de capa 3.

La marcación consiste en cambiar los valores de ciertos bits del *header* de la capa de enlace o red para poder clasificarlos dependiendo de los valores a los que fueron marcados.

Marcando un paquete o un *frame* con esta clasificación permite a los dispositivos de red fácilmente distinguir los paquetes o *frames* e identificar a qué clase pertenecen.

Después de haber identificado la clase a la que pertenecen, los mecanismos de QoS pueden ser uniformemente aplicados para asegurar el cumplimiento de las políticas administrativas de QoS.

2.3.3 CLASIFICACIÓN Y MARCACIÓN EN LA CAPA DE ENLACE PARA QoS EN *FRAME RELAY* Y ATM

Antes de que la *Internet Engineering Task Force* (IETF) defina métodos de QoS para la capa red, la ITU-T (*International Telecommunications Union*), el ATM *Forum* y el *Frame Relay Forum* (FRF) ya tuvieron estándares para QoS en capa enlace en redes *Frame Relay* y ATM.

Frame Relay provee un conjunto de mecanismos para garantizar un *Commited Information Rate* (CIR), una notificación de congestión, y fragmentación *Frame Relay* (FRF.12). Un componente importante de QoS para *Frame Relay* es el que descarta el paquete cuando existe congestión (DE).

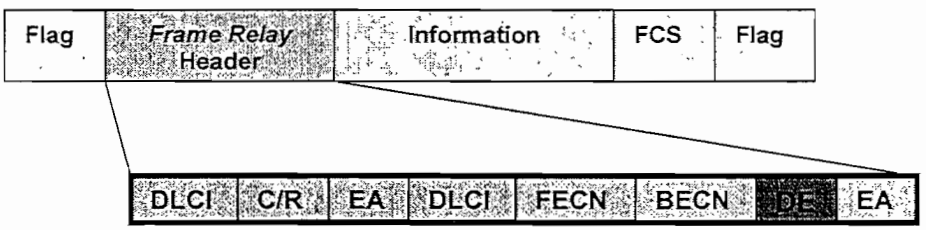


Figura 2-7 Trama de *Frame Relay* [11]

En los dispositivos DTE de las nubes *Frame Relay*, se puede activar el bit DE (figura 2-7) para cuando la red se encuentre congestionada, los dispositivos *Frame Relay* descartarán los *frame*s con el bit DE activo.

En ATM, las celdas consisten de 48 bytes de *payload* y 5 de *header.* En el *header* ATM se incluye el campo de 1-bit *Cell Loss Priority* (CLP), el cual indica la pérdida de prioridad de la celda cuando se mueve a través de una red ATM si ésta se encuentra en extrema congestión. El bit CLP presenta dos valores: 0 para indicar alta prioridad, y 1 para indicar baja prioridad. Activando el bit CLP a 1, se disminuye la prioridad de la celda incrementando la probabilidad de que la celda sea descartada cuando la red ATM experimente congestión.

El bit CLP (figura 2-8) indica que la celda podría ser descartada si se encuentra en congestión cuando se mueve a través de la red.

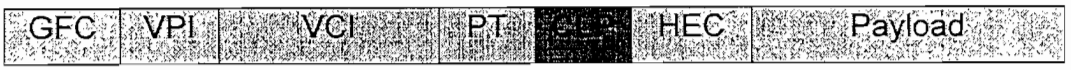


Figura 2-8 Celda ATM [11]

2.3.4 CLASIFICACIÓN Y MARCACIÓN EN LA CAPA DE RED

En la capa de red, los paquetes IP son típicamente clasificados basados en las direcciones IP fuente y destino, longitud del paquete, o el contenido del byte *ToS (Type of Service).*

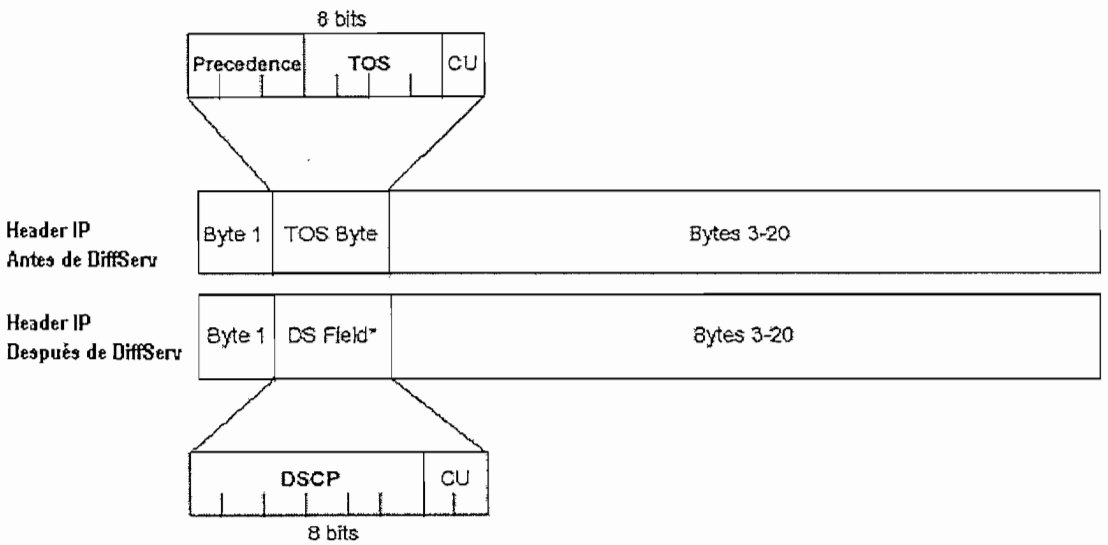


Figura 2-9 Campos IP *Precedence* e IP DSCP del Paquete IPv4 [4]

IP *Precedence* usa tres bits en el campo ToS del *header* de IPv4 (figura 2-9) para especificar la clase de servicio (CoS) para cada paquete. IP *Precedence* tiene rangos de valores del 0 al 7 y permite al administrador de red particionar el tráfico en seis clases de servicio (la 6 y la 7 son reservadas para uso interno de la red).

Los servicios diferenciados (DiffServ) es un modelo que reemplaza y es compatible con IP *precedence*. DiffServ redefine el byte de ToS y usa 6 bits de priorización (figura 2-9) que permite la clasificación en 64 valores (0 a 63), de los cuales 32 son los usados más comúnmente.

El valor de un DiffServ es llamado un **DSCP**. Con DiffServ, la clasificación del paquete se usa para priorizar el tráfico de la red en varios niveles de prioridades o clases de servicio. La clasificación de paquetes usa un descriptor de tráfico DSCP para categorizar un paquete dentro de un grupo específico que define al paquete. Después de que el paquete ha sido definido (clasificado), el paquete es accesible para manipular QoS en la red.

Campo tipo de Servicio (ToS)

El bit de ToS fue implementado dentro del paquete IP, y es un campo que está compuesto de 8 bits, de los cuales 3 bits son para IP *precedence* y 4 bits para un indicador de proveedor de servicio, el 8vo. bit no es usado. Activando este campo, los paquetes con diferentes ToS pueden ser administrados para diferentes niveles de servicio en una red. Dentro del campo de ToS, los bits 3, 4 y 5 representan el perfil de servicio.

En la figura 2-10 se muestra el significado de cada bit. Este campo fue proyectado para proveer un conjunto de parámetros generalizados que caracterizan las opciones de servicios en las redes que constituyen el Internet.

0	1	2	3	4	5	6	7
Precedence			D	T	R	O	O

```
Bit 3:    0 = Retardo Normal          1 = Retardo Bajo
Bit 4:    0 = Throughput Normal       1 = Throughput Alto
Bit 5:    0 = Confiabilidad Normal    1 = Confiabilidad Alta
```

Figura 2-10 Significado de los bits 3, 4, 5 (RFC 791) [5]

El RFC 791 define los primeros 3 bits de este campo para IP *Precedence*. El propósito principal de este subcampo es indicar al *router* los niveles de preferencia para desechar paquetes y para el encolamiento.

El bit *precedence* fue proyectado para proveer un detalle de niveles de servicios diferenciados para los paquetes. En la tabla 2.1 se muestra en detalle estos niveles.

Tabla 2.1 Valores y Nombres de los niveles del campo IP *Precedence* [4]

Campo y Valor (Decimal)	Valor Binario	Nombre
Precedence 0	000	Rutina
Precedence 1	001	Prioridad
Precedence 2	010	Inmediato
Precedence 3	011	Rápido
Precedence 4	100	Sustitución rápida
Precedence 5	101	Crítico
Precedence 6	110	Control de la Intranet
Precedence 7	111	Control de la red

2.4 CONFORMACIÓN DE TRÁFICO Y POLÍTICAS DE CONTROL (*SHAPING AND POLICING*) [11]

En una red existen varias formas de conectividad que pueden tener diferentes costos en una organización. Por ejemplo la conexión de una LAN es considerablemente mucho menos costosa que una WAN por la misma cantidad de ancho de banda. En razón de que el ancho de banda de la WAN es relativamente costoso, a varias organizaciones les gustaría limitar la cantidad de tráfico que alguna aplicación específica pueda enviar. Esto ocurre cuando una red utiliza una conexión a Internet para sitios remotos. Cuando los usuarios se "bajan" del Internet imágenes, música, vídeos, es decir información que no sea crítica para la empresa, esta información puede reducir la cantidad de ancho de banda disponible para ciertas aplicaciones

más importantes de la empresa. La conformación de tráfico y políticas de control (*policing and shaping*), son dos técnicas de QoS que se pueden usar para limitar la cantidad de ancho de banda para alguna aplicación específica.

Las políticas de control de tráfico pueden ser utilizadas para determinar la máxima velocidad de tráfico enviada o recibida en una interfaz. Las políticas de tráfico son generalmente configuradas en interfaces que se encuentran en el extremo de la red para limitar el tráfico entrante y saliente.

La conformación de tráfico puede ser usada para: controlar el flujo que sale de una interfaz, nivelar el flujo a la velocidad de la interfaz remota, y asegurar que el tráfico se ajuste a las políticas contratadas.

La conformación de tráfico y políticas de control difieren en la manera a la que ellas responden a ciertas violaciones de tráfico. Las políticas de control de tráfico típicamente desechan paquetes, mientras que la conformación de tráfico encola el exceso de tráfico. Se usa encolamientos conformados para sostener los paquetes y amoldar el flujo cuando la velocidad de la fuente es más alta que lo esperado.

2.4.1 *TRAFFIC SHAPING*

Traffic shaping se usa para prevenir y administrar congestión en redes ATM y *Frame Relay*, donde el ancho de banda asimétrico se emplea a lo largo de todo el camino del tráfico.

La conformación de tráfico (*Shaping*) ayuda a mantener uniforme la velocidad desigual en la red. Los mecanismos de *shaping* se usan a la salida de las interfaces. Se emplean típicamente para limitar el flujo de un enlace de alta velocidad a un enlace de baja velocidad, y asegurar que el enlace de baja velocidad no llegue a ser saturado con tráfico.

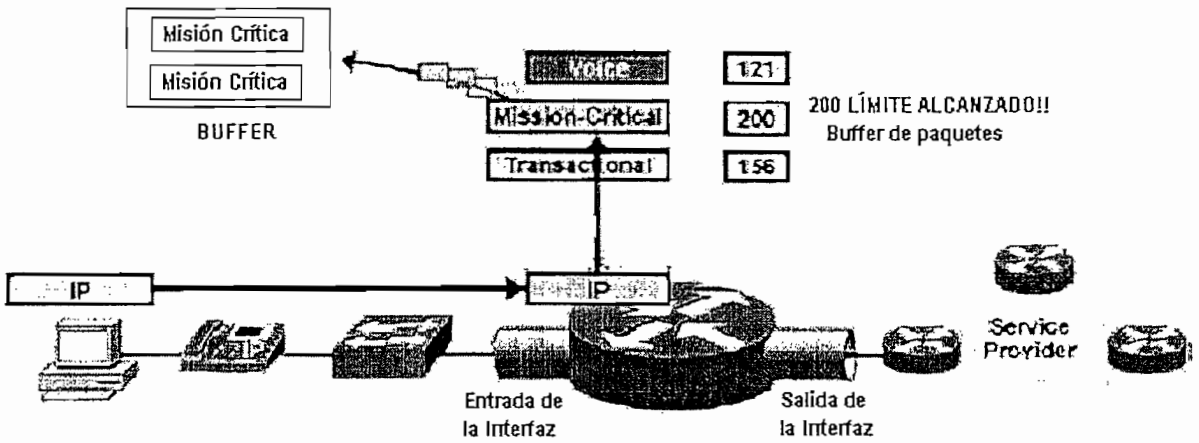


Figura 2-11 *Shaping queuing* [11]

Shaping puede utilizarse para administrar tráfico en un punto en la red donde varios flujos son agregados. El proveedor de servicios usa esto para administrar el flujo de tráfico de clientes, y asegurar que el flujo se ajuste a los servicios acordados entre el cliente y el proveedor.

La conformación del encolamiento se forma cuando un límite predefinido es alcanzado (figura 2-11).

Ejemplo de *Traffic Shaping* [11]

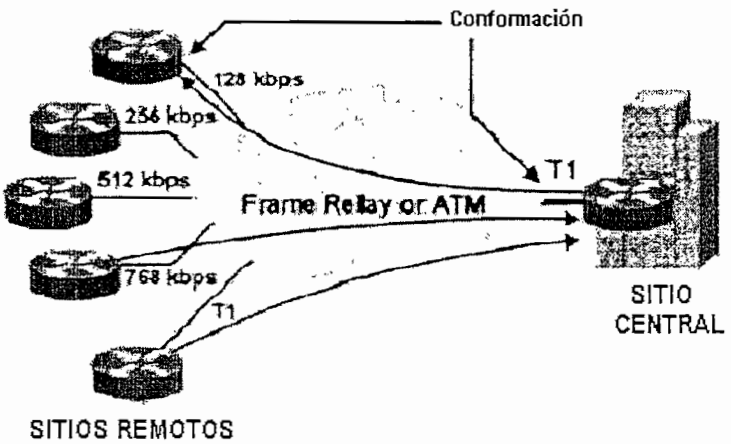


Figura 2-12 Ejemplo de *traffic shaping* [11]

Las herramientas de *traffic shaping* limitan la velocidad de transmisión de una fuente por encolamiento del exceso de tráfico. El límite de velocidad es típicamente un valor menor a la velocidad de transmisión de la interfaz.

Traffic shaping puede ser utilizado para informar de la velocidad desigual que se tiene en redes *nonbroadcast multiaccess* (NBMA), tal como *Frame Relay* y ATM.

En la figura 2-12, existen dos tipos de velocidades desiguales que son:

- El sitio central tiene un enlace de más alta velocidad que los sitios remotos. De esta manera *traffic shaping* puede ser desarrollado en el *router* del lugar central y adaptar el tráfico a la salida de este *router*, para así igualar a la velocidad del enlace de los sitios remotos. Por ejemplo, el *router* central puede adaptar el tráfico saliente del circuito virtual permanente (PVC) a 128 Kbps, para igualar a la velocidad del enlace del sitio remoto. En cada *router* remoto, la conformación de tráfico también se implementa para adaptar los tráficos de los sitios remotos a 128 Kbps e igualar al *Commited Information Rate* (CIR).
- La velocidad del enlace agregado de todos los sitios remotos puede ser más alta que la velocidad del enlace del sitio central. En este caso, los *routers* de los sitios remotos pueden ser configurados para *traffic shaping* y así evitar sobresuscripción en el sitio central.

2.4.2 *TRAFFIC POLICING*

Policing es la capacidad de controlar los tráficos *burst* y uniformes, para asegurar que de manera efectiva los tipos de tráfico consigan su respectivo de ancho de banda. *Policing* descarta y marca paquetes cuando el límite predefinido es alcanzado.

Los mecanismos de *policing* pueden ser utilizados en ambas interfaces, de entrada o de salida. Ellas son típicamente empleadas para controlar el flujo dentro de los

dispositivos de red de un enlace de alta velocidad, desechando el exceso de paquetes de baja prioridad.

Traffic policing se usa generalmente para satisfacer uno de los siguientes requerimientos:

- Limitar el *access rate* en una interfaz cuando se utiliza una infraestructura física de alta velocidad.
- Administrar el ancho de banda para que el tráfico de ciertas aplicaciones o clases de tráfico sigan una política específica de velocidad. Por ejemplo, limitando el tráfico de aplicaciones de archivos compartidos a un máximo de 64 Kbps.

Ejemplo de *Traffic Policing* [11]

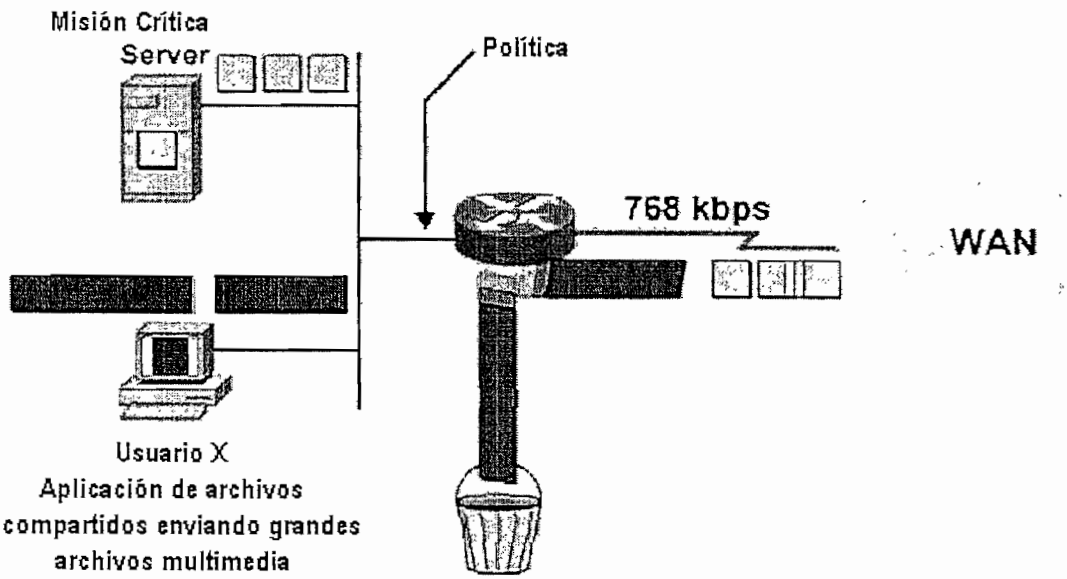


Figura 2-13 Ejemplo de *traffic policing* [11]

En la figura 2-13 se muestra una aplicación para *traffic policing*. *Traffic policing* puede ser utilizado para dividir un recurso compartido (el *upstream* del enlace WAN) entre varios flujos. En este ejemplo, la interfaz *FastEthernet* del *router* tiene una política de *traffic policing* aplicada a ésta. Se observa que un tráfico crítico no es

limitado, pero una aplicación X de archivos compartidos es limitada a 56 Kbps. Toda aplicación de archivos compartidos del usuario X que exceda el límite de 56 Kbps será desechada.

2.4.3 POLICING VS. SHAPING

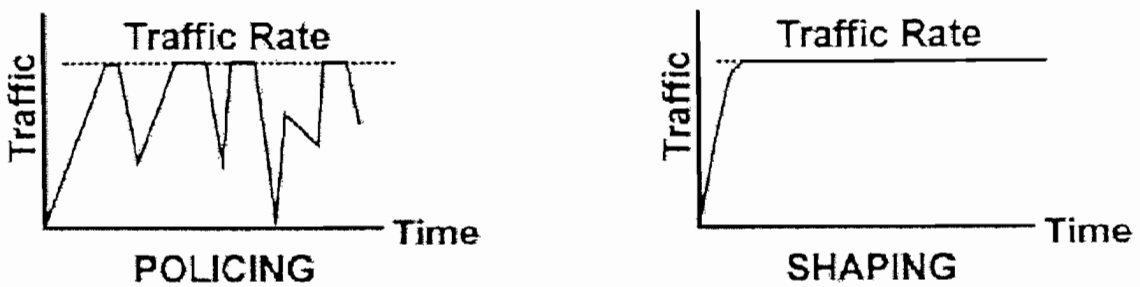


Figura 2-14 *Policing vs. Shaping* [11]

Traffic shaping se utiliza para adaptar el flujo de tráfico que sale de una interfaz cuando el tráfico saliente es más alto que el configurado. *Traffic shaping* iguala el tráfico pero almacenándolo sobre la velocidad configurada en una cola. Por consiguiente, *shaping* incrementa la utilización del *buffer* en un *router* causando un retardo no determinístico.

Traffic shaping se emplea en redes *Frame Relay* y se adapta a condiciones de congestión en capa 2 de la WAN. Por ejemplo si se recibe el bit BECN, el *router* puede bajar el límite de velocidad para ayudar a reducir la congestión en la red *Frame Relay.*

Policing puede ser aplicado en ambas direcciones, a la entrada o a la salida, mientras que *shaping* puede ser aplicado únicamente a la salida. *Policing* desecha paquetes en lugar de encolarlos. *Traffic policing* es más eficiente en términos de utilización de memoria que *traffic shaping,* porque no necesita una cola adicional de paquetes. Ambos, *traffic policing* y *shaping* aseguran que el tráfico no exceda el ancho de banda límite, pero ellos tienen diferentes impactos en el tráfico, así:

- *Policing* desecha paquetes, generalmente causando más retransmisiones de conexiones orientadas a conexión como TCP.
- *Shaping* añade retardo variado de tráfico, posiblemente causando jitter.

2.5 MECANISMOS PARA UN ENLACE EFICIENTE [11]

El tráfico interactivo (Telnet, VoIP) es susceptible al incremento de latencia cuando la red se encuentra con grandes paquetes, como por ejemplo el volumen de FTP atravesando por el enlace WAN. El retardo de paquetes es significativo cuando los paquetes FTP son puestos en cola en enlaces lentos en la WAN. Para resolver estos problemas de retardo en este tipo de enlaces, se requiere un método para fragmentar las grandes tramas, y encolar las tramas más pequeñas entre fragmentos de las grandes tramas. Adicionalmente otras herramientas tal como compresión del *header* y del *payload* se pueden utilizar para reducir el tamaño de las tramas que son enviados en los enlaces WAN.

Mientras varios mecanismos de QoS existen para optimizar el *throughput* y reducir el retardo en el tráfico de una red, los mecanismos de QoS no crean ancho de banda, sino utilizan los recursos existentes, y habilitan las diferencias de tráfico de acuerdo a una política.

Los mecanismos de un enlace eficiente como: la compresión de *payload*, la compresión del *header* y fragmentación son desarrollados en el enlace WAN para optimizar el uso de este enlace.

La compresión del *payload* disminuye el tamaño del *payload* del paquete, por consiguiente incrementa la cantidad de datos que pueden ser enviados en un tiempo dado. La compresión del *payload* se realiza primeramente en los *frame*s de capa 2 y por lo tanto comprime al paquete entero de capa 3.

Todos los métodos de compresión están basados en la eliminación de redundancia cuando se envía los mismos datos o similares sobre un medio de transmisión. Cuando se utiliza mecanismos de compresión del *header*, la mayor parte de la información del *header* puede ser enviada únicamente al principio de la sesión, almacenando en un diccionario, y refiriéndose al último paquete con un índice de este diccionario almacenado.

La técnica de LFI (*Link Fragmentation and Interleaving*) consiste en dividir los grandes *frame*s de capa 2 en pequeños fragmentos de igual tamaño, para poder intercalar *frame*s de otras aplicaciones que sean más sensibles al retardo y al *jitter*. Usando LFI, los grandes *frame*s esperan en el sistema de encolamiento para ser fragmentados; estos pequeños *frame*s son priorizados, y una mezcla de fragmentos se envía sobre el enlace. LFI reduce el retardo de encolamiento de los pequeños *frame*s, debido a que ellos son enviados casi inmediatamente. Por consiguiente la fragmentación del enlace reduce el retardo y el *jitter*.

2.5.1 MÉTODOS DE COMPRESIÓN PARA REDUCIR EL TAMAÑO DE UN PAQUETE

La compresión involucra algoritmos matemáticos que codifican el paquete original en pequeñas cadenas de bytes. Después de que estas pequeñas cadenas de bytes son enviadas al otro extremo del enlace, el algoritmo de compresión en el otro extremo del enlace revierte el proceso, regresando al paquete a su estado original. Dentro de los métodos de compresión, se puede hablar de dos categorías principales: *payload compression* y *header compression*.

Payload compression comprime el *header* y los datos, mientras que *header compression* sólo comprime la cabecera. La figura 2-15 muestra los campos comprimidos por *payload compression*, y por los dos tipos de *header compression* (la abreviación DL de la figura 2-15 significa *Data Link*, representando al *header* y *trailer* de la capa de enlace).

Ambos tipos de compresión consumen ciclos de CPU y memoria. El algoritmo utilizado para comprimir el *payload* utiliza mayor cantidad de CPU y memoria, debido a que tiene que procesar más cantidad de bytes.

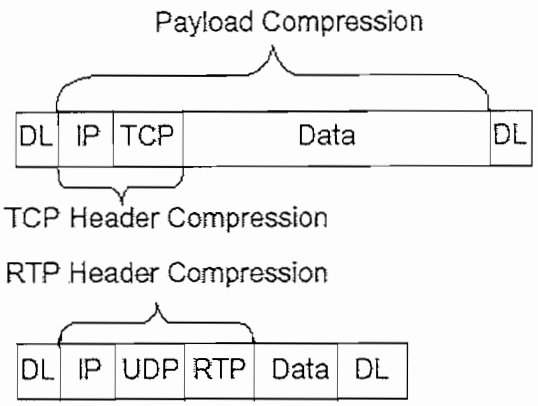


Figura 2-15 Compresión del *Payload* y del *Header* [4]

Al utilizar estos métodos de compresión, el tiempo de CPU requerido para realizar los algoritmos añade retardo a los paquetes. El ancho de banda ganado por la compresión debe ser más importante que el retardo añadido por el proceso de la misma compresión, razón por la cual se debe tomar en cuenta al utilizar estos métodos y a qué aplicación se la implementa.

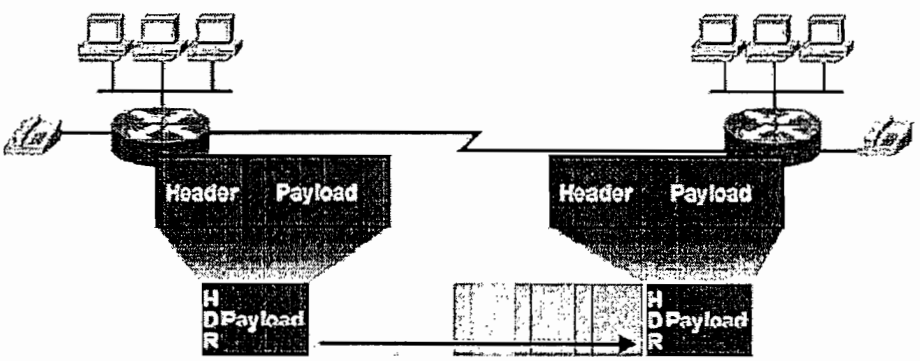


Figura 2-16 Reducción del tamaño del paquete [11]

La compresión del *payload* involucra la reducción del tamaño del *payload* en capa 2. Esta compresión incrementa el *throughput*, porque los paquetes pequeños (con el

payload comprimido) toman menos tiempo para ser transmitidos que un paquete grande sin compresión.

La compresión del *header* en cambio es un método que trabaja sin transmitir información repetida en los *headers* de los paquetes a través de una sesión.

Ambos dispositivos que se encuentran en una conexión punto a punto se ponen de acuerdo en el índice del diccionario del *header* del paquete. El diccionario es construido al comienzo de cada sesión y es utilizado por todos los paquetes subsecuentes.

2.5.1.1 Compresión del *Payload*

La figura 2-17 muestra un diagrama de bloques básico del método de compresión del *payload*. Cuando un *router* envía un paquete, éste se sujeta a un método de compresión de capa 2 después de que haya sido encapsulado en la salida.

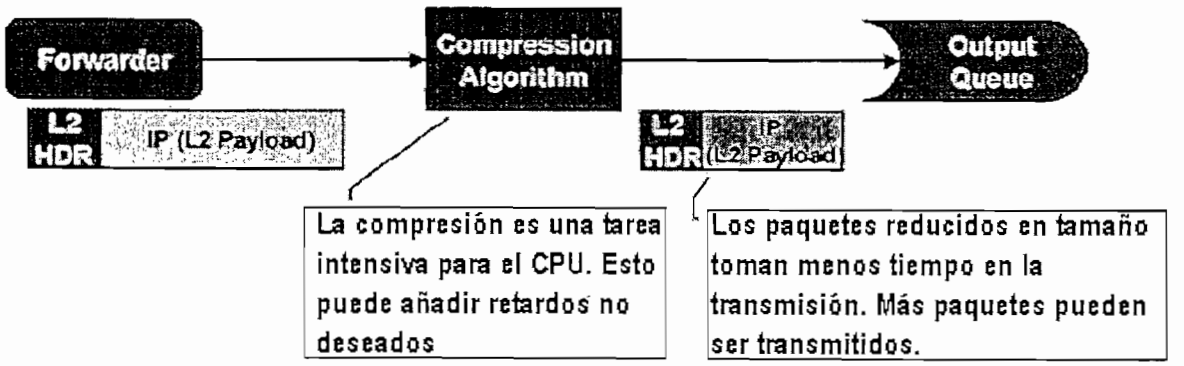


Figura 2-17 Diagrama de bloque del proceso de compresión del *payload* [11]

En este método se reduce el retardo de serialización porque los *frames* son más pequeños. Dependiendo de la complejidad del algoritmo de compresión del *payload* de capa 2, la latencia total puede ser reducida, especialmente en enlaces de baja velocidad.

Se puede hablar de 3 diferentes opciones como herramientas de compresión del *payload* en enlaces seriales: *Stacker*, *Microsoft Point to Point Compression* (MPPC), y *Predictor.*

Hay que considerar los siguientes criterios para escoger las opciones de compresión del *payload*:

- Los tipos de protocolos en la capa de enlace
- La eficiencia del algoritmo de compresión
- Si el dispositivo en el otro extremo del enlace soporta estas herramientas

Stacker y *MPPC* usan el algoritmo de compresión llamado Lempel-Ziv[6]. *Predictor* utiliza menos recursos de CPU y memoria que Lempel-Ziv, pero Lempel-Ziv produce una mejor relación de compresión.

De las tres opciones, *Stacker* soporta más protocolos de capa de enlace que las otras dos herramientas. La tabla 2.2 muestra los principales puntos de comparación de las tres herramientas de compresión del *payload*

Tabla 2.2 Características de comparación entre las herramientas de compresión del *payload* [4]

Característica	***Stacker***	***MPPC***	***Predictor***
Usa Lempel-Ziv	Si	Si	No
Usa Predictor	No	No	Si
Soportado en HDLC	Si	No	No
Soportado en X.25	Si	No	No
Soportado en LAPB	Si	No	Si
Soportado en *Frame Relay*	Si	No	No
Soportado en PPP	Si	Si	Si
Soportado en ATM (usando multilink PPP)	Si	Si	Si

[6] Algoritmo de compresión que durante el proceso de codificación el emisor va construyendo una tabla o diccionario con la información que va tratando

Ejemplo de Compresión del Payload

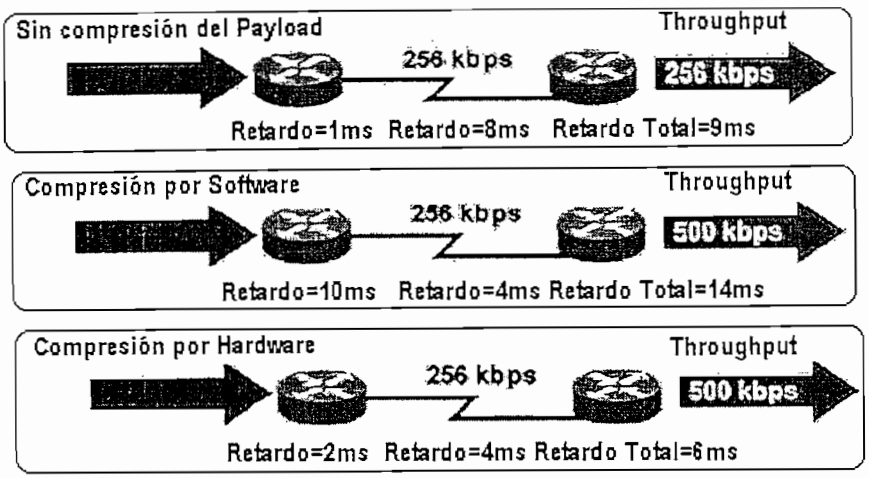


Figura 2-18 Resultados de la compresión de *payload* en capa 2 [11]

En la figura 2-18 se compara el *throughtput*/Latencia de tres enlaces PPP. Si no se usa compresión, el *throughput* está limitado por el ancho de banda del enlace, y el retardo promedio es influenciado únicamente por el retardo del envío, la serialización y la propagación.

Si se habilita la compresión, el retardo de serialización es menor debido a que el *frame* es más pequeño; el retardo de compresión/descompresión puede incrementar la latencia total del enlace.

El *throughput* se incrementa porque se reduce el tamaño del *payload* de capa 2, y así permite enviar más *frames* en un período de tiempo dado. El *throughput* está limitado por la eficiencia del algoritmo de compresión del *payload* de capa 2 y puede ser significativamente más grande que el ancho de banda del enlace.

2.5.1.2 Compresión del *Header*

La compresión del *header* incrementa el *throughput* percibido y reduce el retardo por compresión de los protocolos del *header*. La compresión del *header* es más útil para aplicaciones que generan *payloads* pequeños porque los protocolos de los *headers*

de tal aplicación consumen un significativo porcentaje del ancho de banda disponible relativo a su *payload*.

Las aplicaciones de tiempo real típicamente generan *payload* pequeños. Una aplicación para aplicar *header compression* puede ser Telnet y aplicaciones RTP como VoIP.

La compresión del *header* de TCP y RTP se aplica a todo flujo TCP y RTP. La compresión del *header* de TCP para un volumen de datos (paquetes con grandes *payload*s) produce un pequeño ahorro de ancho de banda.

La figura 2-19 muestra un diagrama de bloques del método de compresión del *header*.

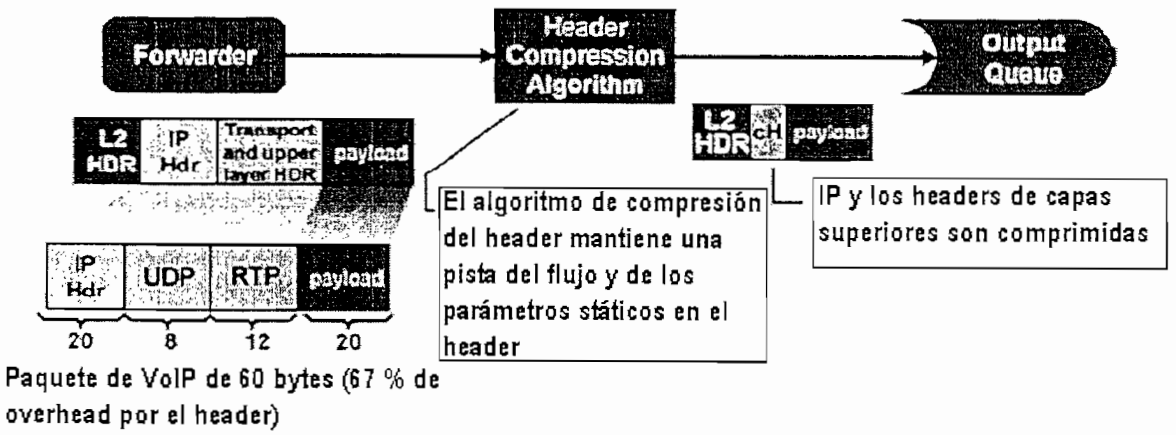


Figura 2-19 Método de compresión del *header* [11]

Por ejemplo, sin compresión del *header* RTP, la sobrecarga del *header* IP/UDP/RTP del paquete de voz que muestra la figura 2-19, es alrededor del 67% (40/60 x 100 %). Con la compresión del *header* RTP, el *header* IP/UDP/RTP puede ser reducido a 2 o 4 bytes (con y sin *checksum*, respectivamente), por lo que la sobrecarga puede ser reducida alrededor del 9% (2/22 x 100%) o 17 % (4/24 x 100%).

En la tabla 1.2 se mostró los requerimientos para la capacidad del canal para varios tipos de tecnologías de capa de enlace, y en la tabla 2.3 se comparan los mismos datos pero ahora con RTP *header compression.*

Tabla 2.3 Requerimientos de capacidad de canal para varios tipos de codecs con cRTP [4]

Tipo de *header* de (capa 2)	Tamaño del *header* (capa2)	Tamaño del *header* comprimido (IP/UDP/RTP)	Codec	Capacidad del *payload*	Capacidad Total requerida
Frame Relay	6 bytes	2 bytes	G.711	64 Kbps	67.2 Kbps
Frame Relay	6 bytes	2 bytes	G.729	8 Kbps	11.2 Kbps

2.5.2 FRAGMENTACIÓN Y ENTRELAZADO DE PAQUETES (LFI)

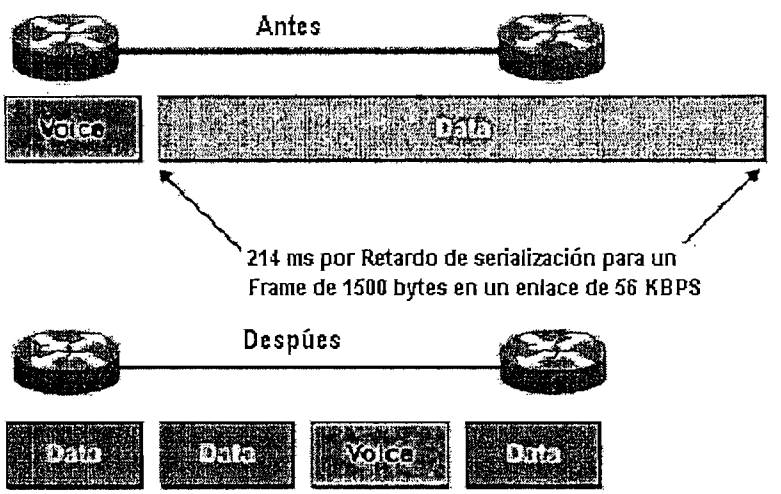


Figura 2-20 Fragmentación y entrelazado [7]

Las herramientas de LFI (*Link Fragmentation and Interleaving*) atacan directamente al problema del retardo de serialización, asegurando que los grandes paquetes no ocasionen retardo a los pequeños paquetes. Para lograr hacer esto, se fragmentan los paquetes grandes (*fragmentation*), y entre estos paquetes fragmentados, se intercalan los pequeños paquetes (*interleaving*) (figura 2-20), de esta manera se reduce el retardo de serialización de los paquetes pequeños.

Por ejemplo el retardo de serialización de un paquete de 1500 bytes sobre un enlace de 56 Kbps llega a ser 214 ms. Para el tráfico de voz el máximo retardo de extremo a extremo recomendado es de 150 ms (tabla 1.5).

Por consiguiente, si se tiene un paquete de 1500 bytes delante de un paquete de voz en un enlace de 56 Kbps, el primero puede causar que la voz se degrade debido al retardo. La solución a éste problema es LFI para que los paquetes grandes no causen que los paquetes de voz esperen por más tiempo que el requerido.

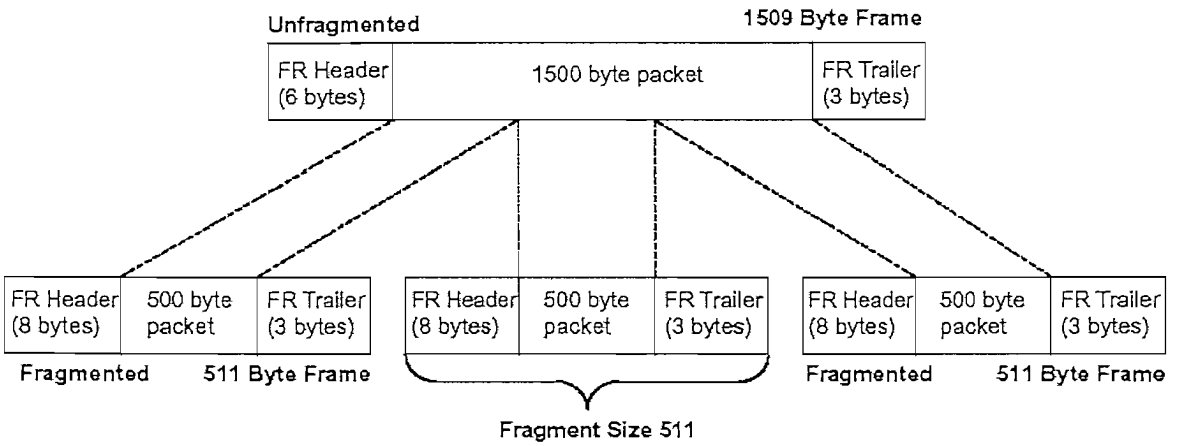


Figura 2-21 Aplicación de LFI a paquetes y *frames*

Las herramientas de LFI requieren que se analice acerca de qué sucede con el paquete, y qué sucede con el *frame*. En la figura 2-21 se muestran algunos detalles de un *frame* no fragmentado, y un *frame* fragmentado, usando *Frame Relay*.

