ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS Y DISEÑO DE UNA RED IMS (IP MULTIMEDIA SUBSYSTEM) PARA EL PROVEEDOR DE SERVICIOS DE INTERNET READYNET

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

AMANDA PAULINA ÁVILA ROSAS
amandapaulina@yahoo.com

NELLY SABRINA CEVALLOS LÓPEZ
sabrina_cevallos@yahoo.com

DIRECTOR: ING. FERNANDO FLORES
fflores@fie-epn.net

Quito, Diciembre 2008

DECLARACIÓN

Nosotros, AMANDA PAULINA ÁVILA ROSAS y NELLY SABRINA CEVALLOS LÓPEZ, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Amanda Paulina Ávila Rosas

Nelly Sabrina Cevallos López

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por AMANDA PAULINA ÁVILA ROSAS y NELLY SABRINA CEVALLOS LÓPEZ, bajo mi supervisión.

Ing. Fernando Flores
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Quiero expresar un profundo agradecimiento a todas las personas que de una u otra forma colaboraron conmigo en la ejecución de este Proyecto de Titulación, entre las mismas quiero poner especial consideración al Ing. Fernando Flores cuya guía permitió que este trabajo culminara de manera exitosa, al personal técnico y profesional de ReadyNet que facilitaron la información necesaria en este proyecto, a la familia Cevallos López que en muchas ocasiones me abrió las puertas de su hogar y finalmente a todos mis amigos y amigas que siempre tuvieron un consejo o una palabra de apoyo en el proceso de esta ardua pero satisfactoria tarea.

Amanda Ávila

AGRADECIMIENTOS

Un profundo agradecimiento al Ing. Fernando Flores por su guía en este proyecto de titulación; a ReadyNet, gente que me ofreció su ayuda y apoyo desinteresado, en especial a mis compañeros de trabajo por su amistad y asesoramiento; a Iván por colaborar conmigo en todo cuanto estuvo a su alcance para el desarrollo de este proyecto; a Amy por su dedicación, esmero y amistad; finalmente a todos mis amigos que fueron un soporte y alegría en todo el tiempo que compartimos juntos.

Sabrina Cevallos

DEDICATORIA

A mi familia por todo el apoyo y la confianza que han depositado en mi, en especial a mi madre por ser el pilar fundamental de mi vida.

Amanda Ávila

DEDICATORIA

A Dios, quien me da la fuerza que me impulsa a seguir adelante, la salud y la vida; a mi padre Raúl Cevallos, hombre que siempre ha sido mi ejemplo de vida, a mi madre Nelly López, mujer que ha dedicado su vida a su familia y se ha desvelado junto a mi, a mis hermanas Alex y Anny, que siempre fueron mis amigas, mi apoyo y admiración; a mis nenas: Lupita por ser mi angelito y a Pame y Micky, quienes son la alegría más grande en mi corazón; a Gabriel por ser esa persona tan especial en mi vida, quien siempre me ha brindado su apoyo y ayuda incondicional.

Sabrina Cevallos

RESUMEN

La capacidad de lanzar innovadores y eficaces servicios se convierte en un elemento crítico para todos los proveedores de servicios.

La convergencia de voz, datos y video se ha vuelto la mejor solución tecnológica ofrecida al usuario, este proyecto de titulación presenta una investigación de las características de Redes de Nueva Generación, enfocándonos en las redes IMS (IP Multimedia Subsystem), como solución para la convergencia de servicios.

En el Capítulo I se tratan los fundamentos teóricos. Se realiza una descripción de Voz IP, definiciones y arquitectura; seguida por la enumeración y desarrollo de las características de los protocolos utilizados en las especificaciones VoIP como son H.323, SIP y MEGACO. Adicionalmente se explica la Calidad de Servicio, protocolos involucrados RTP, RTCP y la Seguridad en Redes Informáticas. Finalmente se realiza un resumen de Redes de Nueva Generación y se detalla IMS características, arquitectura y aplicaciones.

