UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SERVICIOS SOBRE IP

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:
FRANK ALEX SORIANO ROSAS

PROMOCIÓN
1998-II
LIMA-PERU

A mis padres, a mis hermanos, a mi abuelita

Octavia, a mi tío Carlos y en especial a Dios

Por haberme dado las fuerza necesaria para

Dar este paso importante en mi vida.

SERVICIOS SOBRE IP

SUMARIO

En la actualidad la cantidad de servicios que se pueden pasar a través del protocolo IP son bastantes y los cuales según las tendencias actuales siguen aumentando y perfeccionándose, el propósito de este informe es de mostrar los avances que en los últimos años se vino dando en la utilización de IP de tal manera se pueda entender su funcionamiento.

En este informe se presenta los fundamentos en que IP se basa, su grado de escalabilidad y sus perspectivas de desarrollo. Así mismo se presenta toda la gama de servicios en lo que actualmente IP se viene utilizando y además una visión de los avances que este protocolo puede tener en otras tecnologías.

Los avances de la utilización del Protocolo IP a llevado en los últimos años a la integración no solo de servicios si no también de empresas corporativas a nivel mundial y por que no decirlo de países que actualmente sus negocios los pueden hacer en línea con la más alta confiabilidad ayudando al proceso de globalización de la economía mundial.

El tema de IP es muy amplio, intentaremos cubrir los más importantes y lo que consideramos los que les puede ser de mucha utilidad.

ÍNDICE

PROLOGO

El propósito del presente informe es de mostrar los adelantos tecnológicos que en los últimos años se han venido dando y todas las aplicaciones que hasta este momento se están desarrollando en el país, dando un enfoque de los posibles avances que se pueden venir en el campo de las comunicaciones. En esta obra se recoge la experiencia que en los últimos años ha desarrollado un grupo de trabajo muy capaz en el área de Comunicaciones de la Empresa AT&T PERU S.A. Esta obra tiene los conceptos más importantes de Networking que ha hecho posible las comunicaciones en tiempo real tanto de voz, video y datos de las corporaciones trasnacionales originando una revolución de los procesos de gestión de la información.

No puedo dejar de pasar la oportunidad para agradecer profundamente a todos los Ingenieros que más que compañeros de trabajo son amigos, que de alguna forma hicieron que esa información privilegiada pueda concretarse en un informe ambicioso que estoy seguro será de mucha utilidad para los estudiantes de la UNI, egresados y profesionales interesados en el campo del Networking.

CAPÍTULO I
TCP/IP

El nombre de TCP IP significa un conjunto de protocolos de comunicación de data. TCP/IP no es solo 2 protocolos más del conjunto de protocolos, su nombre viene de los 2 más importantes protocolos los cuales son el Protocolo control de Transmisión (TCP) y el protocolo de Internet (IP).

TCP se origino de la investigación que alcanzo dentro de los protocolos de Networking el departamento de defensa (DoD) iniciado en 1969.

El enfoque original de este proyecto fue el de facilitar la comunicación entre la comunidad del DoD, la red que fue construida inicialmente como resultado de este proyecto la cual fue llamado ARPANET, gradualmente fue conocido como el Internet. En los años 1980 el TCP/IP fue desarrollado y en el año 1983 fueron desarrollados los protocolos estándar para el ARPANET.

1.1. ¿Cómo TCP/IP Trabaja?

A continuación describiremos algunos protocolos que componen TCP/IP usando el modelo de referencia de Internet (DoD).

1.1.1. Capa de Acceso de Red

Las funciones en este nivel incluyen la encapsulación de los datagramas IP dentro de frames que son transmitidos por la red, ello también mapean la dirección IP a la dirección física usada por la red. Uno de lo más fuerte de TCP/IP es su esquema de direccionamiento el cual identifica únicamente a cada computadora en la red. Esta

dirección IP necesita ser convertida dentro de cualquier otra dirección que es apropiada para la interfase física sobre cual el datagrama es transmitido. La data a ser transmitida es recibida de la capa de INTERNETWORK, la capa de acceso de red es responsable para el routing y necesita sumar esta información de routing a la data lo cual lo suma en forma de cabecera y lo coloca al comienzo de la data.

1.1.2. Capa de Internetwork

El protocolo TCP/IP más conocido de esta capa es el Protocolo de Internet (IP), cual provee el básico servicio de entrega de paquetes para todas las redes TCP/IP. Además del direccionamiento físico proporcionado por la capa de Acceso a red, el protocolo IP implementa un direccionamiento lógico llamado direccionamiento IP. La dirección IP es usada por la capa de INTERNETWORK y capas más altas a identificar dispositivos y realizar routing entre redes. El ARP habilita al IP para identificar direcciones físicas que machen con una dirección IP dada.

. Protocolo de Internet (IP)

IP es un protocolo no orientado a conexión, lo cual significa que IP no intercambia información de control (handshaking) a establecer una conexión final antes de trasmitir data. En contraste un protocolo orientado a conexión intercambia información de control con la computadora remota a verificar que esta lista a recibir data antes de enviar ello. Cuando el Handshaking es exitoso la computadora dice que se ha establecido la conexión. IP confía en otras capas a establecer la conexión si los servicios orientados a conexión son requeridos.

- Ruta de datagramas a remotos Hosts. Los gateways de Internet son comúnmente llamados routers IP, porque ellos usan IP a rutear paquetes entre las redes.
- Fragmenta y reensambla datagramas. Como un datagrama es ruteado a través de diferentes redes, ello podría ser necesario por el modulo IP en un gateway a dividir el datagrama dentro de pequeñas piezas. Un datagrama recibido de una red podría ser tan grande a ser transmitido en un solo paquete. Cada tipo de red tiene una máxima unidad de transmisión (MTU). Cual es el más largo paquete que ello puede transmitir.

1.1.3. Capa de Transporte Host to Host

Ello es responsable para la integridad de la data end to end. Los 2 protocolos más importantes en esta capa son el Protocolo de Control de Transmisión (TCP) y el protocolo de Usuario de datagrama (UDP).

TCP provee conexión full duplex y confiables, además asegura que la data es reorganizada si en caso un error es detectado. También TCP habilita a los Host a mantener múltiples y simultaneas conexiones. Cuando no-detección de error es requerida se puede usar UDP el cual provee no confiables conexiones (no orientado a conexión) cual eleva el rendimiento de la red en la capa de transporte Host to Host.

1.1.4. Capa de Aplicación

Los más conocidos protocolos de la capa de Aplicación son los siguientes listados abajo:

a).- Protocolo de Transferencia de archivos (FTP).- Desarrolla la básica transferencia de archivos entre Host.

b).- Telnet.- Habilita a los usuarios a desarrollar sesiones de terminal con los remotos host.

c).- Protocolo de transferencia de Correo (SMTP).- Soporta los básicos servicios de entrega de mensajes.

d).- Protocolo de Transferencia de hipertexto (HTTP).- Soporta el transporte de bajo overhead de archivos consistentes de una mixtura de gráficos y textos.

Además a los amplios conocidos protocolos tenemos los siguientes:

e).- Servicio de nombre de dominio (DNS).- También llamado servicio de nombre, este protocolo mapea las direcciones IP a los nombres asignados a los dispositivos de red.

f).- Protocolo de Información de routing (RIP).- El routing es central en la manera de trabajo de TCP/IP. RIP es usado por los dispositivos de red a intercambiar información de routing.

g).- Protocolo de administración de red simple (SNMP) .- Un protocolo que es usado a coleccionar información de administración de los dispositivos de red.

1.2. Protocolo de Internet (IP)

1.2.1. Formato del Paquete IP

Un paquete IP contiene varios tipos de información, como ilustramos en la figura 1.

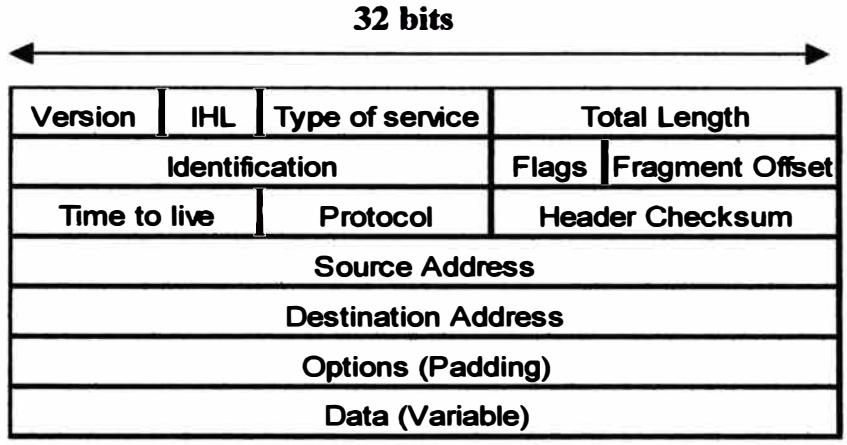

Fig.1.- El Paquete IP comprende 14 Campos.

A continuación pasamos a describir los campos del paquete IP :

- VERSIÓN.- Indica la versión del paquete IP Usado.

- LONGITUD DE LA CABECERA IP (IHL) .- Indica la longitud de la cabecera del datagrama en palabras de 32bits.

- TIPO DE SERVICIO .- Especificado como un protocolo de las capas mas altas permite un corriente datagrama a ser manejado y asigna varios niveles de importancia de datagrama.

- LONGITUD TOTAL .- Especifica la longitud total en bytes del paquete IP incluyendo la data y la cabecera.

- IDENTIFICACIÓN .- Contiene un entero que identifica el corriente datagrama. Este campo es usado a ayudar juntar los fragmentos de datagrama.

- FLAGS .- Consiste de un campo de 3 bits de los cuales los 2 de más bajo orden controla la fragmentación, el bit de más bajo orden indica donde el paquete puede ser fragmentado, el bit del centro indica donde esta el ultimo fragmento del paquete en una serie de paquetes fragmentados. El tercer bit ó de más alto orden no es usado.

- OFFSET DEL FRAGMENTO .- Indica la posición de la data del fragmento relativo al comienzo de la data en el original datagrama, cual permite al IP destino procesar apropiadamente la reconstrucción del datagrama original.
- TIME TO LIVE .- Mantiene un contador que gradualmente se decrementa a cero en cual punto el datagrama es descartado. Esto previene paquetes desde lazos cerrados (loops).
- PROTOCOLO .- Indica cuales protocolos de las capas mas altas reciben paquetes de entrada después que el procesamiento IP es completo.
- HEADER CHECKSUM .- Ayuda asegurar la integridad de la cabecera IP.
- DIRECCIÓN FUENTE .- Indica el nodo que esta enviando la data.
- DIRECCIÓN DESTINO .- Indica el nodo que va recibir la data.
- OPTIONS .- Permite al IP soportar varias opciones tales como seguridad.
- DATA .- Contiene información de las capas más altas.

1.2.2. Direccionamiento IP

Como cualquier otro protocolo de la capa de red IP el esquema de direccionamiento de IP es integral al proceso de routing de los datagramas a través de una red.

Cada host en la red TCP/IP es asignado a una única dirección lógica de 32 bits que es divido en 2 campos principales:

El número de red y el número de host. El número de red identifica a una red y es asignado por el centro de información de red Internet (InterNIC) si la red es parte de Internet.

La dirección IP de 32 bits es agrupada en campos de 8 bits. Separados por puntos y representados en formato decimal, el mínimo valor para el octeto es 0 y el máximo valor para el octeto es 255.

. Clases de Direcciones IP

La dirección IP soporta 5 diferentes clases de direcciones: A, B, C, D y E, solo las direcciones A, B y C son aprovechables para uso comercial. Los bits de lado izquierdo indican la parte de red, la tabla 1 muestra una referencia de la distribución de las clases de direcciones:

CLASE DE DIRECCIÓN IP	FORMATO	PROPÓSITO	RANGO DE DIRECCIONES	No BITS RED / HOST	MAXIMO HOSTS
A	N.H.H.H	Pocas grandes organizaciones	1.0.0.0 a 126.0.0.0	7/24	16777214
B	N.N.H.H	Organizaciones de tamaño medio	128.1.0.0 a 191.254.0.0	14/16	65543
C	N.N.N.H	Organizaciones un poco chicas	192.0.1.0 a 223.255.254.0	22/8	245
D	N/A	Grupos Multicast RFC (1112)	224.0.0.0 a 239.255.255.255	N/A	N/A
E	N/A	Experimental	240.0.0.0 a 254.255.255.255	N/A	N/A

La tabla1.- Información de las 5 direcciones IP

. Direccionando la Subnet IP

Las redes IP pueden ser divididas dentro de redes más pequeñas llamadas subnets, subnetting proveen al administrador de red muchas ventajas incluyendo extra flexibilidad, mas eficiencia en el uso de las direcciones de las redes y capacidad de contener tráfico broadcast.

Una dirección de red dada puede ser dividida dentro de múltiples subredes, por ejemplo las direcciones: 172.16.1.0 , 172.16.2.0 , 172.16.3.0 y 172.16.4.0 son todas subnets dentro de la red 172.16.0.0 .

. Mascara de la Subnet IP:

Una dirección subnet es creada tomando prestado bits del campo de host y diseñando ellos como el campo de subnet. El número de bits prestado varia y es especificado por la mascara de la subnet. La Fig. 2 muestra como los bits son tomados prestados del campo de host a crear el campo de la dirección subnet.