En la parte superior de la figura 2-21, un paquete de 1500 bytes tiene añadidos 9 bytes de *header* y *trailer Frame Relay*, lo que forma un *frame* de 1509 bytes. En la parte inferior de la misma figura, el paquete de 1500 bytes es dividido en tres fragmentos de 500 bytes, y colocados en tramas *Frame Relay*. Debido a FRF.12 (*Frame Relay Forum* 12), se deben añadir 2 bytes a cada *header* para poder administrar los fragmentos, lo que da un total de 511 bytes para cada fragmento.

Algunos *routers* dividen los paquetes en pequeños fragmentos, los cuales están basados en el tamaño del *frame*. Cuando se escoja el tamaño de los fragmentos, se debe recordar que el tamaño del fragmento determina el tamaño del *frame*, no del paquete. Sin embargo se debe considerar la longitud de los *headers* y *trailers* de la capa de enlace cuando se escoja el tamaño de los fragmentos.

CAPÍTULO 3

Desde los EE- hasta la última hoja que está antes de Anexos

3. DISEÑO DE LA RED ENTRE LAS OFICINAS

Este diseño se basa en la unificación de tres oficinas remotas ubicadas en: Quito, Guayaquil y Cuenca, donde cada una de ellas posee usuarios conectados a través de una red LAN Ethernet o FastEthernet, que son las tecnologías más populares y de mayor implementación en el mundo [17].

Se pretende unificar estas oficinas a través de una red WAN con tecnología existente en el país; para esto se consultará a tres proveedores que ofrezcan este tipo de servicio (*carriers*), y así poder realizar un análisis de tecnologías y sobre todo de costos, así como examinar la posibilidad de implementar telefonía a través de esta red.

Como en muchos casos, varias empresas poseen sucursales alrededor del país y se encuentran conectadas a través de una infraestructura de red WAN para el manejo de sus datos, pero en su mayoría poseen redes separadas para el manejo de sus datos y comunicaciones telefónicas. Por esta razón se pretende realizar un dimensionamiento básico, esto es con características generales, para que cualquier empresa que posea una infraestructura de red en sitios remotos pueda tener sus comunicaciones de voz a través de su infraestructura de datos.

El diseño está dirigido a empresas que posean sucursales alrededor del país y requieran que sus empleados tengan acceso a Internet, correo electrónico y soliciten de alguna base de datos; consulta de información como: proveedores, inventario, compras, ventas, etc., facturación, o algún sistema que se pueda manejar de forma centralizada en un servidor principal ubicado en la oficina matriz. Por tal razón se tendría que implementar una incorconexión entre sus oficinas a través de una red WAN para el manejo de sus datos.

El diseño demanda que se deban conocer las necesidades particulares del cliente, pero debido a que este diseño no es para ninguna empresa o cliente en especial, se

analizará un ejemplo con aplicaciones y requerimientos frecuentes que las empresas suelen necesitar considerando que una de estas aplicaciones debe ser la de VoIP.

Además en este proyecto se intenta mostrar que si alguna empresa requiere implementar una red para el manejo de sus datos, se aproveche ésta para que también se piense en que sus comunicaciones telefónicas puedan circular a través de esta red sin que esto afecte al desenvolvimiento normal de la red solo de datos.

3.1 CARACTERIZACIÓN DE LAS REDES LAN [13]

Para el ejemplo y para la caracterización de las redes LAN se indicarán áreas departamentales comunes que las empresas suelen poseer y dónde éstas se encuentran funcionando, ésto para poder tener una densidad de usuarios y obtener una carga aproximada del tráfico de datos. El ejemplo posee una oficina matriz, que es dónde se tendrá la mayor cantidad de usuarios, por lo que se considera que en esta oficina se instale el cuarto principal de servidores. También es importante determinar las aplicaciones que van a circular por las redes LAN, y las que van a circular por la WAN.

3.1.1 PASOS PARA CARACTERIZAR UNA RED [13]

Paso 1: Caracterización de las Aplicaciones

Por medio de una tabla se pueden establecer las características de las aplicaciones como:

- Nombre y tipo de la aplicación: por ejemplo si la aplicación es base de datos, multimedia, correo electrónico, o algún sistema de facturación.
- Número de usuarios: cantidad de usuarios que acceden a la aplicación
- Número de servidores: cantidad de servidores que ofrece cada aplicación
- Comentario: algún tipo de comentario que ayude para el diseño de la red, como escalabilidad, algún tipo de plan para migrar la red, etc.

Paso 2: Caracterización de los Protocolos

De igual manera como con la aplicación, se deben caracterizar los protocolos por: nombre, número de usuarios que usan el protocolo, número de servidores, etc.

Paso 3: Documentación

- ***Topología de la red***

  Se puede dibujar un mapa de la topología de la red, incluyendo información tal como: ubicación geográfica, número de usuarios por cada oficina, ubicación de los servidores, entre otras.

- ***Esquema de direccionamiento***

  Documentar el esquema de direccionamiento utilizado para las distintas redes a las que se pretende unir por medio de una red WAN. Documentar las direcciones IP y máscaras de subred para cada equipo.

- ***Preocupaciones acerca de la red***

  Se puede documentar información que pueda ser útil como por ejemplo: el flujo del tráfico, posibles adecuaciones de la red, sitios donde se pueden tener "cuellos de botella", etc.

El ejemplo, al que corresponde el diseño de la red, posee Departamentos en cada una de sus agencias, y cada uno de sus usuarios tendrá a su cargo un computador personal.

Todas las computadoras dispondrán de tarjetas de red Ethernet/FastEthernet *autosensing* 10/100 Mbps. Estas máquinas estarán conectadas entre sí por medio de un cableado estructurado Cat. 5e.

En la oficina matriz se ubicarán los servidores y el *rack* principal. Cada oficina remota tendrá un *rack* de pared donde se concentrarán todos los puntos de cableado estructurado.

En la tabla 3.1 se resume el número de usuarios que van a utilizar la red. Se considera que los usuarios de las oficinas en Cuenca y Guayaquil realizarán consultas remotas a los servidores que se encontrarán ubicados en la oficina matriz en Quito. Con esta información se podrá analizar el tráfico de datos que va a circular a través de la red WAN.

Tabla 3.1 Distribución de usuarios por Agencias y Departamentos

Ubicación	Departamentos	Usuarios/Dpto.	Usuarios/Agencia
Quito (Oficina Matriz)	Gerencia	2	15
	Secretaría General	2	
	Financiero	2	
	Recursos Humanos	1	
	Servicio Técnico	2	
	Ventas	5	
	Jurídico	1	
Cuenca	Gerencia	2	7
	Supervisor	1	
	Servicio Técnico	1	
	Ventas	3	
Guayaquil	Gerencia	2	7
	Supervisor	1	
	Servicio Técnico	1	
	Ventas	3	
Total Usuarios			29

Para la comparación posterior de la telefonía tradicional con VoIP se considera que cada oficina tiene una central telefónica PBX. La oficina matriz en Quito tendrá cuatro líneas telefónicas públicas, y cada agencia remota, dos líneas telefónica públicas; todos los usuarios mencionados en la lista poseen teléfonos analógicos.

Para el tráfico de datos se analizarán usuarios por aplicación, considerando que todos los usuarios requieren del acceso a Internet y correo electrónico y ciertos usuarios el acceso a la Base de Datos. Se resumen los pasos 1 y 2 en la tabla 3.2.

Tabla 3.2 Caracterización de las aplicaciones y protocolos

Nombre y tipo de Aplicación	Protocolos	No. de usuarios	No. de servidores
Base de Datos (Oracle)	TCP/IP	16	1
Microsoft Exchange e-mail	TCP/IP	29	1
Acceso a Internet	TCP/IP	29	1

3.1.2 CARACTERIZACIÓN DEL TRÁFICO DE LA RED

Uno de los aspectos más difíciles de extraer en lo que se refiere a los requerimientos del cliente, es el comportamiento del tráfico en la red.

Para poder caracterizar el tráfico y los protocolos de la red, se debe entender qué tamaño van a tener los *frames* dependiendo de las aplicaciones que van a transportar estos *frames.* Otros parámetros también son importantes tales como: el tipo de control de flujo, la carga que se produce cuando se inicializa la red, qué datos son compartidos y quién va a estar utilizando los datos, entre otros.

3.1.3 TAMAÑO DEL *FRAME*

El utilizar el *frame* a su tamaño máximo soportado, tendrá un impacto positivo muy significativo en el desempeño de la red. Para una aplicación en particular como la transferencia de archivos, se debería usar la Unidad Máxima de Transferencia (MTU). Dependiendo del *stack* de protocolos que se esté empleando, el MTU puede ser configurado para alguna aplicación específica. Se debe evitar el incremento del MTU a cantidades mayores al máximo, de esta manera impedir la fragmentación y el reensamblado. Cuando los dispositivos tales como los *routers* necesitan fragmentar y reensamblar *frames*, el desempeño se degrada.

Para IP, se usa un *stack* de protocolos que soporte un ***MTU discovery***. Con *MTU discovery*, el software puede dinámicamente determinar y usar el tamaño del *frame*

más grande que podría atravesar por la red sin requerir fragmentación. En la tabla 3.3 se observa la importancia de usar el tamaño máximo del *frame.*

Tabla 3.3 Eficiencia dependiendo del tamaño del *frame* [12]

Tamaño de los datos en bytes	Tamaño del *frame* en bytes	*Overhead*	Eficiencia Máxima
1492	1518 (máximo)	2.5%	97.5%
974	1000	3.8%	96.2%
474	500	7.4%	92.6%
38 (no PAD)	64 bytes (mínimo)	50.0%	50.0%

3.1.4 *WINDOWING* Y CONTROL DE FLUJO

En TCP/IP, el Protocolo de Control de Transmisión (TCP) soporta *windowing* y control de flujo. Algunas aplicaciones que "corren" sobre TCP son:

- *File Transfer Protocol* (FTP): puerto 20 (data) y puerto 21 (control)
- Telnet: puerto 23
- *Simple Mail Transfer Protocol* (SMTP): puerto 25
- *Hypertext Transfer Protocol* (HTTP): puerto 80

User Datagram Protocol (UDP) no ofrece *windowing* y control de flujo. Las aplicaciones que generalmente "corren" sobre UDP son:

- *Simple Network Management Protocol* (SNMP): puerto 161
- *Domain Name System* (DNS): puerto 53
- *Trivial File Transfer Protocol* (TFTP): puerto 69
- *Remote-Procedure Call* (RPC): puerto 111
- *Dynamic Host Configuration Protocol* (DHCP) *server*: puerto 67
- DHCP *client*: puerto 68

Protocolos tales como *Network File System* y *Network Information Service* (NIS) usan RPC.

3.1.5 TRÁFICO CAUSADO POR LA INICIALIZACIÓN DE UNA ESTACIÓN

La tabla 3.4 muestra los paquetes que una estación TCP/IP sin DHCP envía cuando ésta se inicializa. Por encima del tamaño del paquete, se añade *overhead* en la capa de enlace. Dependiendo de la implementación de TCP/IP, los paquetes pueden ser relativamente diferentes que los mostrados aquí.

Tabla 3.4 Paquetes para una inicialización tradicional de un Cliente TCP/IP [13]

Paquete	Fuente	Destino	Tamaño del Paquete en bytes	Número de Paquete	Tamaño Total en bytes
ARP se asegura que la dirección es única. (opcional)	Cliente	*Broadcast*	28	1	28
ARP para algún servidor	Cliente	*Broadcast*	28	Depende del número de servidores	Depende
ARP para el *router*	Cliente	*Broadcast*	28	1	28
ARP *response*	Servidor(es) o *router*	Cliente	28	1	28

En la tabla 3.5 se muestran los paquetes que una estación TCP/IP "corriendo" DHCP envía cuando se inicializa.

Tabla 3.5 Paquetes para la inicialización de un cliente DHCP [13]

Paquete	Fuente	Destino	Tamaño de paquete en bytes	Número de Paquetes	Tamaño total en bytes
DHCP *discover*	Cliente	*Broadcast*	576	Una vez cada pocos segundos hasta que el cliente tenga noticias de un servidor DHCP	Depende
DHCP *offer*	Servidor	*Broadcast*	328	1	328
DHCP *request*	Cliente	*Broadcast*	576	1	576
DHCP ACK	Servidor	*Broadcast*	328	1	328
ARP debe estar seguro de que la dirección es única	Cliente	*Broadcast*	28	3	84
ARP *client*	Servidor	*Broadcast*	28	1	28
ARP *response*	Cliente	Servidor	28	1	28
DHCP *request*	Cliente	Servidor	576	1	576
DHCP ACK	Servidor	Cliente	328	1	328

Los beneficios que ofrece una configuración dinámica pesan más que las desventajas del tráfico extra y los paquetes *broadcast* extra que se envían a la red cuando se utiliza DHCP. (El cliente y el servidor usan paquetes *broadcast* hasta que se conozcan las direcciones IP).

También es importante modelar el tipo de tráfico correspondiente a cada aplicación que va a estar "corriendo" en la red, para determinar cuál va a ser la carga que va a tener la red.

Las tablas 3.6 y 3.7 muestran en detalle varios tipos de tráfico. Con esta información se puede conocer el número de paquetes que son enviados a la red por cada aplicación.

Para este caso de diseño, se van a considerar únicamente tres aplicaciones: MS-Exchange, HTTP, y una Base de Datos, las mismas que ayudarán a caracterizar el tráfico de datos de mejor manera. Los datos de las tablas 3.6 y 3.7 son obtenidos de un estudio de *The Tolly Group, Inc,* por Kevin Tolly, Pres. /CEO y Brian Tolly, *Senior Engineer*, y fueron utilizadas para una comparación entre las marcas CISCO y Extreme Networks.

Tabla 3.6 Número de Paquetes por el tamaño del *frame* – por la duración de la muestra [20]

		Tamaño del paquete en bytes						Duración de la muestra (seg.)
		64-127	128-255	256-512	512-1023	1024-1517	1518	
Tipo de tráfico	Exchange	1981	0	2941	531	4122	4731	9,333
	HTTP	13895	0	2	1485	0	6482	5,54
	Data Base	311	1578	592	380	497	353	2,223
Total		16187	1578	3535	2396	4619	11566	
Porcentaje del tráfico total por tamaño del *frame*		41%	4%	9%	6%	12%	29%	

La tabla 3.6 muestra el número de paquetes transmitidos. Estas muestras fueron capturadas en varios intervalos de tiempo (última columna de la tabla 3.6), y fueron obtenidas sobre seis diferentes tamaños de paquetes.

Tabla 3.7 Número de Paquetes por segundo por el tamaño del *frame* [20]

		Tamaño del paquete en bytes					
		64-127	128-255	256-512	512-1023	1024-1517	1518
Tipo de tráfico	Exchange	212	0	315	57	442	507
	HTTP	2508	0	0	268	0	1170
	DataBase	140	710	266	171	224	159
	TOTAL	**2860**	**710**	**581**	**496**	**666**	**1836**
Porcentaje del tráfico total		**40 %**	**10 %**	**8 %**	**7%**	**9 %**	**26 %**

A diferencia de la tabla 3.6, la tabla 3.7 indica el número de paquetes por segundo que cada aplicación envía a la red, y se la obtuvo dividiendo para el tiempo de captura de cada muestra (tabla 3.6), en los diferentes tamaños del *frame*. Una vez obtenida la cantidad de paquetes por segundo que son enviados por las aplicaciones a la red, resulta más fácil modelar a la red para poder dimensionarla.

3.2 ALTERNATIVAS DE INTERCONEXIÓN ENTRE LAS OFICINAS REMOTAS

En la oficina principal que se encuentra en la ciudad de Quito, se ubicarán los distintos servidores, razón por la que las oficinas remotas realizarán peticiones de información a la oficina de Quito.

La conexión a Internet se lo hará por medio de la oficina en Quito, por lo que las oficinas de Guayaquil y Cuenca para acceder a Internet necesitarán enlazarse a Quito por medio de una infraestructura de red WAN. Ésta provee comunicaciones a los usuarios a través de una amplia área geográfica, en este caso para enlazar

Cuenca – Quito y Guayaquil – Quito. La red WAN generalmente está compuesta de *switches* y *routers* que enlazan las oficinas remotas. Se puede seleccionar los enlaces WAN de diferentes capacidades y utilizar diferentes tecnologías, dependiendo de los requerimientos de cada enlace.

Los enlaces WAN pueden ser implementados a través de una PDN (*Public Data Network*) o de enlaces directos como por ejemplo a través de enlaces de radio, microonda o conexiones directas a través de fibra óptica (figura 3-1).

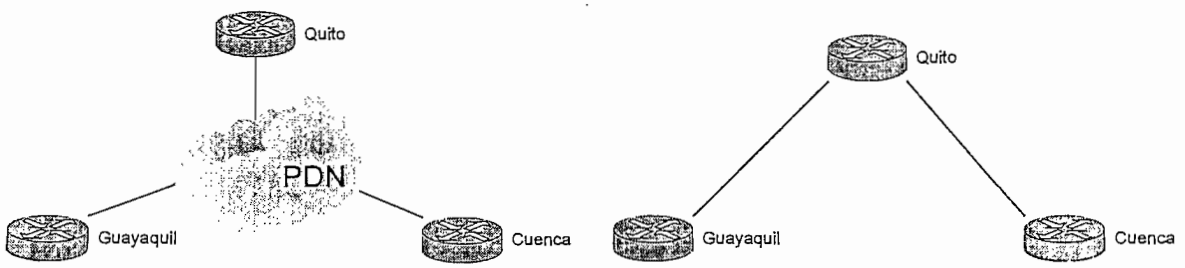


Figura 3-1 Alternativas de enlaces WAN

Una PDN, es un servicio de paquetes o circuitos conmutados proporcionados por los *carriers*, como por ejemplo servicios X.25, *Frame Relay*, SMDS (*Switched Multi-megabit Data Service*), ISDN o ATM.

Este proyecto resulta más conveniente ser implementado a través de una PDN, debido a la relación costo – beneficio que ofrece este tipo de red, ya que se puede rentar únicamente la capacidad que se requiera de una red ya instalada evitando el costo de instalar una red privada. El costo que involucra la implementación de una infraestructura de enlace directo no justifica la carga que va a circular por estos enlaces.

Algunos proveedores ofrecen conexiones a través de sus sistemas, e incluso suelen proporcionar el hardware requerido, y por el uso de sus conexiones cobran ciertas tarifas. Estas tarifas son en base a un costo periódico único independiente de la distancia o del volumen de información.

Para el diseño de la red WAN se recomienda poner mucha atención en el análisis de los requerimientos, la caracterización de la red existente (si la hay), y en el diseño de la nueva topología.

3.2.1 FACTORES DE DISEÑO PARA LA RED WAN

3.2.1.1 Factores de Aplicación

El acceso a la aplicación es un factor importante para el diseño de la WAN. La mayoría de los usuarios tienen acceso remoto a las aplicaciones. Por ejemplo para el acceso a la Base de Datos y el acceso a Internet que se encuentra en la oficina principal, los usuarios de las oficinas remotas lo hacen por medio de la WAN.

Los componentes más importantes que se involucran en este tipo de red son: tiempo de respuesta, *throughput* y confiabilidad.

3.2.1.1.1 Tiempo de respuesta

Es una medida muy importante, debido a que son los usuarios finales de la red los más involucrados con este componente y causaría molestias si éste llega a tener tiempos de respuesta lentos. Los dos componentes específicos de tiempo de respuesta son: retardo y *jitter*.

Cuando se incrementa la cantidad de llamadas de voz por la red, estas medidas producen efectos críticos en la calidad de recepción. Con el tráfico de datos, el retardo contribuye directamente al tiempo de respuesta.

En una conversación de voz, el retardo excesivo puede forzar un estilo de conversación donde un lado habla y el otro únicamente escucha o viceversa. El *jitter* es la variación del retardo. El *jitter* excesivo puede causar vacíos en el flujo de la conversación.

3.2.1.1.2 Throughput

Es la cantidad de datos transferidos en una parte de la red durante un intervalo de tiempo específico. Diferentes aplicaciones demandan diferentes *throughputs* en la red.

El que una aplicación requiera más *throughput* de lo que la WAN puede ofrecer, causaría que los paquetes se pierdan. Estos paquetes perdidos se deben a que las colas llegan a saturarse.

Otra causa de paquetes perdidos es el descarte de paquetes con errores. En las redes de telecomunicaciones, a estos errores se los mide como BER (*Bit Error Rate*). El BER es el porcentaje de bits que tienen errores con respecto al número de bits que fueron recibidos.

Tabla 3.8 Tipos de Aplicaciones y *throughput* [3]

	Base de Datos	**Internet y correo electrónico**	**Voz en tiempo real**
Throughput	Requiere alto *throughput*	Bajo *throughput*	Bajo *throughput*

Una solución para disminuir el BER en una WAN es transmitir los datos a velocidades menores, pero esto también reduciría el *throughput.* La tabla 3.8 muestra los requerimientos de *throughput* para diferentes tipos de aplicaciones.

3.2.1.1.3 Confiabilidad

La confiabilidad para aplicaciones en la red es medida dependiendo de cómo las aplicaciones están disponibles cuando los usuarios quieren accederlas. Algunos diseñadores se refieren a la duración de tiempo que una aplicación se encuentra fuera de servicio, o no está disponible.

Existen algunas aplicaciones que son muy sensibles a la confiabilidad de la red; para solucionar este problema se suele considerar para el diseño de la WAN el uso de redundancia, pero también hay que considerar los costos que involucrarían una red con redundancia.

3.2.1.2 Factores Técnicos

El principal factor técnico cuando se diseña una WAN es la capacidad del canal. La tabla 3.9 presenta capacidades de canal dadas por el uso de ciertas tecnologías.

Tabla 3.9 Capacidades de Canal [3]

Tecnología	**Medio Físico**	**Rango de capacidad de canal**
Modem analógico (*dial-up*)	Cobre	45 Kbps
ISDN	Cobre	Menor a 2 Mbps
Frame Relay	Cobre	Menor a 2 Mbps
ADSL	Cobre	8 Mbps de *downstream*
Cable Modem	Coaxial	27 Mbps de *downstream*; 2.5 Mbps de *upstream*

El requerimiento de la capacidad del canal es directamente proporcional a la cantidad de usuarios que transmiten en una red.

3.2.1.3 Factor Costos

Otro factor muy significativo para el diseño de una WAN es el costo que implica la implementación de la red. El costo principalmente involucra los siguientes aspectos:

- **Compra o renta de equipos**: Incluye modems, CSUs (*Channel Service Units*) o DSUs (*Digital Suscriber Units*), *routers*, interfaces para los *routers*, *switches* y módulos.

- **Alquiler del enlace**: Incluye la carga para establecer el circuito virtual a través de WAN, y conocer la capacidad de canal a contratar.

- **Herramientas de administración de red y plataformas**: Incluye aplicaciones de administración y monitoreo como por ejemplo CiscoWorks u OpenView.

3.2.2 TECNOLOGÍAS WAN PARA ACCESO REMOTO

La figura 3-1 muestra un ejemplo de una topología de red. Este ejemplo necesita soluciones de acceso remoto para proveer servicio a los usuarios remotos de la red y a las oficinas sucursales.

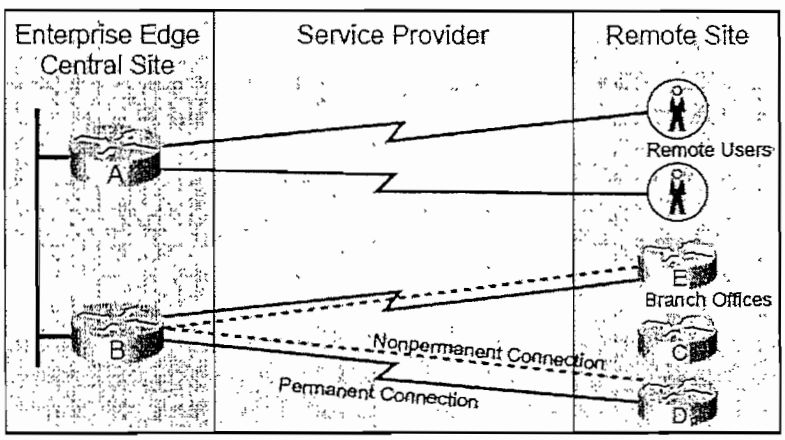


Figura 3-2 Ejemplo de acceso remoto [3]

Como se puede observar en la figura 3-2, la topología del *router* B es muy similar a la red que se está diseñando.

Muchos diseñadores coinciden en escoger conexiones permanentes entre las oficinas remotas y el sitio central usando PVCs de *Frame Relay*. Para el *router* A, se puede escoger conexiones no permanentes *dial – up*.

Como se analizará más adelante se ha escogido una topología *Frame Relay* debido a que ofrece la mejor alternativa en relación a costos, además, es la tecnología más común en el país. Las redes de paquetes conmutados tienen tres topologías:

1. Topología en estrella

   Una topología en estrella especifica un *router* central que sirve como un HUB para las conexiones de la WAN. Muchos autores conocen a esta topología como *hub-and-spoke*. El *router* central se conecta a cada una de las oficinas sucursales; en efecto, estas oficinas sucursales pueden únicamente comunicarse entre sí, a través del *router* central.

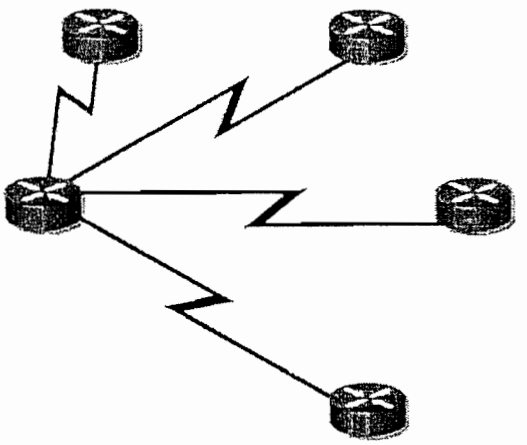


Figura 3-3 Topología en estrella [2]

La principal ventaja de tener una topología como ésta, es la posibilidad de disponer una administración centralizada. Las desventajas de esta topología son las siguientes:

- Si el *router* central falla, todas las comunicaciones de la WAN estarían afectadas.
- El desempeño global de la WAN se basa principalmente en el *router* central, debido a que todo el tráfico circula a través de éste.

2. Topología en malla parcial (*Partial-Mesh)*

   Esta topología se aproxima a las características de los circuitos virtuales que conectan varios (no todos) *routers* de la red. Además tiene *routers* centrales que se unen entre ellos y con otros. Existen varias maneras de formar topologías *Partial-Mesh*.

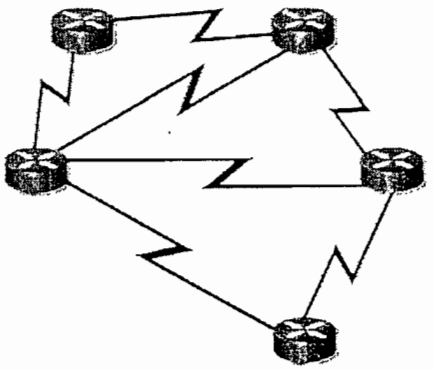


Figura 3-4 Topología *Partial-Mesh* [2]

Las ventajas de esta topología son:

- Desempeño mejorado
- Redundancia mejorada
- Menor circuitos virtuales que una topología *Full-Mesh*

Entre las desventajas se tienen:

- Mayor número de circuitos virtuales que una topología en estrella
- Mayor nivel de especialización para su diseño

3. Topología en malla (*Full-Mesh)*

   En este tipo de topología, todos los nodos (*routers*) se conectan entre sí. Con este diseño se mejora el desempeño por medio de la redundancia.

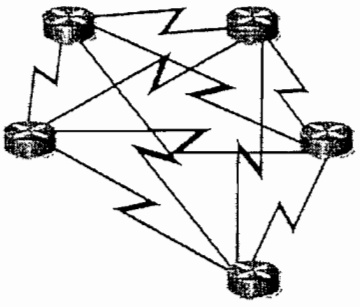


Figura 3-5 Topología *Full-Mesh* [2]

Las ventajas de esta topología son:

- Redundancia
- Mayor desempeño con la configuración apropiada

Entre las desventajas se tienen:

- Mayor costo debido al mayor número de circuitos virtuales requeridos. Existe uno para cada conexión entre *routers*.
- Se requiere de mayor número de paquetes y replicaciones *broadcast* para transmitir a todos los puntos de la red.
- La configuración de los *routers* es más complicada.

3.2.3 CONSIDERACIONES DE DISEÑO PARA LA RED WAN

Para poder diseñar la red WAN, es importante considerar los siguientes aspectos:

1. Identificar las necesidades

   Los requerimientos a considerar en la WAN son: ancho de banda, calidad del enlace, disponibilidad, características del protocolo de capa de enlace, y costos.

   Para el presente caso, el dimensionamiento de la red se lo hará en el numeral 3.4 de acuerdo a la carga total que va a tener la red y la que va a circular sobre los enlaces WAN.

   En lo que corresponde al análisis de los protocolos de capa de enlace y costos, se los revisará en el punto de selección del proveedor, debido a que estos requerimientos son ofrecidos por los proveedores del servicio, dependiendo de lo que exista en el país.

2. Seleccionar la topología requerida para la red WAN

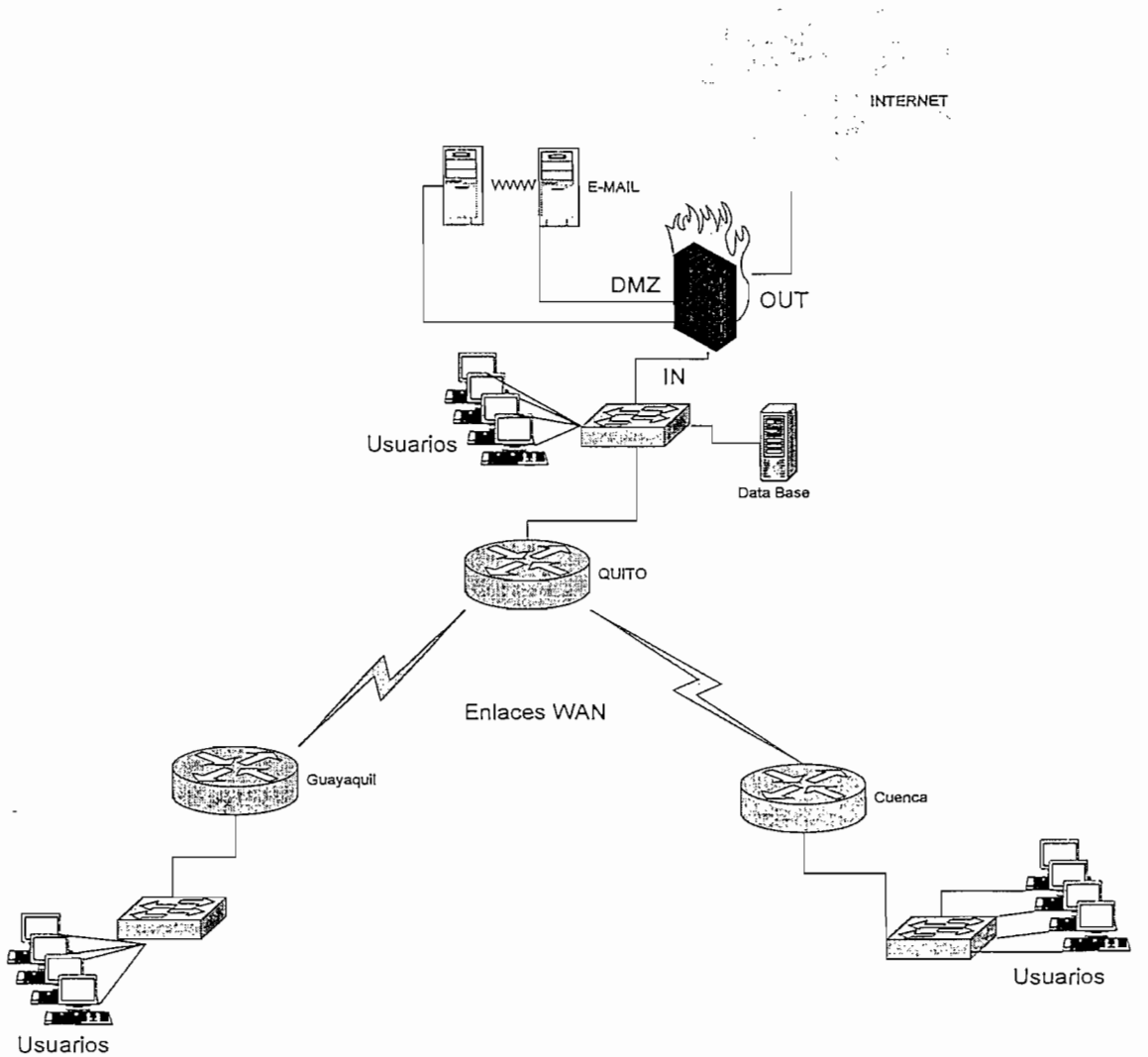


Figura 3-6 Topología de la red

La topología de la WAN incluye la topología Física y Lógica. La topología está estrechamente relacionada con la estructura geográfica, y es importante saber cómo será la interconexión. Para el presente caso se tendrá una topología *Partial-Mesh* o estrella (debido al pequeño número de equipos no existe diferencia entre estas topologías, y comparadas con la *Full-Mesh* son las más económicas).

En la figura 3-6 se observa la topología de la red, la misma que servirá a los diferentes proveedores de servicio para que establezcan las diferentes alternativas de servicios WAN.

Existen compañías que a más de ofrecer servicios portadores, también suministran servicios para una conexión a Internet.

3. Selección de un proveedor de servicio

   Para poder seleccionar un proveedor de servicio, hay que tener en cuenta cuáles son las leyes en el país con respecto a la legislación de los servicios portadores y qué empresas en el país están autorizadas y poseen la cobertura necesaria para poder ofrecer el servicio.

   En el Ecuador las entidades que controlan y regulan este tipo de servicios son el CONATEL, y la SUPTEL. De acuerdo a la SUPTEL: "los servicios portadores son servicios que proporcionan al usuario una capacidad necesaria para el transporte de información, independientemente de su contenido y aplicación, entre dos o más puntos de una red de telecomunicaciones". Estos servicios se pueden prestar bajo dos modalidades: redes conmutadas y redes no conmutadas.

   "Al usuario, se ofrece la capacidad necesaria para la transmisión de signos, señales, datos, imágenes, sonidos, voz e información de cualquier naturaleza entre puntos específicos de terminación de red. Esta capacidad puede ser suministrada a través de redes públicas propias o de terceros, de transporte y de acceso, conmutadas o no conmutadas, físicas, ópticas y radioeléctricas tanto terrestre como espaciales" [16].

   La tabla 3.10 presenta una lista de las empresas que ofrecen estos servicios portadores, la cobertura que ofrecen, y una pequeña estadística de la cantidad de usuarios que se encuentran utilizando estos servicios.

Tabla 3.10 Empresas en el Ecuador que ofrecen servicios portadores [16]

SERVICIOS PORTADORES					
No	OPERADORA	COBERTURA	NÚMERO DE USUARIOS	NÚMERO DE ENLACES	ACTUALIZADO
1	ANDINATEL S.A.	TERRITORIO NACIONAL	2.676	4.858	28-Feb-05
2	CONECEL S.A.	TERRITORIO NACIONAL	77	171	31-Mar-05
3	ECUADORTELECOM S.A.	TERRITORIO NACIONAL	-	-	20-Jun-05 *
4	ETAPA	Cantón Cuenca	170	203	28-Feb-03
5	ETAPATELECOM S.A.	TERRITORIO NACIONAL	71	139	31-Dic-04
6	GILAUCO S.A.	TERRITORIO NACIONAL	-	-	26-Nov-04 *
7	GRUPO BRAVCO CIA. LTDA.	TERRITORIO NACIONAL	9	13	31-Mar-05
8	IMPSATEL DEL ECUADOR S.A.	TERRITORIO NACIONAL	295	1.396	31-Mar-05
9	MEGADATOS S.A.	TERRITORIO NACIONAL	456	888	31-Mar-05
10	NEDETEL S.A.	TERRITORIO NACIONAL	33	41	31-Dic-04
11	OTECEL S.A.	TERRITORIO NACIONAL	39	77	31-Mar-05
12	PACIFICTEL S.A.	TERRITORIO NACIONAL	180	618	31-Mar-05
13	QUICKSAT S.A.	TERRITORIO NACIONAL	1	1	31-Mar-05
14	SETEL S.A.	TERRITORIO NACIONAL	-	-	10-Agos-05 *
15	SURATEL SA.	TERRITORIO NACIONAL	10.946	13.294	31-Mar-05
16	TELCONET S.A.	TERRITORIO NACIONAL	340	382	31-Dic-04
17	TELEHOLDING S.A.	TERRITORIO NACIONAL	-	-	30-Abr-05 *
18	TRANSELECTRIC S.A.	TERRITORIO NACIONAL	1	79	31-Mar-05
19	TRANSNEXA S.A.	TERRITORIO NACIONAL	10	56	31-Ene-05

* Plazo máximo de inicio de operaciones comerciales.

A continuación se determinarán algunas políticas de control para la provisión del servicio, que las empresas que ofrecen los servicios portadores deben cumplir [16]:

- Cumplimiento de obligaciones contractuales, como:
  - Informe mensual de enlaces
  - Reporte mensual del número de usuarios
  - Informe trimestral de calidad del servicio
  - Informe mensual de fallas
  - Informe semestral de quejas
  - Informe mensual de ingresos totales
  - Inspecciones técnicas de control para verificar características técnicas de operación del sistema.

- Supervisión del cumplimiento de Índices de Calidad en los centros de gestión, para verificar los siguientes índices:
  - Porcentaje de averías (PDA).- Averías reportadas por los usuarios del servicio contratado dentro del período de medición aplicable. (Este indicador debe ser menor o igual a 20%)
  - Tiempo medio de reparación de averías (TRA) de circuitos locales y circuitos de larga distancia. Tiempo calculado sobre el total de averías solucionadas dentro del período de medición. Este tiempo es expresado en horas incluyendo fracciones. Este indicador debe ser menor o igual a 8 horas.
  - Porcentaje de averías con tiempo de reparación mayor a 8 horas (PR8) para circuitos locales y de larga distancia. Porcentaje de averías en cuya solución se excedió las 8 horas desde que ésta fue reportada, dentro del período de medición mensual. Este indicador debe ser menor o igual al 5%.
  - Porcentaje de disponibilidad del servicio (PDS) para circuitos locales y de larga distancia. Porcentaje de tiempo de disponibilidad del servicio dentro de un periodo de tiempo. Este indicador debe ser por lo menos 98% en promedio de toda la red del operador.

- Conocer y tramitar las controversias que se susciten entre operadores y/o concesionarios de servicios de telecomunicaciones, a nivel nacional.

Además todas las empresas que ofrecen los servicios portadores, se encuentran legisladas en base a las siguientes leyes:

- Ley Especial de Telecomunicaciones, publicada en el Registro Oficial No. 996 del 10 de agosto de 1992 y sus reformas.
- Reglamento General a la Ley Especial de Telecomunicaciones Reformada, publicado en el Registro Oficial No. 404 del 4 de septiembre del 2001.
- Reglamento para la Prestación de los Servicios Portadores, publicado en el Registro Oficial No. 426 del 4 de octubre del 2001.
- Norma Técnica para la Prestación de Servicios Portadores de Telecomunicaciones Resolución No. 282-11-CONATEL-2002.
- Norma para la Implementación y Operación de Sistemas de Espectro Ensanchado Resolución 388-14-CONATEL-2001. R.O. 215; 30-nov-2000.

De acuerdo a esto, se realizó la consulta a 4 empresas que ofrecen este tipo de servicios, éstas son:

SURATEL: Av. Shyris y Rio Coca, Edif. Euro Centro 2do. Piso
Telf: 2992400 /401/402/403/404/405
Esta empresa ofrece enlaces *Frame Relay*.
Mail: mcarrillo@tvcable.com.ec (Ing. Mauricio Carrillo)

TELCONET: Pedro Gócela 148 y Mariano Echeverría
Telf: 2599215, 2599148
Mail: mescobar@uio.telconet.net (Ing. Moisés Escobar)
Esta empresa ofrece enlaces *Clear Channel* y/o *Frame Relay*

ANDINATEL: Av. Eloy Alfaro y 9 de Octubre Plaza Doral
Telf: 2944824
Mail: jchacon@andinatel.com (Ing. Juan Carlos Chacon)
Esta empresa ofrece enlaces *Clear Channel* y/o *Frame Relay*

IMPSAT: Calle Juan Díaz N37-111
Telf: 2264101
Mail: mperalta@impsat.com (Ing. Miguel Peralta Barahona)
Esta empresa ofrece enlaces *Clear Channel* y/o *Frame Relay*

En su mayoría, las empresas que en el Ecuador ofrecen estos servicios portadores poseen tecnologías TDM (*Clear Channel*) y *Frame Relay* para los enlaces WAN.

Clear Channel: algunos proveedores generalmente ofrecen líneas dedicadas como enlaces punto a punto. Estas líneas dedicadas (*Clear Channel*) son típicamente más confiables (y más costosas) cuando son comparadas con otros tipos de tecnologías WAN, porque ellas son completamente reservadas para la transmisión y están siempre disponibles.