El Capítulo II es el análisis de la red actual de ReadyNet. Se detalla la infraestructura de ISP, se presenta las características de la red en cuanto a topología, servicios, equipos de conectividad que la conforman, empresas con las cuales trabajan para proveer el servicio de Internet. Se describen técnicamente los equipos, servidores y demás elementos. Se realiza una breve evaluación de la red mediante el estudio del tráfico y rendimiento.

Una vez obtenida la visión general de la red, en el Capítulo III se analizan los requerimientos de elementos tecnológicos (capacidad de enlaces, equipos, nuevos servicios) para lograr que ReadyNet sea capaz de ofrecer la convergencia de servicios. Se realiza una estimación del crecimiento del número de usuarios de la red. Con estos datos se procede a dimensionar y diseñar la red convergente. Establecidos los requerimientos y con el respectivo

análisis de los equipos se escogen aquellos que se mantendrán y los nuevos a adquirirse. Complementario a esto es la seguridad de la red, que se representa en equipos enfocados a este fin y las políticas a seguirse para un buen funcionamiento de la red.

En el Capítulo 4 se realiza el Análisis de Costos, en donde se desglosa los Ingresos y Egresos que tiene la empresa. Se realiza cálculos de Flujos de Fondos y el Análisis de Riesgo e Incertidumbre para obtener la viabilidad del proyecto.

El Capítulo V trata las conclusiones obtenidas del desarrollo del presente proyecto de titulación, de igual manera se presentan las recomendaciones que se ponen a consideración para que ReadyNet pueda ser un proveedor con servicios convergentes.

Adicionalmente se presentan los Anexos correspondientes al tráfico y tópicos complementarios al desarrollo de la tesis y las fuentes bibliográficas sean estas libros, páginas web, folletos o proyectos de titulación correspondientes al material de consulta para cada capítulo.

PRESENTACIÓN

La transmisión de información de diferente naturaleza por una única infraestructura es lo que en la actualidad se busca implementar. El desarrollo de la tecnología se enfoca en la convergencia de servicios; es por eso que las Redes de Nueva Generación van tomando importancia.

Las redes informáticas en un inicio se crearon únicamente para la transmisión de datos sin embargo cada vez son más significativas en el desarrollo de una empresa debido a las diferentes aplicaciones y servicios que pueden ofrecer. Cada organización tiene una manera particular para el manejo de la información es por ello que se busca una eficiencia óptima para las aplicaciones críticas y aceptable para el resto de aplicaciones.

Las redes IMS (IP Multimedia Subsystem) permiten agregar nuevos servicios, permitiendo la interoperabilidad entre diferentes redes debido al empleo de interfaces abiertas, estándares y protocolos universalmente aceptados. IMS brinda un entorno rico en servicios, con la posibilidad de sostener sesiones multimedia variadas (texto, audio o video simultáneamente) con una o varias personas.

En IMS resaltan dos objetivos, por un lado se encontró la demanda de servicios multimedia ya que los usuarios buscan servicios de telecomunicaciones que agrupen no solo la capacidad de transmisión de voz sino también el acceso a una amplia gama de información y entretenimiento multimedia de forma sencilla y económica. Y por el otro lado se encontró el beneficio de los operadores de telecomunicaciones debido al uso de arquitecturas y tecnologías de red con costes menores, como son las tecnologías IP.

ReadyNet es una empresa proveedora de servicios, razón por la cual se busca presentar una visión para su crecimiento tecnológico y prever las nuevas necesidades que se presenten a esta empresa ofreciendo una nueva arquitectura tecnológica con la cual pueda ampliar la utilización de la red con

nuevos servicios que se concentren en una sola estructura, simplificando la administración y otorgando calidad de servicio para el buen desempeño de las aplicaciones.

Las consideraciones planteadas buscan lograr que dentro de la red fundamental de este ISP se realice un acoplamiento de nuevos elementos para dar inicio al mejoramiento tecnológico y así aprovechar la utilización de la arquitectura IP para conseguir que esta mediana empresa tenga las bases necesarias para migrar a una red de nueva generación.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1 FUNDAMENTOS TEÓRICOS

1.1 VOZ Y DATOS IP[2][20]

1.1.1 VOZ IP

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 tiempo real; logrando de esta manera la convergencia de voz y datos sobre una sola red.