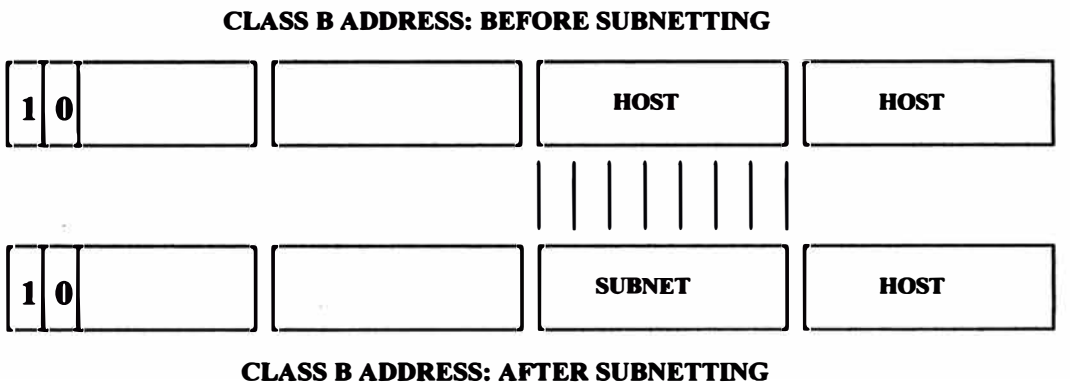

Fig. 2.- Bits son tomados prestados del campo de Host.

La mascara de la subnet utiliza el mismo formato y técnica de representación como la dirección IP, sin embargo la mascara de la subnet tiene todos los bits colocados a uno en el campo de la red y la subred y todos los bits colocados a cero en el campo del host, la figura 3 nos ilustra un ejemplo de mascara de subnet.

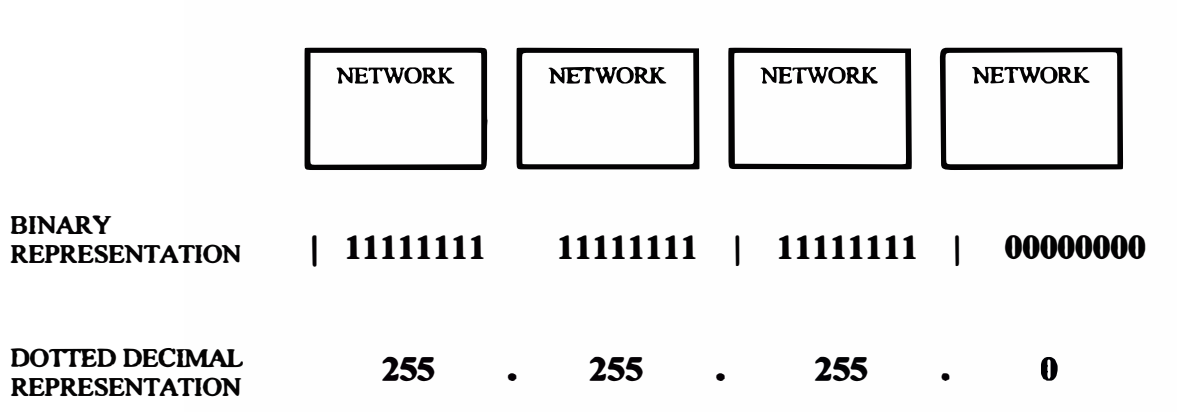

Fig. 3.- Un ejemplo de mascara de Subnet.

CAPÍTULO II
ROUTING EN IP

Routing es el proceso de determinar donde enviar los paquetes de data destinados por la dirección de destino. Los routers mantienen información de routing a habilitar la transmisión y recepción de los paquetes de data. Conceptualmente la información de routing toma la forma de entradas en la tabla de routing, con una entrada por cada ruta identificada. El router puede crear y mantener dinámicamente la tabla de routing y acomodar los cambios de red cada vez que ellos ocurran.

2.1. Protocolo de Interior y Exterior (IGP Y EGP)

Los protocolos de routing son ampliamente divididos en 2 clases, interior gateway protocolos (IGP) y exterior gateway protocolos (EGP).

2.1.1. Protocolo de Gateway Interior

Los protocolos de Interior son usados para redes de routing que están bajo una común administración. Todos los Interior Gateway Protocolos necesitan ser especificados con una lista de redes asociadas antes que el routing activo puede comenzar. Los interior gateway protocolos conocidos son los siguientes:

- Protocolo routing de gateway Internet (IGRP)
- Enhanced Internet gateway routing protocol (EIGRP)
- Open Shortest path first (OSPF)
- Routing Information Protocol (RIP)
- Sistema Intermedio a Sistema Intermedio (IS-IS)

2.1.2. Protocolo de Gateway Exterior

Los protocolos de exterior son usados a intercambiar información de routing entre redes que no comparten una común administración. Los protocolos de gateway exterior requieren 3 seteos de información antes que pueda comenzar a trabajar.

- Una lista de routers vecinos con los cuales va intercambiar información de ruteo.
- Una lista de redes a publicarlas como directamente alcanzables.
- El número del sistema autónomo del router local.

Los protocolos de Gateway exterior más conocidos son:

- Border gateway protocol (BGP)
- Exterior gateway protocol (EGP)

A continuación daremos algunos detalles de la configuración de los Protocolos más conocidos:

2.1.3. Configurando Enhanced IGRP (EIGRP)

Enhanced IGRP usa el mismo algoritmo de vector distancia como IGRP, sin embargo el tiempo de convergencia y la eficiencia operacional a sido mejorada significativamente. Emplea un algoritmo referido como Algoritmo de actualización Difusa (DUAL). Este algoritmo garantiza la operación libre de loops en cada instante a través de una computación de ruta y permite a todos los routers involucrados en un cambio de topología sincronizarse en el mismo tiempo. Los routers que no son afectados en el cambio de topología no son involucrados en la recomputación.

EIGRP Provee los siguientes features:

- Automática redistribución, las rutas IP de IGRP pueden ser redistribuidas dentro de EIGRP y viceversa o si deseas también puedes quitar esta redistribución del router. También puedes quitar completamente IGRP ó EIGRP del router ó solo de especificas interfaces.
- Incrementa el tamaño de la red, con RIP el máximo tamaño de tu red es de 15 saltos, con EIGRP habilitado el mayor tamaño de tu red es de 224 saltos. La métrica de EIGRP esta preparada para soportar miles de saltos, la única barrera a expandir la red es el contador de saltos de la capa de transporte.
- Rápida convergencia, el algoritmo dual permite a la información de routing converger rápidamente.
- Actualizaciones parciales, EIGRP envía actualizaciones (Updates) increméntales cuando el estado del destino cambia, en vez de enviar el entero contenido de la tabla de routing . Este feature minimiza el ancho de banda requerido para paquetes EIGRP.
- Usa menos CPU que IGRP, esto ocurre porque las actualizaciones no necesitan ser procesados cada vez que ellos son recibidos.
- Mecanismo de descubrimiento de los vecinos, este es un simple mecanismo de hello usado a encontrar los routers vecinos. Ello es un protocolo independiente.

a).- Habilitando EIGRP

Para dejar habilitado el proceso de EIGRP en el router es necesario realizar lo siguiente:

Se tiene que habilitar el proceso de routing EIGRP en el modo de configuración global, el comando para habilitar esto es el siguiente:

Router eigrp sistema autónomo

Se tiene que asociar las redes con un proceso de routing EIGRP en el modo de configuración router, el comando para realizar esto es el siguiente:

Network numero de la red

EIGRP envía las actualizaciones a las interfaces en las redes especificadas, si nosotros no especificamos la red de una interfase ellos no serán advertidos en ninguna actualización EIGRP.

2.1.4. Configurando OSPF

Open Shortest Path First (OSPF) es un IGP desarrollado por el grupo de trabajo de OSPF de la fuerza de trabajo de la Ingeniería de Internet. Diseñado expresamente para redes IP. OSPF soporta IP subnetting y tagging de información de routing derivada externamente. OSPF también permite autentificación de paquetes y usa IP multicast cuando envía y recibe paquetes.

OSPF versión 2 fue establecido en 1991 y sus especificaciones están detalladas en el RFC 1247. la gran ventaja de este protocolo de estado del enlace es que es mucho más eficiente y escalable que RIP. La ultima revisión respecto a este protocolo esta en el RFC 2328 desarrollado en Abril de 1998.

a).- Características de OSPF

Entre las características más importantes que el OSPF de cisco soporta son las siguientes:

- Las métricas están definidas por el costo de la ruta.
- Tiene rápida convergencia.
- Soporta VLSM , autentificación, multipath e IP unnumbered.
- Bajo requerimiento de ancho de banda para sus updates.

A continuación vamos a explicar cada uno detalladamente:

- **Métricas**

RIP no tiene concepto de retardo en el enlace ni costo, las decisiones de ruta están hechas puramente en la cantidad de saltos lo cual nos podría llevar a una no optima selección de la ruta para los casos de rutas largas que tiene alto ancho de banda y bajo retardo. OSPF usa un valor de costo cual es basado en la velocidad delas conexiones.

Para calcular la métrica en OSPF se realiza de la siguiente manera:

Métrica = 10 Mbts / BW (ancho de banda)

- **Rápida Convergencia**

En redes grandes la convergencia de RIP puede tomar muchos minutos, en OSPF la convergencia es más rápido porqué los cambios de routing son fluidos inmediatamente y computados en paralelo.

- **Soporta VLSM**

OSPF soporta subnetting y VLSM lo cual significa que puede realizar sumarización de redes. En ves de publicar bastantes específicos prefijos puede solo publicar un solo prefijo sumarizado que contenga todo ello.

- **Uso de Ancho de Banda**

RIP envía toda su tabla de ruteo a sus vecinos cada 30 segundos, lo cual es un problema sobre enlaces Wan de bajo ancho de banda. OSPF no utiliza un broadcast para los updates si no lo hace en forma de multicats y lo realiza cada vez que ocurre un cambio en la red, de esta manera el consumo de ancho de banda de este protocolo es mínimo.

b).- Habilitando OSPF

Como en otros protocolos de routing necesitamos crear un proceso de routing OSPF, especificar el rango de direcciones asociadas con el proceso de routing y adicionalmente se necesita asociar un área ID con ese rango de direcciones IP. Para realizar esto en un router cisco se tiene que realizar las siguientes tareas:

- Habilitar el proceso de routing OSPF lo cual se realiza en el modo de configuración global del router.

Router ospf proceso - ID

- Definir una interfase donde el OSPF va a trabajar o funcionar y adicionalmente se tiene que definir un área-ID para esa interfase.

Network address wildcard – mask **Área** área - ID

CAPÍTULO III
SEGURIDAD EN IP

3.1. Políticas de Seguridad

Qué es una política de seguridad?

Una política de seguridad es una sentencia formal de los roles por los cuales las personas son dadas acceso a la tecnología de una organización o información importante.

Porque crear una política de seguridad?

- Provee un proceso a auditar las existentes redes seguras.
- Provee un esquema de trabajo de seguridad general para implementar la seguridad de las redes.
- Define cual comportamiento esta definido y cual no esta.
- Define un proceso de manejar los incidentes de seguridad de las redes.

Que tipos de políticas de seguridad existen?

Entre las políticas de seguridad que existen son las siguientes:

- Política de seguridad abierta
- Política de seguridad Restrictiva
- Política de seguridad cerrada

3.1.1. Política de Seguridad Abierta

En este caso las compañías prefieren dar a sus usuarios mayor flexibilidad y libertad en la conectividad, la performancia y fácil de usar.

Las compañías en este caso tienden a permitir todas las conexiones de red que no fueron explícitamente denegadas. Esta política de permiso abierto requieren que ellos creen barreras especificas en solo un seleccionado grupo de conexiones.

Entre las características más importantes de este tipo de política de seguridad tenemos:

- Autentificación.- Las empresas utilizan password para la autentificación de los usuarios tanto locales como los remotos los cuales ingresan vía dial-up.
- Control de Acceso.- El control de los accesos de redes remotas se realiza mediante access-list, para este caso no se utiliza Firewalls y tampoco no se utiliza encriptación.

3.1.2. Política de Seguridad Restrictiva

La política de seguridad restrictiva es una combinación de específicos permisos y especificas restricciones. Esta política es más difícil de configurar y administrar, entre las características más importantes de esta política tenemos:

- Autentificación.- Para la identificación de los usuarios remotos las compañías utilizan password de entrada en línea, cual ocurre cuando el usuario accesa dentro del access server antes que el enlace de dialup es establecido. Varios tipos de métodos de autentificación son utilizados tales como PPP y PAP los cuales pueden ser autentificados en un servidor AAA.
- Control de Acceso.- Para el control de acceso de redes remotas tales como el acceso de Internet se realiza mediante lista de accesos, también en este tipo de política es

común el uso de Firewalls, se usa la autentificación de las rutas en los equipos de comunicaciones y finalmente se usa la encriptación de la data.

3.1.3. Política De Seguridad Cerrada

En esta política de seguridad las compañías prefieren un estricto control de conectividad de los usuarios a expensas de la performancia y fácil uso.

Las compañías en este caso tienden a denegar todas las conexiones de red que no son explícitamente permitidas. Entre las características más importantes tenemos:

- Autentificación.- Para este tipo de seguridad las compañías introducen tarjetas digitales y certificados a autorizar y alcanzar sus servidores de autentificación.
- Control de Acceso.- Para controlar el acceso de las redes remotas se utiliza access-list en los gateways y routers, adicionalmente se utiliza firewalls tanto para el acceso a Internet como las conexiones a otras empresas (Extranet), también se utiliza autentificación en los protocolos de ruteo que se utilizan en la red y adicionalmente se usa los features de encriptación tanto para las oficinas remotas que ingresan por línea conmutada o por línea dedicada.

3.2. Modelo AAA

3.2.1. Autentificación

Requiere a los usuarios a proveer información a verificar que ellos realmente son los que ellos dicen que son, esto es usando un usuario y password, tarjetas token y otros métodos.