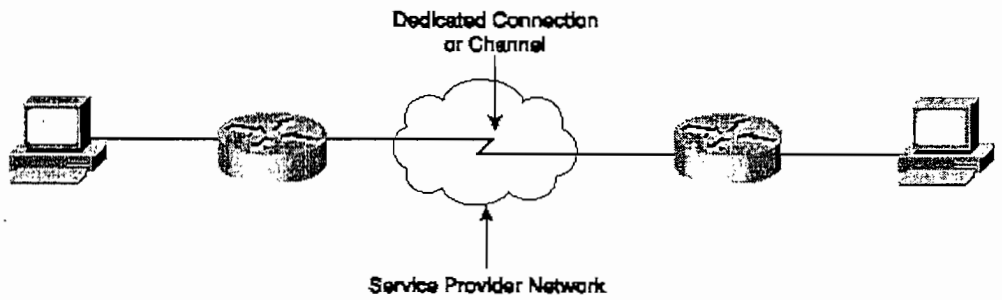


Figura 3-7 Red punto a punto [3]

El enlace punto a punto puede ser sobre un medio dedicado o un canal usando multiplexación por división de tiempo (TDM). Las conexiones seriales

sincrónicas son comúnmente ejemplos de líneas dedicadas. La figura 3-7 muestra una conexión WAN con línea dedicada.

Redes Conmutadas de Paquetes: este tipo de tecnología típicamente reduce los costos tanto al cliente como a la empresa o compañía porque el proveedor del servicio realiza un uso más eficaz de su infraestructura. Esta eficiencia es el resultado de que los clientes comparten los recursos de la WAN, de manera que permite al operador de la red de transporte entrelazar el tráfico de las fuentes a múltiples destinos.

En las redes conmutadas de paquetes, los equipos de la red crean "circuitos virtuales" a través de la WAN compartida, como se muestra en la figura 3-8. Estos circuitos virtuales transportan los datos (segmentados en paquetes) a través de la WAN. Dentro de la tecnología conmutada de paquetes se incluye *Frame Relay.*

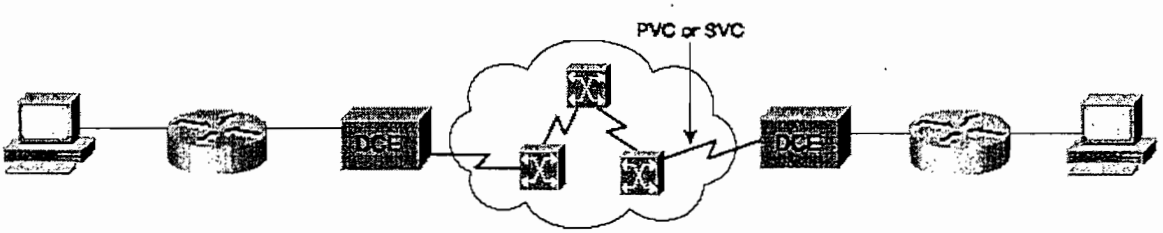


Figura 3-8 Red conmutad de paquetes [3]

Dentro de estos dos tipos de tecnologías que se ofrecen en el país, se va a escoger ***Frame Relay***. Una red conmutada de paquetes ofrece una solución adecuada para la red que se está analizando, debido a que las aplicaciones que van a estar "corriendo" no son constantes, por lo que no necesariamente se necesita un ancho de banda fijo todo el tiempo; adicionalmente por cuestión de costos, una infraestructura *Frame Relay* ofrece planes más económicos que una TDM principalmente porque una red Frame Relay es una red compartida [Anexo A.3].

3.3 CALIDAD DE SERVICIO (QoS) [4]

El diseño de Calidad de Servicio cubre los conceptos en relación a cómo cada aplicación se usa dentro de la compañía, como por ejemplo en una red *Frame Relay*, la manera de escoger un Bc (*Committed Burst*) razonable, o cómo realizar una conformación del tráfico (*traffic shaping*). Estas opciones entre otras se involucran en la obtención de QoS, con el objeto de beneficiar las características o parámetros típicos que existen en la red como ancho de banda, retardos, *jitter* y pérdidas; todo esto para mantener un desempeño óptimo en la red. Por tal razón en este capítulo se analizarán algunas técnicas y lineamientos de QoS que se pueden implementar en la red, para que la carga de VoIP no sea un impedimento y ésta siga funcionando normalmente.

Para aplicar Calidad de Servicio, existen varios métodos y técnicas dependiendo de la infraestructura que se va a instalar en la WAN. Puesto que para el presente diseño se ha escogido *Frame Relay*, todas las técnicas y lineamientos van a estar enfocadas a este tipo de tecnología. Es importante recalcar que la Calidad de Servicio para VoIP es una característica que deben tener los *routers* que se encuentran conectados a la red WAN, porque todo el tráfico de VoIP más el tráfico de datos van a estar circulando por estos dispositivos y es aquí donde se distinguirá y reconocerá cada tipo de tráfico para así poder aplicar Calidad de Servicio.

3.3.1 Lineamientos para diseñar VoIP con QoS en una red *Frame Relay*

Hay dos requerimientos básicos para obtener una buena calidad de la voz:

- Mínimo retardo de extremo a extremo y anulación de *jitter* (variación del retardo).
- Ancho de banda del enlace garantizado y optimizado.

Por lo tanto para garantizar estos requerimientos, se deben seguir las siguientes pautas:

- Prioridad para el tráfico de voz, que se lo puede hacer por medio de un encolamiento de baja latencia LLQ (*Low Latency Queuing*) o con prioridad de paquete IP (*IP RTP priority*).
- *Frame Relay Traffic Shaping*, para asegurar que las velocidades desiguales en los sitios remotos y en el sitio principal sean manipuladas correctamente.
- Fragmentación (FRF.12)
- Reducción de ancho de banda.

3.3.1.1 Prioridad para el tráfico de voz

Existen dos métodos primarios para poder dar una prioridad al tráfico de voz, los cuales se analizarán cada uno de ellos:

- Priorización por paquete IP (*IP RTP Priority*), también llamado PQ/WFQ (*Priority Queuing/WeightedFair Queuing*).
- Baja latencia de encolamiento (LLQ), o CBWFQ (*Classes Based WFQ*).

3.3.1.1.1 Prioridad de paquetes IP (IP RTP Priority)

La prioridad de los paquetes IP en redes *Frame Relay* crea una estricta prioridad de encolamiento en un PVC para un conjunto de paquetes RTP que fluyen hacia un rango de puertos UDP destino.

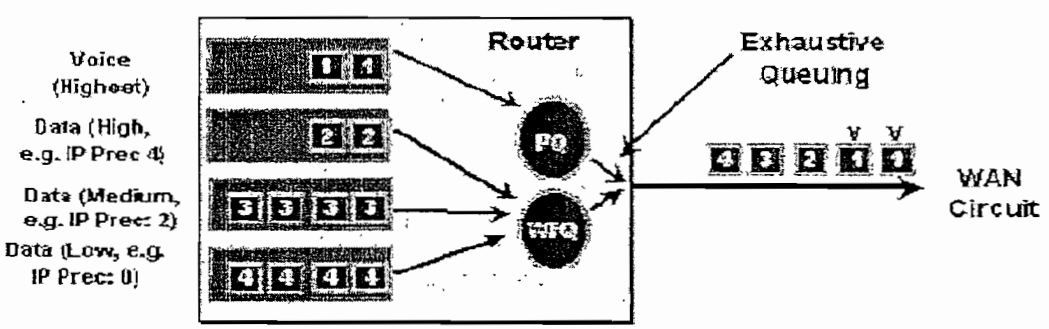


Figura 3-9 Comportamiento de *IP RTP Priority* [9]

Una vez que el *router* reconozca el tráfico VoIP, éste es colocado dentro de un encolamiento prioritario (PQ – *Priority Queuing*). Cuando el PQ esté vacío, las otras colas son procesadas de acuerdo a WFQ. *IP RTP Priority* no se activa hasta que exista congestión en la interfaz. La figura 3-9 ilustra la operación de *IP RTP Priority*.

3.3.1.1.2 LLQ (Low Latency Queuing)

LLQ es una característica que provee una estricta prioridad de encolamiento a CBWFQ (Clases Basadas en WFQ). LLQ habilita un PQ con CBWFQ en las clases.

Cuando se implementa LLQ, los datos que son sensibles al retardo (en la PQ), son sacados de la cola y enviados primero. En VoIP implementando LLQ, este tráfico de voz es situado estrictamente en una cola con prioridad (PQ). La cola PQ es vigilada para asegurar que las colas exactas (*fair queues*) requieran ancho de banda. Cuando se aplica PQ, se debe especificar en Kbps la capacidad máxima de ancho de banda disponible para PQ. Cuando la interfaz está congestionada, la PQ es servida hasta que la carga alcance el valor especificado (Kbps). Cuando se aplica LLQ en redes *Frame Relay*, las colas son activadas por PVC. Cada PVC tiene una PQ y un número de colas exactas asignadas. La figura 3-10 indica cómo trabaja LLQ.

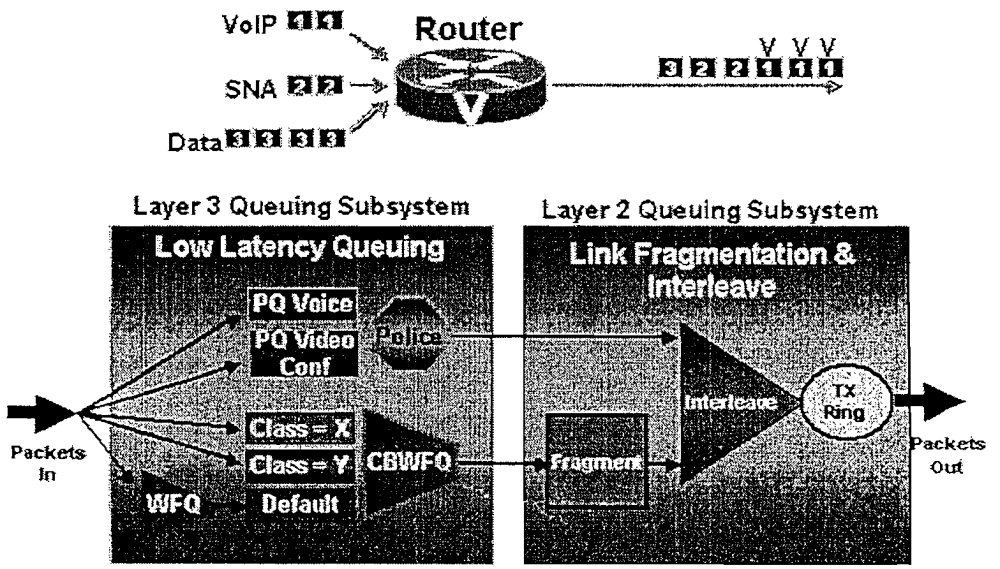


Figura 3-10 Comportamiento de LLQ [9]

Este método es más completo que *IP RTP Priority*. Para escoger entre los dos métodos se deberá analizar las características de tráfico de la red.

3.3.1.1.3 LLQ vs. IP RTP Priority

La tabla 3.11 indica las diferencias principales entre LLQ e *IP RTP Priority*, así como sus ventajas y desventajas.

Tabla 3.11 Comparación entre LLQ e *IP RTP Priority* [9]

LLQ	*IP RTP Priority*
Basado en: - Listas de Acceso, por ejemplo el rango de puertos UDP, direcciones de *host*, campos del paquete IP (ToS) como *IP Precedence* o DSCP - Rango de puertos IP RTP - Protocolos e interfaces de entrada - Criterios basados en CBWFQ Ventajas: - Más flexibilidad en el tráfico emparejado y direccionado a una cola con prioridad PQ y CBWFQ. - Se pueden configurar clases que garanticen el ancho de banda para otro tráfico tal como señalización de VoIP. Desventajas: - Configuración compleja	Basado en: - Puertos RTP/UDP (rango: 16384 – 32767) Ventajas: - Configuración sencilla Desventajas: - Para el tráfico cuando se utiliza RTCP (señalización VoIP) es manejado por la cola WFQ.

3.3.1.2 *Frame Relay Traffic Shaping* (FRTS)

FRTS provee parámetros que se utilizan para la administración de la congestión de una red. FRTS elimina los "cuellos de botella" en redes *Frame Relay* con conexiones

de alta velocidad para el sitio central y conexiones de menor velocidad para los sitios remotos. Se pueden limitar los valores de la velocidad para cada aplicación con la cual los datos son enviados al sitio central. Los valores con los que se puede manipular son: CIR (contratado al proveedor del servicio), Bc, Be, Tc (no puede exceder los 125 ms), y BECN, donde:

- **CIR** (*Committed Information Rate*, o tasa de información comprometida): Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino.
- **Bc** (*Committed Burst Size*, o ráfaga comprometida): Es la cantidad de bits transmitidos en un período Tc a la tasa CIR (**CIR=Bc/Tc**). En las redes *Frame Relay* se permite al usuario enviar picos de tráfico a la red por encima de CIR, durante intervalos de tiempo muy pequeños, incluidos en el periodo **Tc**.
- **Be** (*Excess Burst Size*, o ráfaga en exceso): Es la cantidad de bits transmitidos en el periodo Tc por encima de la tasa CIR. Si la red tiene la capacidad suficiente, admitirá la entrada de este tipo de tráfico en exceso, marcándolo con **DE** activo. El tráfico entrante en la red, por encima de **Bc + Be**, es descartado directamente en el nodo de entrada,

3.3.1.3 Fragmentación en redes *Frame Relay* (FRF.12)

Hay que tomar en cuenta que el tráfico de voz es muy sensible al retardo. Para tener una buena calidad de la voz, este retardo deberá ser menor a 150 ms (tabla 1.5).

Una parte importante del retardo se debe a la serialización en la interfaz. La serialización es el tiempo requerido en enviar un *frame* al medio físico. Si un enlace tiene una velocidad de **x** bps, el tiempo que tomaría en enviar 1 bit, sería 1/x segundos. Si el *frame* tiene **y** bits de longitud, el enviar este *frame* al medio tomaría **y/x** segundos y éste vendría a ser el retardo de serialización; por lo tanto:

Retardo de serialización = tamaño del frame (bits) / Velocidad del enlace (bps) [4]

La tabla 3.12 presenta algunos valores de este retardo de acuerdo a la velocidad del enlace y al tamaño del *frame*.

Por ejemplo, un paquete de datos de 1500 bytes toma 214 ms para transmitirlo desde un *router,* a un enlace de 56 kbps. Si este paquete de datos es enviado, el paquete de voz será encolado hasta que los 1500 bytes del paquete de datos sean transmitidos.

Este tiempo de retardo no es aceptable para el tráfico de voz. Si el paquete de datos es fragmentado en pequeños paquetes, se pueden intercalar los *frames* de voz con los fragmentos de datos. De esta manera los *frames* de datos y voz pueden ser llevados juntos en enlaces de baja velocidad sin causar retardos excesivos en el tráfico de voz.

Tabla 3.12 Tiempos de retardo de serialización de acuerdo a la velocidad del enlace y al tamaño del *frame* [11]

		Tamaño del *frame*					
	1 byte	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1500 bytes
56 Kbps	143 us	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	125 us	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 Kbps	62,5 us	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 Kbps	31 us	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 Kbps	15 us	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 Kbps	10 us	640 us	1,28 ms	2,56 ms	5,1 ms	10,2 ms	15 ms
1536 Kbps	5 us	320 us	640 us	1,28 ms	2,56 ms	5,12 ms	7,5 ms

Velocidad del enlace

Una parte importante del retardo se debe a la serialización en la interfaz, por lo que se recomienda que el retardo de serialización sea de 10 a 15 ms; de esta manera se asegura un mínimo de retardo y *jitter* para los paquetes de voz. El tamaño del fragmento se recomienda que sea de aproximadamente 80 bytes por cada 64 Kbps.

La tabla 3.13 indica el tamaño recomendado que deben tener los fragmentos de paquetes de datos, para asegurar un retardo adecuado de los paquetes de voz, dependiendo de la velocidad del enlace.

Tabla 3.13 Tamaños recomendados de fragmentación para diferentes velocidades [11]

Velocidad del enlace	Tiempos de retardo					
	10 ms	20 ms	30 ms	40 ms	50 ms	100 ms
56 Kbps	70 bytes	140 bytes	210 bytes	280 bytes	350 bytes	700 bytes
64 kbps	80 bytes	160 bytes	240 bytes	320 bytes	400 bytes	800 bytes
128 Kbps	160 bytes	320 bytes	480 bytes	640 bytes	800 bytes	1600 bytes
256 Kbps	320 bytes	640 bytes	960 bytes	1280 bytes	1600 bytes	3200 bytes
512 Kbps	640 bytes	1280 bytes	1920 bytes	2560 bytes	3200 bytes	6400 bytes
768 Kbps	1000 bytes	2000 bytes	3000 bytes	4000 bytes	5000 bytes	10000 bytes
1536 Kbps	2000 bytes	4000 bytes	6000 bytes	8000 bytes	10000 bytes	20000 bytes

Recomendación para voz (< 15 ms)

3.3.1.4 Optimización del Ancho de Banda (cRTP)

Basado en el RFC 2508, cRTP comprime el *header* del paquete IP/UDP/RTP de 40 bytes a 2 o 4 bytes, optimizando el ancho de banda.

cRTP no se requiere para asegurar una buena calidad de la voz, ésta es una característica que reduce el ancho de banda; si se utiliza cRTP se deberían también utilizar otras condiciones que aseguren la calidad de la voz.

3.3.1.5 Especificación del CODEC de acuerdo a la calidad de audio

Cada *codec* provee una cierta calidad del habla. Una característica que se usa para describir esta calidad es la *Mean Opinion Score* (MOS). MOS fue definido en la especificación ITU-T P.800. Ésta fue la primera técnica para medir la calidad de la voz. Fue deducida de una evaluación de varias preselecciones de muestras de voz sobre diferentes medios de transmisión. La calidad de voz fue calificada por un grupo de hombres y mujeres quienes asignaron una clasificación de acuerdo a la calidad.

La calificación fue dada en un rango del 1 al 5, siendo 5 una excelente calidad de audio, y va disminuyendo esta calificación hasta 1. La tabla 3.14 muestra una lista de *codecs* con su respectivo MOS.

Tabla 3.14 Calificación de diferentes *CODECS* [3]

Codec	Velocidad	MOS	Descripción
G.711u	64 Kbps	4.1	PCM ley u, versión usada en EEUU y Japón.
G.711a	64Kbps	4.1	PCM ley A, usada en Europa
G.723.1	6.3 Kbps	3.9	MP-MLQ[7] (*Multipulse Excitation – Maximum Likelihood Quantization*).
G.723.1	5.3 Kbps	3.65	ACELP (*Algebraic Code-Excited Linear Prediction*).
G.726	16/24/32/40 Kbps	3.85	*Adaptive Differential Pulse – Code Modulation* (AD-PCM)
G.729	8Kbps	3.92	CS-ACELP (*Conjugate Structure* ACELP)

3.3.1.6 Control de Admisión de llamadas (CAC)

Herramientas de QoS como las de encolamiento aseguran que los paquetes de voz tengan prioridad sobre los paquetes de datos. Si un enlace se encuentra con sobresuscripción debido a la cantidad de tráfico de voz, los paquetes de datos son descartados, y el resto de las llamadas de voz tendrían problemas.

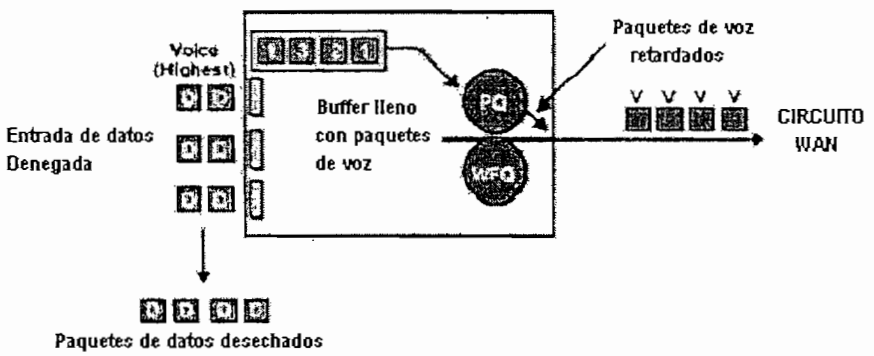


Figura 3-11 Efecto de la sobresuscripción [5]

La figura 3-11 ilustra un ejemplo de sobresuscripción. En esta figura se muestra que PQ (*Priority Queue*) está permitiendo enviar los paquetes de voz, mientras que los paquetes de datos, destinados para WFQ, son denegados y desechados. En este

[7] Esquema de compresión que es cuantizado generando un primer flujo de pulsos que contiene varios pulsos así como una pluralidad de valores en cero.

caso el *buffer PQ* se encuentra lleno, y los paquetes de voz están compitiendo con otros paquetes de voz para acceder al enlace. Esto da como resultado una degradación en las llamadas de voz.

Por lo tanto se necesita configurar un sistema de Control de Admisión de Llamadas (CAC) para asegurar que los recursos no caigan en sobresuscripción. CAC puede ser descrito como una manera de proteger la voz de la voz.

Las llamadas que exceden el ancho de banda estipulado, pueden ser re-enrutadas a una ruta alternativa como la PSTN, o simplemente ser rechazadas. De esta manera las llamadas de voz activas no se degradarán.

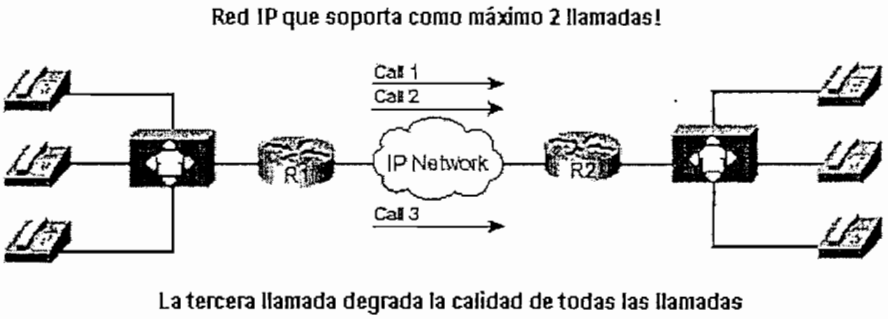


Figura 3-12 Sistema de Control de Admisión de Llamadas (CAC) [5]

En la figura 3-12 se ilustra la necesidad de CAC. Este ejemplo indica que únicamente pueden concretarse como máximo dos llamadas de voz; si se realiza una tercera llamada, ésta será re-enrutada, o dará tono de ocupado. Así, la tercera llamada no impactará en la calidad de las dos llamadas existentes.

Los mecanismos de Control de Admisión de llamadas extienden la capacidad de otros métodos de QoS que aseguran que el tráfico de voz que circula por los enlaces de la red no sufran latencia, *jitter*, o que los paquetes se pierdan.

CAC consigue esta tarea determinando si los recursos de la red están disponibles para proveer una apropiada QoS en una nueva llamada, antes que ésta sea admitida. Simplemente se implementa CAC para proteger las conversaciones de voz de otras conversaciones.

3.3.2 SELECCIÓN DE LOS DISPOSITIVOS DE *NETWORKING* PARA LA WAN

Para poder seleccionar los equipos que se van a utilizar en la red WAN, donde van a estar "corriendo" las aplicaciones de la LAN y VoIP, éstos deberán tener la capacidad de ser configurados, y principalmente tener herramientas de QoS; estos requerimientos son importantes para que la VoIP no tenga problemas en mezclarse con los datos y que la red funcione normalmente, sin que su desempeño disminuya.

En el mercado existe una gran variedad de productos que ofrecen soluciones de telefonía IP, pero lo que interesa es poder aplicar Calidad de Servicio, debido a que los paquetes de VoIP no van a estar viajando solos por la red, ya que estarán acompañados de paquetes de datos de diferentes aplicaciones.

En el país existen dos marcas que encabezan el mercado de productos de *Networking*, ellas son CISCO y 3COM.

3COM

Dentro de la línea 3COM, en los últimos años se han desarrollado equipos que permiten dar soluciones para aplicaciones VoIP; con la presentación de su nueva plataforma en productos de telefonía sobre protocolo de Internet, denominada NBX V3000 IP

3COM anuncia la quinta generación de telefonía VoIP. El producto, dedicado a pequeños negocios con posibilidad de escalar hasta 1.500 extensiones, viene preconfigurado con licenciamiento o servicio para 250 dispositivos que cubren todos los servicios básicos de telefonía.

3COM se enfoca más a la telefonía IP, por medio de su central, la misma que tiene características de QoS que permite a los paquetes tener prioridad, evitar la congestión, los paquetes perdidos, y el *jitter*.

CISCO

Marca líder a nivel mundial dentro del mercado de equipos de *networking,* que ofrece una amplia gama de productos para soluciones de VoIP. Esta marca permite que sus *routers* funcionen también como *gateways* de voz, esto como parte de toda la solución de comunicaciones IP.

Los *routers* que ofrecen este servicio son los que se encuentran dentro de las series 2600, 2800, 3700 y 3800. Estos equipos pueden comunicarse directamente con un administrador de llamadas (*Cisco CallManager*), y permiten desarrollar de mejor manera las soluciones de telefonía IP que son ideales para grandes y pequeñas empresas.

Estos equipos poseen interfaces de voz y protocolos de señalización, que proporcionan conectividad con más del 90 % de PBXs a nivel mundial, y principalmente con la PSTN.

La señalización e interfaces que soportan estos equipos son: T1/E1, [8]PRI (*Primary Rate Interface*), [9]CAS (*T1 Channel Associated Signaling*), E1-R2, protocolo [10]QSIG T1/E1, [11]BRI (*Basic Rate Interface*), FXO (*Foreign Exchange Office*), E&M, y FXS (*Foreign Exchange Station*). Además pueden ser configurados para soportar de 2 a 540 canales de voz.

---

[8] Consiste en un solo canal primario de 64 Kbps (canal D) más 23 (T1) o 30 (E1) canales B para voz o datos.

[9] Canal asociado para señalización, se transmite la información de la señalización para un canal de voz.

[10] Estándar de señalización. Protocolo de señalización de canal común basado en el estándar ISDN Q.931 usabo generalmente para PBXs digitales.

[11] Interfaz ISDN compuesta de dos canales B y un canal D.

Dentro de lo que es el *CISCO IOS Telephony Service* (software para el manejo de telefonía IP), CISCO ofrece una extensa variedad de opciones de Calidad de Servicio, configurables de acuerdo a la necesidad, tecnología y topología de la red.

Dentro del mercado internacional, existe una marca que ofrece similares características a las de CISCO, esta marca se llama, **Juniper**.

Juniper Network, con sus equipos *Routers* de las series T, M y E, posee un gran desempeño en redes convergentes que utilicen aplicaciones de tiempo real como es el caso de VoIP.

Los *routers* Juniper Network son ideales para proveer convergencia entre paquetes de voz y de datos. Dentro de las redes de VoIP, Juniper ofrece:

- Alta velocidad en sus interfaces
- Clase de Servicio
- Baja latencia
- Mínimo *jitter*
- Balanceo de carga
- MPLS[12]
- Seguridad
- Mecanismos confiables

De estos tres fabricantes, el que más se acerca a los requerimientos del presente diseño es la marca **CISCO**, debido a que tiene la mayor capacidad para realizar QoS y la posibilidad de configurar sus equipos de acuerdo a las necesidades que se presenten en la red. Además es una marca registrada en el país y fácilmente se la puede conseguir.

---

[12] Método de conmutación que conmuta los paquetes usando una etiqueta. Esta etiqueta indica a los *routers* o *switchs* de la red dónde se deben enviar los paquetes basados en la información de enrutamiento IP preestablecida.

Cisco entre otras características ofrece soporte para operación; en el país ya existen academias registradas para el aprendizaje del manejo de estos equipos y numerosas empresas (*Resellers*) que ofrecen servicio de mantenimiento y repuestos. Inclusive se puede realizar un contrato de mantenimiento llamado *SmartNet*, que ofrece garantía, servicio técnico, ya sea personalizado por técnicos CISCO o por llamadas telefónicas.

3.3.3 CONFIGURACIÓN DE LOS EQUIPOS PARA EL DESARROLLO DE QoS PARA VoIP [9]

Una vez seleccionada la marca (CISCO), se establecerán los requerimientos, modelos y características de estos equipos que se emplearán en la solución para la implementación de este diseño. Se analizarán las características que tiene el IOS de los equipos para el desarrollo de Calidad de Servicio según los lineamientos dados en el punto 3.3.1 de este capítulo.

3.3.3.1 Configuración de CBWFQ

Antes de configurar CBWFQ, se debe determinar cuántas clases se necesitan para categorizar el tráfico. Para esto probablemente se usen ACLs para categorizar el tráfico que ingresa dentro de las clases. Hay 3 pasos principales para configurar CBWFQ:

- Definir las clases
- Crear la política
- Añadir la política a una interfaz

Crear la clase es determinar el tipo de tráfico que va a cada clase, y que puede ser utilizado por una o más políticas. Las políticas determinan la manera que el tráfico es manipulado. La QoS no es válida hasta que la política sea aplicada a la interfaz.

3.3.3.1.1 Definición de la Clase

Se lo hace por medio del uso de comando **class-map** que permite determinar cómo el tráfico debería ser clasificado.

La clase configurada debe tener un nombre al que después se lo referirá. Por ejemplo [9]:

```
!---En el modo de configuración global se crea la clase.

RouterVoIP(config)#class-map ?
       WORD            class-map name
       match-all       Logical-AND all matching statements under this classmap
       match-any       Logical-OR all matching statements under this classmap

!---Se escoge un nombre descriptivo a la clase.

RouterVoIP(config)#class-map trafico-voz
RouterVoIP(config-cmap)#match ?
       access-group          Access group
       any                   Any packets
       class-map             Class map
       cos IEEE 802.1Q/ISL   class of service/user priority values
       destination-address   Destination address
       input-interface       Select an input interface to match
       ip                    IP specific values
       mpls                  Multi Protocol Label Switching specific values
       not                   Negate this match result
       protocol              Protocol
       qos-group             Qos-group
       source-address        Source address

!--- Se usa access-group para establecer un grupo de acceso, y poder usar
!--- una lista de control de acceso(ACL) para poder asignar la política.

RouterVoIP(config-cmap)#match access-group ?
       <1-2699>       Access list index
       name           Named Access List

!--- Se asigna un número de la ACL.

RouterVoIP(config-cmap)#match access-group 102

!--- Se crea una lista de Acceso y se la asigna a class-map access-group, por
!--- medio del número (102)

RouterVoIP(config)#access-list 102 permit udp any any range 16384 32767

!---la manera más segura y más fácil es dando el rango de puertos UDP 16384-32767.
!---Este es el rango de puertos que el IOS de CISCO utiliza para transmitir los
!---paquetes VoIP.
```

Opcionalmente se puede crear una clase para la señalización de VoIP. Para esto se utilizan los siguientes comandos para completar esta tarea:

```
class-map signaling-voz
match access-group 103
!
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
```

Nota: Las llamadas pueden ser establecidas usando H.323, SIP o MGCP. Para la configuración y solución del diseño y para la facilitar la configuración se va a utilizar H.323, ya que no se requiere ni de agentes ni de servidores para la señalización como sería en SIP o MGCP. Este tipo de señalización lo realizan los routers.

La siguiente lista ayuda como referencia para saber cuáles son los puertos usados para la señalización VoIP y para el control de los canales:

- H.323/H.225 = TCP 1720
- H.323/H.245 = TCP 11xxx (*Standard Connect*)
- H.323/H.245 = TCP 1720 (*Fast Connect*)
- H.323/H.225 RAS = TCP 1719
- MGCP = UDP 2427, TCP 2428 (*CM Encore*)
- SIP = UDP 5060, TCP 5060 (configurable)

3.3.3.1.2 Creación de la política para asociar a la clase de VoIP

Una vez definida la clase, se debe crear una política que especifique la QoS. Para el presente proyecto el propósito de la política es definir cuántos recursos del enlace se deberán compartir o asociar a las diferentes clases.

Se usan los siguientes comandos para completar esta tarea [9] [5]:

```
!--- En el modo de conFiguración global se define la política con un nombre
!--- descriptivo.

RouterVoIP(config)#policy-map POLITICA-VOZ

!--- Se asigna la política a la clase ya creada.
```

```
RouterVoIP(config-pmap)#class trafico-voz

!--- Se da una prioridad de acuerdo a la capacidad de canal que se reserve para
!--- el tráfico de voz (Kbps).

RouterVoIP(config-pmap-c)#priority ?
      <8-2000000> Kilo Bits per second

!--- Por ejemplo para una llamada, con G.711 reservamos 85.6 Kbps (sin cRTP) para
!--- la cola que va a estar recibiendo los paquetes de voz y la cual será
!--- prioritaria (PQ).

RouterVoIP(config-pmap-c)#priority 86

!--- Se realiza el mismo proceso asignando 8 Kbps para la señalización de la voz.

RouterVoIP(config-pmap)#class voice-signaling
RouterVoIP(config-pmap-c)#bandwidth 8

!--- El tráfico de datos restantes se lo puede tratar con WFQ.

RouterVoIP(config-pmap)#class class-default
RouterVoIP(config-pmap-c)#fair-queue
```

3.3.3.1.3 Aplicación de la política a las interfaces

Como paso final se debe añadir la política a la interfaz y así habilitar LLQ [9]:

```
RouterVoIP(config)#interface serial 0/0

!--- Se aplica la política definida para el tráfico saliente de la interfaz, en
!--- la interfaz de la WAN.

RouterVoIP(config-if)#service-policy output POLITICA-VOZ
```

3.3.3.2 Configuración de WFQ (*IP RTP Priority*)

Para configurar RTP en una interfaz se usa el comando **`ip rtp priority`**. Este comando especifica un número de puerto de inicio, el rango, y la capacidad de canal para la cola.

En el caso de voz, se emplean los siguientes comandos [9]:

```
!--- En la conFiguración global se declara una clase para el tráfico en la red
!--- Frame Relay con un nombre descriptivo.

Router(config)#map-class frame-relay VoIPovFR
```

```
!--- luego se asigna prioridad a los paquetes de voz.

Router(config-map-class)#frame-relay ip rtp priority [starting-rtp-port]
[port-range] [bandwidth]
```

donde:

starting-rtp-port: Es el menor número del puerto UDP en la cual los paquetes son enviados. Para VoIP este valor es **16384**.

port-range: Es el rango de puertos UDP destino. Para VoIP se coloca en 16383 porque el puerto más alto para el tráfico de VoIP es 32767. (32767 – 16384 = **16383**).

bandwidth: Es la mínima capacidad permitida en kbps para la cola de prioridad PQ. Este valor se fijará en base al número de llamadas simultáneas que se requiera, y que el sistema soporte.

3.3.3.3 *Traffic shaping* para la voz [5]

Para configurar *traffic shaping* se debe conocer los parámetros de la red *Frame Relay* como por ejemplo el CIR, Bc, Be, y Tc (todos los parámetros se los configura en bps).

Tc no es configurado, este valor es calculado internamente. El parámetro configurable es el Bc (Tc=Bc/CIR). Para el tráfico de voz se recomienda que Tc sea de 10 ms debido al retardo de serialización.

Otro comando que se aplica a esta configuración es el ***mincir*** que es la velocidad mínima de transmisión que deberá tener el canal durante un período de congestión.

```
!--- Se declara la clase de la misma forma como en el punto 3.3.3.2

Router(config)#map-class frame-relay VOIPovFR
Router(config-map-class)#frame-relay cir a
Router(config-map-class)#frame-relay bc b
```

```
!--- donde a es el valor de ancho de banda asignado únicamente para el tráfico de
!--- voz (CIR).
!--- Tc = BC/CIR. En este caso Tc es forzado al mínimo valor conFigurable de 10ms
!--- El Be tiene que ser igual a 0 por defecto.
Router(config-map-class)#frame-relay be 0
Router(config-map-class)#frame-relay mincir a
!--- El minCIR le igualamos al CIR como seguridad ya que se trata de voz.
```

3.3.3.4 Fragmentación (FRF.12)

La fragmentación se habilita generalmente cuando los enlaces son menores a 768 kbps. En la tabla 3.13 se observaron los tamaños de paquetes para la fragmentación de acuerdo a la velocidad del enlace, para asegurar los 10 ms de retardo.

Para realizar la fragmentación, se emplean los siguientes comandos [5]:

```
!--- Se declara la clase de la misma forma como en el punto 3.3.3.2
Router(config)#map-class frame-relay VOIPovFR

!--- Por ejemplo para un enlace de 64 Kbps, se deben fragmentar los paquetes en
!--- tamaños de 80 bytes.

Router(config-map-class)#frame-relay fragment 80
```

3.3.3.5 Configuración de cRTP

Antes de configurar la compresión de la cabecera de RTP, se debe tener configurado el encapsulamiento en la línea serial, en este caso *Frame Relay*. Los comandos para configurar cRTP en *Frame Relay* se habilitan en la interfaz, y éstos son [5]:

```
!--- Se Habilita traffic shaping y luego cRTP.
Router(config)#interface serial 0/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#no fair-queue
Router(config-if)#frame-relay traffic-shaping
Router(config-if)#frame-relay ip rtp header-compression
```

3.3.3.6 Configuración de CAC

Para poder realizar un correcto control de admisión de llamadas, se deben determinar cuántas llamadas simultáneas se pueden tener en la red; esto va ligado al

ancho de banda que ocupa cada llamada. Este cálculo se lo revisará en el dimensionamiento de la red.

El control del número de llamadas simultáneas se lo hace por medio del comando **max-conn a**, donde **a** es el número de llamadas simultáneas. Este comando se lo coloca en la interfaz física por lo que controlará la salida y llegada de llamadas a esa interfaz.

Dentro del IOS de CISCO, existen otras maneras de controlar el número de conexiones simultáneas, pero se ha escogido ésta por facilidad y debido a que únicamente por una interfaz física se conectará la PBX al *router.*

3.4 DIMENSIONAMIENTO DE LA RED

En el dimensionamiento se determinará la carga total que va a estar circulando por los enlaces WAN desde los sitios remotos a la oficina principal, según como se había señalado en la caracterización de la LAN. Como se vió en la tabla 3.7, la mayor parte del tráfico tiene un tamaño de paquetes de 64 bytes y 1518 bytes.

Para el presente cálculo se asume que la red Ethernet está ocupada con un promedio de utilización del 40% [13] por las retransmisiones que ocurran cuando exista colisiones y por el overhead de la trama; en otras palabras 4 Mbps de capacidad de Ethernet se utiliza.

El promedio de utilización del tráfico del 40 % de Ethernet es cuando la red está siendo altamente empleada, desde que las colisiones son muy probables y una gran parte del tráfico de la red es retransmitido. Sin embargo se debe realizar el diseño para el peor de los casos.

Se considerará el tráfico en la Ethernet de acuerdo a la tabla 3.7; esto es:

- paquetes de 1518 bytes, 26 %
- paquetes de ~1270 bytes, 9 %
- paquetes de ~768 bytes, 7 %
- paquetes de ~384 bytes, 8 %
- paquetes de ~192 bytes, 10 %
- paquetes de ~96 bytes, 40 %

Para calcular el total de paquetes por segundo que deberían estar en la Ethernet, se necesita aplicar la siguiente fórmula para cada uno de los diferentes tamaños de paquetes [13]:

Paquetes por Segundo = (Capacidad de ocupación de la red x Porcentaje de utilización) / (Tamaño del paquete x 8 bits/byte)

Usando esta fórmula se tiene:

- (4 Mbps x 26%)/(1518 bytes x 8 bits/byte) = 86 pps
- (4 Mbps x 9%)/(1270 bytes x 8 bits/byte) = 35 pps
- (4 Mbps x 7%)/(768 bytes x 8 bits/byte) = 46 pps
- (4 Mbps x 8%)/(384 bytes x 8 bits/byte) = 104 pps
- (4 Mbps x 10%)/(192 bytes x 8 bits/byte) = 260 pps
- (4 Mbps x 40%)/(96 bytes x 8 bits/byte) = 2083 pps

En total se tienen 2614 pps. Es importante saber la cantidad de paquetes por segundo que van a estar procesándose, para poder escoger a un equipo que soporte una conmutación de la cantidad mínima de pps que se requiera.

Se debe conocer también cuánta capacidad consume una llamada; por ejemplo una aplicación de *Voice Over IP* con un *codec* G729 (8 kbps) usa 50 PPS. VoIP con *codec* G711 (64 kbps) usa aproximadamente 100 PPS.

Para dar soluciones de VoIP dentro de la marca CISCO existen dos modelos: Cisco 1751-V y Cisco 2600, los cuales han sido los más comunes durante los últimos años, las características de ellos se las puede analizar en la tabla 3.15.

De estos dos equipos, la CISCO SYSTEM ha descontinuado a los 1751-V, los *routers* 2600 todavía se encuentran en el mercado.