Entre las prestaciones que ofrece esta tecnología se podría enumerar por ejemplo:

1.- Para el usuario una de las principales ventajas es la rentabilidad. Enfocándonos en el sector empresarial la telefonía IP representa un gasto fijo y controlado en comunicaciones. Una red convergente implica menor inversión en hardware ya que tiene soporte para el tráfico de datos, voz, vídeo, etc.

2.- En cuanto a la Telefonía IP las llamadas telefónicas locales pueden ser automáticamente enrutadas a su teléfono VoIP sin importar el sitio físico en donde esté conectado a la red. En caso de viaje si lleva consigo su teléfono VoIP mientras esté conectado a Internet podrá recibir sus llamadas.

3.- Para el proveedor la principal ventaja es la homogeneidad. Un proveedor que proporcione sus servicios sobre una red IP necesitará poca inversión para incorporar Telefonía IP. Además que la gestión de los servicios sería sobre una única red convergente.

Las ventajas que proporcionan las redes VoIP radican en la utilización de una misma infraestructura para la prestación de un mayor número de servicios y un incremento en la calidad de servicio y en la velocidad.

Sin embargo existe una desventaja en cuanto a la seguridad, debido a que no es posible determinar la duración del paquete dentro de la red hasta que se

concluya la transmisión, además de que existe la posibilidad de pérdida de paquetes ya que el protocolo IP no proporciona confiabilidad en cuanto a la entrega de sus paquetes.

1.1.1.1 Arquitectura

Se definen tres elementos fundamentales en su estructura:

Terminales: Se pueden implementar en software en un PC (programa que emule un Terminal H.323 o SIP (Session Initiation Protocol) o en hardware como teléfonos IP o terminales H.323. Además de terminales no IP los cuales necesitarán de un adaptador IP.

Gatekeeper GK: Se encarga de la administración de llamadas, del control de admisión, del control del ancho de banda. Además maneja los registros y la gestión de los recursos de los gateways para evitar saturación en la red. Su función principal es la traducción de direcciones telefónicas a direcciones IP. Este dispositivo es opcional y se lo conoce también con el nombre de Media Gateway Controller.

Gateway GW: Sirve de puente entre la red PSTN y la red IP, actuando de forma transparente para el usuario. Se encarga de la traslación de protocolos para establecimiento y liberación de llamadas y la conversión de formatos.
La funcionalidad del gateway o del gatekeeper, pueden estar separadas en dispositivos diferentes o integrados en uno solo.

Protocolos: Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión.

En la figura 1.1 se observa una red convergente. Una red que integra el servicio de voz con los datos. Todo tipo de información (voz o datos) es transmitida como paquetes bajo el protocolo IP, por consecuencia el enrutamiento de cada paquete puede variar en el transcurso del tiempo de duración de la comunicación, lo cual permite que los recursos de la red puedan ser utilizados por cualquier otra aplicación, manteniendo al mismo tiempo otras conexiones.

En esta red se encuentran dos puertas de enlace (gateways), una para la interacción de los datos en toda la red, y la otra para la interacción de la RTC (*Red Telefónica Conmutada*) con la red de datos.