3.2.2. Métodos de Autentificación

Los métodos de autentificación pueden variar desde los mas suaves a los más duros los cuales lo mostramos a continuación:

- Sin password ó username
- Con password y username los cuales son asignados por el administrador estáticamente hasta que él lo cambie.
- Con password y username pero los cuales cambian o expiran cada cierto tiempo que en menos grado de los cuales son asignados estáticamente.
- One – time passwords (OTP) .- Es un método fuerte que nos provee el más seguro método de password y username. Ellos son basados en una frase secreta la cual es usada a generar una lista de passwords. Ellos son solo útiles para un solo login y no para cualquier otra persona que a capturado ello.
- Tarjeta Token ó Soft .- Basado en alguna cosa que tu tienes (Token card) y alguna cosa que tu conoces (identificador personal). Las token card son dispositivos electrónicos pequeños cerca del tamaño de una tarjeta de crédito. Hay muchos vendedores de Token card y cada uno tiene su propio servidor de token card.

3.2.3. Autentificación PAP y CHAP

Un importante componente a considerar en la seguridad de los accesos dial-up es la autentificación con el protocolo de autentificación de password (PAP) y el protocolo de autentificación de challenge handshaking.

PPP (protocolo punto a punto) es un protocolo de encapsulación estándar para diferentes protocolos de la capa de red (por ejemplo IP) a través de enlaces seriales. PPP habilita la encapsulación entre los clientes remotos y servidores usando cualquiera de los 2 ya sea PAP ó CHAP.

La autentificación PAP usa el protocolo PPP como mostramos a continuación:

- El cliente remoto establece el enlace vía dial-up.
- El cliente remoto habla al servidor de acceso que el esta corriendo PPP.
- El servidor de acceso notifica al cliente remoto a usar PAP en esta sesión.
- El cliente remoto envía el username y el password en formato PAP.
- El servidor de acceso compara el username y el password almacenado en su base de datos en orden a aceptar o rechazar el username y el password.

PAP no es un fuerte método de autentificación, el username y el password es enviado en texto limpio a través del enlace. Un analizador de protocolo podría ser usado a fácilmente capturar el password.

CHAP provee 3 maneras de handshaking, la secuencia de CHAP es como sigue:

- El establecimiento del enlace PPP es después del dial-up, el servidor del acceso es configurado a soportar PPP y CHAP.
- El servidor del acceso habla al remoto cliente a usar CHAP.
- El cliente remoto responde con OK.
- Las 3 maneras que ocurren handshaking son:

  a).- El servidor de red envía un mensaje de challenge al cliente remoto.

  b).- El cliente remoto responde con un valor de hash.

c).- El servidor de acceso de red procesa el valor de hash recibido.

Si ello coincide con la calculación propia de la estación, la autentificación es reconocida, las claves son enviadas periódicamente sobre el enlace.

CHAP periódicamente verifica la identidad del servidor remoto usando una de las 3 maneras de handshaking, cual es hecho hasta el establecimiento del enlace y ello puede ser repetitivo algún tiempo después que el enlace se ha establecido. El servidor de acceso envía un valor de challenge al nodo remoto, el nodo remoto responde con un valor calculado, una manera de la función hash (típicamente MD5). El servidor de acceso de red chequea la respuesta contra su propio calculo del valor de hash esperado. Si el valor coincide la autentificación es reconocida. De otra manera la conexión es terminada inmediatamente.

3.2.4. Servidores de Seguridad AAA

Cisco soporta servidores locales AAA y servidores remotos AAA. Cual es cubierto a continuación:

a).- AAA Con Una Base de Datos de Seguridad Local

Si se tiene uno ó 2 servidores que proveen acceso a la red, tu probablemente quieras almacenar la información de seguridad de username y el password en el servidor de acceso de red, cual es referido como autentificación local. Las características de autentificación local son las siguientes:

- Usado para redes pequeñas.
- El username y el password son almacenados en el router local.

- El usuario se autentifica contra la base de datos de seguridad local en el router que podría ser de modelo cisco.
- Autorización y accounting son soportados.
- Ahorro de costo de la base de datos de seguridad remota.

b).- AAA Con Una Base de Datos de Seguridad Remota

En la medida que la red crece se debería usar una base de datos de seguridad remota que provee información de username y password a cada uno de los routers en la red. Este servidor de base de datos de seguridad remota reside en un servidor de seguridad de tu red.

Una base de datos de seguridad remota es conveniente cuando se tiene un largo número de routers proveyendo acceso a la red. Una base de datos de seguridad ayuda en la necesidad de estar actualizando cada servidor de acceso de red con un nuevo username de autentificación y autorización para miles de potenciales usuarios dial-up.

El primario beneficio de la base de datos de seguridad remota es que ello simplifica la administración y asegura la consistente administración de políticas para los remotos accesos, accesos dial-up y administración del router a través del control centralizado.

Los protocolos mas conocidos de los servicios de seguridad son los siguientes:

Tacacs, Radius y Kerberos.

3.3. Tacacs +

El sistema de acceso de control de acceso de terminal (TACACS +) es una versión mejorada de TACACS. TACACS + envía información de usuario y clave a un servidor de seguridad centralizado.

TACACS+ tiene los siguientes features:

- TCP para transporte de data confiable, usa TCP/IP como protocolo de comunicación entre el remoto cliente y el servidor de seguridad.
- Soporta arquitectura AAA.
- El enlace es encriptado, la carga útil de los paquetes IP (Paquetes TCP) es encriptado para seguridad y es almacenado en forma encriptada para seguridad en la base de datos de seguridad remota.
- Soporta autentificación PAP y CHAP.
- Es muy usado para seguridad de ambos enlaces wan y lan.
- SLIP, PPP y ARA son soportados para seguridad de enlaces dial-up, las direcciones X.121 que son usados con X.25 son también soportados.
- Soporta autocomando.
- Soporta Callback.
- Access-list por usuario pueden ser asignados en la fase de autorización.

3.3.1. Proceso de Autentificación AAA / Tacacs

EL servidor de acceso intercambia información de autentificación del usuario con el servidor TACACS transmitiendo paquetes TACACS a través de la red de la siguiente manera.

- El servidor de acceso envía un paquete START al servidor TACACS a iniciar el proceso de autentificación.
- El servidor TACACS típicamente envía un paquete GETUSER conteniendo un prompt username al servidor de acceso.
- El servidor de acceso muestra el prompt al usuario y envía el username que el usuario ingresa, esto dentro de un paquete CONTINUE al servidor TACACS.
- El servidor de TACACS típicamente envía un paquete GETPASS al servidor de acceso conteniendo un prompt para el password.
- El servidor de acceso envía un paquete CONTINUE conteniendo el password al servidor TACACS.
- El servidor TACACS chequea el password contra la información almacenada en el archivo de configuración del TACACS con lo cual decide sí el usuario pasa ó falla la autentificación. El servidor TACACS envía un paquete PASS ó FAIL de regreso al servidor de acceso como estatus final.

3.4. Radius

El RADIUS es un sistema cliente servidor distribuido que asegura las redes contra acceso no autorizado. RADIUS es un protocolo totalmente abierto distribuido en formato código fuente que puede ser modificado a trabajar con algún sistema de

seguridad corrientemente aprovechable en el mercado. Cisco soporta autentificación de seguridad bajo el paradigma de seguridad AAA. RADIUS pueden ser usados con otros protocolos de seguridad tales como TACACS, KERBEROS o local username lookup. Como una información adicional podemos decir que RADIUS es soportado en los CISCO 1600, 2500, 2600, 3600, 4000, 5000 y 7000.

Cuando un usuario quiere log in y autentificarse a un servidor de acceso usando RADIUS, ocurren los siguientes pasos:

- El usuario inicia una autentificación PPP al servidor de acceso.
- El usuario es incitado para entrar el username y el password.
- El usuario replica al challenge (si CHAP)
- el username y el password encriptado son enviados sobre la red al servidor RADIUS.
- El usuario recibe uno de las siguientes respuestas desde el servidor RADIUS.

  Accept.- El usuario es autentificado.

  Reject.- El usuario no es autentificado y es incitado a reentrar el username y el password ó el acceso es denegado.

  Challenge.- un challenge es usado por el servidor RADIUS. El challenge colecciona adicional data desde el usuario.
- El cliente RADIUS trabaja en servicios.
- La respuesta ACCEPT ó REJECT es juntada con adicional data que es usada para las sesiones EXEC ó autorización de la red. Se necesita primero completar la

autentificación del RADIUS antes de usar la autorización del RADIUS. Los adicionales datos incluida con los paquetes ACCEPT ó REJECT consisten de lo siguiente:

a).- Los servicios que el usuario puede acceder, incluyendo telnet, rlogin ó conexiones LAT y PPP.

b).- Servicios SLIP ó EXEC.

c).- Parámetros de conexiones incluyendo las direcciones IP del cliente ó Host, access-list y usernames de los timeouts.

TACACS es considerado mejor que el RADIUS debido a :

- Los paquetes TCP en el TACACS son encriptados, en el RADIUS solo es enciptado el password secreto.
- TACACS separa autentificación y autorización haciendo posible servicios de seguridad distribuido.
- RADIUS tiene limitado espacio de nombre para los atributos.

En la tabla 2 se hace una comparación entre TACACS+ y RADIUS

	TACACS	RADIUS
FUNCIONALIDAD	SEPARA AAA	COMBINA AUTENTIFICACION Y AUTORIZACION
PROTOCOLO DE TRANSPORTE	TCP	UDP
CHALLENGE / RESPUESTA	BIDIRECCIONAL	UNIDIRECCIONAL
PROTOCOLO SOPORTADO	FULL SOPORTE	NO ARA NO NETBEUI
CONFIDENCIALIDAD	ENTERO PAQUETE ENCRIPTADO	PASSWORD ENCRIPTADO

Tab. 2.- Comparación entre TACACS+ y RADIUS

3.5. Kerberos

KERBEROS es un protocolo de autentificación de red de llave secreta desarrollado en el instituto de tecnología de Massachusett, que usa el algoritmo de encriptación de la data standard (DES) para desarrollar la encriptación y autentificación.

KERBEROS fue diseñado para autentificar las solicitudes para los recursos de la red. KERBEROS similar a otros sistemas de llaves secretas esta basado en el concepto de un arreglo de tercera parte que desarrolla segura verificación de usuarios y servicios. En el protocolo KERBEROS esta tercera parte es llamada Centro de Distribución de llaves (KDC).

KERBEROS tiene un proceso de autentificación y administración. El siguiente procedimiento describe como un usuario remoto con un ticket granting ticket (TGT) autentifica a los servicios de red dentro de KERBEROS. Asumimos que el usuario remoto en el host A quiere acceder al host B.

- El usuario en el host A inicia una aplicación kerberizada tal como telnet al host B. La aplicación Kerberizada construye una respuesta de servicio credencial y envía ello al KDC. La respuesta de servicio credencial incluye la identificación del usuario y la solicitud de identificar el servicio de red deseado.
- El KDC intenta desencriptar la solicitud del servicio credencial con el TGT ello afecta al usuario en el host A. Si el KDC puede desencriptar el paquete, ello asegura que el usuario autentificado en el host A envía la respuesta. El KDC apunta los servicios de red identificados en la respuesta del servicio credencial.
- El KDC construye un servicio credencial para los servicios de red apropiados en el host B en ves del usuario del host A. El servicio credencial contiene la identidad del cliente y la identidad de los servicios de red deseados.
- El host A tiende a desencriptar el servicio credencial con los TGT de los usuarios. Si el host A puede desencriptar el servicio credencial, ello asegura que la credencial proviene desde el real KDC. El host A envía el servicio credencial al servicio de red deseado.

- Los servicio de red intentan desencriptar el servicio credencial, si los servicios de red pueden desencriptar la credencial ello es seguro que la credencial tuvo un problema desde el KDC.
- En este punto el usuario es autentificado a los servicios de red en el host B, este proceso es repetido cada vez que el usuario quiere acceder a los servicios de red .

3.6. Encriptación

Que es la encriptación?

La encriptación es el proceso de tomar data en forma usable y alcanzable y convertirla en una forma no alcanzable y no usable. Entonces la data puede ser almacenada y transmitida seguramente. La data puede ser desencriptada y convertida de regreso a su forma usable.

La encriptación es útil en:

- Asegura las redes VPN entre empresas de negocios sobre una red de Internet.
- Asegura el comercio desde lugares remotos al campus local.
- Protección de tráfico WAN sobre líneas alquiladas en Internet.
- Seguras transacciones entre servidores Web y usuarios remotos.
- Asegura la comunicación móvil de data desde lugares remotos al lugar principal si un router es usado como site remoto.
- Asegura tráfico de Intranet.

3.6.1. Alternativas de Encriptación

Los administradores de red tienen que escoger la implementación de la encriptación en la comunicación de la data en una de las 3 capas del modelo OSI:

Las capas en las cuales se puede desarrollar la encriptación son la capa de aplicación, la capa de enlace y la capa de red.

La encriptación de la capa de aplicación requiere que cada aplicación en el host que esta generando data sensitiva soporte encriptación. Todos los host con cuales esa aplicación se comunica necesitan hablar el mismo lenguaje de encriptación, igualmente si ellos residen en diferentes plataformas. La encriptación de la capa de aplicación tiene la ventaja de operar entre los puntos ó equipos remotos y puede ser invocado cada vez que el usuario lo necesite. Este control descentralizado de usuario hace difícil para el administrador del sistema controlar la política de seguridad del sistema.

La encriptación de la data en la capa de enlace puede ser implementado en dispositivos de salida del router en enlaces sensitivos. Pero los usuarios necesitan desencriptar el tráfico antes que ello entre al router. Este proceso puede ser repetido en cada enlace donde la seguridad es una preocupación.

Debido a que este método de encriptación no deja una dirección clara para la operación de routing, la desencriptación y reencriptación podría necesitar ocurrir varias veces, lo cual llevaría a incrementar el retardo en la red.