Tabla 3.15 Diferencias entre el *router* Cisco 1751-V y los *routers* de la serie Cisco 2600 [17]

Características	Cisco 1751-V	Cisco 2600
Desempeño (conmutación con paquetes de 64-bytes)	12,000 pps	12,000 a 37,000 pps
IPSec *DES-encrypted* paquetes de 256-bytes	512 Kbps	512 Kbps
Fuente de poder redundante	No	Si
Tarjetas de voz (*Voice Interface Cards*)	Dos puertos E&M, FXO, FXS, DID y ISDN BRI NT/TE, T1/E1 *Multiflex* VWICs	Dos puertos E&M, FXO, FXS, ISDN BRI-N/T-TE y BRI-ST/TE, digital T1/E-1 *packet voice trunk network module*, T1/E-1 *multiflex* WAN/*voice interface card* (*multiflex* WAN/*voice interface card*)
Máximo número de interfaces	Analógico: 4 puertos con 1 *slot* WAN (dual T1/E1 WIC) o 6 puertos sin *WAN access Digital*: 24 llamadas con T1 o E1, o 12 puertos sin acceso WAN	De 2 a 60 llamadas de voz
Tarjetas WAN	4 serial, 2 BRI, 4 A/S	10 BRI, 12 A/S, 36 A, 2 PRI, 1 ATM

En los últimos años, Cisco Systems ha desarrollado una nueva línea de *routers* llamados ISRs (*Integrated Services Routers*) que se han perfeccionado en seguridad,

así como en la rapidez de conmutación y procesamiento para soportar de mejor manera aplicaciones de datos, voz, vídeo y servicios *wireless*.

Estos equipos poseen características adicionales comparadas con las anteriores generaciones de *routers* CISCO a precios similares, pero quintuplicando su desempeño, y hasta mejorar su funcionamiento diez veces más con respecto a seguridad y aplicaciones de voz.

De esta línea, los *routers* de la serie 2800 tienen 4 plataformas (figura 3-13 de arriba hasta abajo): 2801, 2811, 2821 y 2851.

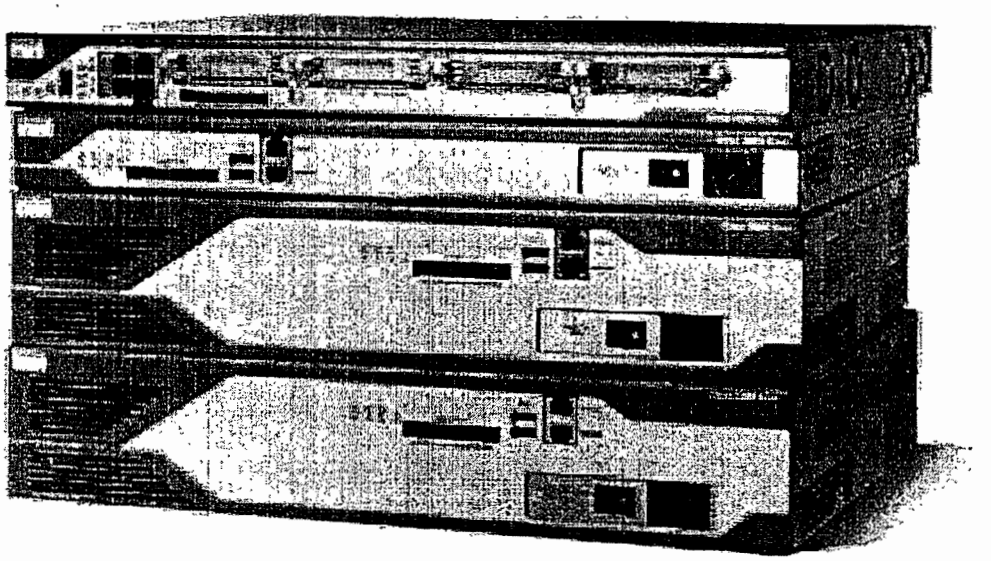


Figura 3-13 *Router* ISRs 2800 [17]

Estos equipos son totalmente compatibles con más de 90 módulos existentes que todavía se utilizan para los *routers* de las series 1700, 2600 y 3700.

Tienen integrados módulos de encripción y DSPs (*Digital Signal Processors* para VoIP), como también acelerador para VPN (*Virtual Private Networks*), entre otras características que se las puede analizar en la tabla 3.16.

Tabla 3.16. Especificaciones de los *Routers CISCO ISRs* 2800 [17]

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Arquitectura del producto				
DRAM	Defecto: 128 MB Máximo: 384 MB	Defecto: 256 MB Máximo: 760 MB	Defecto: 256 MB Máximo: 1 GB	
Compact Flash	Defecto: 64 MB Máximo: 128MB	Defecto: 64 MB Máximo: 256 MB		
Puertos USB 1.1	1	2		
Puertos LAN internos	2-10/100		2-10/100/1000	
Slot AIM (interno)	2			
Slots para interfaces	4 *slots*; 2 *slots* soportan HWIC, WIC, VIC, o módulos tipo VWIC. 1 *slot*:: soporta WIC, VIC, o módulos tipo VWIC. 1 *slot*: soporta VIC o módulos tipo VWIC.	4 *slots*: cada *slot* soporta HWIC, WIC, VIC, o módulos tipo VWIC		
Lugar para módulos de red	No	1 *slot*: soporta NM y módulos tipo NME	1 *slot*: soporta NM, NME módulos tipo NME-X	1 *slot*: soporta NM, NME, NME-X, NMD y módulos tipo NME-XD
Slot para módulo de extensión de voz	0		1	
Slots PVDM (DSP) (internos)	2		3	
Encripción integrada basada en hardware	Si			
Acelerador de VPN en hardware (interno)	DES, 3DES, AES 128, AES 192, y AES 256			
Integrated in-line power (PoE) (Opcional)	Si, requiere fuente de poder AC			
Puerto de consola (115.2 kbps)	1			
Puerto auxiliar (115.2 kbps)	1			
Mínimo Cisco IOS	12.3(8)T			

3.4.1 CÁLCULO DE LA CAPACIDAD PARA DATOS DE CADA ENLACE

En promedio una Base de Datos por usuario ocupa aproximadamente una capacidad de canal de **24 Kbps** [21]. Esta capacidad es utilizada por los usuarios que se encuentren accediendo a la Base de Datos de manera remota. Para el cálculo de cada enlace, únicamente se toma en cuenta a los usuarios que acceden a la Base de Datos (Departamento de Ventas) de cada oficina sucursal.

La tabla 3.17 muestra la capacidad de cada enlace consumida por el acceso a la Base de Datos ubicada en Quito.

Tabla 3.17 Capacidad para el acceso a la Base de Datos de cada oficina sucursal

Enlaces	No. usuarios	Capacidad/usuario	Capacidad Total (No. usuarios x Capacidad c/u)
Quito - Cuenca	3	24 Kbps	72 Kbps
Quito - Guayaquil	3	24 Kbps	72 Kbps

A esto se le debe sumar la capacidad que consumen los servicios de Internet y correo electrónico, que aproximadamente es de **8 Kbps** [21] por usuario. La tabla 3.18 muestra la capacidad de cada enlace consumida por el acceso a Internet y correo electrónico.

Tabla 3.18 Capacidad para el acceso a Internet y correo electrónico

Enlaces	No. usuarios	Capacidad/usuario	Capacidad Total (No. usuarios x Capacidad c/u)
Quito - Cuenca	5	8 Kbps	40 Kbps
Quito - Guayaquil	5	8 Kbps	40 Kbps

Por lo tanto la capacidad total requerida resulta de la integración de todas sus aplicaciones tal como indica la tabla 3.19. En el diseño no se presenta una proyección en cuanto a la capacidad del canal a contratar debido a que cuando se requiera un mayor número de usuarios u otra aplicación se necesite correr,

básicamente se debe incrementar el ancho de banda solicitando tal incremento al proveedor del servicio.

Tabla 3.19 Capacidad total requerida por las aplicaciones de datos

Enlaces	Base de Datos (Tabla 3.17)	HTTP, e-mail (Tabla 3.18)	Capacidad Total (Capac. DDBB + Capac. HTTP, email)
Quito - Cuenca	72 Kbps	40 Kbps	**112 Kbps**
Quito - Guayaquil	72 Kbps	40 Kbps	**112 Kbps**

Esto cálculo es dado para el caso de que todos los usuarios se encuentren usando todas las aplicaciones al mismo tiempo. Hay que considerar que los usuarios de Quito no ocupan los enlaces WAN, debido a que ellos acceden a la Base de Datos y al Internet por medio de su red local.

3.4.2 CÁLCULO DE LA CAPACIDAD PARA LLAMADAS DE VoIP

La capacidad de canal requerida para las llamadas de voz depende del codificador y del protocolo de capa 2 que se van a utilizar en la red.

En la figura 2-2 se mostró el formato del paquete de VoIP que está formado por los *headers* IP, UDP, y RTP, y su respectivo *payload* que depende del tipo de codificador. Otro factor importante es saber si se va a utilizar compresión en estos *headers* (cRTP), como se indicó en la figura 2-3.

En este cálculo intervienen los siguientes parámetros:

- ***Codec Bit Rate* (Kbps):** Depende del tipo de *codec*. Es el número de bits por segundo que necesitan ser transmitidos para consignar una llamada de voz.

codec bit rate = tamaño de la muestra del codec / tiempo de muestreo [10]

- **Tamaño de la muestra del *codec* (Bytes):** Es el número de bytes capturados por el procesador digital de señales (DSP) en cada tiempo de muestreo. Por ejemplo el *codec* G.729 opera en muestreos de 10 ms, correspondientes a 10 bytes (80 bits).

- **Longitud del *payload* de voz (en Bytes):** Este tamaño representa el número de bytes que son encapsulados en un paquete. El tamaño del *payload* de voz es proporcional al tamaño de cada muestra que el *codec* realiza. Por ejemplo, los paquetes en G.729 usan 10, 20, 30, 40, 50, o 60 bytes de longitud (*payload*).

- **Duración del *payload* de voz (en ms):** Es representado en términos de cada muestra. Por ejemplo, la duración del *payload* de voz en G.729 es de 20 ms (dos muestreos de 10 ms), en 20 bytes. [*(20 bytes * 8)/(20 ms) = 8 Kbps*]

- **Paquetes por Segundo (pps):** Representa el número de paquetes que necesitan ser transmitidos en un segundo. Por ejemplo, para una llamada en G.729 con un *payload* de 20 bytes por paquete (160 bits), se necesitan 50 paquetes para ser transmitidos en cada segundo. [*50 pps = (8 Kbps)/(160 bits por paquete)*]

Por lo que la fórmula utilizada para calcular la capacidad requerida para cada llamada es [10]:

Capacidad por llamada = Tamaño total del paquete / # pps

Tamaño total del paquete = *(header de capa 2: Frame Relay o Ethernet) + (header IP/UDP/RTP) + (payload de voz)*
 # pps = *(codec bit rate) / (tamaño del payload de voz)*

Para escoger un correcto *codec*, se debe balancear la calidad de voz contra el costo de capacidad de canal que involucra ese *codec*. Un parámetro que ayuda a escoger

correctamente el *codec* es el MOS (tabla 3.14). Por lo tanto, para la red que se está diseñando se escoge:

- *Codec* G.729 (8 kbps de *codec* bit rate).
- Compresión de *headers* (cRTP),
- *Payload* de 20 bytes para el paquete de voz
- *Frame Relay* (*L2 header*)

Tamaño total del paquete (*bytes*) = (**6** *bytes del header L2 de Frame Relay*) + (**2** *bytes del header comprimido para IP/UDP/RTP*) + (**20** *bytes de payload de voz*) = **28 bytes**

Tamaño total del paquete (*bits*) = (**28** *bytes*) * (**8** *bits por byte*) = **224 bits**

 # PPS = (**8** *Kbps del codec bit rate G.729*) / (160 *bits*) = **50 pps**

Lo que resulta:

Capacidad por llamada = Tamaño total del paquete (224 bits) * 50 pps = 11.2 Kbps

En la tabla 3.20 se muestra las capacidades por llamada para diferentes tipos de *codecs*.

Tabla 3.20 Capacidades de canal por llamada para diferentes tipos de *codecs* [3]

Codec	Tamaño del *payload* por paquete	Tamaño del *header* IP/UDP/RTP	Tipo tecnología de capa 2	Tamaño del *header* de capa 2	Paquetes por segundo	Capacidad por llamada
G.711	160 bytes	40 bytes	Ethernet	14 bytes	50 pps	85,6 Kbps
G.711	240 bytes	40 bytes	Ethernet	14 bytes	33 pps	77,6 Kbps
G.711	160 bytes	40 bytes	*Frame Relay*	6 bytes	50 pps	82,4 Kbps
G.711	160 bytes	2 bytes (cRTP)	*Frame Relay*	6 bytes	50 pps	67,2 Kbps
G.729	20 bytes	40 bytes	Ethernet	14 bytes	50 pps	29,6 Kbps
G.729	20 bytes	40 bytes	*Frame Relay*	6 bytes	50 pps	26,4 Kbps
G.729	30 bytes	40 bytes	*Frame Relay*	6 bytes	33 pps	20 Kbps
G.729	20 bytes	2 bytes (cRTP)	*Frame Relay*	6 bytes	50 pps	11,2 Kbps

Dentro de la red, se necesita tener como máximo 2 llamadas simultáneas entre las oficinas remotas y la oficina principal, es decir que la oficina principal podría realizar 4 llamadas simultaneas, 2 para cada enlace. Ésto para corresponder a las

condiciones iniciales del ejemplo que se indicó (4 líneas telefónicas públicas en la oficina principal, y 2 líneas telefónicas públicas en cada oficina remota), éstas pueden ser para Gerencia y el Departamento Técnico.

Si se utiliza el *codec* G.729, con 2 llamadas simultáneas, se tiene que asegurar un mínimo de 11.2 Kbps x 2 = **22.4 Kbps** para las llamadas de VoIP de los enlaces Quito – Cuenca y Quito – Guayaquil.

3.4.3 CÁLCULO DE LA CAPACIDAD TOTAL PARA CADA ENLACE

La capacidad total para cada enlace no es más que la suma de la capacidad para VoIP y para datos.

Tabla 3.21 Capacidad total para cada enlace por la convergencia de datos y voz

Enlaces	Datos	VoIP	Capacidad Total (Capac. Datos + Capac. VoIP)
Quito - Cuenca	112 Kbps	22.4 Kbps	**134.4 Kbps**
Quito - Guayaquil	112 Kbps	22.4 Kbps	**134.4 Kbps**

Como se puede ver en la tabla 3.21, se ha obtenido la capacidad total que cada enlace necesita en caso de que todas las aplicaciones, y todos los usuarios estuviesen ocupando la red al mismo tiempo.

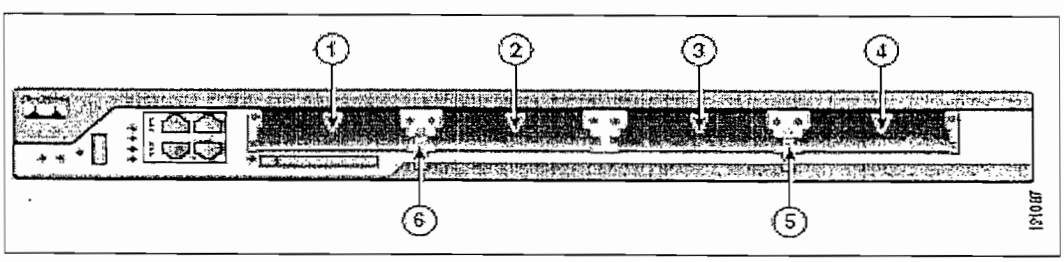
Los proveedores del servicio generalmente ofrecen la renta de PVCs con capacidad de canal en múltiplos de 64 Kbps. Esto da a elección a la empresa de contratar 128 Kbps o 192 Kbps para cada uno de los enlaces. Al contratar el valor inferior (128 Kbps) de la capacidad total (134.4 Kbps) se puede analizar que existe un excedente de aproximadamente 7 Kbps. Como se trata de una red *Frame Relay*, y al ver que este excedente es mínimo; y que el uso de las aplicaciones es esporádico, es decir los usuarios no están constantemente en consulta a la base de datos ni al Internet, sino lo hacen cuando lo requieran, y generalmente esto no ocurre al mismo tiempo, por lo tanto se puede cubrir este excedente con el Be (*Excess Burst Size*), que es la

máxima cantidad de datos que la red intentará transportar, sin ninguna garantía, durante el Tc. Por lo tanto se recomienda contratar un PVC con CIR de **128 Kbps** para cada uno de los enlaces.

3.4.4 DIMENSIONAMIENTO DE LOS EQUIPOS PARA LA RED WAN

De todos los equipos que ofrecen convergencia de datos y VoIP, los *routers* Cisco de la serie 2800 son los que más se acercan a los requerimientos para el presente diseño (tabla 3.16). Con respecto a costos, estos equipos son comparables con los de la serie 2600, pero como ya se había analizado, éstos ofrecen muchas más ventajas en desempeño y tecnología para la implementación de VoIP, y además son totalmente compatibles con las tarjetas y módulos de las anteriores generaciones.

Para el diseño se requieren equipos que tengan interfaces, ya sean internas o que brinden la posibilidad de poder expandirse con módulos o tarjetas. En cada uno de los equipos se requiere que posean interfaces para conexión con la LAN, WAN, y una interfaz de voz para conexión con la PBX. Como se puede analizar en la tabla 3.16, todos los equipos de la serie 2800 ofrecen estas características dentro de su arquitectura. Para el presente diseño se utilizará para todas las oficinas *routers* 2801 (figura 3-14), que además es el más económico de entre los 4 modelos de esta serie.



1	Ranura 3 WIC/VIC/VWIC/HWIC	2	Ranura 2 WIC/VIC/VWIC
3	Ranura 1 WIC/VIC/VWIC/HWIC	4	Ranura 0 VIC/VWIC (Solo voz)
5	Divisor de ranuras	6	Divisor de ranuras

Figura 3-14 Arquitectura física del *router* 2801 [17]

Este equipo posee 2 interfaces FastEthernet que serán utilizadas para la conexión con la red LAN. Se ocupará la ranura 1 para insertar una tarjeta WAN, y la ranura 0 para una tarjeta E&M (conexión con la PBX).

En la ranura 1 se instalará una tarjeta Cisco WIC-1T, que posee un puerto de comunicación serial sincrónica (DB-60) que soporta velocidades de hasta 2.048 Mbps.

Esta tarjeta tiene un LED etiquetado con CONN (Figura 3-15), que se ilumina cuando el puerto serial está conectado. Cuando el puerto se encuentra en modo DTE, este LED indica que las señales DSR (*Data Set Ready*), DCD (*Data Carrier Detect*), y CTS (*Clear To Send*), fueron detectadas. Cuando el puerto se encuentra en modo DCE, el LED indica que las señales DTR (*Data Terminal Ready*), y RTS (*Request To Send*), fueron detectadas.

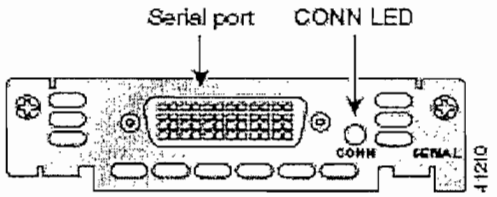


Figura 3-15 Tarjeta serial WIC-1T (*WAN Interface Card*) [17]

Esta tarjeta debe ser conectada a un dispositivo llamado DSU/CSU. La transmisión a través de los enlaces se verifica mediante las DSUs (Unidades de Servicio de Datos).

Las DSUs se pueden considerar como "módems digitales" debido a que ellas convierten la señal unipolar recibida de los DTEs en señales bipolares apropiadas para la transmisión (por ejemplo, en código AMI).

Cisco ofrece 6 tipos de cables seriales para poder conectar la tarjeta WIC-1T a las DSUs/CSUs (figura 3-16), éstos son:

1. **RS-232 (DB-25):** considera las recomendaciones V.24 y V.28. Funciona a una velocidad de 19200 bps y 115200 bps en distancias cortas. Posee modos de transmisión sincrónica y asincrónica.
2. **RS-449:** interfaz de 37 pines, se divide en las siguientes especificaciones: RS-442 (balanceado, V.11) y RS-423 (desbalanceado, V.10)
3. **V.35:** llamado también WINCHESTER, conector de 34 pines, es balanceado (V.11) y desbalanceado (V.10).
4. **X.21:** interfaz únicamente para datos, conector de 15 pines, y maneja una velocidad de 10 Mbps a 10 mts.
5. **RS-530 (DB-25):** está dado por la interfaz 449 (RS-422 y RS-423), maneja velocidades de 20 Kbps a 2 Mbps.

Para el acceso a los servicios de portadora se utilizan las CSUs (Unidades de Servicio de Canal), las cuales tienen funciones de regeneración de señal, monitoreo de señales, servicio de detección de errores y servicios de prueba y diagnóstico.

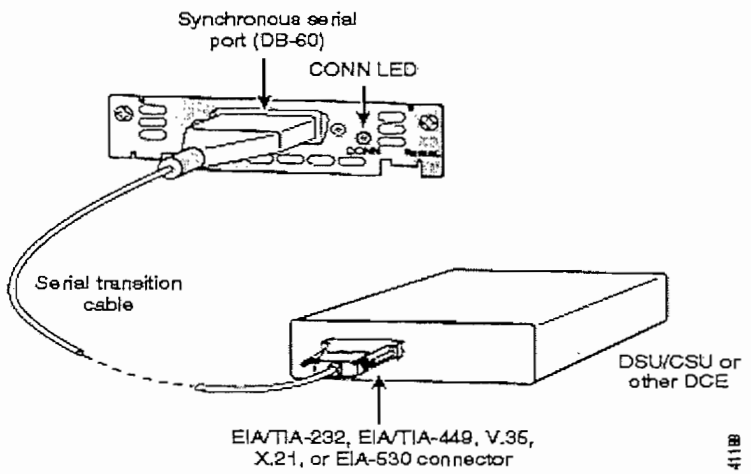


Figura 3-16 Conexión de la tarjeta WAN a la DSU/CSU [17]

Antiguamente se colocaba la DSU antes de la CSU, donde la empresa portadora otorgaba la CSU. Pero actualmente la DSU y la CSU se integran en una sola unidad, la DSU/CSU, la cual efectúa todas las funciones de la DSU y la CSU, y es otorgada por la empresa portadora.

En la ranura 0 se instalará una tarjeta Cisco VIC-2E/M (figura 3-17), la cual posee 2 puertos E&M que se utilizan para conectar las llamadas remotas de una red IP a una PBX.

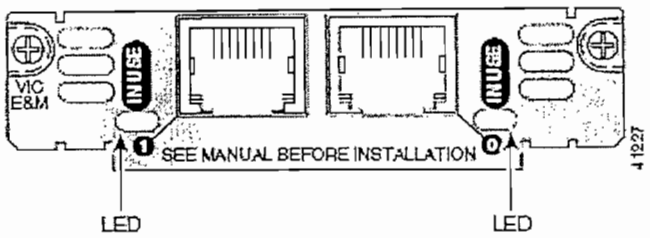


Figura 3-17 Tarjeta de dos puertos E&M VIC-2E/M [17]

Esta tarjeta posee conectores RJ-48, que por medio de un cable directo RJ-48 – RJ-48 se puede conectar a la PSTN o a una PBX por medio de una salida de pared (figura 3-18).

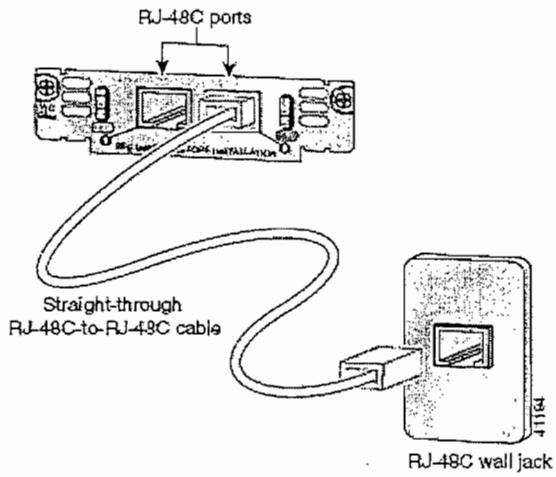


Figura 3-18 Conexión de la Tarjeta de voz E&M [17]

3.4.5 TOPOLOGÍA FINAL DE LA RED

Para poder implementar la solución final de la red, se necesitan adquirir los siguientes equipos:

- **3 CISCO *Router* 2801:** Cada equipo viene con las siguientes características [17]:
  - Memoria DRAM de 128 MB
  - Memoria flash 64 MB

Además del *router*, el paquete debe incluir los siguientes elementos (guía rápida para Routers de la serie CISCO 2800 de Servicios Integrados [17]):

- Un cable de consola azul (de RJ-45 a DB-9)
- Cable de alimentación
- Anclajes de montaje de bastidor de 19 pulgadas con tornillos
- Anclaje de gestión de cables con un tornillo de montaje
- Vigencia de la garantía del hardware: Noventa (90) días.
- Política de sustitución, reparación o devolución del hardware: Cisco o su centro de servicios hará todo lo que sea comercialmente razonable para enviar una pieza de sustitución dentro de los diez (10) días hábiles posteriores a la recepción de una solicitud de Autorización para devolución de materiales (*Return Materials Authorization*, RMA). Los plazos reales de entrega pueden variar según el lugar de residencia del cliente. (Cisco se reserva el derecho a devolver el precio de compra como recurso exclusivo de garantía).

- **3 tarjetas WIC-1T** (una para cada *router*)
- **3 tarjetas E&M VIC-2E/M** (una para cada *router*)

Además de adquirir los equipos, se deberá contratar la renta de los enlaces Quito – Cuenca y Quito – Guayaquil a un proveedor que ofrezca servicios portadores en una red *Frame Relay*.

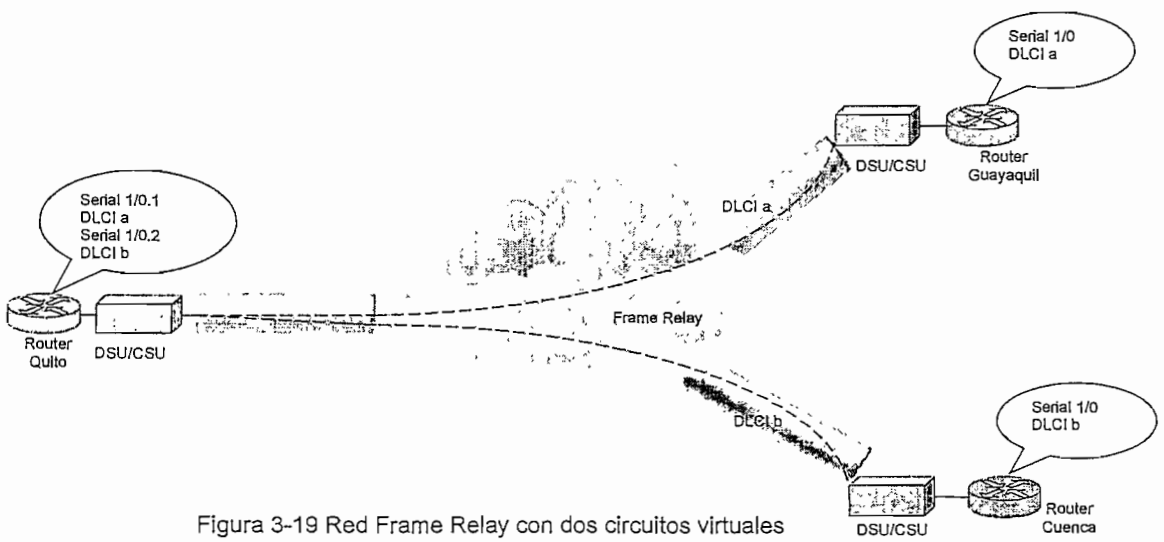


Figura 3-19 Red Frame Relay con dos circuitos virtuales

Como se trata de 2 circuitos virtuales que se centralizarán en el *router* ubicado en Quito, en la configuración de este equipo se distinguirán cada uno de estos circuitos por medio de dos subinterfaces virtuales, donde cada una tendrá diferente DLCI, razón por la cual es suficiente concentrar ambos circuitos virtuales en un solo enlace físico (figura 3-19), el cual estará conectado a una sola interfaz física. El diagrama de la topología final de la red se muestra en la figura 3-20.

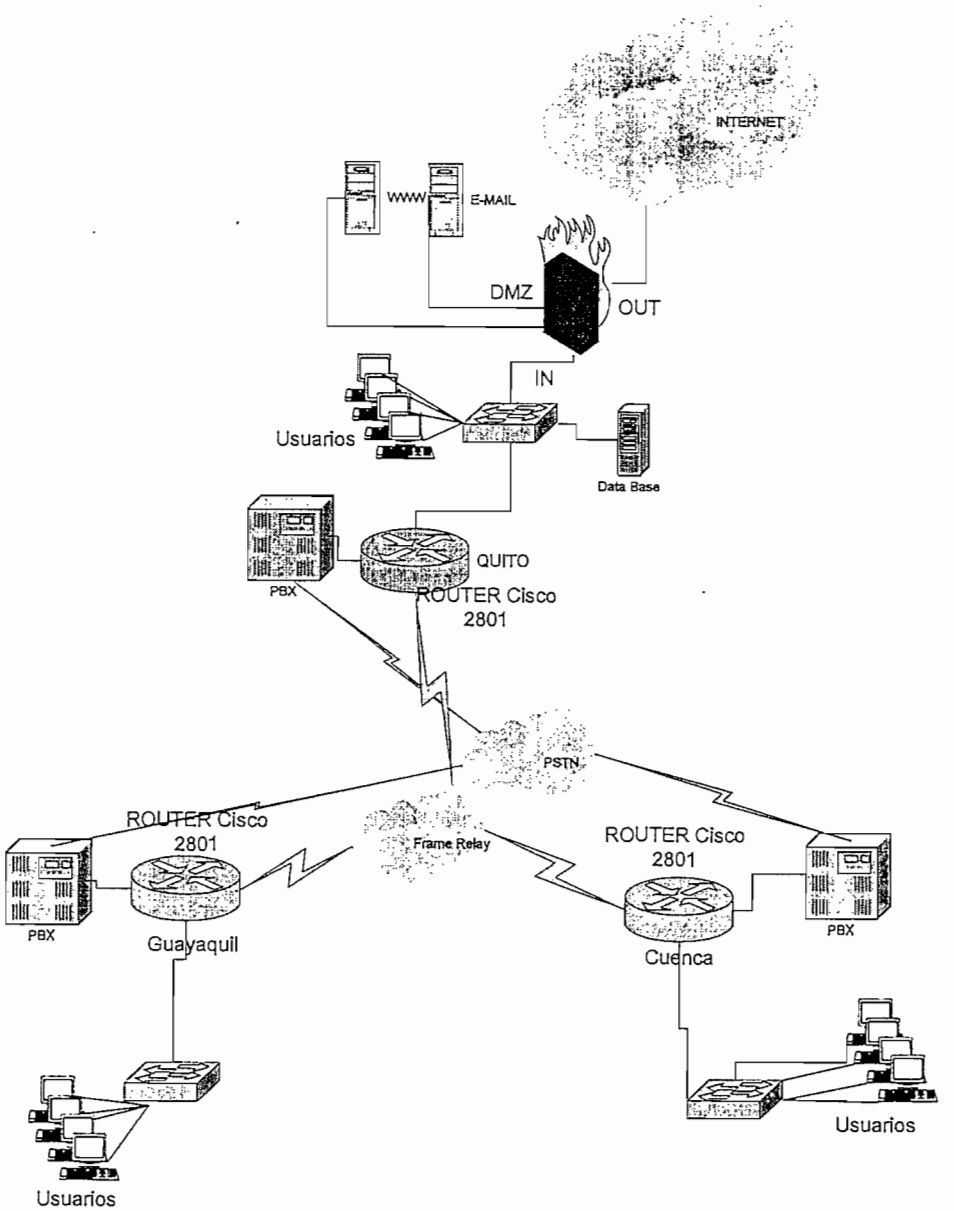


Figura 3-20 Diagrama de la configuración final de la red

3.4.6 ESQUEMA DE DIRECCIONAMIENTO

El espacio de direccionamiento IPv4 es dividido en cinco clases identificadas por el primer bit de la dirección. Las clases de direcciones IP *unicast* son: Clase A, Clase B, y Clase C. Las direcciones IP de Clase D son *multicast*, y las direcciones IP de clase E son reservadas.

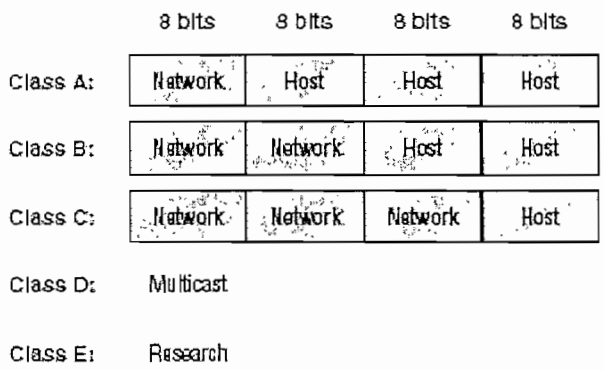


Figura 3-20 Resumen de las Clases de Direcciones IP

Las direcciones IP asignan un número lógico único a un dispositivo o interfaz de red. Este número es de 32 bits, y es dividido en 4 grupos de 8 bits, que ayudan a especificar los bits que son para direcciones de red y para direcciones de *host* (figura 3-20).

Tabla 3.22 Clases de direcciones de IPv4 [3]

Tipo de Clase	Primer Bit (bit más significativo)	Especio de direcciones (32 bits, 4 grupos de 8 bits)
A	0xxxxxxx*	1.0.0.0 a 126.0.0.0 **
B	10xxxxxx	128.0.0.0 a 192.255.0.0
C	110xxxxx	192.0.0.0 a 223.255.255.0
D	1110xxxx	224.0.0.1 a 239.255.255.255
E	1111xxxx	240.0.0.0 a 254.255.255.255

* x puede ser 1 o 0, dependiendo del direccionamiento.

** Las direcciones 0.0.0.0 y 127.0.0.0 son reservadas para propósitos especiales.

Para asegurar la eficiencia del enrutamiento, se definieron bits principales en cada clase, éstos son los bits más significativos (tabla 3.22). Por ejemplo desde que un

router sabe que una dirección de clase A empieza con 0, es capaz de acelerar la velocidad de conmutación de los paquetes después de leer únicamente el primer bit.

Todo este espacio de direcciones, se puede clasificar en direcciones públicas y direcciones privadas. Las direcciones privadas son reservadas especialmente para uso de empresas en su red privada. Estas direcciones no son ruteadas en el Internet, como es el caso de las direcciones públicas. Las direcciones privadas están detalladas en el RFC 1918, *Address Allocation for Private Internets*, publicada en 1996. La tabla 3.23 indica un detalle del espacio de direcciones reservadas para las redes privadas.

Tabla 3.23 Espacio de direcciones para redes privadas [3]

Tipo de Clase	Primera dirección	Última Dirección
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Para el presente diseño se puede utilizar cualquiera de las direcciones de la tabla 3.22, para cada una de las redes, e incluso se puede optimizar si se utiliza una sola dirección y se la divide, es decir creando subredes. Para crear las subredes se deben tomar los bits de la porción de *host* de la dirección IP, y reservarlos para definir la dirección de la subred. Por lo tanto para crear la subred se deben tomar en cuenta los siguientes pasos:

1. Determinar el número direcciones IP de red requeridas:
   - Una para cada red LAN
   - Una para cada conexión WAN

2. Determinar el número de direcciones IP de *hosts* para cada subred:
   - Una para cada *host* TCP/IP
   - Una para cada interfaz del *router*

3. Basados en los pasos 1 y 2, se debe crear lo siguiente:
   - Una máscara de subred para cada subred
   - Una única dirección IP de red para cada segmento físico
   - Un rango de direcciones IP de *host* para cada subred

3.4.6.1 Máscara de subred

Para poder dividir una red en subredes, cada equipo en la red debe saber qué parte de dirección de *host* usará como dirección de subred, y eso se lo realiza por medio de la máscara de subred.

Una máscara de subred es un valor de 32 bits que permite a un dispositivo de capa 3 distinguir en una dirección IP, la parte de red y la parte de *host*. Por lo tanto se creará una máscara de subred de 32 bits, compuesta de números 1s y 0s. Los 1s en la máscara de subred representan la posición que se refiere a las direcciones de red o subred. No todas las redes necesitan ser divididas en subredes (*subnetting*) utilizando la máscara de subred, ya que dependiendo a qué clase pertenezcan, ellas ya poseen una máscara por defecto (tabla 3.24).

Tabla 3.24 Máscaras de subred por defecto [3]

Clase	Formato	Máscara de subred (binario) (Por defecto)	Máscara de subred (decimal)
A	red.host.host.host	11111111.00000000.00000000.00000000	255.0.0.0
B	red.red.host.host	11111111. 11111111. 00000000. 00000000	255.255.0.0
C	red.red.red.host	11111111. 11111111. 11111111. 00000000	255.255.255.0

3.4.6.2 VLSM (*Variable Length Subnet Mask*)

VLSM es una técnica de direccionamiento que permite dividir una red en varias subredes de diferentes tamaños (diferente número de direcciones IP) con el fin de no desperdiciar las direcciones IP.

Tabla 3.25 Direcciones IP de la subred 110.20.78.8/30 [3]

Dirección IP en binario	Dirección IP	Función
1010110.0010000.01001110.00001**000**	110.20.78.8	dirección de subred
1010110.0010000.01001110.00001**001**	110.20.78.9	dirección IP # 1
1010110.0010000.01001110.00001**010**	110.20.78.10	dirección IP # 2
1010110.0010000.01001110.00001**011**	110.20.78.11	dirección de *broadcast*

Por ejemplo si una red clase C usa como máscara de subred 255.255.255.240, entonces esta red se dividirá en 16 subredes, cada una con 14 direcciones IP para *host*. Si existiese un enlace WAN punto a punto, donde se necesitaría únicamente dos direcciones IP, las otras 12 direcciones IP estarías desperdiciadas. Muchos autores representan a una máscara de subred con /n donde n representa el número de 1s. Cada subred posee su dirección IP de red, sus direcciones IP para cada *host* y una dirección de *broadcast*. Por ejemplo en la tabla 3.25 se puede ver a las direcciones IP de la red 110.20.78.8/30.

Para crear VLSM rápidamente, se necesita entender cómo el tamaño de la subred y el esquema (números de *host* por red) trabajan juntos para crear las máscaras VLSM.

Tabla 3.26 Tamaños de subredes para una red clase C [3]

Formato	Máscara (Clase C) 255.255.255.	*Host*	Tamaño de la subred
/26	.192	62	64
/27	.224	30	32
/28	.240	14	16
/29	.248	6	8
/30	.252	2	4

La tabla 3.26 muestra los distintos tamaños de subred usados cuando se utiliza VLSM en una red de clase C. Por ejemplo si se requieren 25 *host*, se deberá escoger un tamaño de subred de 32, o si se requiere 11 *host*, se debe escoger un tamaño de

subred de 16, es decir escoger el tamaño inmediato superior, para que todos los *host* requeridos obtengan su dirección IP.

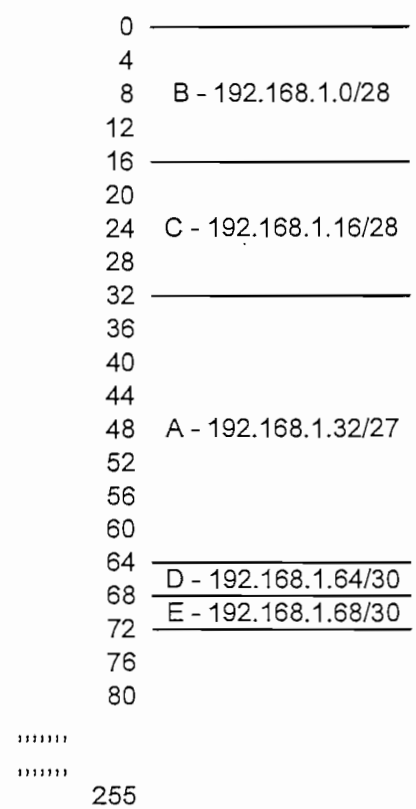
3.4.6.3 Diseño del esquema de direccionamiento

En el presente diseño se va a escoger la dirección IP de red **Clase C 192.168.1.0**, a la cual se la va a dividir (*subnetting*) utilizando VLSM. En la tabla 3.27 se resumen los requerimientos para poder realizar el esquema de direccionamiento.

Tabla 3.27 Identificación de la máscara para cada subred

Red	Descripción	Hosts/red	Tamaño	Formato	Máscara
A	Quito	15	32	/27	.224
B	Cuenca	7	16	/28	.240
C	Guayaquil	7	16	/28	.240
D	Enlace Quito-Cuenca	2	4	/30	.252
E	Enlace Quito-Guayaquil	2	4	/30	.252

Por lo tanto las direcciones utilizadas para cada subred de la red Clase C son:



En la figura 3-22 se puede apreciar el esquema de direccionamiento que se va a emplearen las diferentes redes e interfaces de los equipos.