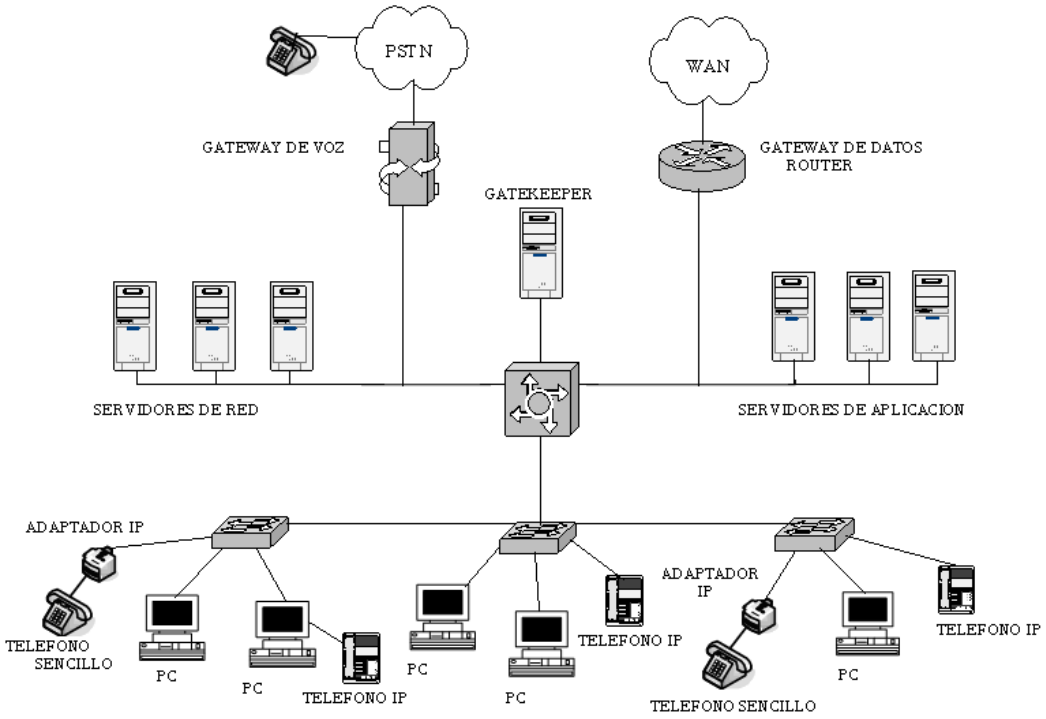


Figura 1.1: Arquitectura Sistema de Telefonia IP[1]

1.1.1.2 Protocolos de Comunicación para Voz sobre IP

La tecnología de VoIP requiere de una pila de protocolos que se complementan e interactúan entre si para efectuar las aplicaciones que esta tecnología ofrece. En la figura 1.2 se puede apreciar la pila de protocolos que trabajan sobre IP

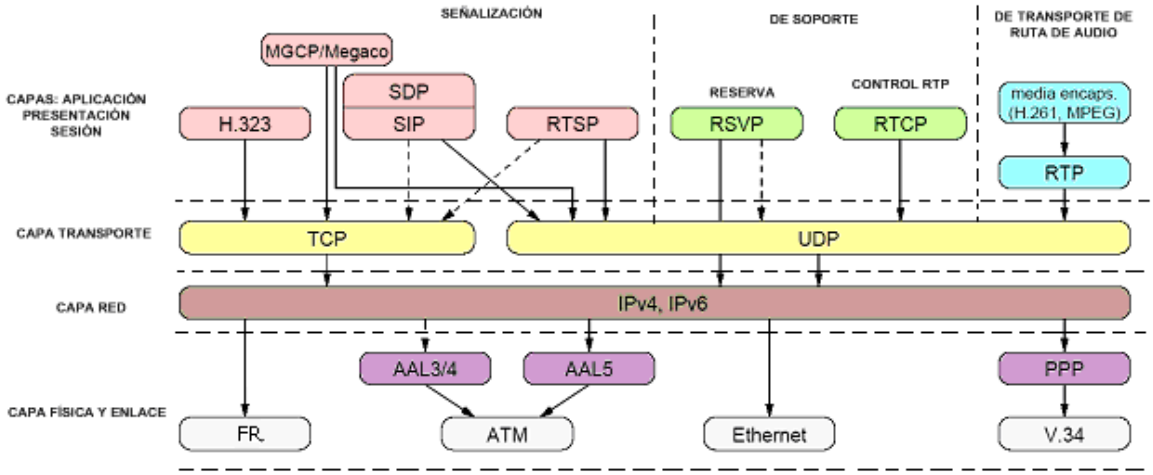


Figura 1.2: Stack de Protocolos usados en Voz sobre IP 1

Al tener establecida una llamada, la voz es digitalizada y transmitida en paquetes IP. Previa la transmisión de los paquetes IP, las muestras de voz son encapsuladas en RTP (protocolo de transporte en tiempo real) y posteriormente en UDP (protocolo de datagrama de usuario). Ya que el protocolo fundamental de esta tecnología es IP las capas física y enlace dependerán de las tecnologías WAN y LAN empleadas para cada tipo de red.