La encriptación de la capa de red puede ser hecho en cualquier lado de la red, y puede ser implementado en todo tráfico sin afectar todas las aplicaciones de los host. Ello también deja la información de la capa 3 y 4 en limpio para uso en routing. Por tanto mientras sumas seguridad a la red los usuarios continúan siendo capaces a desarrollar calidad de servicio (QoS) entre los puntos remotos. La encriptación de la

capa de red tiene la ventaja de operar transparentemente entre subnets y siendo confiable desde la perspectiva del administrador de la red.

Entre las tecnologías de encriptación conocidas tenemos las siguientes:

- Encriptación digital estándar (DES)
- Signatura digital estándar (DSS)
- Intercambio de claves Diffie-Hellman
- Mensajes de dígitos 5 (MD5)

3.6.2. IPSEC

En simples terminos IPSEC provee seguros túneles entre 2 equipos (peers) tales como 2 routers, en la cual se define cuales paquetes serán pasados por este tunel y también los parámetros que serán usados en estos para proteger los paquetes sensitivos.

Mas exactamente estos túneles son asociaciones de seguridad que son establecidos entre 2 parejas IPSEC, las asociaciones de seguridad definen cuales protocolos y algoritmos serán aplicados a los paquetes sensitivos. Las asociaciones de seguridad son unidireccionales y son establecidas por el protocolo de seguridad (AH ó ESP)

Con IPSEC se define que tráfico será protegido entre 2 parejas IPSEC configurando listas de acceso y aplicando estas listas de acceso a las interfaces de tal manera que se configura los crypto map . Por consiguiente el tráfico podría ser seleccionado basado en la dirección fuente y la dirección destino y opcionalmente protocolos de capa 4 y puertos. Las listas de acceso solo definen el trafico que será

protegido con IPSEC no define cual tráfico será bloqueado ó permitido por una interfase.

Un crypto map puede contener múltiples entradas cada una con una diferente lista de acceso. Las entradas del crypto map son alcanzadas en orden. El router atiende a los paquetes que machan con las listas de acceso especificado en esa entrada.

Los estándares soportados por IPSEC son:

Autentificación de cabecera (AH).- Un protocolo de seguridad cual provee autentificación de data y opcionales servicios de antireplay.

Segura encapsulación de la carga útil (ESP) .- Un protocolo de seguridad que provee servicios de data privada y opcional autentificación de la data y opcional servicio de antireplay. ESP encapsula la data a ser protegida.

CAPÍTULO IV
VOZ SOBRE IP

VOIP es un protocolo de capa 3 que usa varios protocolos de capa 2 tales como PPP, frame relay ó ATM para su transporte. VOIP habilita a los routers, access server y concentradores de acceso multiservicio a llevar y enviar tráfico de voz y fax sobre una red IP. En VOIP el procesador de señal digital (DSP) segmenta la señal de voz en frames y lo almacena en paquetes de voz. Estos paquetes de voz son transportados vía IP en combinación con los protocolos de comunicación de voz ó estándar tales como H323, protocolo de control de gateway media (MGCP) ó protocolo de inicio de sesión.

La tabla 3 muestra la relación entre el modelo de referencia OSI y los protocolos y funciones de los elementos de red VOIP.

NUMERO DE LA CAPA OSI	NOMBRE DE LA CAPA OSI	FUNCIONES Y PROTOCOLOS VOIP
	APLICACIÓN	NETMEETING / APLICACIONES
6	PRESENTACIÓN	CÓDIGOS
5	SESIÓN	H323 / MGCP / SIP
4	TRANSPORTE	RTP / TCP / UDP
3	RED	IP
2	ENLACE DATA	FRAME RELAY, ATM, ETHERNET, PPP Y OTROS

Tab. 3.- Relación entre el modelo OSI y los elementos de red de VOIP

Entre los protocolos de control de llamadas tenemos los siguientes:

- H323.- La ITU estandarizo las especificaciones para el envío de voz, video y data a través de una red. Las especificaciones de H323 incluyen muchos estándares tales

como H225 (control de llamada), H235 (seguridad), H245 (ruta media y negociación de parámetros) y H450 (servicios suplementarios).

- MGCP.- Protocolo de control de gateway medio, MGCP es un estándar de la IETF para controlar los gateways de voz a través de una red IP.
- SIP.- Protocolo de iniciación de sesión, definido en el RFC 2543 de la IETF.

Los protocolo de VOIP típicamente usan RTP (protocolo de transporte de tiempo real) como medio de flujo ó ruta de comunicación. RTP usa UDP como su protocolo de transporte. El tráfico de señalización de voz frecuentemente usa TCP como su medio de transporte. La capa IP provee el routing y el direccionamiento de la capa de red, los protocolos de la capa de enlace controlan y dirigen la transmisión de la información sobre el medio físico.

4.1. Beneficios de VOIP

Entre los más importantes beneficios están los siguientes:

- Ahorro de costos.- Trasladando los tráficos de voz sobre una red IP las empresas en la actualidad evitan los gastos producidos si se llevaran sobre una red publica, los proveedores de servicio y usuarios finales pueden conservar ancho de banda invirtiendo en capacidades adicionales solo si ello es necesario.
- Estándar abierto e interoperabilidad con multivendedores.- Optando por estándares abierto tanto los proveedores de negocios y servicios pueden comprar equipos desde diferentes vendedores eliminando su dependencia de soluciones propietarias.

- Redes de datos y voz integrados.- Haciendo la voz otra aplicación IP las compañías pueden tener redes integradas de voz y datos, estas redes integradas no solo proveen la confiabilidad y calidad de las redes publicas de telefonía de estos días si no que ellos habilitan a las compañías a tomar más rápida ventaja de flexibilidad para las oportunidades en las comunicaciones del mundo de hoy.

4.2. Proceso de Establecimiento de Una Llamada de Voz

Antes de seguir avanzando en el tema de la configuración de VOIP debemos tener claro que sucede cuando se realiza una llamada de VOIP usando H323.

- El usuario ó persona que va realizar la llamada levanta el teléfono, señalando una condición de off-hook a la capa de aplicación de VOIP.
- La capa de sesión realiza un tono de dial esperando que la persona quien quiere llamar ingrese los dígitos apropiados.
- Cuando la persona que quiere llamar dial up los números, estos son acumulados y recepcionados por la capa de sesión.
- Después que suficientes dígitos son almacenados en orden que machen con un dial plan configurado, el numero de teléfono es mapeado vía este dial plan a un host IP. Este host IP tiene una directa conexión con el numero telefónico ó la PBX que es responsable para completar la llamada al patrón destino configurado.
- La capa de sesión corre un protocolo de sesión H323 a establecer una canal de transmisión y una canal de recepción para cada dirección sobre la red IP. Si la llamada esta siendo manejada por una PBX esta envía la llamada al teléfono destino. Si el

protocolo de reservación de recursos esta siendo utilizado (RSVP), las reservaciones RSVP son colocadas en efecto para lograr la calidad deseada sobre la red IP.

- Los codificadores y decodificadores son habilitados en ambos extremos de la conexión y la conversación procede usando RTP/ UDP /IP como el protocolo stack.
- Algunas indicaciones de progreso de llamadas u otras señalizaciones pueden ser llevadas sobre la ruta de voz tan pronto como el canal de comunicación es establecido. La señalización que puede ser detectado por los puertos de voz (por ejemplo los dígitos DTMF) es también detectado por la capa de sesión en cualquier extremo de la comunicación y llevados sobre la red IP encapsulados en el Protocolo de Conferencia de Tiempo Real (RTCP) usando el mecanismo de extensión RTCP APP.
- Cuando cualquiera de los extremos de la comunicación cuelga la llamada las políticas de RSVP son terminadas y la comunicación se termina. Cada extremo de la comunicación se coloca en estado disponible para la siguiente comunicación.

4.3. Flujo Básico de La Voz

El flujo de un circuito de voz comprimido es mostrado en la figura 4 La señal análoga desde el teléfono es digitalizada dentro de señales PCM por el codificador y el decodificador. Las muestras PCM son entonces pasadas al algoritmo de compresión cual comprime la voz en un formato de paquetes para poder ser trasmitida sobre la wan. En el otro extremo de la nube las mismas funciones son desarrolladas en orden reverso.

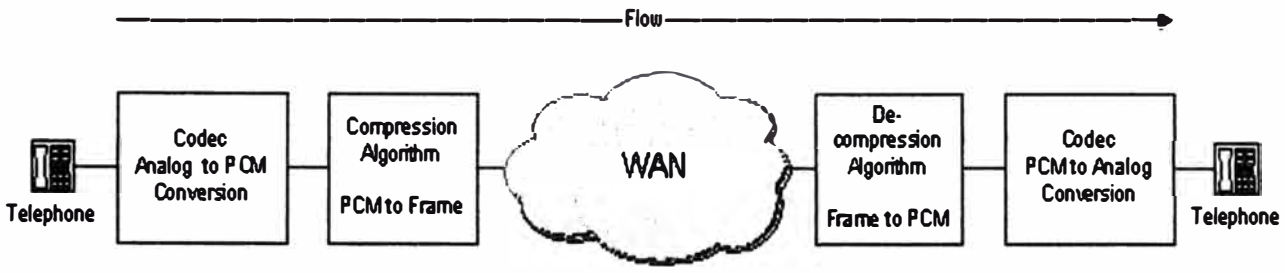

Fig. 4.- Diagrama de flujo de la voz extremo a extremo

Dependiendo como la red es configurada el router ó el gateway puede desarrollar ambas funciones tanto la de codificación y compresión o solamente una de ellas, por ejemplo si un sistema de voz análogo es usado, el router realiza la función de codificación y compresión tal como lo mostramos en la figura 5.

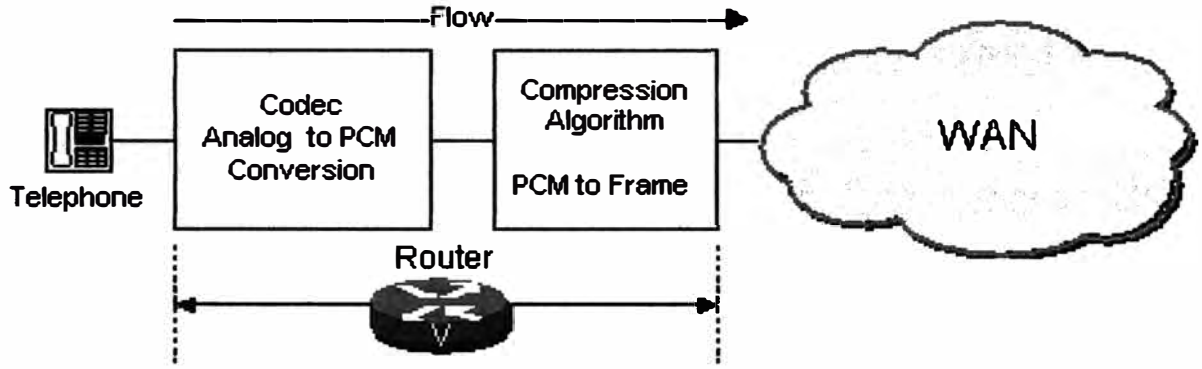

Fig. 5.- Función de codificación en un router como gateway

En vez de eso una PBX digital es usado, la PBX desarrolla la función de codificación y el router desarrolla la función de compresión, un ejémplo es mostrado en la figura 6.

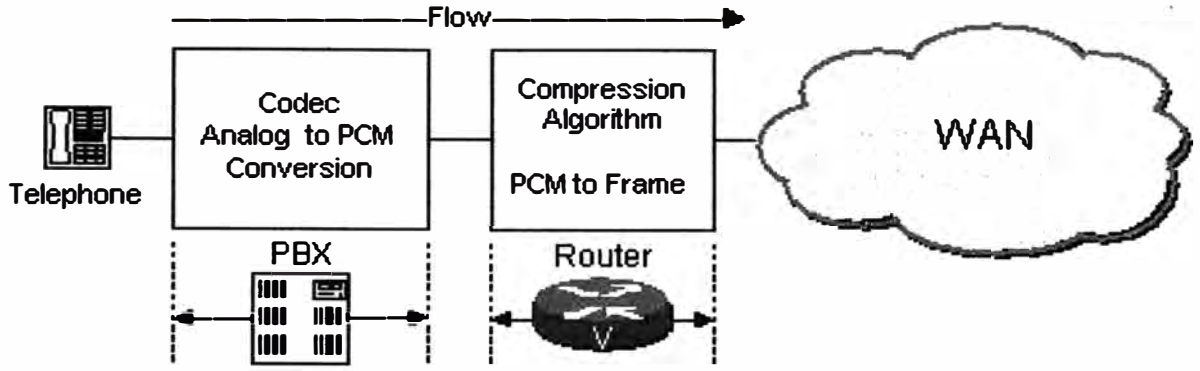

Fig. 6.- Función de codificación de la PBX

4.4. Como Trabaja La Compresión de La Voz

La alta complejidad del algoritmo de compresión usado por los routers cisco trabajan analizando una muestra de bloque PCM entregado por el codificador de voz. Estos bloques varían de longitud dependiendo en el tipo de codificador, por ejemplo el básico bloque usado por el algoritmo G729 es 10ms, el básico bloque usado por el algoritmo G723.1 es de 30ms, un ejemplo como el sistema de compresión trabaja es mostrado en la figura 7.