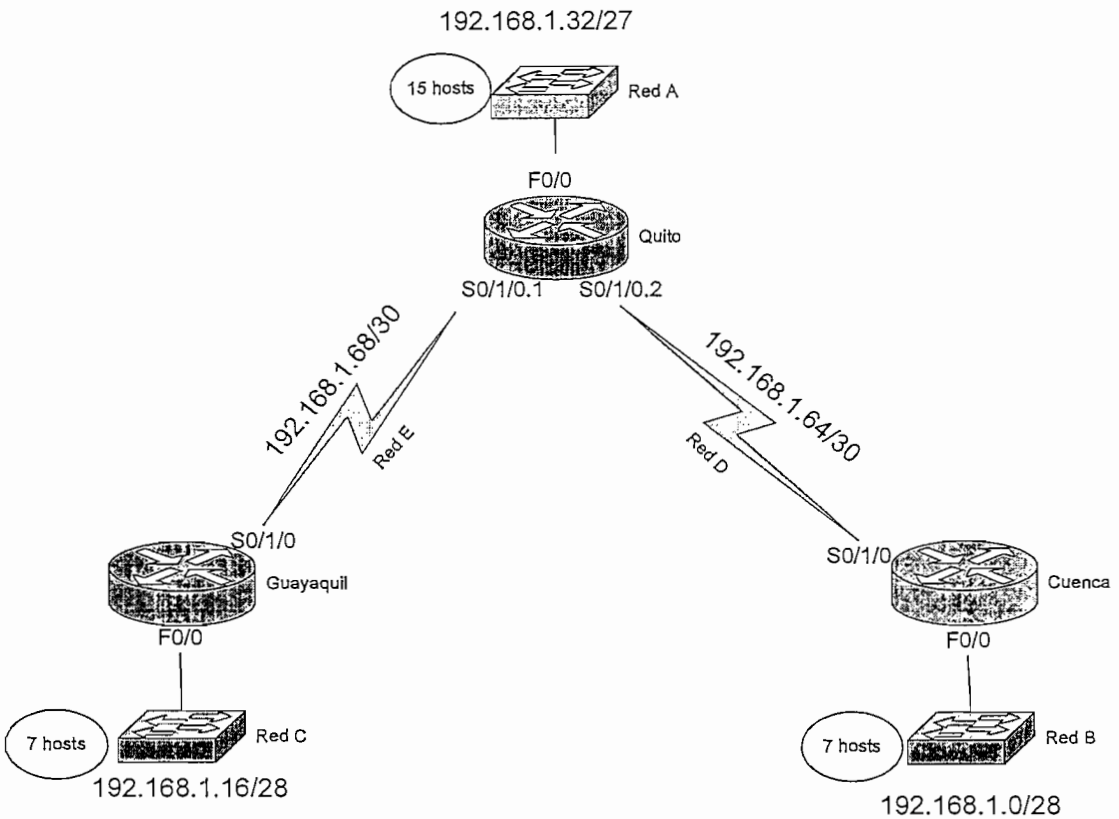


Figura 3-22 Esquema de direccionamiento IPv4

Es muy importante considerar que se utiliza VLSM para subdividir una sola dirección de red en subredes, pero en el caso de que el número de host sobrepase el calculado para la subred, al administrador le tocará volver a dimensionar todo el sistema de direccionamiento.

Como se va a utilizar direcciones públicas, en el diseño también se puede ocupar el espacio de direcciones que ofrece cada una de las clases, es decir sin realizar VLSM. Por ejemplo ocupar una dirección clase C para cada una de las redes (Quito,, Guayaquil, Cuenca y enlaces WAN) como se puede apreciar en la tabla 3.28.

Tabla 3.28 Identificación de la máscara para cada subred

Red	Descripción	Dirección de red	Mascara de subred
A	Quito	192.168.1.0	255.255.255.0
B	Cuenca	192.168.2.0	255.255.255.0
C	Guayaquil	192.168.3.0	255.255.255.0
D	Enlace Quito-Cuenca	192.168.4.0	255.255.255.0
E	Enlace Quito-Guayaquil	192.168.5.0	255.255.255.0

En la figura 3-23 se puede apreciar el esquema de direccionamiento, sin utilizar VLSM, ocupando el espacio de direcciones de una dirección clase C.

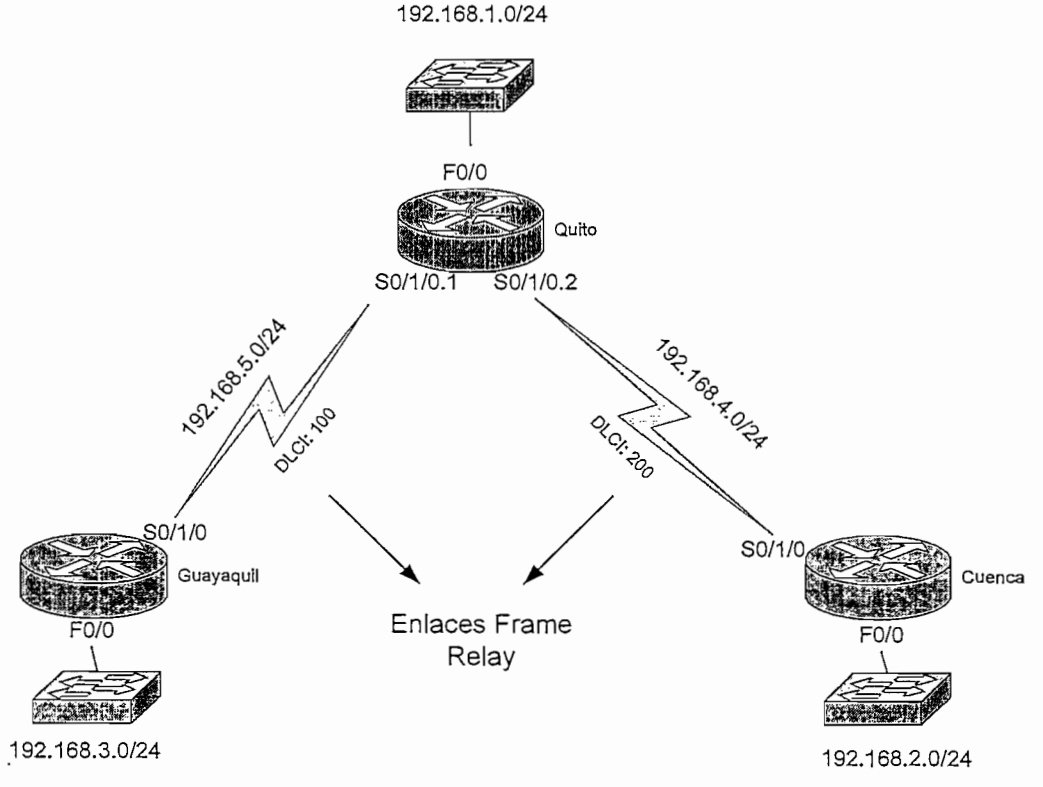


Figura 3.23 Esquema de direccionamiento sin considerar VLSM

3.4.7 SELECCIÓN DEL PROTOCOLO DE ENRUTAMIENTO

Los *routers* para escoger cuál va a ser el mejor camino por donde van a enviar los paquetes, definen tablas de rutas. Estas tablas permiten dar la información sobre

cuál interfaz del equipo se alcanza una dirección de red determinada, incluyendo además ciertos criterios de selección de rutas (métricas). Las tablas de rutas pueden formarse por enrutamientos estáticos o dinámicos.

El enrutamiento estático se define manualmente. La principal ventaja de este tipo de enrutamiento es que no se genera sobrecarga en la red por algún protocolo de enrutamiento, que son los utilizados por el canal para intercambiar información con otros dispositivos.

El enrutamiento dinámico determina la mejor ruta a un destino. Se usa en los *routers* por medio de protocolos de enrutamiento que permiten intercambiar información para crear y actualizar sus tablas de rutas. Cuando la topología de la red cambia, los protocolos de enrutamiento se ajustan a la nueva topología sin necesidad de intervención administrativa. Los protocolos de enrutamiento usan métricas para determinar el mejor camino hacia la red destino, éstas pueden ser:

- Números de saltos (*hop count*)
- Ancho de Banda (*bandwidth*)
- Retardo (*delay*)
- Carga (*load*)
- Confiabilidad (*Reliability*)
- MTU (Unidad Máxima de Transferencia)
- Costo (*cost*)

Los protocolos de enrutamientos utilizan algoritmos para establecer la mejor ruta; estos algoritmos son: vector – distancia, estado de enlace e híbrido (características de vector – distancia y estado de enlace).

El algoritmo vector – distancia hace llamadas a los *routers* vecinos para intercambiar periódicamente sus tablas de rutas, pero no permite que tengan un conocimiento global de la topología de la red.

Por el contrario en el algoritmo estado de enlace, también llamado SPF (*Short Path First*), cualquier cambio de la topología de la red se hace conocer a todos los *routers* por medio de mensajes LSA (*Link State Advertisement*).

Para escoger un protocolo de enrutamiento, hay que considerar que los protocolos de enrutamiento que usan el algoritmo de vector – distancia ocupan más el canal que los protocolos que utilizan estado de enlace. Los protocolos que usan vector – distancia generan más sobrecarga por las actualizaciones periódicas de sus tablas de enrutamiento. Pero los protocolos que emplean estado de enlace utilizan más recursos de memoria y CPU de los *routers*.

En la tabla 3.29 se pueden observar algunos protocolos de enrutamiento con sus características más relevantes. El protocolo de enrutamiento que se va a utilizar para el diseño de la red es el **protocolo EIGRP**, debido a que no inunda el canal con actualizaciones periódicas ya que utiliza un protocolo híbrido, y además posee la menor distancia administrativa.

Tabla 3.29 Características de algunos protocolos de enrutamiento [3]

Características	**RIPv1**	**RIPv2**	**IGRP**	**EIGRP**
Protocolo	Vector Distancia	Vector Distancia	Vector Distancia	Híbrido
Soporta VLSM	No	Si	No	SI
Métrica	# de saltos (máx. 15)	# de saltos (máx. 15)	saltos, ancho de banda y retardo	saltos, ancho de banda y retardo
Intervalo de actualizaciones	Cada 30 seg.	Cada 30 seg.	Cada 90 seg.	cuando existe cambios
soporta autenticación	no	si	no	si
Distancia Administrativa	120	120	100	90

Para la implementación de QoS para VoIP los equipos utilizan bastante procesamiento y no se debería saturarles más con el algoritmo de estado de enlace, y porque se trata de una red pequeña que no es importante que los equipos conozcan toda la topología de la red.

La distancia administrativa se utiliza para valorar la fidelidad de la información de enrutamiento recibida en un *router* de un *router* vecino. Una distancia administrativa es un número entero de 0 a 255, donde 0 significa la ruta más confiable, y 255 significa que no pasará tráfico por esa ruta. Para decidir la mejor ruta, lo primero que los equipos analizan es la distancia administrativa, luego analizan las métricas y otros criterios de selección de rutas.

3.4.8 CONFIGURACIÓN DE VoIP EN LOS *ROUTERS* CISCO [7]

Antes de configurar un sistema de VoIP en los *routers* CISCO, se analizarán ciertos conceptos que ayudarán a entender el procedimiento de configuración. Cuando una llamada se realiza, se marcan dígitos como una manera de señalización para saber dónde la llamada debería terminar.

Cuando estos dígitos ingresan a un puerto de voz de un *router,* éste debe ver la forma de decidir si la llamada puede ser ruteada, y a dónde será enviada. El *router* hace este proceso buscando una lista de marcación llamada *dial peers.*

Un *dial peer* es un punto de llamada direccionable. La dirección es llamada *destination pattern* y es configurada en cada *dial peer. Destination pattern* puede apuntar a un número telefónico o a un rango de números telefónicos.

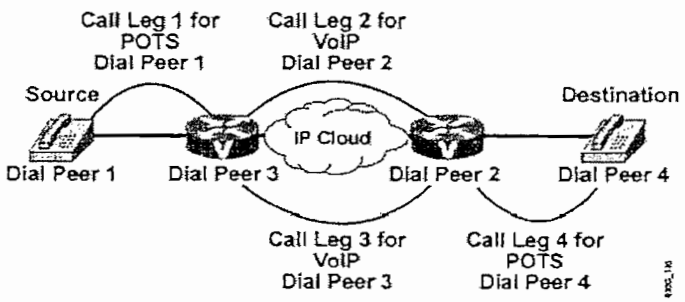


Figura 3-24 *Dial – Peer Call Legs* [7]

El *router* usa *dial peers* para establecer conexiones lógicas entre dos dispositivos telefónicos, como *routers* o *gateways*. Estas conexiones lógicas son conocidas como *call legs* (figura 3-24), y son establecidas en ambas direcciones: de entrada (*inbound*) o de salida (*outbound*).

Cuando una llamada *inbound* llega, ésta es procesada hasta que el destino sea determinado. Cuando esto se consigue, una segunda llamada de salida (*call leg outbound*) se establece, y la llamada de entrada (*call leg inbound*) se conmuta a un puerto de salida de voz (*outbound voice port*).

Cisco System habilitó en los *routers* de voz dos tipos de *dial peers* (figura 3-25).

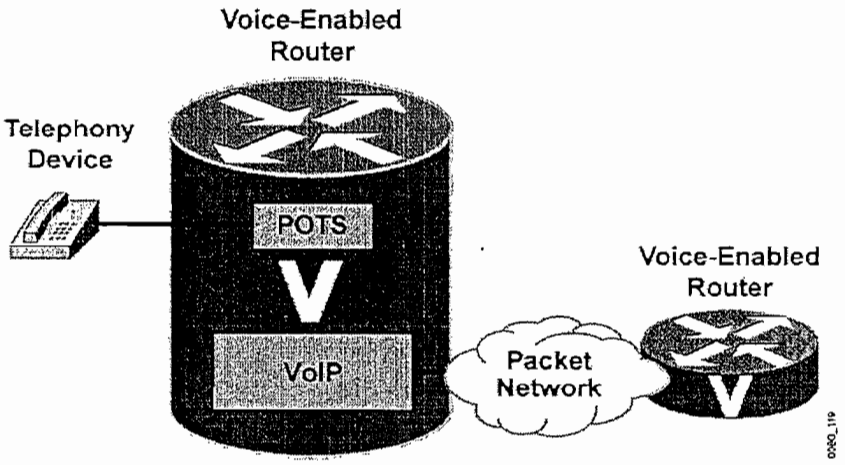


Figura 3-25 *Dial Peer* [7]

- **POTS *dial peers***: Se conecta directamente una red de telefonía tradicional, como la PSTN o una PBX, o dispositivos de telefonía como teléfonos o máquinas de fax. Tiene las siguientes funciones:
  - Provee una dirección (número telefónico o rango de números telefónicos).
  - Apunta a un puerto específico de voz que conecta dispositivos telefónicos.

- **VoIP *dial peers***: Se conecta a una red de paquetes. Posee las siguientes funciones:

- Provee una dirección destino (número telefónico o rango de números telefónicos) para un dispositivo que esté localizado a través de la red.
- Asocia la dirección con el *router* destino.

3.4.8.1 Configuración de *Dial – Peers*

Se analizarán ejemplos de configuraciones para POTS *dial peer* y VoIP *dial peer*.

Configuración para *dial peer* 1 en R1 de acuerdo a la figura 3-26 [7].

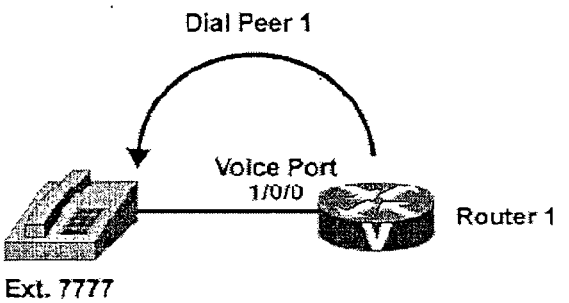


Figura 3-26 POTS *Dial Peer* [7]

```
Router1#configure terminal
Router1(config)#dial-peer voice tag {pots|VoIP}

!---tag es un número entre 1 y 2147483647, y puede o no coincidir con el número
!---de las extensiones

Router1(config)#dial peer voice 1 pots
Router1(config-dial-peer)#destination-pattern 7777
Router1(config-dial-peer)#port 1/0/0
Router1(config-dial-peer)#end
```

Configuración para *dial peer* 2 en R1 de acuerdo a la figura 3-27 [7].

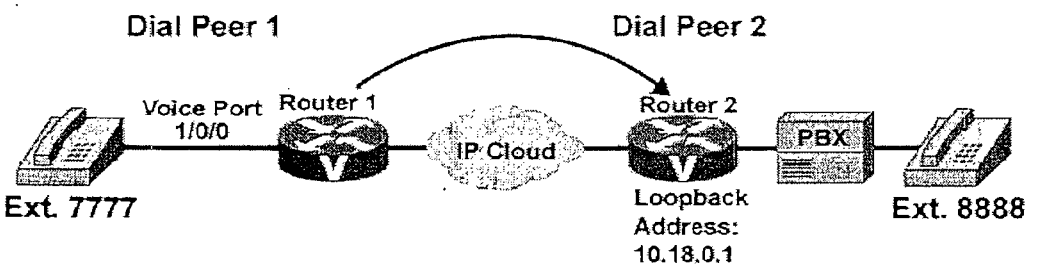


Figura 3-27 VoIP *Dial Peers* [7]

```
Router1#configure terminal
Router1(config)#dial peer voice 2 VoIP
Router1(config-dial-peer)#destination-pattern 8888
Router1(config-dial-peer)#session target ipv4:10.18.0.1

!---El comando session target especifica la dirección IP del router destino

Router1(config-dial-peer)#end
```

3.4.8.2 Configuración de puertos de voz

Ejemplo 1: Configuración de puertos FXS [5]

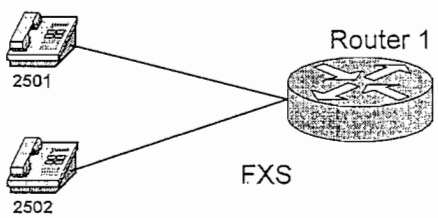


Figura 3-28 Ejemplo 1: *Router* 1 con dos teléfonos conectados a los puertos FXS [5]

Tabla 3.30 *Dial Plan* para dos teléfonos analógicos [5]

Dial Peer Tag	*Destination Pattern*	Tipo	Puerto de voz	*Session Target*
2501	2501	POTS	1/0/0	FXS
2502	2502	POTS	1/0/1	FXS

```
Router1#configure terminal

!---Se debe ingresar al puerto de voz
!---Se repite esta conFiguración para el puerto de voz 1/0/1

Router1(config)#voice-port 1/0/0
Router1(config-voiceport)#description << puerto FXS >>

!---Se debe conFigurar el tipo de señalización para esta interfaz.

Router1(config-voiceport)#signal loop-start
Router1(config-voiceport)#no shutdown
Router1(config-voiceport)#exit
Router1(config)#dial-peer voice 2501 pots
Router1(config-dial-peer)#destination-pattern 2501
Router1(config-dial-peer)#port 1/0/0
Router1(config-dial-peer)#exit
Router1(config)#dial-peer voice 2502 pots
Router1(config-dial-peer)#destination-pattern 2502
Router1(config-dial-peer)#port 1/0/1
```

Ejemplo 2: Configuración de puertos E&M y FXS [5]

En este ejemplo se analizará la conexión de dos *routers*. En el uno se conectará una central PBX al puerto E&M, y en el otro se conectarán directamente teléfonos analógicos a puertos FXS (Figura 3.29).

La tabla 3.31 muestra el *Dial Plan* para el *router 2*, el cual está conectado a la PBX por medio del puerto de voz E&M.

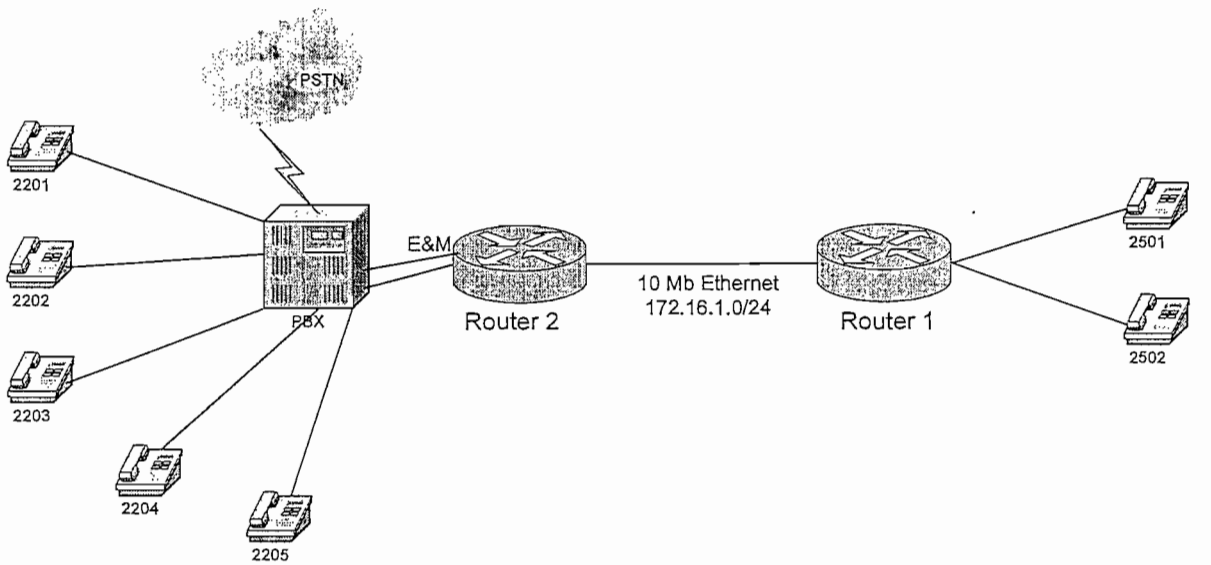


Figura 3-29 Ejemplo 2 [5]

Tabla 3-31 *Dial plan* para el *Router* 2 [5]

Dial Peer Tag	*Destination Pattern*	Tipo	Puerto de voz	*Session Target*
110	22xx	POTS	1/1/0	E&M
111	22xx	POTS	1/1/1	E&M
2501	2501	VoIP	-	172.16.1.2
2502	2502	VoIP	-	172.16.1.2

- **Configuración del puerto:** aquí se establecen los parámetros con los que el puerto E&M funciona, estos parámetros pueden variar dependiendo del tipo de central PBX que se utilice [5].

```
Router2(config)#voice-port 1/1/0
Router2(config-voiceport)#description << puerto E&M >>

!---Se escoge un tono de marcación multifrecuencial (dtmf)

Router2(config-voiceport)#dial-type dtmf

!---La señalización es de tipo wink-star, con esta señalización.

Router2(config-voiceport)#signal wink-start

!---Se debe escoger el tipo de conFiguración E&M, se escoge el tipo II

Router2(config-voiceport)#type 2

!--- Se escoge la conFiguración física a 4 cables

Router2(config-voiceport)#operation 4-wire
Router2(config-voiceport)#no shutdown

!--- Se repite la misma conFiguración para el puerto 1/1/1
```

- **Configuración de los *dial peers* pots** [5]:

```
Router2(config)#dial-peer voice 110 pots
Router2(config-dial-peer)#destination-pattern 22..
Router2(config-dial-peer)#port 1/1/0
Router2(config)#dial-peer voice 111 pots
Router2(config-dial-peer)#destination-pattern 22..
Router2(config-dial-peer)#port 1/1/1
```

Como se necesita direccionar la llamada para poder comunicarse por medio de la red, hay que configurar los *dial peer* VoIP [5].

```
!---Como se puede ver en la Figura 3-27, la conexión es por medio del puerto
!---Ethernet, por lo que se deben conFigurar las direcciones IP.

Router2(config)#interface Ethernet0
Router2(config-if)#ip address 172.16.1.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit

Router2(config)#dial-peer voice 2501 VoIP
Router2(config-dial-peer)#destination-pattern 2501
Router2(config-dial-peer)#session target ipv4:172.16.1.2
Router2(config-dial-peer)#exit

Router2(config)#dial-peer voice 2502 VoIP
Router2(config-dial-peer)#destination-pattern 2502
Router2(config-dial-peer)#session target ipv4:172.16.1.2
Router2(config-dial-peer)#exit
```

Para el *router* 1 se mantiene la configuración del ejemplo 1, y se debe añadir a esa configuración los *dial peers* VoIP y las direcciones IP [5].

```
Router1(config)#interface Ethernet0
Router1(config-if)#ip address 172.16.1.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit

Router1(config)#dial-peer voice 2200 VoIP
Router1(config-dial-peer)#destination-pattern 22..
Router1(config-dial-peer)#session target ipv4:172.16.1.1
Router1(config-dial-peer)#exit
```

3.4.8.3 Configuración final de los *routers* Cisco 2801

Para la configuración final de la red del presente proyecto, se deben recordar los siguientes datos que fueron analizados en la sección 3.4.6.3.

En el diseño se considerará el esquema de direccionamiento de la tabla 3.28 (sin VLSM), para considerar proyección. Esto no afectará al procesamiento de los equipos.

***Router* Quito:**

Interfaz F0/0:	192.168.1.1	(Red LAN)
Interfaz S0/1/0.1:	192.168.5.1	(Enlace WAN Quito - Guayaquil)
DLCI:	100	(Número otorgado por la empresa portadora)
Interfaz S0/1/0.2:	192.168.4.1	(Enlace WAN Quito - Cuenca)
DLCI:	200	(Número otorgado por la empresa portadora)

Tabla 3.32 Dial Plan *Router* Quito

Dial Peer Tag	*Destination Pattern*	Tipo	Puerto de Voz	*Session Target*
10	10..	POTS	0/0/0	E&M
11	10..	POTS	0/0/1	E&M
2000	20..	VoIP	-	192.168.2.1
3000	30..	VoIP	-	192.168.3.1

En la tabla 3.32 se muestra el *Dial Plan* para el *Router* de Quito. Los números de extensiones para Quito pueden ser desde el **1001** hasta el **1099** ya que cuando se coloca un punto en lugar de un número, éste podrá valer desde el 0 al 9.

***Router* Cuenca:**

Interfaz F0/0: 192.168.2.1 (Red LAN)
Interfaz S0/1/0: 192.168.4.2 (Enlace WAN Cuenca - Quito)
DLCI: 200 (Número otorgado por la empresa portadora)

Tabla 3.33 Dial Plan *Router* Cuenca

Dial Peer Tag	*Destination Pattern*	Tipo	Puerto de Voz	*Session Target*
20	20..	POTS	0/0/0	E&M
21	20..	POTS	0/0/1	E&M
1000	10..	VoIP	-	192.168.1.1
3000	30..	VoIP	-	192.168.3.1

En la tabla 3.33 se muestra el *Dial Plan* para el *Router* de Cuenca. Los números de extensiones para Cuenca pueden ser desde el **2001** hasta el **2099**.

***Router* Guayaquil:**

Interfaz F0/0: 192.168.3.1 (Red LAN)
Interfaz S0/1/0: 192.168.5.2 (Enlace WAN Guayaquil - Quito)
DLCI: 100 (Número otorgado por la empresa portadora)

Tabla 3.34 Dial Plan *Router* Guayaquil

Dial Peer Tag	*Destination Pattern*	Tipo	Puerto de Voz	*Session Target*
30	30..	POTS	0/0/0	E&M
31	30..	POTS	0/0/1	E&M
1000	10..	VoIP	-	192.168.1.1
2000	20..	VoIP	-	192.168.2.1

En la tabla 3.34 se muestra el *Dial Plan* para el *Router* de Guayaquil. Los números de extensiones para Guayaquil pueden ser desde el 3**001** hasta el 3**099**.

En la figura 3-30 se puede ver el diagrama para la configuración de toda la red.

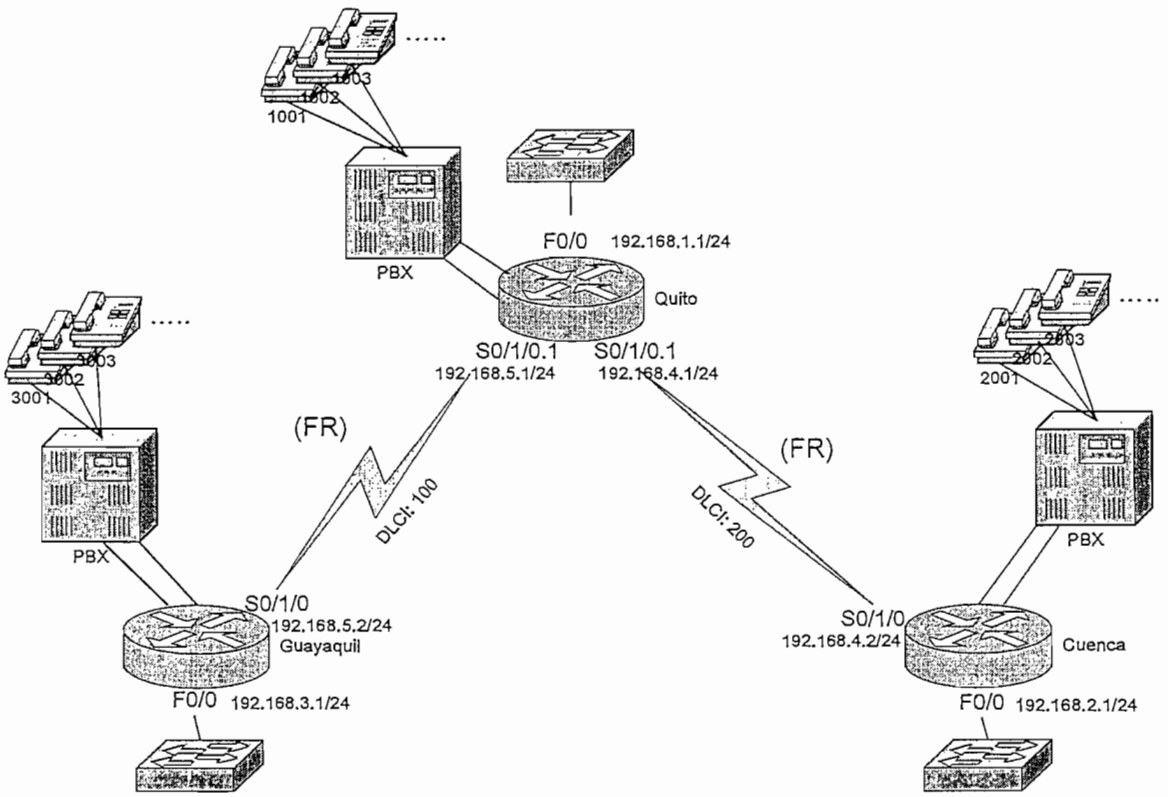


Figura 3-30 Diagrama para la configuración de toda la red

3.4.8.3.1 ***Configuración Router Quito***

Los parámetros que se configurarán en este equipo son:

- Direcciones IP a cada una de las interfaces (LAN y WAN), para este equipo se configurará una dirección para cada enlace (Cuenca y Guayaquil).
- Tipo de encapsulación de capa 2 (*Frame Relay*)
- El DLCI, uno para cada enlace (Cuenca y Guayaquil)
- El protocolo de enrutamiento (EIGRP)
- Los *dial peers* (POTS y VoIP, ver tabla 3.32)
- Los parámetros para la interfaz E&M (*voice-port*)

```
version 12.3(8)T
service password-encryption
!
hostname quito
!
enable secret 5 $1$rjjd$ULzQ51g5vQTSlXwLElrPz.
!
!

class-map signaling-voz
  match access-group 103
class-map trafico-voz
  match access-group 102
!
policy-map POLITICA-VOZ
  class trafico-voz
    priority 24
  class signaling-voz
    bandwidth 8
  class class-default
    fair-queue

!
!
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
  no shutdown

!
interface Serial0/1/0
  description Red Frame Relay
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay ip rtp header-compression

!
interface Serial0/1/0.1 point-to-point
  description Enlace frame-relay a Guayaquil
  bandwidth 128
  ip address 192.168.5.1 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  frame-relay interface-dlci 100
    class VOIPovFR

!
interface Serial0/1/0.2 point-to-point
  description Enlace frame-relay a Cuenca
  bandwidth 128
  ip address 192.168.4.1 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  frame-relay interface-dlci 200
    class VOIPovFR

!
router eigrp 100
  network 192.168.1.0
  network 192.168.4.0
  network 192.168.5.0
```

```
!
map-class frame-relay VOIPovFR
  frame-relay cir 32000
  frame-relay bc 320
  frame-relay be 0
  frame-relay mincir 32000
  service-policy output voice-policy
  frame-relay fragment 160
!
access-list 102 permit udp any any range 16384 37276
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720

!
dial-peer voice 10 pots
  destination-pattern 10..
  port 0/0/0
!
dial-peer voice 11 pots
  destination-pattern 10..
  port 0/0/1
!
dial-peer voice 2000 VoIP
  max-conn 2
  destination-pattern 20..
  session target ipv4:192.168.2.1
  codec g729r8
  ip precedence 5
!
dial-peer voice 3000 VoIP
  max-conn 2
  destination-pattern 30..
  session target ipv4:192.168.3.1
  codec g729r8
  ip precedence 5
!
voice-port 0/0/0
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
voice-port 0/0/1
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
line con 0
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 0559100A2F585B1B1C
login
!
!
end
```

3.4.8.3.2 Configuración Router Cuenca

Los parámetros que se configurarán en este equipo son:

- Direcciones IP a cada una de las interfaces (LAN y WAN)
- Tipo de encapsulación de capa 2 (*Frame Relay*)
- El DLCI, para el enlace a Quito
- El protocolo de enrutamiento (EIGRP)
- Los *dial peers* (POTS y VoIP, ver tabla 3.33)
- Los parámetros para la interfaz E&M (*voice-port*)

```
version 12.3(8)T
service password-encryption
!
hostname cuenca
!
enable secret 5 $1$rjjd$ULzQ51g5vQTS1XwLElrPz.
!
!
class-map signaling-voz
  match access-group 103
class-map trafico-voz
  match access-group 102
!
policy-map POLITICA-VOZ
  class trafico-voz
    priority 24
  class signaling-voz
    bandwidth 8
  class class-default
    fair-queue
!
!
interface FastEthernet0/0
  ip address 192.168.2.1 255.255.255.0
  no shutdown
!
interface Serial0/1/0
  description Red Frame Relay
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay ip rtp header-compression
!
interface Serial0/1/0.1 point-to-point
  description Enlace frame-relay a Quito
  bandwidth 128
  ip address 192.168.4.2 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  frame-relay interface-dlci 200
    class VOIPovFR
!
```

```
router eigrp 100
  network 192.168.2.0
  network 192.168.4.0
!
map-class frame-relay VOIPovFR
  frame-relay cir 32000
  frame-relay bc 320
  frame-relay be 0
  frame-relay mincir 32000
  service-policy output voice-policy
  frame-relay fragment 160
!
!
access-list 102 permit udp any any range 16384 37276
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
!
dial-peer voice 20 pots
  destination-pattern 20..
  port 0/0/0
!
dial-peer voice 21 pots
  destination-pattern 20..
  port 0/0/1
!
dial-peer voice 1000 VoIP
  max-conn 2
  destination-pattern 10..
  session target ipv4:192.168.1.1
  codec g729r8
  ip precedence 5
!
dial-peer voice 3000 VoIP
  max-conn 2
  destination-pattern 30..
  session target ipv4:192.168.3.1
  codec g729r8
  ip precedence 5
!
!
voice-port 0/0/0
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
voice-port 0/0/1
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
line con 0
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 0559100A2F585B1B1C
login
!
end
```

3.4.8.3.3 Configuración Router Guayaquil

Los parámetros que se configurarán en este equipo son:

- Direcciones IP a cada una de las interfaces (LAN y WAN)
- Tipo de encapsulación de capa 2 (*Frame Relay*)
- El DLCI, para el enlace a Quito
- El protocolo de enrutamiento (EIGRP)
- Los *dial peers* (POTS y VoIP, ver tabla 3.34)
- Los parámetros para la interfaz E&M (*voice-port*)

```
version 12.3(8)T
service password-encryption
!
hostname guayaquil
enable secret 5 $1$rjjd$ULzQ51g5vQTS1XwLE1rPz.
!
class-map signaling-voz
  match access-group 103
class-map trafico-voz
  match access-group 102
!
policy-map POLITICA-VOZ
  class trafico-voz
    priority 24
  class signaling-voz
    bandwidth 8
  class class-default
    fair-queue
!
interface FastEthernet0/0
  ip address 192.168.3.1 255.255.255.0
  no shutdown
!
interface Serial0/1/0
  description Red Frame Relay
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay ip rtp header-compression
!
interface Serial0/1/0.1 point-to-point
  description Enlace frame-relay a Quito
  bandwidth 128
  ip address 192.168.5.2 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  frame-relay interface-dlci 100
    class VOIPovFR
!
router eigrp 100
  network 192.168.3.0
  network 192.168.5.0
```

```
map-class frame-relay VOIPovFR
  frame-relay cir 32000
  frame-relay bc 320
  frame-relay be 0
  frame-relay mincir 32000
  service-policy output voice-policy
  frame-relay fragment 160
!
access-list 102 permit udp any any range 16384 37276
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
!
dial-peer voice 30 pots
  destination-pattern 30..
  port 0/0/0
!
dial-peer voice 31 pots
  destination-pattern 30..
  port 0/0/1
!
dial-peer voice 1000 VoIP
  max-conn 2
  destination-pattern 10..
  session target ipv4:192.168.1.1
  codec g729r8
  ip precedence 5
!
dial-peer voice 2000 VoIP
  max-conn 2
  destination-pattern 20..
  session target ipv4:192.168.2.1
  codec g729r8
  ip precedence 5
!
voice-port 0/0/0
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
voice-port 0/0/1
  description << Puerto de voz E&M >>
  dial-type dtmf
  signal wink-start
  operation 4-wire
  type 2
!
line con 0
line aux 0
line vty 0 4
exec-timeout 0 0
password 7 0559100A2F585B1B1C
login
!
end
```

Los comandos que se encuentran en **negrilla** de los tres *routers*, corresponden a la configuración de Calidad de Servicio, que fue analizada en el numeral 3.3.3.

3.5 ANÁLISIS FINANCIERO DEL PROYECTO

El análisis que se va a realizar está enfocado al proyecto de VoIP, en relación al gasto que se tiene en la red telefónica pública por llamadas telefónicas entre las oficinas. Una de las grandes ventajas que se obtiene al tener una red convergente es que se puede tener una administración centralizada de todo el sistema, tanto para la voz, como para los datos. Esto involucra un determinado ahorro ya que no necesariamente se debe tener personal por separado para la administración de voz y datos, sino puede reducirse al mismo administrador de la red para que maneje todo el sistema convergente.

Se puede afirmar que especialmente es en el área técnica donde más se consume el servicio de telefonía pública, porque los técnicos se demoran un número considerable de minutos en asesorar al personal que se encuentra en las oficinas remotas dando indicaciones del manejo del sistema o asesorando cuando haya existido algún problema. En muchas ocaciones también el consumo telefónico se ve reflejado en conferencias que realizan los gerentes entre oficinas para solucionar algún problema o tomar ciertas decisiones. A este consumo habrá que agregar las llamadas normales que se hacen entre oficinas, especialmente las consultas o solicitudes telefónicas de las oficinas remotas a la oficina principal, o entre oficinas remotas.

La empresa ficticia del ejemplo, a la que se le está diseñando la red integrada de voz y datos, necesariamente tiene que alquilar los enlaces WAN para la circulación segura de su información. Para el caso del transporte de VoIP por la red WAN, se ha analizado que no se necesitará incrementar la capacidad del canal de la que se contrataría si por la red únicamente se transmitieran datos, ya que los proveedores de servicio ofrecen velocidades estándares para los enlaces WAN, por lo que la transmisión de voz por la WAN no involucra un gasto adicional con respecto a la renta del canal [sección 3.5.1.1 y 3.5.1.2].

En este caso se concluye que por la misma red de datos se pueden realizar llamadas telefónicas, y los costos básicamente se incrementarían con la adquisición de tarjetas de voz y servicio técnico [sección 3.5.1.2]. Por lo tanto, para poder evaluar correctamente este proyecto, se pueden tomar en cuenta los siguientes criterios:

a) Costo – beneficio

Esta técnica permite la cuantificación en cifras de los beneficios y costos; además permite la valoración de diferentes alternativas a partir de los indicadores tanto financieros como económicos. Este criterio es utilizado generalmente en los proyectos cuyos beneficios se los puede apreciar de manera física o económica. Este criterio puede utilizarse para la evaluación financiera donde se puede tener una estimación de ingresos y costos, cuyo objetivo para el inversionista es la rentabilidad. Para proyectos cuyo objetivo es, mejora de calidad y bienestar, sus beneficios no son fácilmente medibles y cuantificables, por lo tanto se puede seguir el criterio de costo – eficiencia.

b) Costo – eficiencia

Este criterio cuantifica los costos del proyecto y valora los beneficios. Esta técnica es usualmente utilizada para proyectos en los cuales no es fácil estimar y cuantificar en cifras los beneficios de un proyecto. Se utilizan indicadores e índices que permiten, de alguna manera, inferir y comparar los posibles beneficios de cada alternativa. Este criterio es utilizado especialmente en proyectos sociales, como educación y salud, donde se pueden describir los beneficios, pero resulta complicado evaluar su rentabilidad.

c) Costo – mínimo

En este criterio se estiman los costos que implica la realización del proyecto, suponiendo que cualquiera de las alternativas posibles genera los mismos

beneficios. Esto quiere decir que con una alternativa u otra se obtendrían los mismos resultados, pero con recursos y costos diferentes.

De los tres criterios el que más se asemeja a este proyecto es el de **costo – mínimo**, ya que únicamente se está analizando los costos que involucran la implementación de VoIP, comparados con los costos de seguir utilizando la PSTN, y en este análisis se refleja el ahorro que otorga la implementación de VoIP, ya que no se tendría que pagar demasiado por el consumo telefónico de la red pública específicamente en las llamadas internas de la empresa.