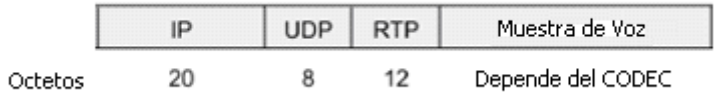


Figura1.3: Encapsulamiento de una Trama VoIP [2]

1.1.1.3 Paquete VoIP

El paquete de VoIP está formado de muestras de codec o tramas encapsuladas en cabeceras IP/UDP/RTP (*RTP, Real time Transport Protocol).* RTP en conjunto con RTCP (*Real time Transport Control Protocol*), realizan la transmisión de aplicaciones en tiempo real. Y poseen técnicas de compresión como CRTP (*RTP comprimido*) y CRTP multiplexado de tunnelling para mejorar la capacidad del ancho de banda.

UDP es el protocolo de transporte utilizado, ya que las aplicaciones en tiempo real no utilizan la retransmisión debido a que el procesamiento de tramas retransmitidas resulta inútil debido a la demora de la llegada de estas tramas.

Los protocolos empleados para señalización, intercambio de capacidades, control de medios y servicios adicionales de las llamadas son los estándares H.323 y SIP.

1.1.2 PROTOCOLOS

1.1.2.1 Protocolo H.323

H.323 es un grupo de estándares definidos por el ITU los cuales comprenden especificaciones para voz sobre IP, vídeo-conferencias y aplicaciones en tiempo real.

H.323 es utilizado para las comunicaciones multimedia entre terminales, equipos de interconectividad y servicios sobre redes LAN. Este estándar es utilizado en redes que no garantizan una calidad de servicio (QoS) ni un retardo fijo, como por ejemplo TCP/IP e IPX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más utilizada en la que se están implementando H.323 es IP (Internet Protocol).

1.1.2.1.1 Componentes H.323

El estándar define los siguientes componentes que se muestra en la figura 1.4:

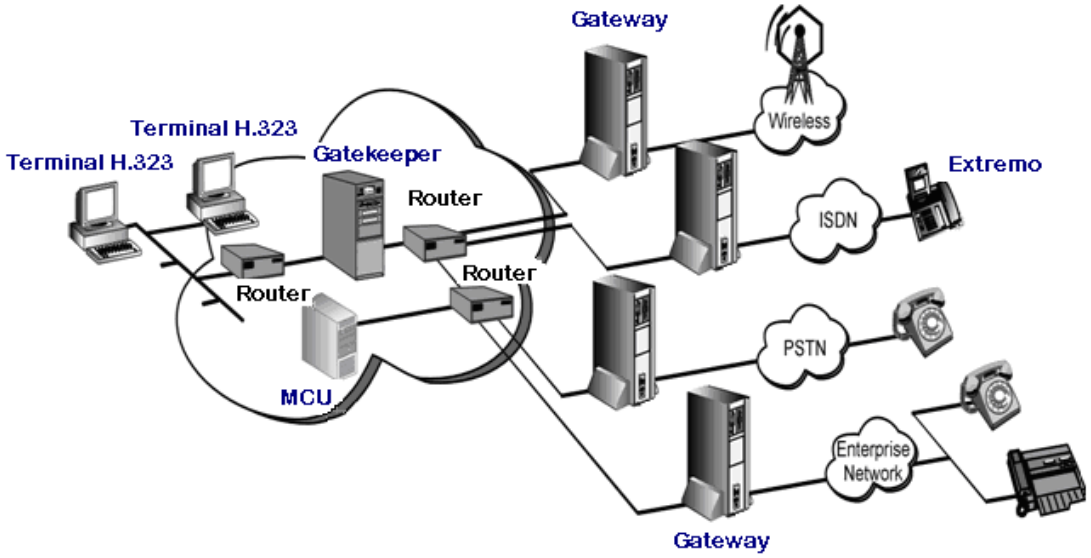


Figura 1.4: Componentes H.323[3]

***Entidad*:** cualquier componente que cumpla con el estándar H.323.

Extremo: es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

Terminal: es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y/o datos entre los dos terminales.