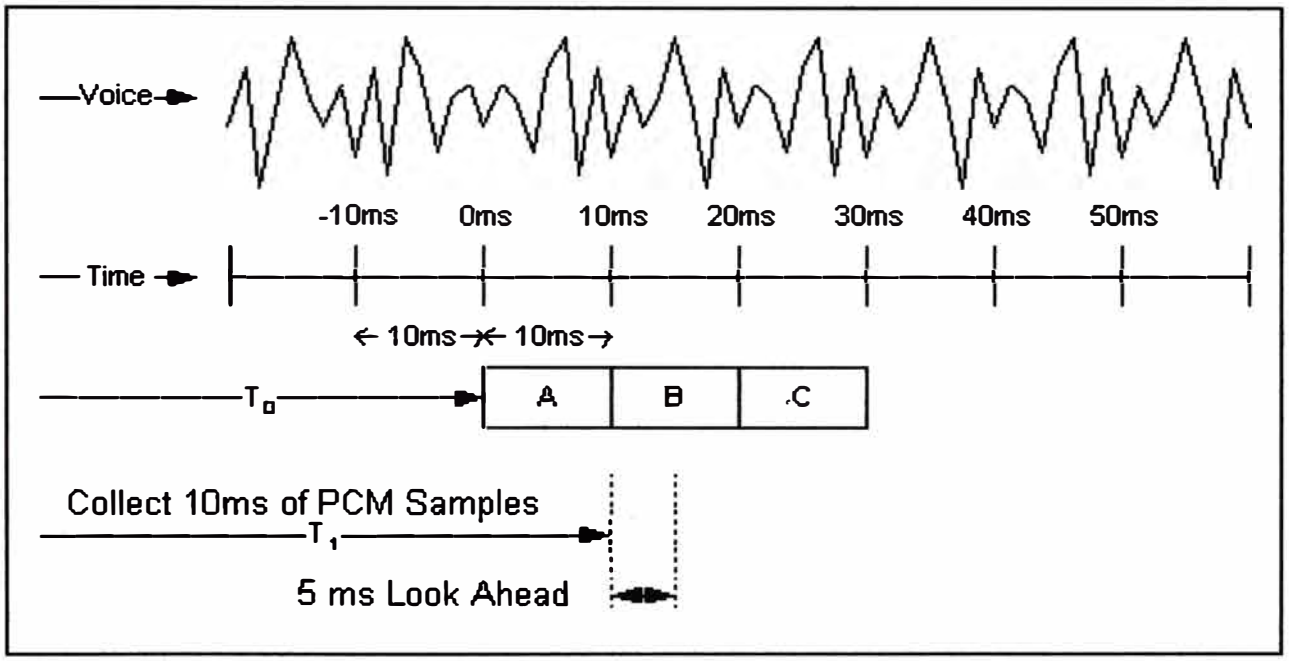

Fig. 7.- Compresión de la voz

La cadena de voz análoga es digitalizada en muestras PCM y entregada al algoritmo de compresión en incrementos de 10ms.

4.5. Retardos en Los Paquetes de Voz

La ITU tiene consideraciones del retardo de la red para las aplicaciones de voz las cuales la presenta en las recomendaciones G.114, estas especificaciones define 3 rangos las cuales mostramos en la tabla 4.

RANGO EN MILISEGUNDOS	DESCRIPCIÓN
0 - 150	Aceptable para muchas aplicaciones de los usuarios.
150 - 400	Aceptable teniendo en cuenta que los administradores estén conscientes del tiempo de transmisión y de su impacto en la calidad de transmisión de las aplicaciones de los usuarios.
Arriba de 400	No aceptable para los generales propósitos de las redes, sin embargo es reconocido que en algunos casos el limite será excedido.

Tab. 4.- Especificaciones de retardo

4.5.1. Fuentes de Retardo

Hay 2 distintos tipos de retardo, el fijo y el variable.

- Las componentes de retardo fijo están relacionados sobre todo al retardo en las conexiones.
- Los retardos variables se suman desde los retardos de encolamiento en los buffers de los puertos seriales conectados a las interfaces wan. Estos buffers crean variable retardos llamados jitter a través de la red. Los retardos variables son manejados por el buffer de-jitter en el gateway.

La figura 8 identifica las fuentes de retardo fijo y variable en la red.

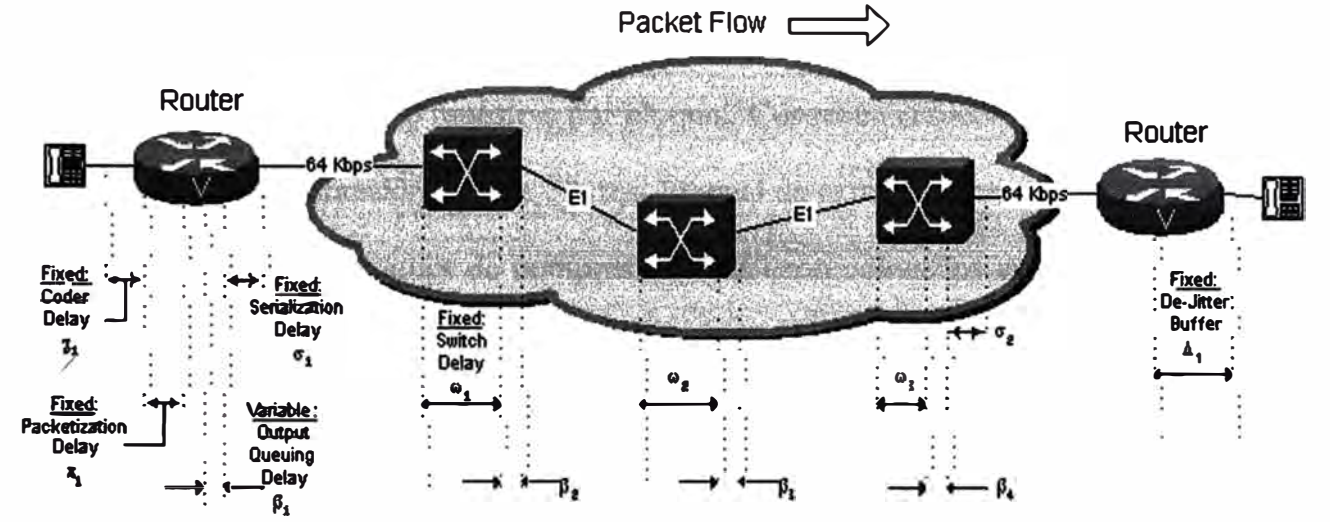

Fig. 8.- Fuentes de retardo fijo y variable

4.5.2. Retardo del Codificador

También llamado retardo de procesamiento, el retardo del codificador es el tiempo que toma el procesador de señal digital (DSP) a comprimir un bloque de muestras PCM. Por que los diferentes codificadores trabajan de diferente manera este retardo varía con el codificador de voz usado y velocidad del procesador. Por ejemplo el algoritmo de Predicción lineal de código algebraico excitado (ACELP) trabaja 10ms por bloque de muestra PCM.

El tiempo de compresión para ACELP de estructura conjugada (CS-ACELP) es de un rango de 2,5ms a 10ms dependiendo en la carga del procesador DSP. Si el DSP esta totalmente cargado con los 4 canales de voz el retardo del codificador será de 10ms. Si el DSP es cargado con uno de los 4 canales el retardo del codificador será de 2,5ms. Para propósitos de diseño se utilizara el peor de los casos es decir 10ms.

El tiempo de descompresión es 10% por cada bloque sin embargo como ello podría ser de múltiples muestras por cada bloque el tiempo de descompresión es proporcional al numero de muestras por bloque. Consecuentemente para un bloque de 3 muestras la descompresión será de 3*1ms. Lo cual da como resultado un tiempo de 3ms. Generalmente 2 ó 3 bloques de compresión G729 son colocados en un frame mientras una solo muestra de compresión G723.1 es colocado en un solo frame.

4.5.3. Retardo del Algoritmo

El algoritmo de compresión necesita tener conocimiento de las características de voz a correctamente procesar el bloque de muestra N, necesita tener algunos conocimientos de que esta en el bloque N + 1 a exactamente reproducir el bloque de muestra N, esta mirada hacía adelante, cual es un adicional retardo es llamado retardo del algoritmo y efectivamente incrementa la longitud del bloque de compresión.

Por supuesto que esto sucede repetidamente tal que el bloque N +1 mira dentro del bloque N + 2 y así sucesivamente. El efecto del retardo de la red es unos 5ms. adicionales al retardo del enlace.

- Retardo del algoritmo para G726 es 0ms.
- Retardo del algoritmo para G729 es 5ms.
- Retardo de algoritmo para G723.1 es 7.5ms.

4.5.4. Retardo de Paquetización

El retardo de paquetización es el tiempo tomado a llenar la carga útil de un paquete con información codificada y comprimida. El retardo es una función del tamaño del bloque de la muestra y el numero de bloques colocados en un frame. El retardo de

paquetización puede ser llamado retardo de acumulación, como los paquetes de voz se van acumulando en un buffer antes de ser liberados.

Como una regla debería ser que el retardo de paquetización no debería ser mayor que 30ms. En la tabla 5 nos muestra el retardo para diferentes tamaños de paquetes.

CODER	COMPRESIÓN	TAMAÑO DEL PAYLOAD	RETARDO DE PAQUETIZACIÓN	TAMAÑO DEL PAYLOAD	RETARDO DE PAQUETIZACIÓN
PCM G711	64Kbps	160	20	240	30
ADPCM G726	32Kbps	80	20	120	30
CS-ACELP G729	8Kbps	20	20	30	30
MP-MLQ G723.1	6.3Kbps	24	24	60	48
MP-ACELP G723.1	5.3Kbps	20	30	60	60

Tab. 5.- Retardo de paquetización

4.5.5. Retardo de Serialización

El retardo de serialización es el tiempo requerido a sincronizar un paquete de voz ó data dentro de la red, y ello esta directamente relacionado con el clock rate en la troncal. Recordar que enlaces de bajo clock y pequeños tamaños de frame, el extra flag necesario a separar los frames es significante.

La tabla 6 nos muestra el retardo de serialización requerido para diferentes tamaños de frames y diferentes velocidades de línea. Esta tabla usa el tamaño de frame total, no solo el tamaño del payload.

TAMAÑO DEL FRAME (b	VELOCIDAD DE LINEA (KBps)										
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	768	1024	1544	2048
38	15.83	5.43	4.75	2.38	1.19	0.79	0.59	0.4	0.3	0.2	0.15
48	20	6.86	6	3	1.5	1	0.75	0.5	0.38	0.25	0.19
64	26.67	9.14	8	4	2	1.33	1	0.67	0.5	0.33	0.25
128	53.33	18.29	16	8	4	2.67	2	1.33	1	0.66	0.5
256	106.7	36.57	32	16	8	5.33	4	2.67	2	1.33	1
512	213.3	73.14	64	32	16	10.7	8	5.33	4	2.65	2
1024	426.7	146.3	128	64	32	21.3	16	10.7	8	5.31	4
1500	625	214.3	188	93.8	46.9	31.3	23.4	15.6	11.7	7.77	5.86
2048	853.3	292.6	256	128	64	42.7	32	21.3	16	10.6	8

Tab. 6.- Retardo de serialización en milisegundos.

4.6. Ancho de Banda por Llamada de Voz

Uno de los más difíciles conceptos de comprender es del consumo de ancho de banda por llamada, para el calculo del ancho de banda por llamada se debe tener en cuenta los siguientes datos:

Tamaño del paquete de voz = (Cabecera de la capa 2) + (Cabecera IP/UDP/RTP) + (carga útil del paquete de voz)

Paquetes de voz por segundo (PPS) = velocidad del código / Tamaño carga útil.

Ancho de banda = Tamaño del paquete de voz * PPS

La tabla 7 muestra una combinación de codecs, tamaño de carga útil, Compresión de cabecera RTP y detección de actividad de voz (VAD). La compresión de la cabecera también es referida como cRTP.

Las siguientes suposiciones son adoptadas en la tabla:

La cabecera de IP / UDP / RTP es de 40 bytes.

La cRTP reduce el tamaño a 2 ó 4 bytes.

Multilink PPP ó Frame relay suma 6 bytes de cabecera de la capa de enlace.

Bajo segura condiciones de red, VAD podría reducir en un largo numero de llamadas sobre el tiempo en un porcentaje de 35% del ancho de banda. Para el propósito de los cálculos de la tabla se asumió que VAD redujo la utilización del ancho de banda a 65% del total.

técnica de compresión (codec bit rate)	Tamaño carga útil	Ancho de banda en full rate y MLPPP/FRF.12	Ancho de banda con cRTP y MLPP/FRF.12	Ancho de banda en full rate ,VAD y MLPPP/FRF.12	Ancho de banda con cRTP, VAD y MLPPP/ FRF.12
	(Bytes)	(Kbps)	(Kbps)	(Kbps)	(Kbps)
G.711 (64K)	240	76	66	50	43
G.711 (64K)	160 (Def)	83	68	54	44
G.726 (32K)	120	44	34	29	22
G.726 (32K)	60 (Def)	57	36	37	24
G.726 (24K)	80	38	27	25	17
G.726 (24K)	40 (Def)	52	29	34	19
G.728 (16K)	80	25	18	17	12
G.728 (16K)	40 (Def)	35	19	23	13
G.729 (8K)	40	17.2	9.6	11.2	6.3
G.729 (8K)	20 (Def)	26.4	11.2	17.2	7.3
G.723.1 (6.3K)	48	12.3	7.4	8	4.8
G.723.1 (6.3K)	24 (Def)	18.4	8.4	12	5.5
G.723.1 (5.3K)	40	11.4	6.4	7.4	4.1
G.723.1 (5.3K)	20 (Def)	17.5	7.4	11.4	4.8

Tab. 7.- Ancho de banda por llamada de voz

Por ejemplo para un codec de G729 y teniendo una capa de enlace ethernet se tiene:

Que el codec bit rate es de 8Kbps, la capa de enlace tiene una cabecera de 14bytes. Entonces haciendo los cálculos arriba mencionados tenemos:

Tamaño del paquete de voz = 14 + 40 +20 = 74bytes.