3.5.1 FLUJO DE FONDOS (FF)

La evaluación financiera identifica los ingresos y egresos de un proyecto y su rentabilidad. Se va a utilizar el flujo de fondos como instrumento de evaluación.

El flujo de fondos provee información sobre los costos implícitos en cada alternativa y ayuda a identificar en qué medida éstos pueden cubrirse mediante el diseño de un plan de financiamiento.

La evaluación financiera, entonces, tiene una fase de presentación de costos y beneficios realizada a través del flujo de fondos, y un indicador que permite la comparación entre las dos alternativas.

El flujo de fondos presenta la información de costos e ingresos que se generan en un proyecto en un período establecido (el registro se hace período por período). Como guía para la elaboración de un flujo de fondos se identifican algunos rubros generales o partes del flujo de fondos. Para el presente caso, únicamente se va a tomar en cuenta los gastos que se tiene al adquirir un sistema de VoIP, y se va a comparar los gastos que se tienen al utilizar la red telefónica pública.

3.5.1.1 Alternativa A: FF del proyecto utilizando la Red Telefónica Pública

Se estima que el primer año es un período de inversión, implementación, planeación y evaluación (Año base, año 0) y, a partir del año 1, el proyecto empezará su funcionamiento [tabla 3.35].

3.5.1.1.1 Costos de inversión

Corresponde a todas aquellas inversiones que deben realizarse para poner en marcha el proyecto.

Tabla 3.35 Costos de los equipos

Equipo de la oficina principal (Quito)	
Router Cisco 2801 (2801 *Router*/AC PWR, 2FE, 4slots (2HWICs), 2AIMS, IP BASE, 64F/128D)	$ 1.995,00*
Equipos de las oficinas remotas (Cuenca)	
Router Cisco 2801 (2801 *Router*/AC PWR, 2FE, 4slots (2HWICs), 2AIMS, IP BASE, 64F/128D)	$ 1.995,00*
Equipos de las oficinas remotas (Guayaquil)	
Router Cisco 2801 (2801 *Router*/AC PWR, 2FE, 4slots (2HWICs), 2AIMS, IP BASE, 64F/128D)	$ 1.995,00*
Total	**$ 5.985,00**

* Estos precios no incluyen IVA

3.5.1.1.2 Costos de operación

Estos egresos hacen referencia a los desembolsos por utilización periódica de recursos (insumos, servicios) dentro del ciclo productivo del proyecto. Se contempla bajo esta categoría: arrendamientos, gastos de mantenimiento, etc. Uno de los costos de operación más importantes son los costos del servicio telefónico que se van a tener entre las oficinas de la institución. Aproximadamente una empresa utiliza el servicio telefónico público para llamar a sus oficinas remotas alrededor de **2 horas diarias** en promedio. Como se está hablando de una empresa comercial, el costo de llamadas nacionales asciende a **4 ctv el minuto**.

Por lo que, al utilizar la red telefónica pública en llamadas nacionales la empresa está gastando alrededor de: *0.04 usd x 120 min* = **4.8 dólares** diarios por agencia (llamadas Quito – Cuenca o Cuenca – Quito y llamadas Quito – Guayaquil o Guayaquil – Quito). Los gastos de operación se presentan en la tabla 3.36.

Tabla 3.36 Gastos de Operación (Alternativa A)

Descripción	Mensuales	Anuales
Contratación Internet Quito de 512/128 Kbps (ver anexo A.1)	$ 275,00	**$ 3.300,00**
Servicio de portadora (WAN) 128 Kbps (ver anexo A.2)	$ 760,00	**$ 9.120,00**
Mantenimiento	$ 50,00	**$ 600,00**
Servicio Telefónico entre Agencias	$ 192,00	**$ 2.304,00**
TOTAL	**$ 1.277,00**	**$15.324,00**

*3.5.1.1.3 **Depreciación***

Es el costo de un bien mueble o inmueble distribuido a lo largo de su vida útil. Existen varios métodos para el cálculo de la depreciación, pero el más común es el método lineal en el cual se distribuye uniformemente el valor del bien en el número de períodos de su vida útil. La depreciación no tiene efectos en el flujo de fondos, ya que no es un egreso real, sino se calcula como la pérdida de valor de un bien a través del tiempo. Sin embargo, se tiene en cuenta en el flujo de fondos ya que afecta a la base gravable de impuestos. Al final del flujo de fondos se adiciona, para obtener el cálculo real del movimiento de efectivo durante el período en mención.

Para evaluar este proyecto, a los equipos se los va a depreciar en un **período de 5 años**, que es el tiempo que generalmente CISCO SYSTEM no les descontinúa.

Depreciación de los equipos (*ROUTERS*):

Depreciación anual = 5.985,00/5 = **1.197**

Depreciación acumulada año 5 = 5.985

Valor en libros = 5.985 – 5.985 = 0

Venta año 5 = 5.985 * 30 % (*valor otorgado por CISCO*) = 1.796

Utilidad en venta = 1.796 – 0 = **1.796,00**

El impuesto por ganancia en venta de activos, se lo analizará con el 25 % [Ley de Régimen Tributario Interno Art. 37]. La entidad no paga impuestos por el desarrollo de su actividad.

Impuesto por venta estimado año 5 = 1.796 * 25% = **449**

3.5.1.1.4 Esquema de Flujo de Fondos

En la tabla 3.37 se muestra un esquema que podrá ser utilizado como guía para la clasificación de gastos. A partir de la información suministrada se puede obtener:

- **Ganancias gravables**: corresponden a los resultados por el desarrollo de la actividad y éstos se ven afectados por impuestos [22].

Ganancias gravables = Ingresos de operación + ingresos financieros – costos de operación – depreciación.

- **Ganancias Netas:** resultado después de haber sido aplicados los impuestos correspondientes tanto a renta como por venta de activos.

Tabla 3.37 Esquema de flujo de fondos (Alternativa A)

Concepto	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
+ Ingresos de Operación	$ 0,00					
- Costos de operación						
Internet		$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00
WAN		$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00
Mantenimiento		$ 600,00	$ 600,00	$ 600,00	$ 600,00	$ 600,00
Telefonía		$ 2.304,00	$ 2.304,00	$ 2.304,00	$ 2.304,00	$ 2.304,00
TOTAL COSTOS DE OPERACIÓN		$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00
- Depreciación						
Equipos		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
TOTAL DEPRECIACIÓN		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
GANANCIAS GRAVABLES	$ 0,00	-$ 16.521,00	-$ 16.521,00	-$ 16.521,00	-$ 16.521,00	-$ 16.521,00
+ Valores de salvamento (Utilidad/Pérdida en venta)						
Equipos						$ 1.796,00
TOTAL VALOR SALVAMENTO						$ 1.796,00
- Impuestos a la utilidad en venta de activos						$ 449
GANANCIAS NETAS		-$ 16.521,00	-$ 16.521,00	-$ 16.521,00	-$ 16.521,00	-$ 15.174,00
+ Depreciación						
Equipos		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
TOTAL DEPRECIACIÓN		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
- Costos de Inversión						
compra de Equipos	$ 5.985,00					
TOTAL INVERSIÓN	$ 5.985,00					
FLUJO DE FONDOS NETO	-$ 5.985,00	-$ 15.324,00	-$ 15.324,00	-$ 15.324,00	-$ 15.324,00	-$ 13.977,00

3.5.1.2 Alternativa B: FF del proyecto utilizando VoIP

Para poder realizar este flujo de fondos, se ha pedido proformas de 3 proveedores de servicios de portadora, y entre las 3 opciones se escogió la de **SURATEL del grupo TvCable**, que ofrece enlaces *Frame Relay.* Se ha escogido esta opción debido a que, de entre todas las propuestas que ofrecen enlaces *Frame Relay*, la de SURATEL es la más económica. (Proformas en anexos A).

3.5.1.2.1 Costos de inversión

El costo de inversión es igual al costo de inversión de los equipos, añadido los componentes para desarrollar VoIP.

Tabla 3.38 Costos de los elementos para VoIP

Equipos (*Routers*) (*mismos Equipos*)	$ 5.985,00*
3 tarjetas de Voz E&M (*Two-port Voice Interface Card - EandM-Spare*) ($ 400,00 c/u)	$ 1.200,00*
Configuración de Equipos ($200,00 c/u)	$ 600,00*
TOTAL	**$ 7.785,00**

*Estos precios no incluyen IVA

3.5.1.2.2 Costos de operación

En este caso el costo de llamadas telefónicas por medio de la red de datos no tiene costo alguno. Los gastos de operación para esta alternativa se presentan en la tabla 3.39.

Tabla 3.39 Gastos de Operación

Descripción	Mensuales	Anuales
Contratación Internet Quito 512/128 Kbps (ver anexo A.1)	$ 275,00	**$ 3.300,00**
Servicio de portadora (WAN) 128 Kbps (ver anexo A.2)	$ 760,00	**$ 9.120,00**
Mantenimiento	$ 50,00	**$ 600,00**
Servicio Telefónico entre Agencias	$ 0,00	**$ 0,00**
TOTAL	$ 1.085,00	**$ 13.020,00**

3.5.1.2.3 Depreciación

Al igual que en la alternativa A, a los equipos y a los componentes VoIP se los va a depreciar a 5 años.

Depreciación de los componentes VoIP:

Depreciación anual = 1.200,00/5 = **240**

Depreciación acumulada año 5 = 1.200

Valor en libros = 1.200 – 1.200 = 0

Venta año 5 = 1200 * 50 % (valor otorgado por CISCO) = 600

Utilidad en venta = 600 – 0 = **600**

El impuesto por ganancia en venta de activos, se lo analizará con el 25 %. La entidad no paga impuestos por el desarrollo de su actividad.

Impuesto por venta estimado año 5 = 600 * 25% = **150**

3.5.1.2.4 Esquema de Flujo de Fondos

En la tabla 3.40 se muestra el flujo de fondos con los costos que representan la implementación de VoIP.

Tabla 3.40 Esquema de flujo de fondos (Alternativa B)

Concepto	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
+ Ingresos de Operación	$ 0,00					
- Costos de operación						
Internet		$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00
WAN		$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00
Mantenimiento		$ 600,00	$ 600,00	$ 600,00	$ 600,00	$ 600,00
TOTAL COSTOS DE OPERACIÓN		$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00
- Depreciación						
Equipos		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
Componentes VoIP		$ 240,00	$ 240,00	$ 240,00	$ 240,00	$ 240,00
TOTAL DEPRECIACIÓN		$ 1.437,00	$ 1.437,00	$ 1.437,00	$ 1.437,00	$ 1.437,00
GANANCIAS GRAVABLES	$ 0,00	-$ 14.457,00	-$ 14.457,00	-$ 14.457,00	-$ 14.457,00	-$ 14.457,00
+ Valores de salvamento (Utilidad/Pérdida en venta)						
Equipos						$ 1.796,00
Componentes VoIP						$ 600,00
TOTAL VALOR SALVAMENTO						$ 2.396,00
- Impuestos a la utilidad en venta de activos						$ 150,00
GANANCIAS NETAS		-$ 14.457,00	-$ 14.457,00	-$ 14.457,00	-$ 14.457,00	-$ 12.211,00
+ Depreciación						
Equipos		$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00	$ 1.197,00
Componentes VoIP		$ 240,00	$ 240,00	$ 240,00	$ 240,00	$ 240,00
TOTAL DEPRECIACIÓN		$ 1.437,00	$ 1.437,00	$ 1.437,00	$ 1.437,00	$ 1.437,00
- Costos de inversión						
compra de Equipos	$ 5.985,00					
compra componentes VoIP	$ 1.200,00					
Configuración Equipos	$ 600,00					
TOTAL INVERSIÓN	$ 7.785,00					
FLUJO DE FONDOS NETO	-$ 7.785,00	-$ 13.020,00	-$ 13.020,00	-$ 13.020,00	-$ 13.020,00	-$ 10.774,00

3.5.2 EVALUACIÓN DEL PROYECTO

Para realizar la evaluación del proyecto existen indicadores que ayudan a escoger entre las alternativas la más rentable. Entre éstos están:

3.5.2.1 Valor Presente Neto (VPN) [22]

Representa el valor de los ingresos y egresos de cada período a valores presentes descontados a una tasa determinada (tasa de oportunidad). Esta tasa refleja el costo de oportunidad del inversionista. Es el rendimiento frente al cual se comparan los resultados de los proyectos. El costo de oportunidad del inversionista corresponde a los beneficios que deja de percibir un inversionista por la realización de un proyecto o inversión. Por lo tanto la tasa de oportunidad corresponde a los rendimientos que se dejan percibir por realizar una inversión.

Para identificar esta tasa se requiere establecer y analizar los rendimientos generados en inversiones alternativas. Se puede tomar como base la tasa del mercado financiero (para el Ecuador es aproximadamente de un **8%** [Produbanco]). El objetivo es identificar el mejor uso alternativo y utilizar esta tasa como base para la identificación de rendimientos del proyecto. En otras palabras el VPN es la suma de ingresos – egresos (flujo de fondos neto de cada período) y trasladado a valores del año base. El VPN se lo puede calcular en base a la siguiente fórmula [22]:

$$VPN = FFN(inicial) + \frac{FFN_1}{(1+TD)^1} + \frac{FFN_2}{(1+TD)^2} + \frac{FFN_3}{(1+TD)^3} + \ldots\ldots\ldots\ldots + \frac{FFN_n}{(1+TD)^n}$$

donde:

VPN:	Valor Presente Neto
FFN inicial:	Flujo de Fondos Neto del período inicial (período base)
FFN:	Flujo de Fondos Neto por período
TD:	Tasa de oportunidad
n:	Período de vida útil del proyecto

Se identifica el VPN para cada alternativa posible, y aquella cuyo VPN sea mayor será la que mayor rentabilidad a una tasa de oportunidad represente, por cuanto será la mejor opción.

El VPN es utilizado para proyectos que utilicen el criterio COSTO–BENEFICIO. En el presente proyecto no se está analizando la rentabilidad con respecto a una inversión en el mercado financiero.

Este indicador puede ayudar a establecer cuál de las dos alternativas involucra más gastos a la empresa. Aplicando la fórmula del VPN con los datos del flujo de fondos, a una tasa del 8 %, se obtienen los siguientes resultados:

Alternativa A: VPN = - 61.344,95
Alternativa B: VPN = - 53.927,31

Por lo tanto como resultado del análisis se puede concluir que la mejor opción es la alternativa B, porque ésta sería la menos costosa analizada en un período de 5 años.

Otro indicador para evaluar un proyecto es el TIR (Tasa Interna de Retorno) que expresa el rendimiento de la inversión.

Para este tipo de proyectos el TIR no contempla un buen método de evaluación, debido a que no se toma en cuenta los ingresos, todos los valores del flujo de fondos netos van a representar egresos más no rendimientos para la institución.

3.5.2.2 Valor Actual de Costos (VAC) [22]

Para este proyecto se va a utilizar el criterio COSTO – EFICIENCIA o COSTO MÍNIMO, con el fin de poder seleccionar la mejor alternativa posible.

Teniendo en cuenta el flujo de fondos explicado anteriormente, se escoge una solución con el mínimo costo, que incluya indicadores de beneficio adecuados para la solución del problema. Como criterio para la elección de la mejor alternativa al menor costo posible generalmente se utiliza el indicador de Valor Actual de Costos, el cual es aplicable a las alternativas que generen indicadores de beneficio similares.

El valor actual de costos se puede identificar mediante el siguiente procedimiento:

1. Se suman los costos de los componentes para cada período con el cual se obtiene el "Valor por período de costos del proyecto" (VPC).
2. Se debe trasladar el valor de los costos de cada período a precios del período base y sumar los datos. Esto se realiza a través de la aplicación de la siguiente fórmula [22]:

$$VAC = VPC(inicial) + \frac{VPC_1}{(1+TD)^1} + \frac{VPC_2}{(1+TD)^2} + \frac{VPC_3}{(1+TD)^3} + ... + \frac{VPC_n}{(1+TD)^n}$$

donde:

VAC:	Valor Actual de los costos del proyecto
VPC inicial:	Valor por período de costos para el período inicial (año base)
VPC:	Valor por período de costos
TD:	Tasa de descuento
n:	Período de vida útil del proyecto

Se identifica el VAC para cada alternativa posible y aquella cuyo VAC sea menor, será la que menor costo represente a precios actuales y por tanto, si los beneficios son similares será la mejor opción.

En las tablas 3.41 y 3.42 se pueden analizar el flujo de fondos para el cálculo de VAC para cada una de las alternativas a una tasa del 8 %.

Tabla 3.41 Flujo de fondos para el cálculo del VAC (Alternativa A)

FLUJO DE FONDOS	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Costos de operación						
Internet		$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00
WAN		$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00
Mantenimiento		$ 600,00	$ 600,00	$ 600,00	$ 600,00	$ 600,00
Telefonía		$ 2.304,00	$ 2.304,00	$ 2.304,00	$ 2.304,00	$ 2.304,00
TOTAL COSTOS DE OPERACIÓN		$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00
Costos de inversión						
compra de Equipos	$ 5.985,00					
TOTAL COSTOS DE INVERSIÓN	$ 5.985,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
FLUJO DE FONDOS NETO	$ 5.985,00	$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00	$ 15.324,00

VAC = 67.169,29

Tabla 3.42 Flujo de fondos para el cálculo del VAC (Alternativa B)

FLUJO DE FONDOS	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Costos de operación						
Internet		$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00	$ 3.300,00
WAN		$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00	$ 9.120,00
Mantenimiento		$ 600,00	$ 600,00	$ 600,00	$ 600,00	$ 600,00
TOTAL COSTOS DE OPERACIÓN		$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00
Costos de inversión						
compra de Equipos	$ 5.985,00					
compra de Componentes VoIP	$ 1.200,00					
Configuración	$ 600,00					
TOTAL COSTOS DE INVERSIÓN	$ 7.785,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00	$ 0,00
FLUJO DE FONDOS NETO	$ 7.785,00	$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00	$ 13.020,00

VAC = 59.770,08

Por medio de este análisis se concluye que la alternativa A tiene un VAC superior a la alternativa B, por lo tanto, si se obtienen los mismos beneficios, se optará por la opción B que implica un menor costo.

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Los beneficios de poseer una sola red convergente para la manipulación de datos y voz son evidentes, y se puede mencionar entre los más importantes el ahorro de costos de comunicaciones, pues las llamadas entre las distintas delegaciones de la empresa saldrían relativamente gratis. La integración de servicios y unificación de la estructura de comunicaciones, ha dado lugar a un crecimiento tecnológico y fácil de aplicar en las redes de muchas empresas de este país, pues las comunicaciones todavía están siendo enviadas por redes separadas tanto para datos como para voz.

- Cuando se diseña una red, es importante empezar con una buena y sólida topología. La topología ayudará a entender y visualizar, de mejor manera, las características generales que se involucran en una red, como: el esquema de direccionamiento, la dirección del flujo de tráfico de las aplicaciones, posibles problemas por congestionamiento, permisos de acceso a usuarios y aplicaciones, etc. Con una buena topología resultará más fácil caracterizar y entender a las aplicaciones que van a estar "corriendo" sobre la red y de esta manera poder dimensionarla correctamente. Hay que tomar muy en cuenta que no existe un modelo fijo para una infraestructura de red, la topología puede variar de acuerdo a las necesidades de la red. Muchos autores definen modelos generales que se los pueden tomar como base para el diseño que se esté realizando.

- La Voz sobre IP (VoIP, *Voice over IP*) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos; en cambio la Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando dispositivos como PCs, *gateways* y teléfonos estándares, todos ellos administrados por medio de un servidor central o Central

IP. Por ejemplo en el caso de utilizar teléfonos IP, dentro del proceso de señalización se debe incluir un Protocolo de Control de llamada, el cual fluye en cada uno de los teléfonos IP y la Central IP. Después de que la señalización haya sido completada, un RTP va a circular entre los dos teléfonos, la Central IP no influye completamente en la llamada, sino básicamente en el inicio y finalización de la sesión, en este caso los *routers* no realizan la creación del paquete RTP, tal como se lo hace al utilizar PBXs conectadas a interfaces E&M o teléfonos analógicos conectados a interfaces FXS, sino son los mismos dispositivos IP los que crean estos paquetes.

- Las aplicaciones de tiempo real, tal como VoIP, tienen diferentes características y requerimientos con respecto a las aplicaciones de datos tradicionales. Las aplicaciones de voz toleran pequeñas variaciones en la cantidad de retardo, estas variaciones de retardo afectan directamente a la entrega de los paquetes de voz; la pérdida de paquetes y el *jitter* degradan la calidad de las transmisiones de voz, por lo tanto por estos factores es que se debe aplicar QoS para que la calidad de la voz no se degrade. De esta manera la QoS ha encontrado la forma de optimizar una red proporcionando los algoritmos eficazmente para asegurar la entrega de la información y hacer que una red funcione eficientemente. QoS es la habilidad de poder seleccionar varios tipos de tráfico y tratarlos a cada uno dependiendo de sus necesidades; la QoS no se encuentra inherente en una infraestructura de red, la QoS es implementada para estratégicamente habilitar características apropiadas a través de la red. Por lo tanto para un correcto diseño con QoS se debería poner mucha atención a los requerimientos de capa 2 (QoS incluye FRF.12, LFI y *traffic shaping*), requerimientos de calidad de servicio tales como LLQ, RTP, dentro de lo que es administración de congestión, planificación del número total de llamadas permitidas, para no sobrepasar el ancho de banda contratado.

- En la utilización de VoIP sobre *Frame Relay*, se debe facilitar la fragmentación de los grandes *frames* de datos para permitir el entrelazado de los pequeños paquetes de voz, esta fragmentación es lograda gracias al FRF.12, debido a que

FRF.12 adhiere un *header* entendido al *frame Frame Relay* que identifica al *frame* como fragmentado e indica un número de secuencia para el reensamblado. La fragmentación es necesaria únicamente en enlaces de velocidad menor a 768 Kbps [11], por que en estos enlaces es donde puede existir el suficiente retardo como para degradar la calidad de la voz. Éste es uno de los beneficios de utilizar un red *Frame Relay*, por que a pesar de que es una red compartida, se puede aplicar mecanismos para el tratamiento de la VoIP y lograr una buena calidad en este tipo de transmisiones.

- Otro de los factores importantes a especificar en un diseño de red es la capacidad del canal, definida como la cantidad de información que puede fluir a través de una conexión de red en un período de tiempo dado. Este factor es esencial para entender el concepto de ancho de banda, y poder aplicarlo cuando se esté dimensionando una red en especial. Por ejemplo:

  - Se debe tomar en cuenta el medio que se esté usando para la construcción de la red, ya que el ancho de banda es limitado por las leyes físicas (dependiendo del material) y por la tecnología usada para colocar la información en el medio.
  - Para la adquisición de equipos, o para el alquiler de enlaces, una buena compresión de ancho de banda puede ahorrar a un usuario o a una empresa una significante cantidad de dinero. Un administrador de red necesita tomar las decisiones correctas sobre el tipo de equipos y servicios a comprar.
  - En cuanto se construyan nuevas tecnologías e infraestructuras de red para proporcionar un mayor ancho de banda, se pueden crear nuevas aplicaciones para aprovechar estas capacidades y dar varios beneficios a los usuarios.

  Sin embargo, es importante que un administrador de red considere que este factor no es gratuito; debe ser tomado muy en cuenta al diseñar y administrar la red para tratar de optimizarla lo mayormente posible, sin perder el desempeño normal de la misma, y que además se mantenga la capacidad requerida para la

voz, ya que si este se ve afectado por la carga de datos, o es disminuida por el ahorro de costos, la calidad de la voz se va a perder notablemente. Hay que considerar que la VoIP de acuerdo al MOS [tabla 3.14] posee una buena calidad de audio, pero no tan nítida como es la de la telefonía tradicional.

- La evaluación de proyectos se complementa con la planeación. La evaluación verifica y la planeación prevee, la evaluación se puede realizar utilizando criterios de costo – beneficio, costo – eficiencia, y costo – mínimo, dependiendo de la información que se posea y la facilidad para estimar los beneficios; el flujo de fondos es una herramienta que ayuda a identificar ingresos y costos, para poder establecer las necesidades de recursos o ganancias en una unidad de tiempo. En este proyecto para identificar la mejor alternativa se utilizó el criterio de costo – eficiencia o costo mínimo, ya que, la única información que se obtuvo para evaluar el proyecto financieramente entre las dos alternativas fueron los costos. Para el método de evaluación se utilizó el indicador financiero denominado "Valor Actual de Costos" que consiste en reconocer los costos por período e identificar el valor total incluyendo la valoración a precios del período base.

- El modelo del diseño, el plan a ejecutar, y la implementación de la red deben proporcionar ingresos económicos que justifiquen la inversión. El modelo es el punto de partida, y siempre debe estar sujeto a una re-reexaminación constante. Ningún modelo fijo es apropiado para una empresa. En algunas organizaciones, la información es el producto, por lo que se invierte más en una infraestructura de red. Otras organizaciones miden el éxito de acuerdo al crecimiento del rédito o a la contención del costo. Por lo tanto, la parte económica juega un papel muy importante en el diseño, para poder lograr en lo posible el mejor servicio al costo más bajo. Un administrador o un diseñador de red, debe enfocarse principalmente en los componentes que causan el incremento o disminución del costo del diseño; estos componentes generalmente son ancho de banda, una calidad de servicio garantizada, disponibilidad, seguridad y administración. Una parte estratégica dentro del proceso de diseño de una red es tratar de medir la ganancia que

involucra realizar una inversión como ésta. Generalmente las empresas usan esta herramienta como un componente financiero para tomar la decisión adecuada y medir la actuación de la empresa en el mercado.

- El utilizar una red privada para la realización de llamadas telefónicas entre sitios remotos no es la única opción para tener este tipo de comunicaciones a bajo costo. Una alternativa para la realización de comunicaciones telefónicas es utilizar una red que ya se encuentra completamente instalada y que además existe en todo el mundo, es decir el Internet. Actualmente por medio del uso del Internet, las tarifas son cobradas únicamente por el servicio, independientemente de hacia donde se realice la llamada. La telefonía en Internet reduce muchos costos, ya que la voz se encapsula en paquetes de datos, los cuales son transmitidos a través de la misma infraestructura donde viajan otros paquetes de datos cómo los de correos electrónicos, mensajería instantánea, solicitudes de HTML (navegadores), etc. El mayor potencial de la telefonía Internet está en las llamadas de larga distancia ya que es ahí donde podrá tener una reducción importante en los costos. Para quienes tengan conexiones de Internet sin cargo o a un precio fijo, las ventajas son evidentes, ya que este sistema les posibilita comunicarse con cualquier lugar del mundo a un precio inmejorable.

- La telefonía en Internet es una alternativa a la telefonía tradicional para las comunicaciones de una empresa, pero posee algunos problemas que deben ser analizados según los requerimientos y necesidades de cada compañía. Entre estos problemas se puede mencionar la fiabilidad; las tecnologías empleadas en las redes telefónicas tradicionales presentan una fiabilidad muy alta; a menudo se hace referencia a los "cinco nueves" al hablar de ella (esto es, al 99.999%, lo que significa unos pocos segundos de mal funcionamiento al año). Las tecnologías utilizadas en Internet y, en particular, las creadas alrededor de VoIP, están todavía lejos de alcanzar esas cifras. Otro de los problemas es la seguridad; como es bien conocido, la seguridad que ofrecen las redes IP y, en particular, el Internet es deficiente en algunos aspectos. Ataques del tipo de denegación de servicios o

posibles violaciones con la confidencialidad de las conversaciones son, entre otros aspectos, problemas que se encuentran presentes. Por tal razón una de las maneras de solucionar estos problemas es la implementación de calidad de servicio. A diferencia de las redes telefónicas tradicionales, que reservan y garantizan los recursos a cada llamada, el servicio "mejor esfuerzo" ofrecido por IP no es adecuado. A pesar de los grandes esfuerzos que se están invirtiendo en la definición de modelos de QoS, todavía no se ha alcanzado una solución global que permita crear un Internet con QoS. Mientras este modelo no exista, VoIP es una solución adecuada para redes IP privadas donde se puede tener la administración global de toda la red.

- La parte económica no es la única razón para que las empresas realicen inversiones en hacer converger las redes de voz y datos. Otros motivos para invertir en una red convergente son las aplicaciones. La integración de redes facilita la creación de nuevas aplicaciones que integran voz y datos, como la mensajería unificada, que permite englobar bajo un único interfaz de usuario, accesible desde cualquier parte de la red, a todos los servicios de los cuales se recibe mensajes (correo electrónico, fax, teléfonos, contestadores, etc.). O, por mencionar otros ejemplos, la integración de "centros de llamadas" en los servidores Web corporativos, que permitirá una atención rápida y especializada a los clientes; las aplicaciones de vídeoconferencia, teleenseñanza, etc.

- El éxito creciente de la telefonía por Internet o VoIP, a más de amenazar las fuentes de ingresos de los operadores nacionales de telefonía fija, especialmente respecto a la telefonía internacional, es que ahora lanza un desafío a la telefonía móvil que, en numerosos países, cuenta con más líneas que la telefonía fija. La Organización para la Cooperación y el Desarrollo Económico (OCDE) indica que las nuevas ofertas de servicios de los operadores tradicionales, como las *hotspots* wi-fi en las ciudades, serán una fuerte competencia para los operadores de

telefonía 3G[13]. En resumen otra tecnología que está creciendo en el mercado mundial es la VoIP inalámbrica. La solución consiste en Teléfonos IP inalámbricos Wi-Fi, adaptadores FXS para teléfonos convencionales, Adaptadores FXO para conexiones a la línea local telefónica y Servidores SIP para rutear llamadas IP. Es decir que si se implementa en las ciudades *hotspots* wi-fi, los usuarios que posean teléfonos *wireless* IP, tendrán características de movilidad, similar a la de los celulares pero a un costo mucho más económico, especialmente si las llamadas son internacionales.

- El diseño presentado en este proyecto habla básicamente de la implementación de VoIP sobre una red privada utilizando equipos CISCO. Dependiendo de los requerimientos de la empresa, CISCO, como en este proyecto, ofreció una alternativa a un costo literalmente económico, ya que únicamente se está utilizando el servicio de voz con QoS. El hecho de poseer una red convergente de voz y datos abre paso a la realización de varias aplicaciones que pueden ser beneficiosas para las necesidades de los usuarios. Es decir que si se desea tener una solución completa de VoIP, la convergencia da la posibilidad de implementar un sistema completo de telefonía IP. En los últimos años la adquisición de Centrales IP ha ido desplazando poco a poco a la de las PBX, ya que una Central IP ofrece más servicios que las PBXs tradicionales. Las empresas ven que las PBXs y redes basadas en TDM tenderán a desaparecer. La convergencia empieza a ser una realidad, por tal razón varios fabricantes han comenzado a desarrollar PBX con soporte IP.

- En el mercado existe una gran variedad de productos y marcas de diferentes precios. Cisco con su CallManager permite realizar aplicaciones de cualquier central IP, la desventaja de implementar un sistema completo de telefonía IP CISCO es el precio, ya que CISCO es una de las marcas más costosas en el mercado en lo que se refiere a implementación de infraestructuras de Telefonía IP.

[13] Tercera generación de telefonía móvil, en esta generación ya se considera el manejo de elementos multimedia como gráficos, video full color, y acceso a Internet.

4.2 RECOMENDACIONES

- Es muy recomendable la utilización de VoIP dentro de una empresa que posea oficinas alrededor del país y además posea una infraestructura de red de datos para las comunicaciones entre ellas, debido a que si se realiza una correcta implementación de QoS en esa red, el ancho de banda y la utilización de recursos para aplicar VoIP no es mucha. Además por medio de la utilización de VoIP la empresa optimiza los costos de las comunicaciones telefónicas, y convierte a la empresa en ágil, moderna y competitiva.

- Dentro de todos los codificadores de voz, se recomienda utilizar G.729 debido a que este codificador es el que optimiza el ancho de banda de la red, y entrega una calidad de voz aceptable para el entendimiento de la comunicación, y debido a que ha sido calificada con 3.92/5 dentro de la tabla de MOS.

- Dentro de las tecnologías que se utilizan para la WAN, en el país, básicamente las empresas ofrecen servicios portadores *Clear Channel* y *Frame Relay*, siendo *Frame Relay* una tecnología mucho más económica que un *Clear Channel*, por lo que para aplicaciones de VoIP se recomienda la utilización de enlaces *Frame Relay*. Esto se debe a que las llamadas telefónicas son esporádicas y no todo el tiempo y no es necesario tener un ancho de banda completamente fijo. Además como ya se había mencionado, existen herramientas y mecanismos de QoS específicamente para enlaces *Frame Relay*.

- Una vez implementada la red, se recomienda al administrador encargado que realice periódicamente un análisis del comportamiento de la red. El análisis de tráfico de red permitirá al administrador equilibrar la carga de la red, identificar problemas y resolverlos, perfeccionar la actuación de la red, y poder crear un plan para un posible crecimiento a futuro. En el mercado existen varias herramientas para poder realizar un correcto análisis del tráfico, existen programas de administración y monitoreo para poder tener un control centralizado de toda la red,

y tener un reporte completo de flujos de tráfico, disponibilidad de la capacidad, retardos, etc. En los últimos años, gracias a estos análisis realizados a las redes, se han encontrado reportes de ataques, por lo que los administradores han visto en la necesidad de reforzar sus diseños implementando seguridad a los mismos. La seguridad se refiere a la autenticación, control de acceso, confidencialidad e integridad de los datos, entre otras. La administración de la seguridad incluye el mantenimiento y distribución de autenticación y autorización de cierta información, tal como claves y encriptación de llaves. En otras palabras, la administración de la seguridad permite al administrador controlar quién tiene acceso a determinados recursos. Por lo que para finalizar un correcto diseño, también se recomienda realizar una inversión en la implementación de un sistema completo de seguridad y administración.

- Se ha recomendado la marca CISCO para el diseño de Calidad de Servicio debido a que a más de ser líder en el mercado de ruteadores, es la única que ofrece la posibilidad de utilizar una gran cantidad de herramientas para aplicar Calidad de Servicio a una red, además que ofrece una completa bibliografía e información, así como una variedad de productos para el desarrollo de este tipo de tecnologías como es el caso de VoIP. La desventaja de este producto es la complejidad en la utilización, debido a que para su configuración se necesita tener conocimientos avanzados de la teoría de Redes de Datos y de los comandos de su sistema operativo (IOS), a pesar de que esta marca ya posee interfaces gráficas que facilitan su configuración. Dentro de lo que es el IOS se puede implementar de una manera más fácil la QoS, esto es con AutoQoS, que es una característica reciente de CISCO que usa comandos simples para habilitar QoS para VoIP en ambientes LAN y WAN. AutoQoS reduce significativamente la cantidad de líneas de comando necesarias para soportar VoIP en la red. Por ejemplo para la WAN, Auto QoS provee las siguientes características:

  - Automáticamente clasifica el control de paquetes de VoIP
  - Provee LLQ para el tráfico de Voz

- Provee un mínimo de ancho de banda garantizado usando CBWFQ para el control del tráfico de VoIP
- Habilita *Traffic Shaping* en la WAN, cuando es requerida
- Habilita LFI y RTP

- Se puede diseñar una red con VoIP, utilizando la infraestructura antigua de teléfonos analógicos y digitales conectados a una central PBX, y ésta a su vez conectarle a un *router* y pasar las llamadas analógicas a través de la infraestructura de datos, esto en caso de querer abaratar los costos en comparación de instalar una infraestructura completa de telefonía IP. Pero si se quisiera instalar una infraestructura más robusta se recomienda hacer por medio de la telefonía IP, es decir una central IP para la administración de llamadas y teléfonos IP conectados a la red; en este caso se deberá considerar el tráfico en la LAN que producirán las llamadas telefónicas. Lo conveniente para esto es diseñar la red LAN con dispositivos en los que también se pueda aplicar calidad de servicio.

- Si se desea instalar una infraestructura con un sistema de telefonía IP, se recomienda analizar fabricantes de centrales IP. Entre estos fabricantes se puede mencionar a Alcatel, que se ha convertido en el tercer suministrador de telefonía IP para medianas y grandes empresas en los Estados Unidos. La propuesta que ha permitido a Alcatel lograr su objetivo estratégico de aumentar penetración en el mercado estadounidense es la plataforma OmniPCX 4.400.

- Otro fabricante muy recomendable es 3COM, que ha sido uno de los principales contribuidores a la industria de la convergencia desde la introducción, en 1998, de la primera PBX-IP del mundo, el sistema 3Com® NBX®. El módulo *3Com® VCX™ IP Telephony* fue introducido en 2003 para grandes empresas. Hoy, la compañía combina esos productos bajo la *Suite* de Aplicaciones Convergentes 3Com, la cual incluye Telefonía IP, Mensajería IP, Conferencia IP, y *Contact Center IP*.

- Algunas empresas han optado en desarrollar su propia Central IP, que es una de las opciones muy recomendables para la implementación de VoIP, y que además ha crecido a nivel mundial gracias al aparecimiento del protocolo de señalización SIP, que es de código abierto con el que se pueden desarrollar aplicaciones de telefonía IP. SIP abre muchas posibilidades de integración de soluciones de comunicación con aplicaciones comerciales y permite que el cliente indique por si mismo sus preferencias. Una de las marcas más conocidas que utiliza este protocolo es Asterisk. Éste es un software muy simple de utilizar y es la solución ideal para construir una Central telefónica para la casa o para la oficina. Asterisk es una central completa basada en software, y de código abierto. Puede ejecutarse en cualquier ordenador basado en Linux y provee todas las funciones que se pueden esperar de una central, y algunas más.

- Como es de conocimiento, el Internet es una red insegura, y utilizarle como medio para las comunicaciones telefónicas, especialmente cuando éstas son confidenciales, resulta un problema. Desafortunadamente existen numerosas amenazas que conciernen a las redes VoIP, muchas de las cuales no resultan obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables. La información sobre una llamada es tan valiosa como el contenido de la voz. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación; incluso puede grabar absolutamente todo, y retransmitir todas las conversaciones. Se ha hablado de las ventajas de la tecnología de telefonía IP sobre el Internet, y se ha encontrado problemas de seguridad. Afortunadamente, la situación no es irremediable. Para solucionar este problema se recomienda utilizar métodos de encriptación como VPNs (*Virtual Private Networks*), con la utilización del protocolo IPSec (IP segura) y otros protocolos como SRTP (*secure RTP*). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación. Esto ayudará a evitar cualquier tipo de amenaza. Por

último, se puede emplear un *firewall* y un IDS (*Intrusion Detection System*) para ayudar a proteger la red de voz. Los *firewalls* de VoIP son complicados de manejar y tienen múltiples requerimientos como por ejemplo el manejo de todos los puertos UDP que se abren y cierran cuando se utiliza VoIP y que pueden ser sectores vulnerables. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el costo está lejos de verse oscurecido por la cantidad de beneficios, así que se recomienda el perfeccionamiento de los controles de acceso. Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores.

- Otra de las aplicaciones que están surgiendo y que se puede implementar en un diseño de una red y que además utiliza VoIP es la vídeoconferencia. Desde hace varios años, la vídeoconferencia se ha convertido en una herramienta común para instituciones educativas, empresas y hasta para individuos, dado que es posible establecer sesiones interactivas con audio y vídeo en tiempo real. La vídeoconferencia permite a un grupo de personas ubicadas en lugares distantes llevar a cabo reuniones como si estuvieran todas en una misma sala.

REFERENCIAS BIBLIOGRÁFICAS

[1] Michael E. Flannagan, CCNA, CCDA, CISCO **QoS ADMINISTERING IP NETWORKS**, Copyright © 2001 by Syngress Publishing.

[2] Robert Padjen, Todd Lammle, CCDP™: **Cisco Internetwork Design Study Guide,** *Copyright ©2000 SYBEX , Inc., Alameda, CA*

[3] A. Anthony Bruno, CCIE No. 2738, Jacqueline Kim, **CCDA Exam Certification Guide,** Second Edition, Copyright © 2004 Cisco Systems, Inc.
Published by:
Cisco Press
800 East 96th Street, 3rd Floor
Indianapolis, IN 46240 USA

[4] Wendell Odom, Michael J. Cavanaugh, **Cisco DQOS Exam Certification Guide**
Copyright © 2004 Cisco Systems, Inc.
Cisco Press logo is a trademark of Cisco Systems, Inc.
Published by:
Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

[5] Michael E. Flannagan CCIE No. 7651, Jason Sinclair CCIE No. 9100, **Configuring Cisco Voice over IP,** Second Edition
Copyright © 2002 by Syngress Publishing, Inc. All rights reserved.
800 Hingham Street
Rockland, MA 02370

[6] Sean Christensen, **Voice over IP Solutions** Copyright © 2001, Juniper Networks, Inc. 1194 North Mathilda Avenue Sunnyvale, CA 94089 USA 408 745 2000 or 888 JUNIPER

[7] **Enterprise Voice Over Data Design (EVODD)**, Version 4.2 Copyright © 2004, Cisco Systems, Inc.

[8] Cisco System CCIP, **Designing for Cisco Interwork Solutions**, Volumen 1, version 1.0, Copyright 2002

[9] **VoIP over Frame Relay with Quality of Service**, All contents are Copyright © 1992-2003 Cisco Systems, Inc.