Las funciones de control que realizan los terminales son las siguientes:
H.245 para negociación del canal.
H.225.0 (Q.931) para señalización y control de llamada.
H.225.0 (Register Admission Status RAS) para comunicación con el gatekeeper (registro, admisión y señalización del estado).

También implementan los protocolos *Real-time Transport Protocol* (RTP)/RTCP, UDP para la transmisión de paquetes.

Los terminales además pueden abarcar protocolos de comunicación de datos T.120 que son utilizados para fax y el MCU para las aplicaciones de videoconferencia.

Gatekeeper (GK): es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs.

Las funciones que debe desarrollar un gatekeeper son las siguientes:
• Control de la señalización, tiene la capacidad de ordenar, aprender y conocer los terminales para conectar la llamada.

• Control de acceso y administración de recursos, permite o niega el acceso mediante la autorización de la llamada, las direcciones de fuente, direcciones de destino, etc.

• Traducción de direcciones, convierte los alias de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS.

• Gestión del ancho de banda, fija el número de conferencias que pueden estar dándose simultáneamente en la LAN, rechazando las nuevas peticiones que se dan por encima de un nivel establecido, garantizando el ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

• Autorización de llamadas, en conjunto con el Gateway tienen la capacidad de restringir las llamadas a ciertos números dentro de la red.

Para el desarrollo de estas funciones, entre el gatekeeper y el terminal se emplea el protocolo RAS (Registration /Admission /Status) sobre UDP.

El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la Zona de control H.323.

Esta zona es un conjunto de dispositivos administrativamente definidos que controla el GK.

Gateway (GW): es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada.

Los gateways realizan la traducción de la señalización, información de control e información de usuario, haciendo posible la interoperabilidad entre redes heterogéneas tales como la PSTN y las redes IP.

Los gateways cursan información de usuario soportada en RTP/UDP/IP.

MCU (Multipoint Control Units): dispositivo que soporta la conferencia entre tres o más puntos, bajo el estándar H.323. Se encarga de la negociación entre terminales para establecer las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

Consta de dos componentes:

- ***Controlador Multipunto (MC):*** se encarga del control de los canales de medios.
- ***Procesador Multipunto (MP):*** envía y recibe flujos de medios hacia y desde los participantes en la conferencia. Realiza la combinación de flujos, conmutación o cualquier otro procesamiento.

1.1.2.1.2 Protocolos

H.323 entrega servicios de comunicación multiparte, multimedia y de tiempo real sobre una red QoS ya existente. Mediante el siguiente esquema se resume los protocolos usados por H.323:

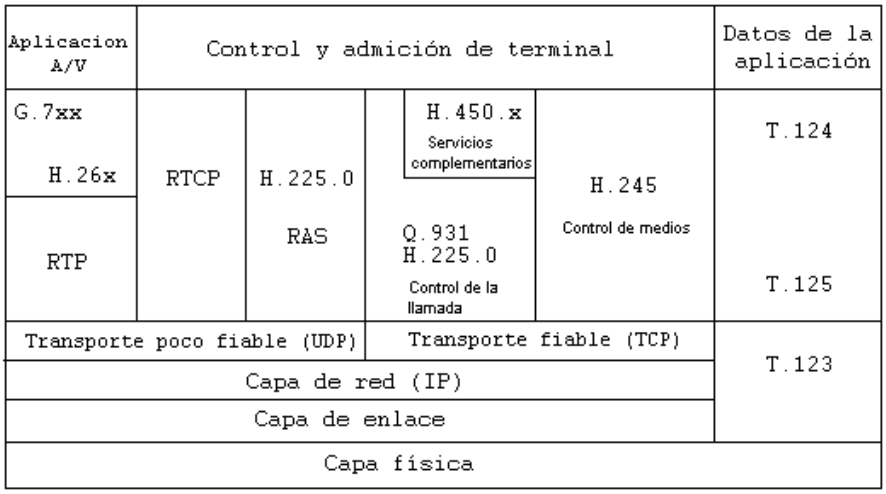


Figura 1.5: Protocolos H.323 [2]

En la tabla 1.1 se observa la descripción de las recomendaciones de la ITU que forman parte de las especificaciones de señalización.