PPS = (8*1024) / (20*8) = 51.2pps.

Entonces BW = 51.2 * 74 * 8 = 30.3kbps

4.7. Compresión de Cabecera RTP

Todos los paquetes de voz están compuestos por 2 componentes, las muestras de voz y la cabecera IP/ UDP/ RTP. Aunque las muestras de voz son comprimidas por la DSP y las cuales podrían variar de tamaño de acuerdo al codec utilizado, la cabecera tiene un tamaño constante de 40bytes. Si comparamos los 20bytes de carga útil para el codec G729 notamos que 40bytes de cabecera ocasiona bastante overhead. Usando cRTP esta cabecera se puede reducir a 2 ó 4 bytes lo cual nos da un ahorro de ancho de banda para la voz sobre IP.

La gráfica de continuación nos muestra la cabecera RTP después de la compresión.

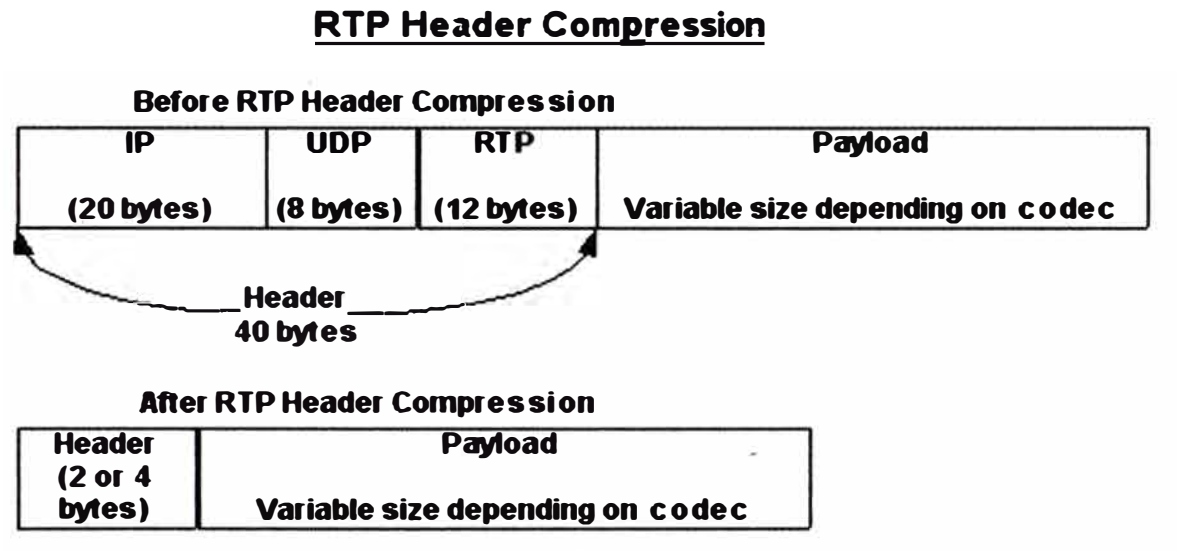

Fig. 9.- Compresión RTP

4.8. H323

H323 fue originalmente creado a proveer un mecanismo para el transporte de aplicaciones de multimedia sobre redes LAN, aunque H323 todavía sigue siendo usado para videoconferencia, ello a sido utilizado para el crecimiento de la VOIP y sus necesidades. Ahora H323 es mas comúnmente usado para señalización en VOIP y control de llamadas con portadores nacionales e internacionales.

H323 es considerado un protocolo fundamental por que ello define los aspectos de la transmisión de la llamada desde el establecimiento a la capacidad de intercambiar los recursos de la red. H323 esta basado en el protocolo ISDN (Q931) cual permite a ello operar fácilmente con las redes de voz tales como la PSTN ó sistema de señalización numero 7.

Como un protocolo de arquitectura distribuida, H323 permite a las compañías grandes tener redes que son escalables y redundantes. Ello provee mecanismos para interconectar con otras redes de VOIP y soportan redes inteligentes en cualquiera de sus puntos finales ó Gatekeepers.

4.8.1. Protocolos H323

Señalización Ras H225

RAS es un protocolo de señalización usado entre gateways y gatekeepers. El canal RAS esta abierto antes que cualquier otro canal y es independiente del seteo de la llamada y canales del medio de transporte.

RAS usa puertos UDP 1719 (mensaje RAS H225) y 1718 (unicast de descubrimiento de gatekeeper).

Señalización de Control de Llamada H225

La señalización de control de llamada H225 es usada para establecer las conexiones entre puntos finales H323. Las recomendaciones de la ITU H225 especifica el uso y soporte de mensajes de señalización Q931.

Un confiable canal de control de llamada (TCP) es creado a través de una red IP en el puerto TCP 1720. Este puerto inicia los mensajes de control de llamada para los propósitos de conexión, mantenimiento y desconexión de llamadas.

Cuando un gateway esta presente en la zona de red, los mensajes de seteo de llamada H225 son intercambiados ya sea por vía de señalización de llamada directa ó señalización de llamada de gatekeeper ruteado. Si no hay Gatekeeper presentes, los mensajes H225 son intercambiados directamente entre los puntos finales.

TRANSPORTE Y CONTROL DE MEDIO H245

H245 maneja el control de los mensajes extremo a extremo entre las entidades H323. H245 procede a establecer canales lógicos para la transmisión de audio, video, data e información del control del canal, ello es usado a negociar el uso del canal y capacidades tales como:

- Control de flujo
- Capacidad de intercambio de mensajes

La gráfica 10 nos muestra el protocolo de señalización H323.

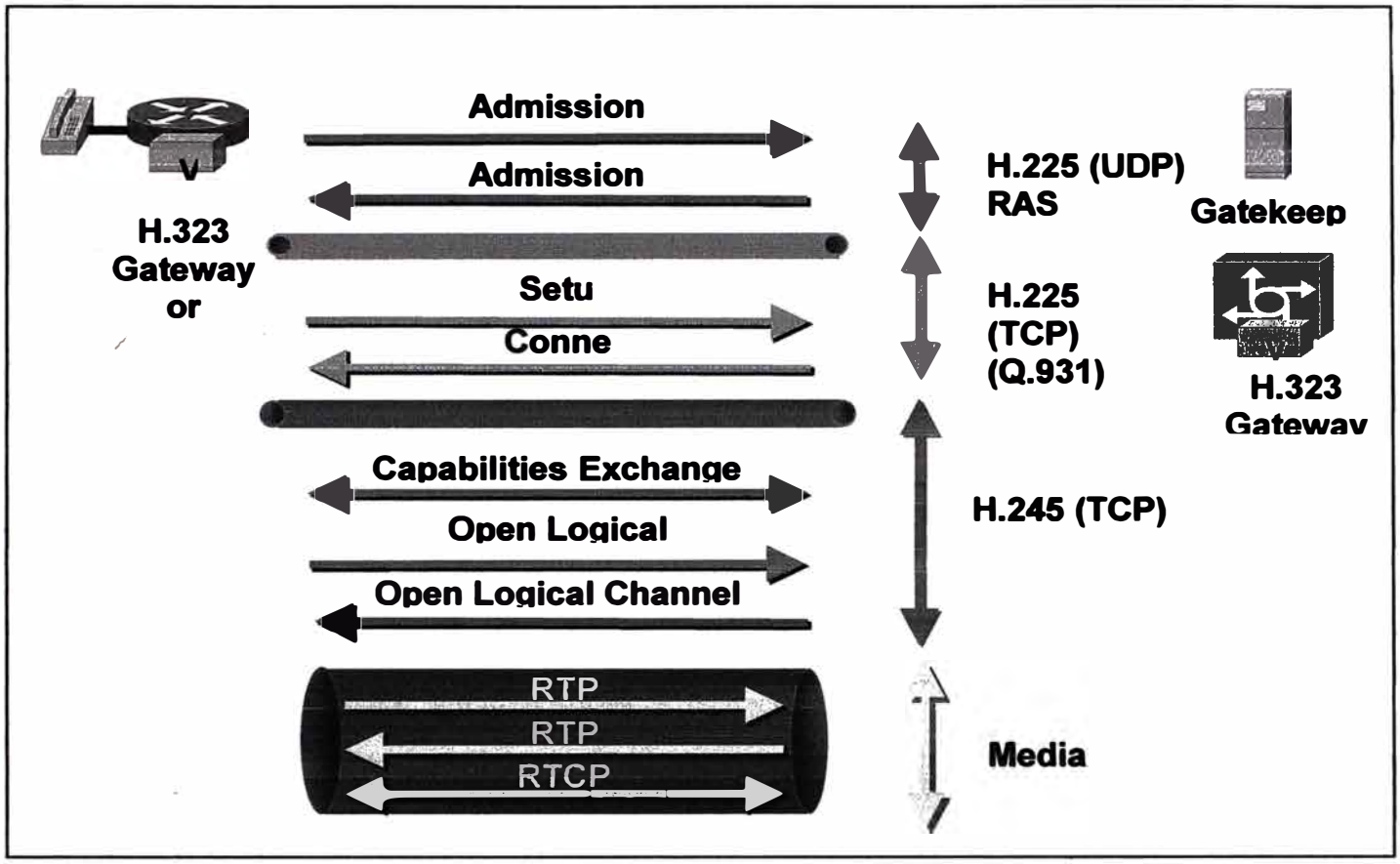

Fig. 10.- Protocolos de señalización H323

4.9. Telefonía IP

La telefonía IP permite transmitir video, data y voz por un solo canal de infraestructura de red, actualmente las empresas están optando por esta opción de implementación ya que esto implica reducción de costos de comunicación.

La telefonía IP ofrece los siguientes beneficios:

- Reducido costos administrativos.
- Incrementa la productividad del personal y del grupo de trabajo.

- Habilita a las oficinas remotas a utilizar las mismas aplicaciones que utiliza la oficina principal sin la necesidad que ellos tengan que invertir en su propia infraestructura y software.
- Provee a la oficina central mas alto grado de control de lo que ya ha sumado a la red, por consiguiente asegura mejor integración de los sistemas y seguridad de los mismos.

4.9.1. Congestión de La Red

La congestión de la red nos puede llevar a la perdida de paquetes y retardos de paquetes variables. La perdida de los paquetes en la red son causados por el llenado de los buffers de transmisión de las interfaces de los equipos de comunicación, como los enlaces de trasmisión llegan al 100% de utilización el servicio de colas de las interfases se llenaran, cuando las colas están llenas y un nuevo paquete quiere entrar este será descartado.

a).- Retardo y Jitter

El retardo es la cantidad de tiempo que toma a un paquete alcanzar el punto remoto de recepción después que ha sido enviado por el otro punto remoto. Este periodo de tiempo es llamado retardo extremo a extremo, este retardo puede ser definido dentro de 2 áreas:

- Retardo de red definida.
- Retardo de red variable.

Al jitter lo podemos definir como el delta de variación de retardo entre 2 paquetes de voz recibidos en un flujo de voz dado.

4.9.2. Gatekeeper

El Gatekeeper es una entidad H323 en la red que provee traslación de direcciones y servicios de control de accesos para terminales H323, gateways y MCU, también puede proveer otros servicios como control de ancho de banda y los dial-plan pueden ser centralizados a proveer escalabilidad.

Los Gatekeepers están separados lógicamente desde los terminales H323 tales como Gateways, ellos pueden ser opcionales en el funcionamiento de una red. Pero si un Gatekeeper esta presente los puntos remotos necesitan usar los servicios que ellos proveen.

a).- Subnets y Zonas del Gatekeeper

Una zona es una colección de Gateways, terminales y MCU registrados con el Gatekeeper. Solo puede haber un solo Gatekeeper activo por zona. Estas zonas pueden cubrir subnets y un Gatekeeper puede cubrir Gateways en una ó más subnets.

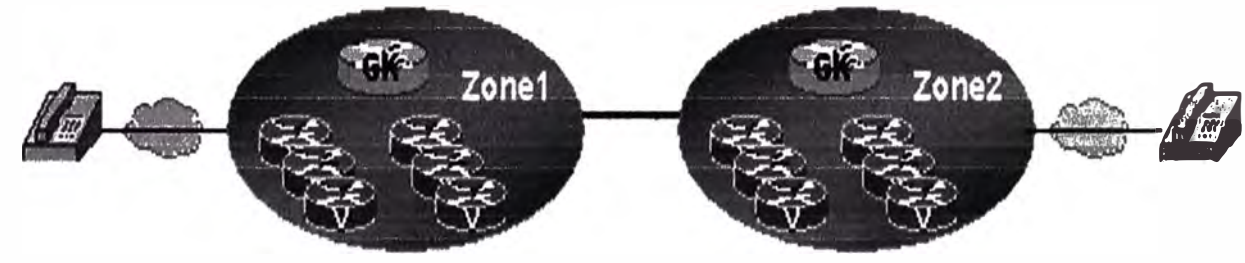

Fig. 11.- Zonas del Gatekeeper

b).- Funciones del Gatekeeper

Traslación de Direcciones

Traslada los ID H323 (tal como gwy1@dominio.com) y números E.164 (números de teléfonos estándar) a direcciones IP de los puntos remotos.

Control de Admisión

Controla la admisión de los puntos remotos dentro de la red H323, a lograr esto el Gatekeeper usa lo siguiente:

- Registración H225, admisión y estatus de mensajes RAS.
- Solicitud de Admisión (ARQ).
- Confirmación de Admisión (ACF).
- Negación de Admisión (ARJ).

Administración de Ancho de Banda

Consiste en la administración de los requerimientos de ancho de banda de los puntos remotos, a lograr esto el Gatekeeper usa los siguientes mensajes RAS H225:

- Solicitud de ancho de banda (BRQ).
- Confirmación de ancho de banda (BCF).
- Negación de ancho de banda (BRJ).