[10] **Voice over IP Quick Start Guide**, Cisco System, Inc., 170 West Tasman Drive San Jose, CA 2001

[11] **Implementing Cisco Quality of Service (QoS) v2.0**, Copyright 2004, KnowledgeNet.com, Inc. All rights reserved.

[12] Breyer and Riley, "**Switched and Fast Ethernet: How It Works and How to Use It**," Ziff-Davis Press, 1995

[13] **Cisco Certified Design Associate Self-Study**, Copyright Cisco Systems, Inc.- version 2.0 7/98

[14] www.recursosvoip.com

[15] www.monografias.com

[16] http://www.supertel.gov.ec/telecomunicaciones/portadores

[17] www.cisco.com

[18] www.3com.com

[19] www.juniper.net

[20] Enterprise-Class convergence and QoS: Taking it: to an Extreme, The Tolly Group, Inc, 2251 Landmark Manasquan, NJ 08736

[21] www.netequalizer.com

[22] Luís facundo Maldonado Granados, Diana Patricia Maldonado Rey, **Gestión de Proyectos en la Sociedad de la Información**, Colección ISDN Bogotá, D.C. Colombia. 2001

ANEXOS

ANEXO A

PROFORMAS DE PROVEEDORES DE SERVICIO DE PORTADORA

A.1. Servicio de Internet Corporativo, Grupo TVCABLE

A.2. Servicio de Transmisión de Datos Corporativo, Grupo TVCABLE

A.3. Propuesta de Servicios de Telecomunicaciones, IMPSAT

A.4. Cotización de Servicio de Provisión de Datos, TelcoCarrier

ANEXO A.1

SERVICIO DE INTERNET CORPORATIVO

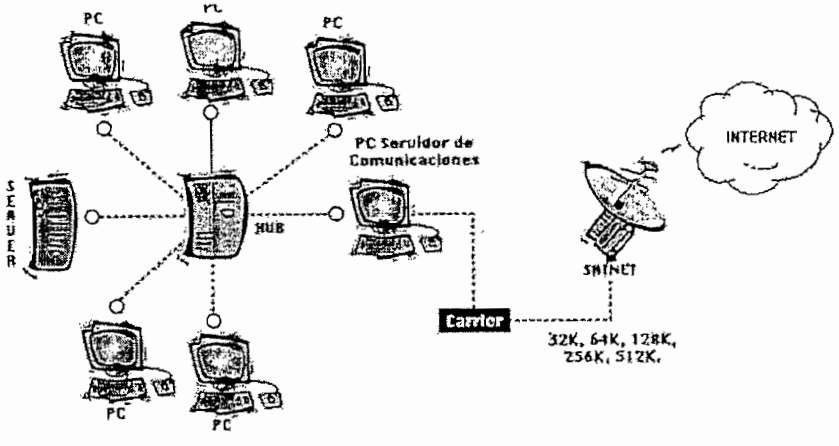
CON EL RESPALDO DE

CLIENTE:
EVOLUTIONET
Atención: SR. FERNANDO CABRERA
Ciudad: Quito
Fecha: jueves, 05 de mayo de 2005

Ponemos a su consideración la siguiente propuesta de servicios de Internet corporativo.

DIAGRAMA DE CONEXION

CONEXION DEDICADA



SERVICIO DE TRANSMISIÓN DE DATOS O ULTIMA MILLA MAS INTERNET

UM-IP MAS INTERNET	
ANCHO DE BANDA (PIR/CIR)	VALOR MENSUAL
512K/128K	$275,00
512K/256K	$395,00
INSTALACIÓN:	$300,00

EQUIPOS REQUERIDOS PROVISTOS POR EL CLIENTE

- Servidor de Internet en el cual ejecutaran los programas de Proxy Server, Mail Server.

CARACTERÍSTICAS DEL SERVICIO DE TRANSMISIÓN DE DATOS

Características de los servicios:
Servicio Premium:

- Up time: 99.6%
- Reacción frente a fallas o peticiones de servicio: 2 horas laborables
- Tiempo máximo de solución a problemas de enlace: 4 horas laborables
- Tiempo máximo frente a fallas de red troncal o de backbone: 6 horas laborables
- Soporte técnico 24 horas al día 7 días a la semana (7*24*365)

- Supervisión y administración del enlace las 24 horas del día
- Técnico asignado al cliente
- Reportes Mensuales de calidad de servicio

CARACTERISTICAS DEL SERVICIO DE INTERNET:

- Incluye hasta 6 direcciones IP, según requerimientos del cliente
- 40 MB de Hosting
- 1 cuenta Dial Up ilimitada
- Soporte para configuración de servidor Proxy, en caso que requiera el cliente.
- Si el cliente no posee dominio se proveera de hasta 20 cuentas con el dominio de Satnet.

NOTAS:

- Los precios no incluyen impuestos de ley
- Tiempo de entrega 15 días a partir de la solicitud aceptada
- Validez de oferta 30 días
- Forma de pago: prepago mensual

Saludos cordiales,

Mauricio Carrillo P.
NEGOCIOS CORPORATIVOS
GRUPO TVCABLE
mcarrillo@tvcable.com.ec
Telefono: 2992-410/415 Ext: 138
Fax: 2992-400 Ext: 203

ANEXO A.2

SERVICIO DE TRANSMISION DE DATOS CORPORATIVO

CON EL RESPALDO DE

CLIENTE:
EVOLUTIONET
ATT: SR. FERNANDO CABRERA

FECHA: jueves, 05 de mayo de 2005

Ponemos a su consideración la siguiente propuesta de servicios de transmisión de datos e internet corporativo.

SERVICIO DE TRANSMISIÓN DE DATOS INTERURBANO QUITO-SUCURSALES GUAYAQUIL-CUENCA

FRAME RELAY	
ANCHO DE BANDA	VALOR MENSUAL
64K	$440,00
128K	$760,00
256K	$1320,00
INSTALACIÓN:	$400,00

Se incluye costos de ultimas millas en los dos puntos, No se incluyen routers, costo del enlace para cada ciudad

Características del Servicio Premium:

- Up time: 99.6%
- Reacción frente a fallas o peticiones de servicio: 2 horas laborables
- Tiempo máximo de solución a problemas de enlace: 4 horas laborables
- Tiempo máximo frente a fallas de red troncal o de backbone: 6 horas laborables
- Soporte técnico 24 horas al día 7 días a la semana (7*24*365)
- Supervisión y administración del enlace las 24 horas del día
- Técnico asignado al cliente
- Reportes Mensuales de calidad de servicio

NOTAS:

- Los precios no incluyen impuestos de ley
- Se debe rentar los routers a razon de $80 cada uno, en caso de que el cliente no los tenga.
- Se requiere verificar la factibilidad en las ultimas millas.
- Tiempo de entrega 15 días a partir de la solicitud aceptada
- Validez de oferta 30 días
- Forma de pago prepago mensual

Saludos cordiales,
Mauricio Carrillo P.
NEGOCIOS CORPORATIVOS
GRUPO TVCABLE
mcarrillo@tvcable.com.ec
Telefono: 2992-410/415 Ext: 138
Fax: 2992-400 Ext: 203

ANEXO A.3

Quito, 3 de Mayo 2005

Ingeniero
Fernando Cabrera
EVOLUTION NET
Ciudad

Estimado Fernando:

Prop. Comercial Nº **200505-161**

Tenemos el agrado de dirigirnos a usted a efectos de hacerle llegar nuestra propuesta por la provisión de los servicios de telecomunicaciones que Impsat brinda a través de su Red de Banda Ancha y de servicios satelitales.

Para cubrir las necesidades de EVOLUTION NET, Impsat les propone esta alternativa de servicios, implementada con tecnología de avanzada, que permite contar con una red totalmente digital, de alta confiabilidad y disponibilidad.

Sin otro particular quedamos a vuestra entera disposición para cualquier consulta, haciendo propicia la ocasión para saludarlo muy cordialmente.

Miguel Peralta B.
S&S CORPORATE
IMPSAT ECUADOR
☎ **Phone: (593-2) 2264101 Ext. 5165**
☎ **Cel: (593-9) 9726-939**
✉ **Email: mperalta@impsat.com**

Propuesta de Servicios de Telecomunicaciones para EVOLUTION NET

Quito 3 de Mayo 2005

CONTENIDO

1] Resumen Ejecutivo

1.1. Introducción

Impsat Fiber Network Inc., tuvo sus inicios en 1990, en Argentina. Durante esa década, el modelo de negocios se exportó a siete países: Colombia, Venezuela, USA, Ecuador, Perú, Brasil y Chile, En Ecuador, la operativa fue fundada en 1995, y, como las demás, se dedicó a proveer servicios de telecomunicaciones al mercado de las grandes y medianas empresas.

Hoy, casi 10 años después, **Impsat del Ecuador** se ha consolidado como líder en el mercado de telecomunicaciones en el sector corporativo. Sus clientes y socios estratégicos son las más destacadas empresas en la banca, industria y comercio. Para quienes la multinacional desarrolla e implementa soluciones de transmisión de datos que ayudan al crecimiento de su negocio de acuerdo a las necesidades que tenga.

Impsat del Ecuador cuenta ahora con cerca de 250 clientes en todo el país. Su EBITDA (utilidades antes de intereses, impuestos, depreciaciones y amortizaciones) en el 2002 fue de 4.9 millones de dólares. Las ventas, por su lado, crecieron de 15.8 millones de dólares en el 2001 a 16.7 millones de dólares en el 2002.

Impsat en cifras

- Operaciones en 8 países en América
- Redes metropolitanas en 15 ciudades (1,000 kilómetros-ruta de fibra óptica)
- Larga distancia regional en cuatro países (más de 8.880 kilómetros-ruta)
- 14 Data Centers en las ciudades más importantes
- Foco en grandes empresas
- 2877 clientes corporativos
- Más de $1,200MM en inversiones
- **2002 Ingresos de $230 MM**
- EBITDA positivo desde 1992

Nuestra misión

"Ser líderes en la provisión de soluciones de comunicación de la más alta calidad, para el mercado latinoamericano, conformando un grupo extraordinario, que se esfuerza por añadir el máximo valor a sus clientes, manteniendo una larga y rentable vinculación para ambos"

impsat

Hitos

	1990-1 Inserción	1992-4 Exportación de un modelo exitoso	1995-8 Crecimiento	1999-2001 Expansión de la red Banda Ancha	2002 Reorganización
Entorno	Desregulación de los servicios de datos		Comienzo de las operaciones de Internet	Grandes expectivas del mercado de datos. Buena predisposición de los capitales financieros para invertir en el mercado.	Mercados Financieros y crisis en Lationamérica
Desarrollo	Comenzó la provisión de servicios de redes privadas en Argentina.	Expansión a Colombia y Venezuela	Expansion a Ecuador, México y USA	Inicio de operaciones en Brasil y conclusión del proyecto de red de Banda Ancha.	Expansion de la oferta de servicios y segmentación del mercado.
Financiamiento	Grupo Fundador	Financiación local	Acciones Privadas y deuda pública	Acciones públicas y Vendor Financing	Reestructuración financiera

Nuestra plataforma

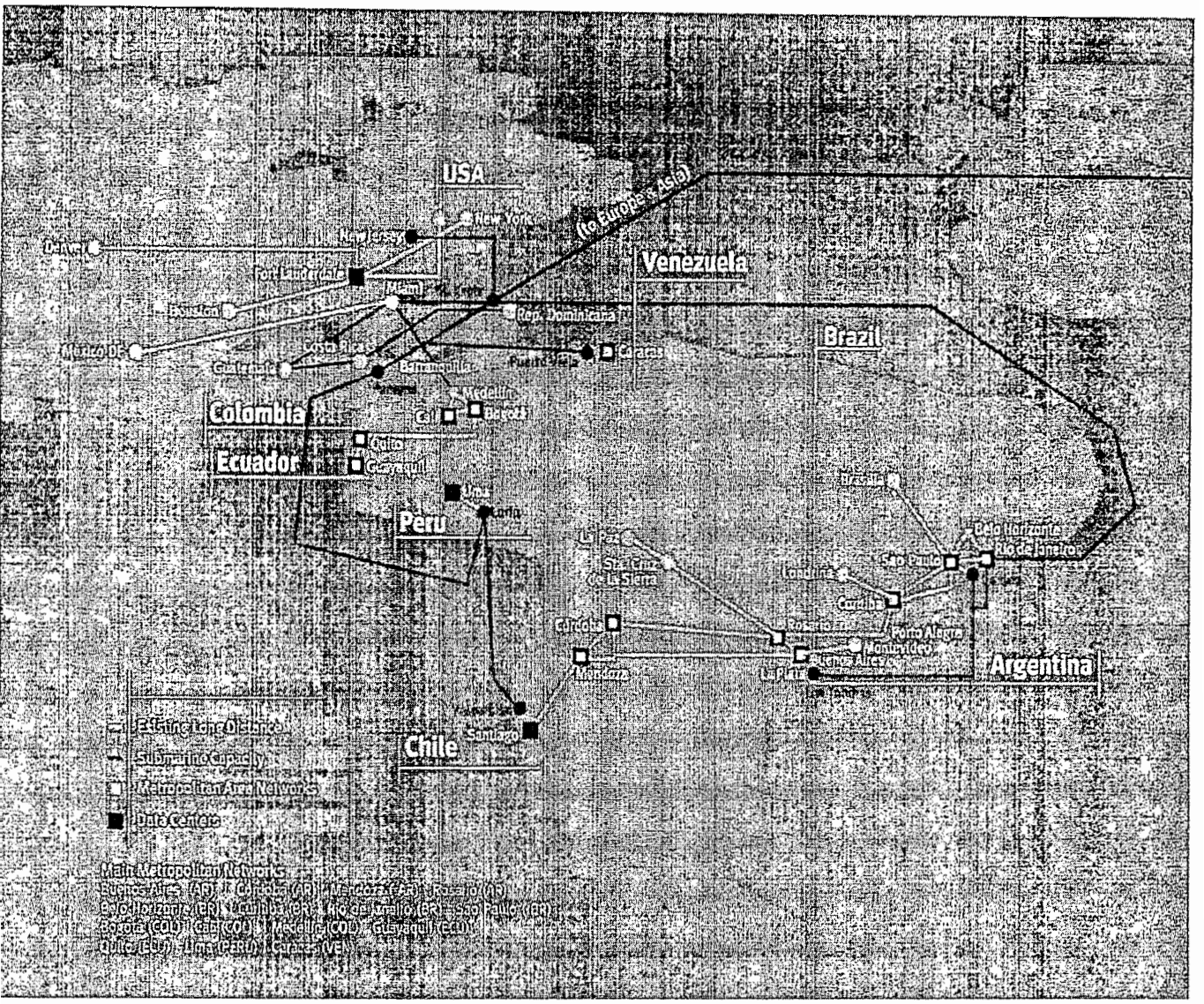
La única Red Lationamericana totalmentne integrada

Red Metropolitana y Long Haul Banda Ancha en Operación

El mejor equipo de profesionales del mercado

Una importante cartera de clientes

Nuestra red



15 áreas metropolitanas:

ARGENTINA (4) ✓ Buenos Aires ✓ Córdoba ✓ Rosario ✓ Mendoza BRAZIL (4)	PERU (1) ✓ Lima COLOMBIA (3) ✓ Cali ✓ Bogotá ✓ Medellín VENEZUELA (1) ✓ Carac

impsat

Portafolio de servicios

ransmisión de Datos — Clear Channel, Frame Relay, LAN-to-LAN, Dataplus, Vsat/IPAdvantage, Interplus.

Internet — Servicios de Backbone, Conexiones Corporativas, Acceso Dial-up Mayorista, Seguridad gerenciada, Teleworker.

Data Centers & E-Business — Web-hosting y housing, Data Center, Servicios profesionales, Soluciones de IT, Comercio electrónico, BCP.

Servicios soportados en tecnologías:

Satelital, Fibra Optica y Microondas Digitales

ImpSat

Descripción de servicios

Transmisión de datos

1. Enlaces transparentes (Clear Channel)

Los enlaces transparentes ImpSat son una solución integral de conectividad incluyendo acceso y equipamiento que posibilita enlaces digitales extremo a extremo con la mayor disponibilidad y calidad.

Los enlaces transparentes ImpSat permiten soportar las aplicaciones más exigentes en anchos de banda ya sea en enlaces punto a punto ó punto multipunto con accesos de 2.4 Kbps hasta STM-1 (155 Mbps).

Los enlaces transparentes Impsat posibilitan la conexión full-time de dos puntos de la red a través de circuitos bi direccionales de velocidad constante y totalmente transparentes. A través de interfaces estándares y vínculos urbanos, interurbanos e internacionales, le permite el desarrollo de múltiples servicios, cualquiera sea su localización, en forma rápida y eficiente.

2. Enlaces Frame Relay

Los enlaces Frame Relay ImpSat le permiten a su empresa operar con la máxima flexibilidad, confiabilidad y disponibilidad que solo la Banda Ancha de ImpSat puede garantizar.

Los enlaces Frame Relay ImpSat permiten soportar las aplicaciones más exigentes en anchos de banda, de enlaces punto multipunto con accesos de 9,6 Kbps hasta 34 Mbps (E3).

El cliente podrá contar con enlaces seguros y disponibles en todo momento gracias a una optima planificación del caudal de información utilizado.

Por cada acceso con los sitios a los que usted necesita enlazarse, se definen previamente los Circuitos Virtuales permanentes (PVC).

Cada PVC tiene asignada una velocidad de transferencia de información mínima (CIR), garantizada por la red, de acuerdo con las necesidades de las aplicaciones de su empresa. Y, si así lo requiere su actividad, podrá utilizar mayor velocidad de transferencia de información en la hora pico, que la mínima garantizada (hasta un máximo determinado por la velocidad física del acceso)

El servicio Frame Relay ImpSat brinda ventajas decisivas en:

- Reducción de costos del cliente en la adquisición de equipos.
- Racionaliza los costos gracias a la planificación del uso de la red.

3. Lan to Lan

Lan to Lan de ImpSat permite integrar las necesidades de comunicaciones del cliente al interconectar redes de área local (LAN´s) que se encuentran dispersas geográficamente.

A través de la generación de una plataforma base para el desarrollo de intranets, favorece la eficiencia de las comunicaciones dentro de la empresa, optimizando los procesos de negocios, con las siguientes características y beneficios.

- La conexión IP se establece vía fibra óptica
- La integración de las LAN´s a muy altas velocidades evita la congestión de las soluciones tradicionales.
- Se asegura la gestión integrada de la red.
- Permite compartir los recursos y la información en tiempo real.
- El monitoreo del servicio durante las 24 horas, los 365 días, garantiza calidad y conexión permanente.
- El equipamiento provisto para el servicio (routers) evita riesgos tecnológicos para el cliente.
- Asegura un máximo control del gasto en comunicaciones gracias a la tarifa plana.

4. Dataplus

Solución satelital diseñada para transferir grandes caudales de información entre dos ó más puntos del territorio. Un servicio diseñado de acuerdo a los requerimientos del cliente y con total adaptabilidad a sus equipos informáticos.

La solución Dataplus utiliza la capacidad satelital que IMPSAT posee en Intelsat y Panamsat.

5. Vsat/IP Advantage

Las soluciones satelitales VSAT e IP Advantage están diseñadas para interconectar puntos distantes y distribuidos en un gran territorio, mediante microestaciones terrenas ubicadas según sus necesidades, en línea con los equipos informáticos de la empresa.

Las soluciones VSAT e IP Advantage de IMPSAT permiten transmitir datos, voz (canal de orden) a puntos dispersos dentro del territorio nacional.

6. Interplus

La solución satelital Interplus esta desarrollada para las corporaciones internacionales que requieran la transmisión simultanea de diversos tipos de información, teles como datos, voz desde diferentes lugares del mundo donde se realizan sus actividades financieras y comerciales, y también para empresas locales con oficinas u operaciones en el exterior.

Internet

1. Servicios de Backbone

El servicio de Backbone IMPSAT, permite generar de forma autónoma, políticas de intercambio de información dentro de la red.

El servicio de Backbone esta desarrollado especialmente para: Portales, Internet Service Providers (ISP´s), Applications Service Providers (ASP´s), proveedores de acceso gratuitos y compañías de telecomunicaciones.

El servicio de Backbone de Internet IMPSAT ofrece los siguientes beneficios:

- IMPSAT Cuenta con la Red de Banda Ancha en América Latina con más de 100 puntos de presencia en la región. En Colombia IMPSAT pertenece al NAP, siendo uno de los proveedores que genera mayor tráfico de Internet.
- IMPSAT tiene presencia operativa en Estados Unidos, con capacidad técnica de gestión y objetivos estratégicos para generar acuerdos de interconexión.
- Garantía de niveles de calidad según requerimientos del cliente (sistemas gerenciados)
- Sistema integral de gestión. Soporte técnico 24X7 a través del CAC (Centro de Atención al Cliente)
- Equipo de especialistas altamente calificados.
- Alto nivel de redundancia que garantiza máxima disponibilidad.
- Herramientas de monitoreo, Auditoría y gestión.

El servicio de Backbone de Internet IMPSAT presenta las siguientes características y tipos de servicio:

- Full E1 (2 Mbps)
- Full y fraccional – Escalables de a 1 Mbps: E3 (34 Mbps), DS3 (45 Mbps), STM1 (155 Mbps).
- Provisión de conectividad al Backbone de Internet en modalidad simétrica y asimétrica.
- Conectividad al Backbone nacional e internacional.
- Ruteo estático y BGPv4.

2. Acceso dedicado

El acceso dedicado IMPSAT provee un vínculo exclusivo entre su compañía e Internet, sin compartir el acceso con otros usuarios. Atiende las necesidades generadas por navegación, correo, acceso a aplicaciones a web, implantación de VPN (Redes Privadas Virtuales)

Este servicio esta desarrollado especialmente para Corporaciones, Empresas, Instituciones, Organizaciones, Comercio, Microempresas y profesionales.

El servicio de acceso dedicado IMPSAT, ofrece velocidades E1 fraccionales (nX64 Kbps) y E1 full (2 Mbps).

3. Acceso Dial up Mayorista

Ofrece a su empresa u organización toda la infraestructura necesaria para permitir la oferta de servicios de Internet Dial –Up a sus clientes o usuarios, sin necesidad de inversiones en equipamientos ni adquisición de know how.

Acceso Dial Up mayorista IMPSAT le permite focalizar sus actividad en las áreas clave de su negocio desligándolo de la complejidad y el riesgo de poseer infraestructura propia. Es un servicio desarrollado especialmente para Empresas, Internet Service Providers (ISP´s), Proveedores de Acceso Gratuito y Portales.

Las características y tipos de servicios del acceso Dial Up Mayorista son:

- Puertos exclusivos (con ó sin líneas telefónicas)
- Puertos virtuales (cobertura geográfica dinámica)
- Paquetes de cuentas
- Flexibilidad en el ancho de banda y usuarios por puerto.
- Sistemas de administración de usuarios.

4. Seguridad Gerenciada

El conocimiento y experiencia en la tecnología de Internet y en Seguridad Informática permite que Impsat sea la mejor opción para cubrir las necesidades que implican estar conectado en forma confiable a la red de redes.

Las soluciones de seguridad se administran desde el SOC (Security Operation Center) de Impsat en Argentina, vía Internet o vía Telefónica, con un constante monitoreo de las funcionalidades de los sistemas de seguridad que garantiza la permanente prestación de los servicios contratados. Y por sobre todo, el sólido respaldo de nuestros expertos en seguridad, certificados en las tecnologías de software y hardware más representativas del mercado.

El servicio incluye:

- Equipamiento en venta, alquilado o financiado
- Las licencias SW y sus actualizaciones

- Paquete integrado de administración, que consiste en:
  - Monitoreo 7x27 de la funcionalidad del firewall
  - Backup de la configuración del firewall
  - Updates y hot fixes que afecten la funcionalidad del firewall
  - Cambios mensuales de políticas
  - Interfaces para auditorias de políticas

Opcionales:

- Antivirus
- Scanning perimetral
- IDS (Sistema de Detección de Intrusos)
- Autenticación fuerte
- Consultoría

Tecnologías

- Nokia Checkpoint
- Cisco Pix
- SonicWall

5.- Teleworker

Una tecnología que le permite utilizar aplicaciones como correo electrónico, intranets, extranets y servidores de archivos que utiliza en su lugar de trabajo, sin estar ahí. Todo con absoluta seguridad, utilizando la red pública de Internet y la más novedosa y eficiente tecnología de encripción de datos, IPSEC, conformando una Red Privada Virtual o "Virtual Private Network" (VPN).

Datacenter

1. Hosting dedicado y compartido

Los servicios de hosting dedicado y compartido consisten en la integración de equipamiento de hardware de servidores, dispositivos de almacenamiento, software de base, subsistemas de administración asociados, utilitarios y herramientas de acceso remoto a través de vínculos de comunicaciones a su medida, en forma dedicada ó compartida, con servicios de respaldo de la información (backup) incluidos.

Indicado para empresas que no dispones de espacio para implementar ó ampliar su centro de procesamiento de datos, o grandes empresas que prefieran implementar en modo aislado un nuevo servicio ó aplicación para que no interfiera en su operación de IT. También recomendado para incubadoras, ISP´s, ASP´s y puntoComs.

2. Housing

Consiste en la provisión de espacio físico para alojamiento de equipamiento de clientes, ofreciendo energía eléctrica, aire acondicionado, seguridad, accesibilidad y conectividad.

Diseñado para instalar equipos de servidores, unidades de almacenamiento de datos y comunicaciones, permite la total administración y procesamiento de sus aplicaciones, con permanente monitoreo de presencia activa de los servidores.

El servicio de housing IMPSAT ofrece de tres formas de alojamiento de equipamiento:

- Full Rack y minirack
- Jaulas privadas
- Salas Privadas (Private room)

3. Datacenter

Los Datacenter IMPSAT están diseñados para albergar con total seguridad las soluciones de IT y/o Internet de las empresas optimizando el desempeño y calidad de los servicios y mejorando la estructura de costos de las empresas.

Otros servicios que presta el Datacenter son:

- Housing de Aplicaciones: Incluye la provisión de recursos de hardware, software y storage utility para el albergue, administración y operación de aplicaciones.
- Recuperación de Desastres: Esta solución abarca la provisión de servicios de Back Up de servidores y unidades de almacenamiento de datos existentes en centros de computo de clientes, contemplando la recuperación de bibliotecas, datos y procedimientos de emergencia ante situaciones de contingencia.
- Storage Utility
- Gerenciamiento de Bases de Datos
- Balanceo de Carga, Cache y distribución de contenido.
- Seguridad

4. BCP Business Continuity Plan

BCP (Plan de Continuidad de Negocios) es el conjunto de operaciones, procesos y procedimientos probados que aseguran la continuidad estratégica del negocio, garantizando la operación de misión crítica que genera los ingresos, ante las interrupciones graves del servicio cortas o largas (daños en equipos críticos, descargas eléctricas, desastres de la naturaleza, atentados terroristas, etc.)

IMPSAT ofrece la metodología validada internacionalmente con ingenieros certificados. La metodología permite:

- Definir objetivos del plan de continuidad de negocios
- Obtener y mantener el respaldo de la alta gerencia
- Asignar los recursos y el tiempo necesario para construir el plan

- Probar, mantener y actualizar permanentemente el BCP.

1.2. CAC Y NOC

Es intención de Impsat proporcionar a través de este punto la mayor información posible nuestros teléfonos de contactos para servicio al cliente en horario 24/7.

DIRECCION	QUITO	GUAYAQUIL
	Urbanización Iñaquito Alto	Parque Tecnológico ESPOL
	Calle Juan Díaz N37-111	La Prosperina
	Quito-Ecuador	Guayaquil-Ecuador
SERVICIO AL CLIENTE	**CAC**	**NOC**
Horario 24/7	7h00 a 18h59	19h00 a 6h59
Teléfonos	593-2-264101 Ext. 5110, 5111, 5112, 5113, 5114	593-2-264101 Ext. 5115, 5116, 5117, 5118, 5119
Celulares	593-9-9830226/227/228/186	593-9-9830226/227/228/186

2] Propuesta Técnica

2.1 CARACTERISTICAS TÉCNICAS

La propuesta técnica de Impsat es proveer a EVOLUTION NET una solución de comunicaciones confiable, de gran desempeño y escalable.

En las oficinas de Cuenca y Guayaquil se proveerá de un acceso dedicado de 256 kbps, los mismos que por medio de nuestras troncales se enlazarán a nuestro Telepuerto ubicado en la ciudad de Quito.

A partir de aquí, por medio de un canal de 512 Kpbs , se transportará la información encriptada proveniente de Guayaquil y Cuenca hasta las oficinas de EVOLUTION NET en la ciudad de Quito ubicadas en la calle Páez N24-42.

Los equipos de routing que permitan la administración y gestión de los canales son propiedad de EVOLUTION NET.

3] Propuesta Comercial

La siguiente es nuestra propuesta económica para la implementación de la solución integral de Telecomunicaciones, de acuerdo con las configuraciones descritas anteriormente.

SERVICIOS PORTADORES DE COMUNICACIONES DE DATOS EVOLUTION NET					
roducto	Capacidad	Desde	Hasta	COSTO MENSUAL DEL SERVICIO	COSTO INSTALACION UNICA VEZ
Oficinas Quito:					
ervicio teledatos - Acceso última milla EVOLUTION			EVOLUTION NET - QUITO		
ET Quito - Páez N24-42 - 512 KBPS	512 KBPS	TELEPUERTO QUITO			
Oficinas Guayaquil:					
ervicio teledatos - Acceso última millaEVOLUTION			EVOLUTION NET - GUAYAQUIL		
ET - BOYACA Y CLEMENTE BALLEN	256 KBPS	TELEPUERTO GUAYAQUIL			
RONCAL FRAME RELAY QUITO - GUAYAQUIL	256 KBPS	TELEPUERTO QUITO	TELEPUERTO GUAYAQUIL		
Oficinas Cuenca:					
ervicio teledatos - acceso última milla EVOLUTION			EVOLUTION CUENCA		
ET - AV. AMERICAS Y JUAN LARREA	256 KBPS	NODO CUENCA			
RONCAL UIO CUENCA	256 KBPS	NODO CUENCA	TELEPUERTO QUITO		
		Total		*$ 2.656,25*	*$ 2.200,00*

3.1. Condiciones Comerciales

Precio: Los precios indicados en la presente oferta son en Dólares Estadounidenses y no incluyen los impuestos de ley correspondientes.

Duración del Contrato: El cargo mensual se ha calculado teniendo como base una duración del contrato de prestación de servicios de (12) meses.

Alcance de los Cargos

Instalación: Comprende el proyecto de instalación, el transporte de todos los materiales y equipamiento involucrado y el pago de las tasas a los organismos gubernamentales correspondientes para cada uno de los servicios contratados.

Cargo Mensual: Comprende la provisión del servicio, el alquiler de equipos, el enlace de interconexión de última milla, el mantenimiento preventivo y correctivo del equipamiento, el pago de las tasas correspondientes al estado ecuatoriano y actualización tecnológica.

Forma de Pago

Cargos Único por Habilitación e Instalación:

- 50% del valor con la Orden de Servicio.
- 50% dentro de los cinco (5) días hábiles siguientes a la recepción satisfactoria de cada una de las instalaciones.

Cargo Mensual

El cargo mensual se pagará por adelantado, dentro de los cinco (5) primeros días hábiles del mes, contra presentación de la cuenta de cobro respectiva.

Impuestos

Instalación: Los cargos de instalación pagan el 12% del IVA.

Cargo Mensual: Los cargos mensuales se dividen en 2 partes:

- 52% como Servicio de Telecomunicaciones el cual se grava el 12% del IVA, más el 15% de impuestos al Agua y al Deporte.
- 48% como Renta de equipos el cual se grava el 12 % de IVA.

Porcentaje total aplicado: 19,8%.

Iniciación del Servicio: ImpSat empezará a prestar sus servicios de anillo de fibra óptica sobre infraestructura de IMPSAT en un plazo estimado no mayor a 15 días, contados a partir de la fecha de la firma del contrato respectivo, o de la aceptación por escrito por parte de su empresa y siempre y cuando los requisitos de instalación a cargo de **EVOLUTION NET** hayan sido completados a satisfacción de ImpSat. Los trabajos empezarían a partir del día 20, en caso de aceptación se propondrá el cronograma respectivo.

Garantía: ImpSat se compromete a prestar el servicio ofrecido con equipos de la más alta calidad. En el caso de que dichos equipos no funcionen adecuadamente, se cambiarán por otros similares que presten la calidad del servicio ofrecida.

Mantenimiento: Tanto el mantenimiento preventivo como correctivo de los equipos y programas involucrados dentro del servicio ofrecido por ImpSat a **EVOLUTION NET** están incluidos dentro del valor del cargo mensual.

Propiedad de los Equipos: Los equipos empleados por ImpSat para la prestación del servicio son propiedad de ImpSat, y el hecho de que sean instalados en las oficinas o dependencias de **EVOLUTION NET**, no representa derechos de propiedad sobre los equipos por su parte.

Validez de la Oferta: La presente oferta es válida por treinta (30) días contados a partir de la fecha de recibo de la misma por parte de **EVOLUTION NET**.

3.2. Coordinación de Actividades

Las actividades a realizarse para la instalación de los servicios ofrecidos en esta oferta son las siguientes:

A cargo de ImpSat

- Inspección de los sitios de instalación y elaboración de los planos o esquemas de instalación de ductos, bases penetrantes, etc. Cuando corresponda.
- Provisión y montaje de las bases no penetrantes, cuando corresponda.
- Instalación de las unidades interiores y demás equipos electrónicos y tendido del cableado dentro de los edificios de **EVOLUTION NET**, incluyendo la sujeción de los mismos.
- Interacción con **EVOLUTION NET** para las actividades de Ingeniería de Aplicaciones
- Puesta en marcha del sistema y verificación de los enlaces.

A cargo de EVOLUTION NET:

- Tramitación y obtención de los permisos correspondientes ante la copropiedad de los edificios para la instalación, cuando corresponda.
- Recepción y protección de los equipos electrónicos hasta el día de la instalación.
- Construcción de las bases penetrantes de hormigón y de los ductos para cables, de acuerdo con los informes de inspección de los sitios, presentados por ImpSat.
- Provisión e instalación de pararrayos, el cableado correspondiente y varillas de tierra, de acuerdo con los informes de inspección de los sitios, presentados por ImpSat.
- Mejoramiento de los sistemas de tierras e instalación de pararrayos, cuando corresponda.

- Provisión de torres para radios y de "racks" para instalar los equipos. En caso de no disponerse de los mismos, ImpSat los podrá proveer a solicitud de **EVOLUTION NET**, con un costo adicional.
- Provisión de alimentación de energía eléctrica regulada, de acuerdo a instrucciones a proporcionar por parte de ImpSat, incluyendo circuitos independientes desde los tableros generales, con sus respectivas protecciones y cumpliendo las especificaciones de estabilidad y tensión entre fase y neutro, y entre neutro y tierra.
- Protección de los equipos interiores contra humedad, polvo y otros agentes contaminantes o nocivos. De requerirse aire acondicionado en algún caso, dicha circunstancia será informada oportunamente a **EVOLUTION NET.**

ANEXO A.4

TelcoCarrier

Quito, mayo 5 de 2005

Señores
EVOLUTIONET
Attn: Ing. Fernando Cabrera
Gerente de Tecnología
Páez N24-42 y Mercadillo (cerca Cordero)
Ciudad
Telf.: 249.2802 ***Celular: 09.619.8139***
e-mail: fercab30@uio.telconet.net

Estimado Ing. Cabrera,

Agradecemos sobremanera su gentil solicitud, y tengo el agrado de ofertarle nuestro servicio para provisión de trasmisión de datos para sus diferentes locaciones a nivel nacional.

Las condiciones de provisión para los equipos que se cotizan a continuación son las siguientes:

Condiciones de provisión:

Forma de Pago:	*Instalación y arriendo mensual por adelantado.*
Tiempo/entrega:	*20 días laborables*
Validez de la oferta:	*30 días*
Plazo del contrato:	*1 año (12 meses) renovables*
Garantía:	*Las indicadas por los fabricantes de cada uno de los productos.*
Instalación:	*Los costos de instalación son únicos y dependen del tipo de tecnología, mas no del Servicio. El tiempo de legalización del enlace es de 45 días corridos, si el cliente requiere instalación urgente deberá someterse a las* ***posibles*** *multas o penalizaciones que dictamina la ley y la Superintendencia de Telecomunicaciones.*

Sin otro particular, y esperando llenar sus expectativas aprovecho la ocasión para extender mis respetuosos saludos.

Cordialmente,

Mercedes Landeta
Gerente de Cuentas Corporativas
TELCONET S.A.
Cel: 09.607.5434
Telf. 259.9216 ext. 151
e-mail: mlandeta@uio.telconet.net meles@uio.telconet.net
www.telcocarrier.net
www.uio.telconet.net

Telco Carrier

ALTERNATIVA FIBRA ÓPTICA
INSTALACION NODO MATRIZ QUITO Y GUAYAQUIL(un solo pago)

Cantidad	Descripción	Precio Unitario	Precio Total
1	**Instalación de Nodo de Fibra Óptica enlace Quito - Guayaquil** Instalación y configuración de Fibra Optica (Un solo pago) **Transceiver** Tranceiver de FO a cable UTP **Fusión** Fusión de la Fibra Optica para conectar al backbone de Telconet **Conexión de red** Punto de red con cable UTP categoria 5 **Configuración del sistema operativo de red** Configuración e instalación de los servicios del Linux Servidor de correo electrónico Servidor de Web Servidor Domain Name Services (DNS), File Transfer Protocol (FTP) y Telnet. Servidor Proxy **Nota:** El cliente debe proveer un equipo con las siguientes caracteristicas: *Procesador Intel Pentium 4* *128 Mb de memoria RAM* *20 Gb libres en disco duro* *Dos (2) tarjetas de red* *Sistema operativo de red LINUX (Provisto por Telconet)*	1.000	1.000
	SubTOTAL		1.000,0
	12% I.V.A.		120,0
	TOTAL		1.120,0

COTIZADO EN: *USD DOLARES AMERICANOS*

Telco Carrier

RADIO ENLACE NACIONAL
INSTALACION (UN SOLO PAGO)

Cantidad	Descripción	Precio Unitario	Precio Total
1	**Instalación Radio Enlace para Quito - Cuenca** Instalación y configuración del Radio Enlace. **Mástil** Mástil metálico de hasta 5 metros de altura con empotramiento **Caja protectora** Caja contra intemperie para proteger al Bridge **Conexión eléctrica** Punto eléctrico para alimentación del Bridge **Conexión de red** Punto de red con cable UTP nivel 5 **Configuración de bridge** Alineamiento de antenas y configuración de los bridges dentro de la red de datos **Configuración del sistema operativo de red** Configuración e instalación de los servicios del Linux Servidor de correo electrónico Servidor de Web Servidor Domain Name Services (DNS), File Transfer Protocol (FTP) y Telnet. Servidor Proxy **Nota:** El cliente debe proveer un equipo con las siguientes caracteristicas: *Procesador Intel Pentium 4* *128 Mb de memoria RAM* *20 Gb libres en disco duro* *Dos (2) tarjetas de red* *Sistema operativo de red LINUX (Provisto por Telconet)*	1.000	1.000
	SubTOTAL		1.000,0
	12% I.V.A.		120,0
	T O T A L		1.120,0

COTIZADO EN: *USD DOLARES AMERICANOS*

Telco Carrier

RED PRIVADA: TARIFA MENSUAL SEA UIO-GYE ó UIO-CUE

Cantidad	Descripción	Precio Unitario	Total con IVA
1	**Enlace Nacional: Tarifa Mensual (128 Kbps)**	650	728
1	**Enlace Nacional: Tarifa Mensual (256 Kbps)**	1.000	1.120
	Arrendamiento mensual de la infraestructura de última milla: Quito - otras ciudades		
	Soporte técnico		
	Soporte técnico telefónico y monitoreo 7x24x365		
	Respaldo		
	Equipos de respaldo con la finalidad de solventar cualquier desperfecto en un máximo de 2 horas en predios metropolitanos y 4 en provincia		
	Ancho de banda		
	Simétrico: 128/128 - 256/256 Kbps up and downlink		
	Ampliación de ancho de banda		
	Los enlaces propuestos pueden soportar ampliaciones de hasta 150 Mbps.		
	Garantía de funcionamiento		
	Considerando el tipo de tecnología ofrecido por Telconet, se extiende una garantía de funcionamiento del 99%		
	El 1% del tiempo sin servicio incluye fallas y mantenimiento de última milla.		
	Enlace principal que dispone Telconet entre Quito y Guayaquil		
	Telconet dispone de un enlace propio de microonda terrestre SDH entre Quito, Guayaquil y Cuenca		
	Ancho de banda: 1 STM-1 (155 Mbps)		
	Disponiblidad: 99.9%		

COTIZADO EN: *USD DOLARES AMERICANOS*

ANEXO B

DATA SHEET DE CISCO 2800 SERIES INTEGRATED SERVICES ROUTERS

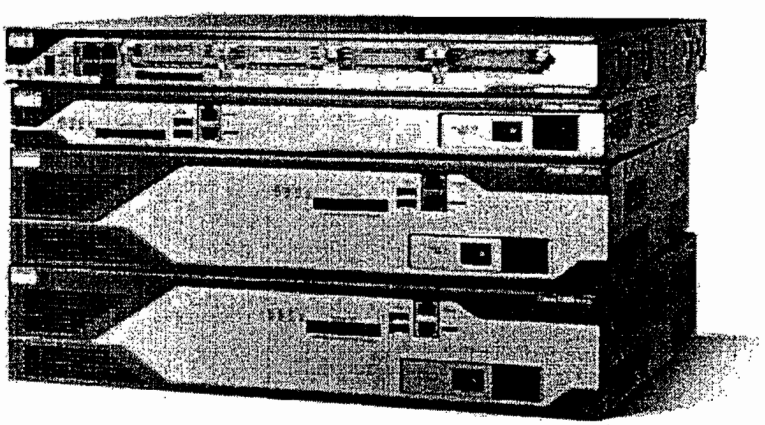
CO SYSTEMS

TA SHEET

CISCO 2800 SERIES INTEGRATED SERVICES ROUTERS

sco Systems®, Inc. is redefining best-in-class enterprise and small- to- midsize business routing with a new line of egrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, video, and reless services. Founded on 20 years of leadership and innovation, the Cisco® 2800 Series of integrated services uters (refer to Figure 1) intelligently embed data, security, voice, and wireless services into a single, resilient system fast, scalable delivery of mission-critical business applications. The unique integrated systems architecture of the sco 2800 Series delivers maximum business agility and investment protection.

gure 1. Cisco 2800 Series



RODUCT OVERVIEW

e Cisco 2800 Series comprises four platforms (refer to Figure 1): the Cisco 2801, the Cisco 2811, the Cisco 2821, and the Cisco 2851. The Cisco 00 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold formance improvement, up to a tenfold increase in security and voice performance, embedded service options, and dramatically increased slot formance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, sco 2600, and Cisco 3700 Series.

e Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL nnections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion vention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide ge of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements l advanced applications.