Medio	**Formato**
Audio	G.711 (requerido), G.722, G.723.1, G.728, G729, GSM, ISO/IEC 11172-3 y ISO/IEC 13818-3.
Video	H.261, H.262, H.263.
Protocolo de datos	Series T.120.

Tabla 1.1: Formato de medios apoyados por la ITU para H.323 [2]

G.711	Estándar de compresión de audio, usado principalmente en telefonía. Basado en modulación PCM (Modulación por Impulsos Codificados) con tasa de muestreo de 8 KHz con flujos de 64 Kbps.
G.722	Estándar de codificación de audio, utiliza la técnica ADPCM (A D Modulación por Impulsos Codificados). Tiene una tasa de muestreo de 16 KHz y una tasa de bits de 64 Kbps.
G.723	Estándar de codificación que utiliza ADPCM (Adaptación diferencial de código de modulación de impulsos) a 24 y 40 kbps, con frecuencia de muestreo de 8 KHz.
G.728	Estándar de codificación de voz a 16 Kbps con tasa de muestreo de 8KHz. Utilizado en VoIP y sistemas de videoconferencia que funcionan a 56 Kbps o 64 Kbps.
G.729	Estándar de compresión de audio, opera con una tasa de 8 kbps y con una tasa de muestreo de 8KHz. G.729 se usa en mayor parte en aplicaciones de Voz sobre IP VoIP por sus bajos requerimientos en ancho de banda.
GSM	Groupe Spécial Mobile es un estándar que posee una tasa de bits de 13Kbps y tasa de muestreo de 8KHz.

Tabla 1.2: Formato de Audio [5]

ISO / IEC 11172-3	(international organization for standardization/ international Electrotechnical Commission) Especificaciones de la codificación y decodificación de las señales de audio de alta calidad.
ISO / IEC 13818-3	Especificaciones de la codificación de audio e imágenes en movimiento.

Tabla 1.3: Formato de Audio ISO/IEC [5]

H.261	Estándar de codificación para la señal de video en sistemas de telefonía visual. Este estándar se basa en una codificación de vídeo para velocidades entre 40 Kbps y 2 Mbps.
H.262	También conocido como MPEG-2, es un estándar de codificación de video utilizado por el DVD y la televisión digital.
H.263	Estándar creado para la codificación de video en banda estrecha utilizado para videoconferencia

Tabla 1.4: Formato de Video [5]

Recomendación de la ITU	Descripción
H.225.0	Protocolo de señalización de llamada, registro y admisión y paquetización/sincronización de flujos de medios para sistemas de comunicación multimedia basados en paquetes.
H.235	Seguridad y cifrados de los terminales multimedia de la serie H.
H.245	Protocolo de control de comunicación multimedia. Describe los mensajes y procedimientos utilizados para abrir y cerrar canales lógicos para audio, video y datos, capacidad de intercambio, control e indicaciones.
H.450.x	Servicios complementarios de H.323 (Call Park, Call Pickup, Call Hold, Call Transfer, Call Diversion, MWI, etc).
H.239	Describe el uso de la doble trama en videoconferencia, normalmente uno para video en tiempo real y el otro para presentación.
H.281	Describe el control de cámara lejana para movimientos PTZ (Pan-Tilt-Zoom)
Series T.120	Protocolo de datos para conferencia multimedia.

Tabla 1.5: Recomendaciones de la ITU que soportan la señalización H.323 [2]

RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.

RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar acciones correctoras si este fuera el caso.