Administración de La Zona

El Gatekeeper provee la administración de la zona para todos los terminales remotos registrados en la zona, por ejemplo controlando el proceso de registrar los puntos remotos.

c).- Protocolos H323 con Gatekeeper

Los protocolos H323 trabajan en 3 áreas de control:

Señalización RAS (225).

Control de llamada y setup de llamada (H225).

Control del medio y señalización de transporte (H245).

En la siguiente gráfica 12 nos muestra el funcionamiento de los protocolos H323 en una red con Gatekeeper.

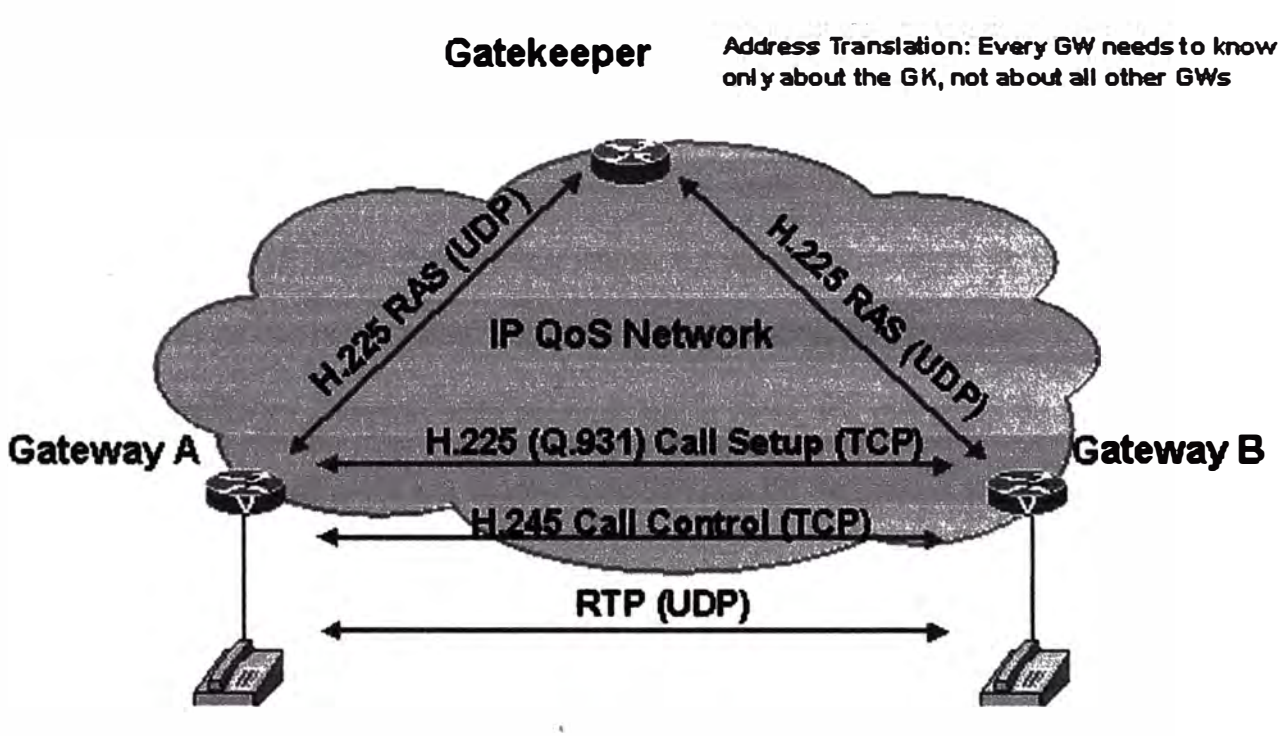

Fig. 12.- Protocolos H323 con Gatekeeper

Señalización Ras H225

RAS es el protocolo de señalización utilizado entre gateways y Gatekeepers. El canal RAS es abierto antes que otro canal y es independiente del setup de la llamada y canal del medio de transporte.

RAS utiliza los puertos UDP 1719 (mensaje de RAS H225) y 1718 (unicast para el descubrimiento del Gatekeeper).

Señalización de Control de Llamada H225

La señalización de control de llamadas H225 es usada para el setup de las conexiones entre puntos remotos H323. La ITU H225 recomienda el uso y soporte de mensaje de señalización Q931.

Un confiable canal (TCP) de control de llamada es creado a través de la red IP, usa el puerto TCP 1720. Este puerto inicia el mensaje de control de llamada Q931 para el propósito de conexión, mantenimiento y desconexión de llamadas.

Cuando un Gateway esta presente en la zona, los mensajes de setup de llamada H225 son intercambiados vía directa señalización de llamada ó señalización de llamada de Gatekeeper ruteado (GKRCS).

Si no hay ningún Gatekeeper presente en la red, los mensajes H225 son intercambiados directamente entre los puntos finales.

Transporte y Control de Media H245

H245 maneja mensajes de control extremo a extremo entre las entidades H323. Los procedimientos H245 establecen canales lógicos para la transmisión de audio, video,

data e información de control del canal. Ello es usado a negociar el uso del canal y sus capacidades tales como:

- Control de flujo.
- Mensajes de intercambio de capacidades.

CAPÍTULO V
DISEÑO DE UNA RED IP

Teniendo como base los capítulos tocados anteriormente tal como routing y seguridad se puede montar sobre ello muchos servicios tales como es VOIP, video sobre IP, también podemos encapsular muchos otros protocolos tales como SNA, X25, IPX etc.

Para el ejemplo de diseño vamos a considerar una empresa que tenga 20 locales remotos, un local principal en la cual tiene todos los servidores Principales y acceso a Internet.

Sobre esta plataforma, los servicios que tiene son Cajeros ATM que funcionan con X25, otros que funcionan con SNA, se debe de considerar que en su LAN tienen aplicativos que funcionan únicamente con IP y otros con SNA. Como se sabe sobre IP se puede implementar muchos aplicativos tales como correo, base de datos, etc.

Como es normal en estos días se quiere ahorro de costos en la comunicación telefónica y se esta optando por utilizar VOIP para las conexiones de centrales, teléfonos IP, POS y FAX.

5.1. Plan de Direccionamiento

Para el diseño de una red IP se tiene que empezar por el plan de direccionamiento el cual tiene que ser un rango privado para no tener problemas con conexiones de Host en Internet.

Un rango privado bien utilizado es la red 172.16.X.X , para propósitos de escalabilidad y orden de la red se puede utilizar la siguiente regla de formación.

172.16. **Y** . **X**

donde :

Y = # de agencia

X = Los host de los puntos remotos.

La mascara de la red de cada punto remoto será una mascara C es decir:

255.255.255.0

A continuación en la tabla 8 nos muestra el plan de direccionamiento a utilizar.

AGENCIA	SUB INTERFACE ATM	PVC	BW	IP PRINCIPAL	IP WAN REMOTO	MASK	LAN REMOTA	MASK	LOOPBACK
AGENCIA 1	ATM6/0.101	101	256	10.8.34.1	10.8.34.2	29	172.16.1.0	24	10.8.33.1
AGENCIA 2	ATM6/0.102	102	256	10.8.34.9	10.8.34.10	29	172.16.2.0	24	10.8.33.5
AGENCIA 3	ATM6/0.103	103	256	10.8.34.17	10.8.34.18	29	172.16.3.0	24	10.8.33.9
AGENCIA 4	ATM6/0.104	104	256	10.8.34.25	10.8.34.26	29	172.16.4.0	24	10.8.33.13
AGENCIA 5	ATM6/0.105	105	256	10.8.34.33	10.8.34.34	29	172.16.5.0	24	10.8.33.17
AGENCIA 6	ATM6/0.106	106	256	10.8.34.41	10.8.34.42	29	172.16.6.0	24	10.8.33.21
AGENCIA 7	ATM6/0.107	107	256	10.8.34.49	10.8.34.50	29	172.16.7.0	24	10.8.33.25
AGENCIA 8	ATM6/0.108	108	256	10.8.34.57	10.8.34.58	29	172.16.8.0	24	10.8.33.29
AGENCIA 9	ATM6/0.109	109	256	10.8.34.65	10.8.34.66	29	172.16.9.0	24	10.8.33.33
AGENCIA 10	ATM6/0.110	110	256	10.8.34.73	10.8.34.74	29	172.16.10.0	24	10.8.33.37
AGENCIA 11	ATM6/0.111	111	256	10.8.34.81	10.8.34.82	29	172.16.11.0	24	10.8.33.41
AGENCIA 12	ATM6/0.112	112	256	10.8.34.89	10.8.34.90	29	172.16.12.0	24	10.8.33.45
AGENCIA 13	ATM6/0.113	113	256	10.8.34.97	10.8.34.98	29	172.16.13.0	24	10.8.33.49
AGENCIA 14	ATM6/0.114	114	256	10.8.34.105	10.8.34.106	29	172.16.14.0	24	10.8.33.53
AGENCIA 15	ATM6/0.115	115	256	10.8.34.113	10.8.34.114	29	172.16.15.0	24	10.8.33.57
AGENCIA 16	ATM6/0.116	116	256	10.8.34.121	10.8.34.122	29	172.16.16.0	24	10.8.33.61
AGENCIA 17	ATM6/0.117	117	256	10.8.34.129	10.8.34.130	29	172.16.17.0	24	10.8.33.65
AGENCIA 18	ATM6/0.118	118	256	10.8.34.137	10.8.34.138	29	172.16.18.0	24	10.8.33.69
AGENCIA 19	ATM6/0.119	119	256	10.8.34.145	10.8.34.146	29	172.16.19.0	24	10.8.33.73
AGENCIA 20	ATM6/0.120	120	256	10.8.34.153	10.8.34.154	29	172.16.20.0	24	10.8.33.77

Tabla 8.- Plan de Direccionamiento de la red de los locales

Como se puede apreciar se ha considerado un IP loopback en los locales remotos esto para hacer más flexibles las conexiones PEER a PEER.

Se esta utilizando equipos con interfase ATM en el punto principal, en los puntos remotos se esta utilizando equipos con interfase ethernet.

5.2. Diseño de La Arquitectura

Para el diseño del tipo de equipos que vamos a utilizar para satisfacer las necesidades de la empresa comenzaremos primero analizando el local principal y después los puntos remotos.

5.2.1. Diseño de La Red en el Local Principal

Para el mejor manejo de la infraestructura de los equipos en el local principal usaremos la marca cisco. Entre las consideraciones que deberíamos tener son las siguientes:

a).- Se debe tener un equipo central con la capacidad de soportar alto procesamiento de tablas de ruteo, gran cantidad de memoria y opción a soportar interfases ATM para conexiones de alta velocidad. Un equipo adecuado para este propósito es un router Cisco del modelo 3660, el cual tendrá 128M de memoria RAM, con interfases ATM , y 2 puertos fast ethernet (100baseT).

b).- Para la parte de VOIP se necesita un Gateway de voz el cual tiene que ser un Access Server 5300, el cual tendrá una tarjeta E1 con 30 DSP y estará conectado a la PBX central.

c).- Para la parte de la telefonía IP se utilizara un Call Manager de marca Cisco en el punto central el cual manejara los teléfonos IP de los puntos remotos y del punto central.

d).- Para el lado de la red LAN se tiene que usar un Switch 6506 el cual es optimo por la capacidad de procesamiento y cantidad de interfases que puede soportar.

e).- El router central 3660 tendrá el software de Gatekeeper para poder manejar los ATA de los puntos remotos. Los ATA son terminales H323 que tienen 2 interfases de voz. Los cuales pueden manejar canales analógicos, FAX ó conexiones con Modems.

5.2.2. Diseño de La Red en Los Locales Remotos

Para los locales remotos se debe de tener en cuenta las siguientes consideraciones:

a).- Como los locales remotos van a manejar VOIP y telefonía IP se debe utilizar en cada punto routers Cisco, los modelos mas apropiados para estos puntos serían los R2611. Los cuales tendrían 40M de memoria RAM con 2 interfases de VOZ FXS.

b).- Adicionalmente en cada punto remoto se tendría teléfonos IP Cisco, los modelos mas apropiados por su costo y uso serían los 7910.

c).- En cada punto remoto también utilizaríamos equipos ATA, los cuales nos servirían paras las conexiones con los FAX y módems analógicos.

d).- Finalmente cada router remoto estaría equipado con tarjetas seriales para la conexión con los Cajeros Automáticos y servidores SNA de las agencias de la empresa.

Un esquema del equipamiento de cada local será mostrado en la gráfica 13.