ECURE NETWORK CONNECTIVITY FOR DATA, VOICE, AND VIDEO

curity has become a fundamental building block of any network. Routers play an important role in any network defense strategy because curity needs to be embedded throughout the network. The Cisco 2800 Series features advanced, integrated, end-to-end security for the delivery converged services and applications. With the Cisco IOS® Software Advanced Security feature set, the Cisco 2800 provides a robust array of mmon security features such as a Cisco IOS Software Firewall, intrusion prevention, IPsec VPN, advanced application inspection and control, cure Shell (SSH) Protocol Version 2.0, and Simple Network Management Protocol (SNMPv3) in one secure solution set. Additionally, by egrating security functions directly into the router itself, Cisco can provide unique intelligent security solutions other security devices cannot, ch as network admissions control (NAC) for antivirus defense; Voice and Video Enabled VPN (V3PN) for quality-of-service (QoS) enforcement gen combining voice, video, and VPN; and Dynamic Multipoint VPN (DMVPN) and Easy VPN for enabling more scalable and manageable PN networks. In addition, Cisco offers a range of security acceleration hardware such as the intrusion-prevention network modules and advanced tegration modules (AIM) for encryption, making the Cisco 2800 Series the industry's most robust and adaptable security solution available for anch offices. As Figure 2 demonstrates, using a Cisco 2800 Series uniquely enables customers to deliver concurrent, mission-critical data, voice, d video applications with integrated, end-to-end security at wire-speed performance.

ONVERGED IP COMMUNICATIONS

s shown in Figure 2, the Cisco 2800 Series can meet the IP Communications needs of small-to-medium sized business and enterprise branch fices while concurrently delivering an industry-leading level of security within a single routing platform. Cisco CallManager Express (CME) an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones, including wired and cordless WLAN ones. This solution is for customers with data-connectivity requirements interested in deploying a converged IP telephony solution for up to 72 phones and-as of Cisco IOS 12.3(11) release-for up to 96 IP phones. With the Cisco 2800 Series, customers can securely deploy data, voice, and telephony on a single platform for their small-to-medium sized branch offices, helping them to streamline their operations and lower their network sts. The Cisco 2800 Series with optional Cisco CME support offers a core set of phone features that customers require for their everyday business eds and takes advantage of the wide array of voice capabilities that are embedded in the Cisco 2800 Series (as shown in Table 1) together with tional features available in Cisco IOS Software to provide a robust IP telephony offering for the small to medium-sized branch-office environment.

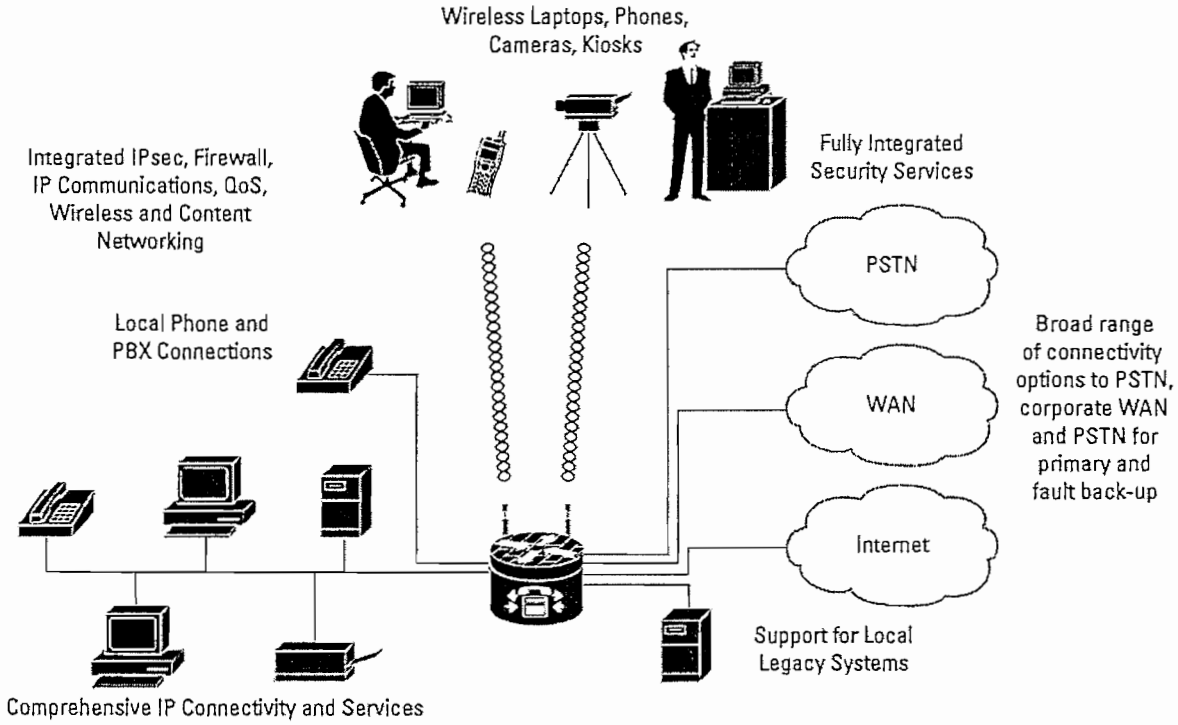
IRELESS SERVICES

ıe Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless rvices enable greater mobility for employees, partners, and customers, resulting in increased productivity. The Cisco 2800 Series supports an tegrated access point for wireless LAN connectivity, Wi-Fi Hotspot services for public access, wireless infrastructure services for cordless *LAN telephony and* for larger sites, and land mobile radio over IP for radio users.

TEGRATED SERVICES

gure 2 also highlights the fact that with the unique integrated services architecture of the Cisco 2800 Series, customers can now securely deploy Communications with traditional IP routing while leaving interface and module slots available for additional advanced services. With the optional tegration of a wide array of services modules, the Cisco 2800 Series offers the ability to easily integrate the functions of standalone network pliances and components into the Cisco 2800 Series chassis itself. Many of these modules, such as the Cisco Network Analysis Module, Cisco ice Mail Module, Cisco Intrusion Detection Module, and Cisco Content Engine Module, have embedded processors and hard drives that allow em to run largely independently of the router while allowing management from a single management interface. This flexibility greatly expands the tential applications of the Cisco 2800 Series beyond traditional routing while still maintaining the benefits of integration. These benefits include se of management, lower solution costs (CAPEX and OPEX), and increased speed of deployment.

gure 2. Secure Network Connectivity with Converged IP Communications (Update figure with WLAN connectivity to 1 laptop, 1 cordless WLAN phone, and 1 WLAN access point)



chitecture-Features and Benefits

e Cisco 2800 Series architecture has been designed specifically to meet the expanding requirements of enterprise branch offices and small-to-dium-sized businesses for today's and future applications. The Cisco 2800 Series provides the broadest range of connectivity options in the lustry combined with leading-edge availability and reliability features. In addition, Cisco IOS Software provides support for a complete suite transport protocols, Quality-of-Service (QoS) tools, and advanced security and voice applications for wired and wireless deployments.

ble 1. Architecture-Features and Benefits

eature	Benefit
lodular Architecture	• A wide variety of LAN and WAN options are available. Network interfaces can be upgraded in the field to accommodate future technologies. • Several types of slots are available to add connectivity and services in the future on an "integrate-as-you-grow" basis. • The Cisco 2800 supports more than 90 modules, including most of the existing WICs, VICs, network modules, and AIMs (Note: the Cisco 2801 router does not support network modules).
mbedded Security Hardware cceleration	• Each of the Cisco 2800 Series routers comes standard with embedded hardware cryptography accelerators, which when combined with an optional Cisco IOS Software upgrade help enable WAN link security and VPN services.
ncreased Default Memory	• The Cisco 2811, 2821, and 2851 Routers offer 64 MB of Flash and 256 MB of DRAM memory. • The Cisco 2801 router comes with 64 MB Flash and 128 MB DRAM memory.
ntegrated Dual Fast Ethernet r Gigabit Ethernet Ports	• The Cisco 2800 Series provide two 10/100 on the Cisco 2801 and Cisco 2811 and two 10/100/1000 on the Cisco 2821 and Cisco 2851
eature	Benefit
upport for Cisco IOS Software elease 12.3T Feature Sets	• The Cisco 2800 helps enable end-to-end solutions with full support for the latest Cisco IOS Software-based QoS, bandwidth management, and security features. • Common feature and command set structure across the Cisco 1700, 1800, 2600, 2800, 3700 and 3800 series routers simplifies feature set selection, deployment, management, and training.
ptional Integrated Power Supply for istribution of Power Over Ethernet PoE)	• An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.
ptional Integrated Universal DC ower Supply	• On the Cisco 2811, 2821, and 2851 routers an optional DC power supply is available that extends possible deployments environments such as central offices and industrial environments (Note: not available on the Cisco 2801).
ntegrated Redundant-Power-Supply RPS) Connector	• On the Cisco 2811, 2821, and 2851 there is a built in external power-supply connector that eases the addition of external redundant power supply that can be shared with other Cisco products to decrease network downtime by protecting the network components from downtime due to power failures.

odularity-Features and Benefits

e Cisco 2800 Series provides significantly enhanced modular capabilities (refer to Table 2) while maintaining investment protection for customers. e modular architecture has been redesigned to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, d fully integrated power distribution to modules supporting 802.3af PoE or Cisco in-line power, while still supporting most existing modules. ith more than 90 modules shared with other Cisco routers such as the Cisco 1700, 1800, 2600, 3700, and 3800 series, interfaces for the Cisco 2800 ries can easily be interchanged with other Cisco routers to provide maximum investment protection in the case of network upgrades. In addition, ting advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing ge network rollouts, and maintaining configurations across a variety of branch-office sizes.

ble 2. Modularity-Features and Benefits

eature	Benefit
nhanced Network-Module (NME) Slots	• The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only) • NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE). • NME slots are highly flexible with future support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).
igh-Performance WIC (HWIC) Slots ith Enhanced Functionality	• Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations. • HWICs slots can also support WICs, VICs, and VWICs • HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput) and Power over Ethernet (POE) support. • A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.
ual AIM Slots	• Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for more details on specific platform support).
acket Voice DSP Module (PVDM) lots on Motherboard	• Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.
xtension-Voice-Module (EVM) Slot	• The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).
SB Support	• Up to two USB ports are available per Cisco 2800 series router. The routers' Universal Serial Bus (USB) ports enable important security and storage capabilities.

cure Networking-Feature and Benefits

e Cisco 2800 Series features enhanced security functionality as shown in Table 3. Integrated on the motherboard of every Cisco 2800 Series router ıardware-based encryption acceleration that offloads the encryption processes to provide greater IPsec throughput with less overhead for the router U when compared with software-based solutions. With the integration of optional VPN modules (for enhanced VPN tunnel count), Cisco IOS ftware-based firewall, network access control, or content-engine network modules, Cisco offers the industry's most robust and adaptable security ution for branch-office routers.

ble 3. Secure Networking-Feature and Benefits

eature	Benefit
isco IOS Software Firewall	• Sophisticated security and policy enforcement provides features such as stateful, application-based filtering (context-based access control), per-user authentication and authorization, real-time alerts, transparent firewall, and IPv6 firewall.
nboard VPN Encryption Acceleration	• The Cisco 2800 Series supports IPsec Digital Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) 128, AES 192, and AES 256 cryptology without consuming an AIM slot.
etwork Admissions Control (NAC)	• A Cisco Self-Defending Network initiative, NAC seeks to dramatically improve the ability of networks to identify, prevent, and adapt to threats by allowing network access only to compliant and trusted endpoint devices.
ultiprotocol Label Switching (MPLS) PN Support	• The Cisco 2800 Series supports specific provider edge functions plus a mechanism to extend customers' MPLS VPN networks out to the customer edge with virtual routing and forwarding (VRF) firewall and VRF IPsec. For details on the MPLS VPN support on the different versions of the Cisco 2800 Series, please check the feature navigator tool on http://www.cisco.com.
SB eToken Support	• USB eTokens from Aladdin Knowledge Systems (available at http://www.aladdin.com/etoken/cisco/) provides secure configuration distribution and allows users to store VPN credentials for deployment
IM-Based Security Acceleration	• Support for an optional dedicated security AIM can deliver 2 to 3 times the performance of embedded encryption capabilities with Layer 3 compression.
ıtrusion Prevention System (IPS)	• Flexible support is offered through Cisco IOS® Software or a high-performance intrusion-detection-system (IDS) network module. • The ability to load and enable selected IDS signatures in the same manner as Cisco IDS Sensor Appliances
dvanced Application Inspection nd Control	• Cisco IOS Firewall includes HTTP and several email inspection engines that can be used to detect misuse of port 80 and email connectivity.
isco Easy VPN Remote and erver Support	• The Cisco 2800 Series eases administration and management of point-to-point VPNs by actively pushing new security policies from a single headend to remote sites.
ynamic Multipoint VPN (DMVPN)	• DMVPN is a Cisco IOS Software solution for building IPsec + generic routing encapsulation (GRE) VPNs in an easy and scalable manner.
RL Filtering	• URL filtering is available onboard with an optional content-engine network module or external with a PC server running the URL filtering software.
isco Router and Security Device lanager (SDM)	• This intuitive, easy-to-use, Web-based device-management tool is embedded within the Cisco IOS Software access routers; it can be accessed remotely for faster and easier deployment of Cisco routers for both WAN access and security features.

Telephony Support-Features and Benefits

e Cisco 2800 Series allows network managers to provide scalable analog and digital telephony without investing in a one-time solution (refer to ble 4 for more detail), allowing enterprises greater control of their converged telephony needs. Using the voice and fax modules, the Cisco 2800 ies can be deployed for applications ranging from voice-over-IP (VoIP) and voice-over-Frame Relay (VoFR) transport to robust, centralized utions using the Cisco Survivable Remote Site Telephony (SRST) solution or distributed call processing using Cisco Call Manager Express ME). The architecture is highly scalable with the ability to support up to 12 T1/E1s trunks, 52 foreign-exchange-station (FXS) ports, or 36 eign-exchange-office (FXO) ports concurrent with data routing and other services.

ble 4. IP Telephony Support-Features and Benefits

eature	Benefit
' Phone Support	• Optional support for Cisco in-line power distribution to Ethernet switch network modules and HWICs can be used to power Cisco IP phones.
VM Module Slots	• Extension Voice Module Slots, available only on the Cisco 2821 and Cisco 2851, provide support for the Cisco High-Density Analog and Digital Extension Module for Voice and Fax, providing support for up to 24 total voice and fax sessions without consuming a Network Module Slot.
VDM (DSP) Slots on Motherboard	• DSP (PVDM2) modules deliver support for analog and digital voice, conferencing, transcoding, and secure Real-Time Transport Protocol (RTP) applications.
ntegrated Call Processing	• Cisco CME is an optional solution embedded in Cisco IOS Software that provides call processing for Cisco IP phones. Cisco CME delivers telephony features similar to those that are commonly used by business users to meet the requirements of the small to medium-sized offices.
ntegrated Voice Mail	• Support for up to a 100 mailboxes using the Cisco Unity® Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module.
road Range of Voice Interfaces	• Interfaces for local telephone, private branch exchange (PBX), and gateway connections include FXS; FXO; direct inward dialing (DID); ear and mouth (E&M); Centralized Automated Message Accounting (CAMA); ISDN Basic Rate Interface (BRI); and T1, E1, and J1 with ISDN Primary Rate Interface (PRI); QSIG; and several additional channel-associated-signaling (CAS) signaling schemes.
upport of Survivable Remote Site elephony (SRST) Feature	• Branch offices can take advantage of centralized call control while cost-effectively providing local branch backup using SRST redundancy for IP telephony.

ireless Support-Features and Benefits

e Cisco 2800 Series can provide a complete wireless solution for branch offices, small/medium sized businesses, and Wi-Fi hotspots. Wireless rvices enable greater mobility for employees, partners, and customers, resulting in increased productivity.

ble 5. Wireless Support-Features and Benefits

Feature	Benefit
VLAN Connectivity	• The 802.11b/g or 802.11a/b/g HWIC access point interface card can be used to provide integrated WLAN connectivity to mobile clients at sites requiring a single access point, resulting in mobility and enhanced productivity for users. • Dual RP-TNC connectors enable diversity and allow for optimum coverage through the use of external antennas.
Wireless Infrastructure Services	• Telephony support for wired and WLAN IP phones is delivered by Cisco CallManager Express (CCME) or by Survivable Remote Site Telephony (SRST) with Cisco CallManager. Cordless WLAN IP phones allow users to be mobile and more productive. • Integrated switch modules with Power over Ethernet (POE) enable support for Cisco Aironet access points (for larger sites) as well as wired IP phones. • Mobility for clients from WLAN to cellular networks is enabled by Mobile IP home agent support. • IEEE 802.1x local authentication using LEAP provides enhanced reliability through survivable authentication for WLAN clients during WAN failures. • Customizable guest access is enabled with the service selection gateway features, along with the Subscriber Edge Services Manager.
Land Mobile Radio Over IP	• LMR over IP support allows radio users (e.g., security personnel, maintenance personnel, police officers, etc.) to communicate via IP with phone and PC users, delivering improved communications and productivity.
Wi-Fi Hotspot Services	• The access zone router and service selection gateway services features can be used to deploy secure public WLAN access services with an integrated HWIC-AP for small sites or with Cisco Aironet access points for larger sites. Wi-Fi hotspot services can be offered for additional revenue for public locations (e.g., restaurants, hotels, airports, etc.) or a value-added service for customer satisfaction.

st of Ownership and Ease of Use-Features and Benefits

e Cisco 2800 Series continues the heritage of offering versatility, integration, and power to branch offices. The Cisco 2800 Series offers many ıancements to help enable the support of multiple services in the branch office as shown in Table 5.

ble 6. Cost of Ownership and Ease of Use-Feature and Benefits

eature	Benefit
ıtegrated Channel Service Unit/Data ervice Unit (CSU/DSU), Add/Drop ultiplexers, Firewall, Modem, ompression, and Encryption	• Consolidates typical communications equipment found in branch-office wiring closets into a single, compact unit; this space-saving solution provides better manageability
ptional Network Analysis Module	• Provides application-level visibility into network traffic for troubleshooting, performance monitoring, capacity planning, and managing network-based services (Note: Cisco 2811, 2821, and 2851 only)
isco IOS Software Warm Reboot	• Reduces system boot time, and decreases downtime caused by Cisco IOS Software reboots (Note: Cisco 2801 will support the Cisco IOS Software Warm Reboot at a later point in time)
nhanced Setup Feature	• Optional setup wizard with context-sensitive questions guides the user through the router configuration process, allowing faster deployment
iscoWorks Support	• Offers advanced management and configuration capabilities through a Web-based GUI
isco AutoInstall	• Configures remote routers automatically across a WAN connection to save cost of sending technical staff to the remote site

JMMARY AND CONCLUSION

companies strive to lower the cost of running their network and increase the productivity of their end users with network applications, more elligent branch-office solutions are required. The Cisco 2800 Series offers these solutions by providing enhanced performance and increased odular density to support multiple services at wire speed. The Cisco 2800 Series is designed to consolidate the functions of many separate devices o a single, compact package that can be managed remotely. Because the Cisco 2800 Series routers are modular devices, interface configurations easily customized to accommodate a wide variety of network applications, such as branch-office data access, integrated switching, voice and data egration, wireless LAN services, dial access services, VPN access and firewall protection, business-class DSL, content networking, intrusion evention, inter-VLAN routing, and serial device concentration. The Cisco 2800 Series provides customers with the industry's most flexible, aptable infrastructure to meet both today's and tomorrow's business requirements for maximum investment protection.

ODUCT SPECIFICATIONS

le 7. Chassis Specifications

sco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
oduct Architecture				
RAM	Default: 128 MB	Default: 256 MB	Default: 256 MB	
	Maximum: 384 MB	Maximum: 760 MB	Maximum: 1 GB	
mpact Flash	Default: 64 MB		Default: 64 MB	
	Maximum: 128MB		Maximum: 256 MB	
ed USB 1.1 Ports	1		2	
board LAN Ports	2-10/100		2-10/100/1000	
board AIM (internal) ot			2	
erface card slots	4 slots; 2 slots support HWIC, WIC, VIC, or VWIC type modules 1 slot supports WIC, VIC, or VWIC type modules 1 slot supports VIC or VWIC type modules	4 slots, each slot can support HWIC, WIC, VIC, or VWIC type modules		
twork-module slot	No	1 slot, supports NM and NME type modules	1 slot, supports NM, NME and NME-X type modules	1 slot, supports NM, NME, NME-X, NMD and NME-XD type modules
tension Voice Module ot	0		1	
DM (DSP) slots on otherboard	2		3	
egrated hardware-based cryption	Yes			
N hardware eleration motherboard)	DES, 3DES, AES 128, AES 192, and AES 256			
ional integrated in-line er (PoE)	Yes, requires AC-IP power supply			
sole port (up to 115.2 s)	1			
liary port (up to 115.2 s)	1			
num Cisco IOS ware release	12.3(8)T			
k mounting	Yes, 19-inch		Yes, 19- and 23-in. options	
mounting	No	Yes	No	No
wer Requirements				
nput voltage	100 to 240 VAC, autoranging			
input frequency	47-63 Hz			
nput current	2A (110V) 1A (230V)		3A (110V) 2A (230V)	

isco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
C input surge current	50A maximum, one cycle (-48V power included)			
C-IP maximum in-line ower distribution	120W	160W	240W	360W
C-IP input current	4A (110V) 2A (230V)		8A (110V) 4A (230V)	
C-IP input surge current	50A maximum, one cycle (-48V power included)			
C input voltage	No DC Power Option available	24 to 60 VDC, autoranging positive or negative		
C input current	No DC Power Option available	8A (24V) 3A (60V) Startup current 50A<10 ms	12A (24V) 5A (60V) Startup current 50A<10 ms	
ower dissipation-AC ithout IP phone support	150W (511 BTU/hr)	170W (580 BTU/hr)	280W (955 BTU/hr)	280W (955 BTU/hr)
ower dissipation-AC with P phone support-system nly	150W (511 BTU/hr)	210W (717 BTU/hr)	310W (1058 BTU/hr)	370W (1262 BTU/hr)
ower dissipation-AC with P phone support-IP hones	180W (612 BTU/hr)	160W (546 BTU/hr)	240W (819 BTU/hr)	360W (1128 BTU/hr)
ower dissipation-DC	Not applicable	180W (614 BTU/hr)	300W (1024 BTU/hr)	300W (1024 BTU/hr)
PS	No	External only, connector for RPS provided by default		
ecommended RPS unit	No RPS option	Cisco RPS-675 Redundant Power System		
nvironmental Specifications				
perating temperature	32 to 104°F (0 to 40°C)			
perating humidity	10 to 85% non-condensing		5 to 95%, non-condensing	
on-operating temperature	–		4° to 149°F (-20° to 65°C)	
peration altitude (derate .5C per 1000 ft)	25°C @ 3 km/10 kft 40°C @ sea level		27.5°C @ 15 kft 35°C @ 3km/10 kft 40°C @ sea level	
imensions (H x W x D)	1.72 x 17.5 x 16.5 in. (43.7 x 445 x 419 mm)	1.75 x 17.25 x 16.4 in. (44.5 x 438.2 x 416.6 mm)	3.5 x 17.25 x 16.4 in. (88.9 x 438.2 x 416.6 mm)	
ack height	1 rack unit (1RU)		2RU	
eight (fully configured)	13.7 lb (6.2 kg)	14 lb (6.4 kg)	25 lb (11.4 kg)	
oise level (min/max)	39 dBA for normal operating temperature (<90°F/32.2°C) 53.5 dBA (@ maximum fan speed)	47 dBA for normal operating temperature (<90°F/32.2°C) 57 dBA (@ maximum fan speed)	44 dBA for normal operating temperature (<90°F/32.2°C) 53 dBA (@ maximum fan speed)	
egulatory Compliance				
EBS	No	Yes		Future
afety	UL 60950 CAN/CSA C22.2 No. 60950 IEC 60950 EN 60950-1 AS/NZS 60950			

Cisco 2800 Series	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Immunity			EN300386	
			EN55024/CISPR24	
			EN50082-1	
			EN61000-6-2	
EMC			FCC Part 15	
			ICES-003 Class A	
			EN55022 Class A	
			CISPR22 Class A	
			AS/NZS 3548 Class A	
			VCCI Class A	
			EN 300386	
			EN61000-3-3	
			EN61000-3-2	
TELCOM**	For all four platforms, Telecom compliance standards depend upon country and interface type. Interfaces comply with FCC Part 68, CS-03, JATE Technical Conditions, European Directive 99/5/EC and relevant TBR's. For specific information see the datasheet for the specific interface card. Homologation requirements vary by country and interface type. For specific country information, see the on-line approvals data base: http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH&module=EXTERNAL_SEARCH			

MODULAR SUPPORT

Table 8. Modules and Interface Cards Supported

Network Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Ethernet Switching Network Modules					
NME-16ES-1G-P	One 16-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 10/100/1000 port, and IP Base	No	√	√	√
NME-X-23ES-1G-P	One 23-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 10/100/1000 port w/ 802.3af, and IP Base	No	No	√	√
NME-XD-24ES-2S-P	One 24-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 SFP, Cisco StackWise connectors, and IP Base	No	No	No	√
NME-XD-48ES-2S-P	One 48-port 10/100 Cisco EtherSwitch service module w/ 802.3af, 2 SFPs, and IP Base	No	No	No	√
NM-16ESW	16-port 10/100 Cisco EtherSwitch® Network Module	No	√	√	√
NM-16ESW-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with 1 Gigabit Ethernet (1000BASE-T) port	No	√	√	√
NM-16ESW-PWR	16-port 10/100 Cisco EtherSwitch Network Module with in-line power support	No	√	√	√
NM-16ESW-PWR-1GIG	16-port 10/100 Cisco EtherSwitch Network Module with in-line power and Gigabit Ethernet	No	√	√	√
MD-36ESW	36-port 10/100 Cisco EtherSwitch High-Density Services Module (HDSM)	No	No	No	√

etwork Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
MD-36ESW-2GIG	36-port 10/100 Cisco EtherSwitch HDSM with 1 Gigabit Ethernet (1000BASE-T) port	No	No	No	√
MD-36ESW-PWR	36-port 10/100 Cisco EtherSwitch HDSM with in-line power support	No	No	No	√
MD-36ESW-PWR-2G	36-port 10/100 Cisco EtherSwitch HDSM with in-line power and Gigabit Ethernet	No	No	No	√
erial Connectivity Network Modules					
M-1T3/E3	1-port clear-channel T3/E3 network module	No	√	√	√
M-1HSSI	1-port High-Speed Serial Interface (HSSI) network module	No	√	√	√
M-4A/S	4-port asynchronous/synchronous serial network module	No	√	√	√
M-8A/S	8-port asynchronous/synchronous serial network module	No	√	√	√
M-16A/S	16-port asynchronous/synchronous serial network nodule	No	√	√	√
M-16A	16-port asynchronous serial network module	No	√	√	√
M-32A	32-port asynchronous serial network module	No	√	√	√
hannelized T1/E1 and ISDN Network Modules					
M-1CE1T1-PRI	1-port Channelized E1/T1/ISDN PRI network module	No	√	√	√
M-2CE1T1-PRI	2-port Channelized E1/T1/ISDN PRI network module	No	√	√	√
M-4B-S/T	4-port ISDN BRI network module (S/T interface)	No	√	√	√
M-4B-U	4-port ISDN BRI network module with integrated Network Termination 1 (NT1) (U interface)	No	√	√	√
M-8B-S/T	8-port ISDN BRI network module (S/T interface)	No	√	√	√
M-8B-U	8-port ISDN BRI network module with integrated NT1 (U interface)	No	√	√	√
TM Network Modules					
M-1A-T3	1-port DS-3 ATM network module	No	√	√	√
M-1A-E3	1-port E3 ATM network module	No	√	√	√
nalog Dialup and Remote Access Network Modules					
M-8AM-V2	8-port analog modem network module with v.92	No	√	√	√
M-16AM-V2	16-port analog modem network module with v.92	No	√	√	√
oice Network Modules and Accessories					
M-HD-1V	1-slot IP Communications voice and fax network module	No	√	√	√
M-HD-2V	2-slot IP Communications voice and fax network module	No	√	√	√
M-HD-2VE	2-slot IP Communications enhanced voice and fax network module	No	√	√	√
M-HDA-4FXS	High-density analog voice and fax network module with 4 FXS slots	No	√	√	√
M-HDV2	IP Communications high-density voice and fax network module	No	√	√	√

etwork Module		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
M-HDV2-1T1/E1	1-port T1/E1 IP Communications high-density voice and fax network module	No	√	√	√
M-HDV2-2T1/E1	2-port T1/E1 IP Communications high-density voice and fax network module	No	√	√	√
M-HDV=	High Density Voice/Fax Network Module (Single VIC Slot)	No	√	√	√
M-HDV-1T1-12	1-port 12-channel T1 voice and fax network module	No	√	√	√
M-HDV-1T1-24	1-port 24-channel T1 voice and fax network module	No	√	√	√
M-HDV-1T1-24E	Single-port 24 enhanced channel T1 voice and fax network module	No	√	√	√
M-HDV-2T1-48	2-port 48-channel T1 voice and fax network module	No	√	√	√
M-HDV-1E1-12	1-port 12-channel E1 voice and fax network module	No	√	√	√
M-HDV-1E1-30	1-port 30-channel E1 voice and fax network module	No	√	√	√
M-HDV-1E1-30E	1-port 30-enhanced-channel E1 voice and fax Network Module	No	√	√	√
M-HDV-2E1-60	2-port 60-channel E1 voice and fax network module	No	√	√	√
M-HDV-1J1-30	1-port 30-channel J1 high-density voice network module	No	√	√	√
M-HDV-1J1-30E	1-port 30-enhanced-channel J1 high-density voice network module	No	√	√	√
M-HDV-FARM-C36	36-port transcoding and conferencing DSP farm	No	√	√	√
M-HDV-FARM-C54	54-port transcoding and conferencing DSP farm	No	√	√	√
M-HDV-FARM-C90	90-port transcoding and conferencing DSP farm	No	√	√	√
pplication Network Modules					
M-CE-BP-40G-K9	Cisco Content Engine Network Module, basic performance, 40-GB IDE hard disk	No	√	√	√
M-CE-BP-80G-K9	Cisco Content Engine Network Module, basic performance, 80-GB IDE hard disk	No	√	√	√
M-CIDS-K9	Cisco IDS Network Module	No	√	√	√
M-CUE	Cisco Unity Express Voice-Mail Network Module	No	√	√	√
M-NAM	Cisco 2600, 3660, and 3700 series network analysis module	No	√	√	√
larm Monitoring and Control Network Modules and Accessories					
M-AIC-64	Alarm monitoring and control network module	No	√	√	√
ircuit Emulation over IP (CEoIP) Network Modules					
M-CEM-4SER	4-port serial Circuit Emulation over IP (CEoIP) network module	No	√	√	√
M-CEM-T4E1	4-port T1/E1 Circuit Emulation over IP (CEoIP) network module	No	√	√	√
xtension Voice Modules		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
VM-HD-8FXS/DID	High density voice/fax extension module -8 FXS/DID	No	No	√	√

terface-Card Support		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
thernet Switching HWICs					
WIC-4ESW	4-port single-wide 10/100BaseT Ethernet switch HWIC	√	√	√	√
WIC-D-9ESW	9-port double-wide 10/100BaseT Ethernet switch HWIC	√	√	√	√
WIC-4ESW-POE	4-port Ethernet switch HWIC, Power over Ethernet capable	√	√	√	√
WIC-D-9-ESW-POE	9-port Ethernet switch HWIC, Power over Ethernet capable	√	√	√	√
igabit Ethernet HWICs					
WIC-1GE-SFP	No	√	√	√	
Vireless HWICs					
WIC-AP-G-A WIC-AP-G-E WIC-AP-G-J	802.11b/g HWIC access point interface card (A–Americas; E–Europe; J–Japan)	√	√	√	√
WIC-AP-AG-A WIC-AP-AG-E WIC-AP-AG-J	802.11a/b/g HWIC access point interface card (A–Americas; E–Europe; J–Japan)	√	√	√	√
Serial HWIC/WICs					
VIC-1T	1-port high-speed serial WIC	√	√	√	√
VIC-2T	2-port high-speed serial WIC	√	√	√	√
HWIC-4T	4-Port Serial HWIC	√	√	√	√
VIC-2A/S	2-port Asynch/Synch serial WIC	√	√	√	√
HWIC-4A/S	4-Port Async/Sync Serial HWIC	√	√	√	√
HWIC-8A/S-232	8-Port Async/Sync Serial HWIC, EIA-232	√	√	√	√
HWIC-8A	8-Port Async HWIC	√	√	√	√
HWIC-16A	16-Port Async HWIC	√	√	√	√
CSU/DSU WICs					
VIC-1DSU-T1-V2	1-port T1/Fractional-T1 DSU/CSU WIC	√	√	√	√
VIC-1DSU-56K4	1-port 4-wire 56-/64-kbps CSU/DSU WIC	√	√	√	√
SDN BRI WICs					
VIC-1B-U-V2	1-port ISDN BRI with integrated NT1 (U interface)	√	√	√	√
VIC-1B-S/T-V3	1-port ISDN BRI with S/T interface	√	√	√	√
SL WAN Interface Cards					
VIC-1ADSL	1-port asymmetric DSL (ADSL) over POTS service WIC	√	√	√	√
VIC-1ADSL-DG	1-port ADSL over basic telephone service with dying-gasp WIC	√	√	√	√
VIC-1ADSL-I-DG	1-port ADSL over ISDN with dying-gasp WIC	√	√	√	√
VIC-1SHDSL	1-port G.shdsl WIC (two wire only)	√	√	√	√
VIC-1SHDSL-V2	1-port G.shdsl WIC (two or four wire)	No	√	√	√

Interface-Card Support		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
Analog Modem WICs					
WIC-1AM	1-port analog modem WIC	√	√	√	√
WIC-2AM	2-port analog modem WIC	√	√	√	√
T1, E1, and G.703 Multiflex Trunk Voice Cards and WICs					
VWIC2-1MFT-T1/E1	1-Port T1/E1 Voice/WAN w/ Drop & Insert	√	√	√	√
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk-T1	√	√	√	√
VWIC2-2MFT-T1/E1	2-Port T1/E1 Voice/WAN w/ Drop & Insert	√	√	√	√
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk-T1	√	√	√	√
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk-T1 with drop and insert	√	√	√	√
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk-E1	√	√	√	√
VWIC2-1MFT-G703	1-Port T1/E1 Voice/WAN w/ D&I & unstructured E1 (G703)	√	√	√	√
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk-G.703	√	√	√	√
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk-E1	√	√	√	√
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk-E1 with drop and insert	√	√	√	√
VWIC2-2MFT-G703	2-Port T1/E1 Voice/WAN w/ D&I & unstructured E1 (G703)	√	√	√	√
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk-G.703	√	√	√	√
VICs					
VIC-2DID	2-port DID voice and fax interface card	√	√	√	√
VIC-1J1	1-port digital VIC (J1) for Japan	No	√	√	√
VIC-4FXS/DID	4-port FXS or DID VIC	√	√	√	√
VIC2-2FXS	2-port VIC-FXS	√	√	√	√
VIC2-2FXO	2-port VIC-FXO (universal)	√	√	√	√
VIC2-4FXO	4-port VIC-FXO (universal)	√	√	√	√
VIC2-2E/M	2-port VIC-E&M	√	√	√	√
VIC2-2BRI-NT/TE	2-port VIC card-BRI (NT and TE)	√	√	√	√
Advanced Integration Modules		2801	2811	2821	2851
AIM-ATM	High-performance ATM SAR AIM	No	√	√	√
AIM-COMPR2-V2	Data compression AIM	No	√	√	√
AIM-CUE	Cisco Unity Express Voice-Mail AIM	√	√	√	√
AIM-VPN/EPII-PLUS	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM	√	√	√	√
DSP (PVDM) Support on Motherboard Slots		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
PVDM2-8	8-channel fax and voice DSP module	√	√	√	√
PVDM2-16	16-channel fax and voice DSP module	√	√	√	√
PVDM2-32	32-channel fax and voice DSP module	√	√	√	√
PVDM2-48	48-channel fax and voice DSP module	√	√	√	√
PVDM2-64	64-channel fax and voice DSP module	√	√	√	√

SB Flash Storage		Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851
EMUSB-64FT	64Mb USB Flash	√	√	√	√
EMUSB-128FT	128Mb USB Flash	√	√	√	√
EMUSB-256FT	256Mb USB Flash	√	√	√	√

AILABILITY

e Cisco 2800 Series has been orderable since September, 2004, with first customer shipments at the end of September 2004.

DERING INFORMATION

place an order, visit the Cisco Ordering Home Page.

ble 9. Ordering Information for Cisco 2800 Integrated Services Routers

art Number	Product Name
ISCO2801	Integrated services router with AC power, 2FE, 4 Interface Card Slots, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2801-AC-IP	Integrated services router with AC power including Inline power distribution capability, 2FE, 4 Interface Card Slots, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2811	Integrated services router with AC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2811-AC-IP	Integrated services router with AC power including Inline power distribution capability, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2811-DC	Integrated services router with DC power, 2FE, 1 NME, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2821	Integrated services router with AC power, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2821-AC-IP	Integrated services router with AC power including inline power distribution capability, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2821-DC	Integrated services router with DC power, 2GE, 1 NME-X, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2851	Dual Gigabit Ethernet integrated services router with AC power, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2851-AC-IP	Integrated services router with AC power including inline power distribution capability, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software
ISCO2851-DC	Integrated services router with DC power, 2GE, 1 NME-XD, 1 EVM, 4 HWICs, 3 PVDM slots, 2 AIMs, and Cisco IOS IP Base Software

so, check with your Cisco representative regarding security, xDSL, and voice bundles for the Cisco 2800 Series.

rdownload the software, visit the Cisco Software Center.

le 10. Software Ordering Information

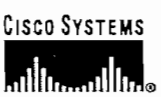
rt Number	Product Name	Supported Platform
8IPB	Cisco 2800 IP Base	Cisco 2801
8IPV	Cisco 2800 IP Voice	Cisco 2801
.8ASK9	Cisco 2800 Advanced Security	Cisco 2801
.8EB	Cisco 2800 Enterprise Base	Cisco 2801
.8SPSK9	Cisco 2800 SP Services	Cisco 2801
8ESK9	Cisco 2800 Enterprise Services	Cisco 2801
.8AISK9	Cisco 2800 Advanced IP Services	Cisco 2801
.8AESK9	Cisco 2800 Advanced Enterprise Services	Cisco 2801
.8NIPB	Cisco 2800 IP Base	Cisco 2811, 2821, 2851
.8NIPV	Cisco 2800 IP Voice	Cisco 2811, 2821, 2851
.8NASK9	Cisco 2800 Advanced Security	Cisco 2811, 2821, 2851
.8NEB	Cisco 2800 Enterprise Base	Cisco 2811, 2821, 2851
.8NSPSK9	Cisco 2800 SP Services	Cisco 2811, 2821, 2851
.8NESK9	Cisco 2800 Enterprise Services	Cisco 2811, 2821, 2851
.8NAISK9	Cisco 2800 Advanced IP Services	Cisco 2811, 2821, 2851
.8NAESK9	Cisco 2800 Advanced Enterprise Services	Cisco 2811, 2821, 2851

RVICE AND SUPPORT

co offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique ıbination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your vork investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power our business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Advanced Services.

R MORE INFORMATION

more information about the Cisco 2800 Series, visit http://www.cisco.com/en/US/products/hw/routers/ or contact your local account esentative.



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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

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

205290.BA_ETMG_CC_6.05

Printed in the USA