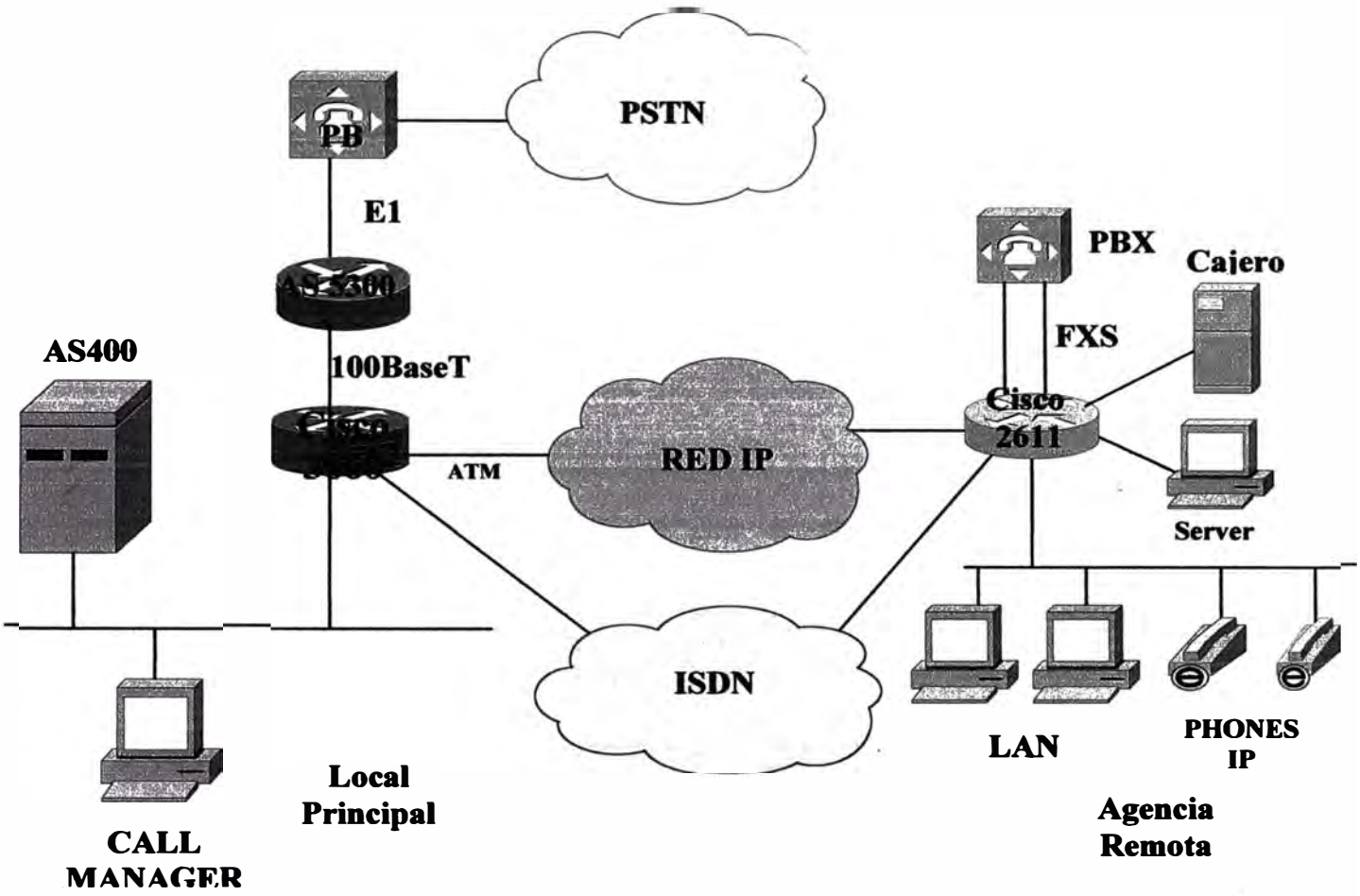

Fig. 13.- Red IP

5.3. Configuraciones Realizadas

Para tener una idea clara como las configuraciones fueron desarrolladas en cada punto tomaremos las configuraciones por tipo de servicio.

5.3.1. Configuraciones Para el Servicio de VOIP

Para el servicio de VOIP se desarrollaron una serie de configuraciones tanto en el local Principal como en el local remoto.

a).- Configuración del AS5300

El Access Server 5300 manejaba un E1, para la conexión con la PBX central se desarrollo mediante una señalización E1 PRI. El plan de numeración de los anexos de la oficina central son la serie 1XX y 2XX. Y la de los locales remotos son la serie 3YYX donde YY representa el numero de agencia.

Adicionalmente a la configuración de VOIP se tiene que configurar el AS5300 como gateway para la interoperabilidad con el GateKeeper quien maneja el direccionamiento de los ATA. También en el AS5300 se tiene que enrutar las llamadas a los teléfonos IP que maneja el Call Manager.

Un ejemplo de las configuraciones utilizadas se muestra en la tabla 9.

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8

controller E1 0
 framing NO-CRC4
 clock source line primary
 Primary timeslots 1-15,17-31
 cas-custom 0


interface Ethernet0
 description enlace_3660
 ip address 10.8.51.234 255.255.255.252
 h323-gateway voip interface
 h323-gateway voip id GK-FASA ipaddr
152.10.10.108 1718
 h323-gateway voip h323-id GW-
FASA@fasa.com
 h323-gateway voip tech-prefix 1#
 h323-gateway voip tech-prefix 2#
```

```
dial-peer voice 1 pots
 destination-pattern +1..
 port 0:0
 prefix 1

dial-peer voice 2 pots
 destination-pattern 2..
 port 0:0
 prefix 2

dial-peer voice 3183 voip
 destination-pattern 3183
 voice-class codec 1
 session target ras

dial-peer voice 100 voip
 destination-pattern +3...
 voice-class codec 1
 session target ipv4:152.10.10.113
 dtmf-relay h245-alphanumeric
 ip precedence 5
 no vad
```

Tabla 9.- Configuraciones de VOIP del AS5300

b).- Configuraciones de Los R2611 Remotos

Los routers 2611 remotos básicamente tienen configuraciones para las configuraciones de VOIP de las líneas analógicas que este maneja. En la tabla 10 nos muestran las configuraciones realizadas.

```
voice-port 1/0/0
 input gain 2
 echo-cancel coverage 24
 timeouts call-disconnect 0
!
voice-port 1/0/1
!
!
dial-peer voice 1 pots
 destination-pattern +73120
 port 1/0/0
!
dial-peer voice 50 voip
 destination-pattern 9....
 ip precedence 5
 no vad
 session target ipv4:10.8.51.234
```

Tabla 10:- Configuraciones de los routers 2611.

c).- Configuración del 3660 Para Gatekeeper

El router 3660 se configura para que pueda funcionar como Gatekeeper y pueda manejar terminales H323 tales como los ATA cisco. En la tabla 11 nos muestra un ejemplo sencillo de configuración.

```
interface Ethernet0/0
 description enlace_AS5300
 ip address 10.8.51.233 255.255.255.252
 half-duplex

interface Ethernet0/1
 ip address 152.10.10.108 255.255.0.0
 ip nat inside
 half-duplex

gatekeeper
 zone local GK-FASA fasa.com
152.10.10.108
 no shutdown
```

Tabla 11.- Configuración del router 3660

5.3.2. Configuraciones Para ATM

Estas configuraciones son realizadas para que el router central pueda trabajar a la vez con ATM e IP al mismo tiempo en las interfases creadas para cada punto remoto.

En esta oportunidad se opto por una de las ultimas tecnologías que en el mundo se esta desarrollando y es el ATM route-bridged IP. En la tabla 12 mostramos un ejemplo de estas configuraciones.

```
interface ATM2/0.101 point-to-point
CID 17915  Local San Borja
 mtu 1500
 ip address 10.8.45.1 255.255.255.248
 atm route-bridged ip
 pvc CID17915 0/101
 !
!
interface ATM2/0.102 point-to-point
 CID 17909 Local Miraflores Pardo
 mtu 1500
 ip address 10.8.45.9 255.255.255.248
 atm route-bridged ip
 pvc CID17909 0/102


router eigrp 120
 redistribute static
 network 10.0.0.0
 distribute-list 10 out ATM2/0.101
 distribute-list 10 out ATM2/0.102
 no auto-summary
 eigrp log-neighbor-changes

ip route 0.0.0.0 0.0.0.0 Null0
```

Tabla 12.- Configuraciones para ATM.

Adicionalmente en la tabla 12 se muestra como se levanto el protocolo EIGRP para el tema de enrutamiento entre los locales con el punto principal. Como se pueda apreciar con un protocolo de ruteo es muy fácil manejar el enrutamiento y realizas políticas las cuales son muy importantes para la seguridad de las redes.

5.3.3. Configuraciones Para DLSW

Esta configuración es realizada para encapsular el tráfico SNA en IP, entre las conexiones más típicas son SDLC a LLC, SDLC a SDLC, LLC a LLC. En los equipos de comunicaciones es más conveniente manejarlo tomando como referencia IP loopbacks de los routers ya que estos son internos de los routers y son independientes de las conexiones WAN.

a).- Configuración del Router Central 3660

En la tabla 13 se muestra la configuración del router central con DLSW para encapsular SNA en IP.

```
dlsw local-peer peer-id 10.8.33.249 lf 1500
dlsw remote-peer 0 tcp 10.8.33.1 lsap-output-list 201
dlsw remote-peer 0 tcp 10.8.33.5 lsap-output-list 201
dlsw bridge-group 1

interface Loopback0
 ip address 10.8.33.249 255.255.255.252
 no ip directed-broadcast

interface Ethernet0/1
 ip address 152.10.10.108 255.255.0.0
 bridge-group 1

 bridge 1 protocol ieee
```

Tabla 13.- Configuración del 3660 para DLSW

b).- Configuración del Router Remoto 2611

En los routers remotos se tienen que configurar para que manejen SDLC para que los cajeros y servidores SNA puedan ser interconectados.

En la Tabla 14 mostramos las configuraciones de los routers 2611 para SNA.

```
dlsw local-peer peer-id 10.8.33.1 lf 1500
dlsw remote-peer 0 tcp 10.8.33.249 lsap-output-list 201
dlsw bridge-group 1
!
interface Loopback0
 description enlace_SNA
 ip address 10.8.33.1 255.255.255.252
 no ip directed-broadcast
!
interface Serial0/0
 description CONEXION PARA FBSS(01 ES PARA PU 2.0)
 encapsulation sdlc
 no ip mroute-cache
 no keepalive
 half-duplex
 nrzi-encoding
 clockrate 19200
 sdlc role primary
 sdlc vmac 4000.8825.0100
 sdlc address 01
 sdlc xid 01 05D20025
 sdlc partner 4200.0000.0024 01
 sdlc address 05 xid-poll switched
 sdlc partner 4200.0000.0024 05
 sdlc saps 05 08 08
 sdlc dlsw 1 5
```

Tabla14.- Configuración del 2611 para DLSW

5.3.4. Configuraciones Para RDSI

Las configuraciones de RDSI son importantes para las líneas de respaldo las cuales trabajaran cuando los enlaces principales fallen. En estas configuraciones hechas se debe aprovechar todas las capacidades de la red, para lo cual se diseño para que funcionen a 128Kbps tal como trabaja una conexión de video sobre RDSI.

Como se podrá apreciar sobre un enlace ISDN también se puede transportar el protocolo IP y sobre esto todos los servicios antes mencionados.

a).- Configuración del Router Remoto Para RDSI

En la tabla 15 se puede apreciar la configuración de RDSI en la cual se aplico la técnica de BUNDLE la cual une la mayor cantidad de canales ISDN según los requerimientos de las conexiones.

Normalmente una línea de respaldo solo usa 64Kbps en una conexión con esta técnica se puede unir canales y aumentar el ancho de banda incluso hasta 1Mbps, esto se logra con la técnica PPP multilink.

```
interface BRI0/0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 dialer pool-member 1 priority 100 max-link 2
 isdn switch-type basic-net3
 ppp authentication chap


interface Dialer1
 ip address 10.80.32.42 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 dialer remote-name Rsudamericano1
 dialer pool 1
 dialer string 2124211 class bansud
 dialer string 2124209 class bansud
 dialer string 2124207 class bansud
 dialer load-threshold 1 either
 dialer-group 1
 ppp authentication chap
 ppp multilink


map-class dialer bansud
 dialer idle-timeout 60
 dialer fast-idle 5
 dialer wait-for-carrier-time 2

access-list 130 deny   eigrp any any
access-list 130 permit ip any any

dialer-list 1 protocol ip list 130
```

Tabla 15:- Configuración remota para la línea RDSI

CONCLUSIONES

1.- En estos días el protocolo IP es cada día más utilizado y los servicios que ello puede transportar cada día van aumentando.

2.- Los servicios sobre le Protocolo IP son fáciles de habilitar y el grado de escalabilidad de los mismos es mucho mayor que cualquier otro.

3.- El desarrollo de las aplicaciones con IP fueron muy importantes para el avance del Internet y otras tecnologías de bases de datos que hacen que la información de las empresas hoy en día estén actualizada en todo momento.

4.- Una típica característica de las aplicaciones con IP es que los servicios se hacen más manejables pudiéndose aplicar políticas de seguridad sobre las mismas.

5.- Un gran problema que actualmente se tiene para IP es el tema de la cabecera que suma al paquete de data. Lo cual genera cierta desventaja de consumo de ancho de banda para paquetes pequeños y más aún cuando el medio de trasmisión es ethernet.

6.- IP ofrece aún un gran campo todavía por explorar lo que podría hacer que las telecomunicaciones puedan seguir desarrollándose en los años siguientes.

BIBLIOGRAFÍA

1. MANAGING CISCO NETWORK SECURITY.- Chris Kevin Calkins, Editorial Cisco Systems Inc. San José CA 95134-1706 USA

2. ROUTING TCP/IP .- Jeff Doyle. Editorial Macmillan Technical, Indianapolis. Publicado: 11 de Abril del 2001

3. IP ADDRESSING FUNDAMENTALS.- Mark Sportack, Editorial Cisco System Inc. San José. Publicado: 31 de Octubre del 2002.

4. WEB SECURITY FIELD GUIDE.- Steve kalman, Editorial Cisco System Inc. San José. Publicado: 11 de Noviembre del 2002.

5. NETWORK SECURITY PRINCIPLES AND PRACTICES.- Saadak Malit , Editorial Cisco System Inc. San José. Publicado 11 Noviembre del 2002.

6. INTEGRATING VOICE AND DATA NETWORKS.- Scott Keagy, Editorial Cisco Systems Inc. San José . Publicado el 20 de Octubre del 2000.

7. CISCO OSPF COMMAND AND CONFIGURATION HANDBOOK.- William Parkhurst, Editorial Cisco System Inc. San José. Publicado el 18 de Abril del 2002.