1.1.2.1.3 Flujo de Llamadas[5,20]

Establecimiento de llamada H.323 enrutada mediante un *gatekeeper*

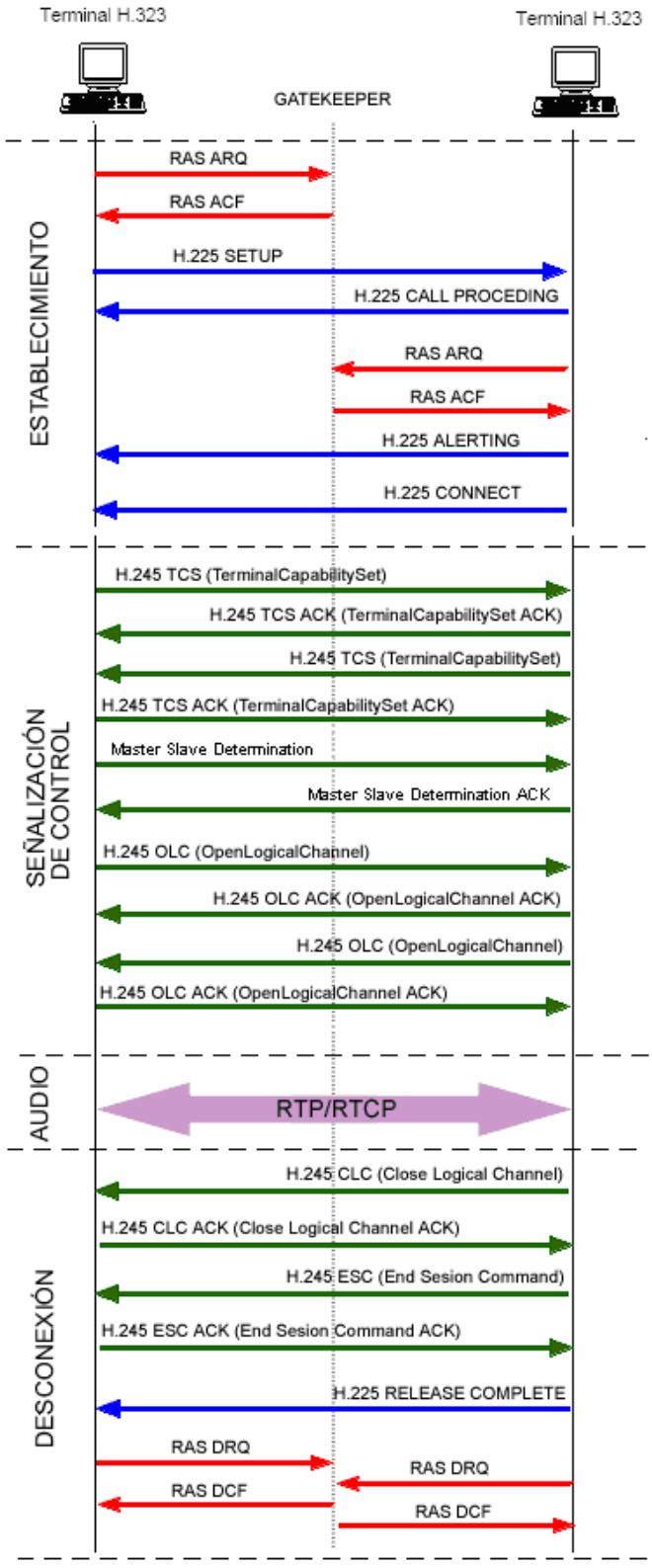


Figura 1.6: Establecimiento de llamada H.323 enrutada mediante un *gatekeeper*[5]

Una llamada H.323 se compone de las siguientes fases:

Primera Fase: Establecimiento

- Fase RAS (Registro, admisión y estado) el primer paso es el intercambio de mensajes entre el gatekeeper y el terminal, para la traducción de direcciones, autorización de llamadas y gestión del ancho de banda mediante los mensajes ARQ y ACF.

- Fase Q.931 (H.225) en esta fase se realiza el intercambio de mensajes entre terminales para establecimiento y liberación de la llamada. Se envía un mensaje de **SETUP** para iniciar una llamada H.323. Parte de la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.

El terminal llamado contesta con un mensaje **CALL PROCEEDING** informando del intento de establecer una llamada.

En este momento el segundo terminal tiene que registrarse con el gatekeeper utilizando el protocolo RAS de manera similar al primer terminal.

El mensaje **ALERTING** indica el inicio de la fase de generación de tono.
Finalmente el mensaje **CONNECT** indica el comienzo de la conexión.

Segunda Fase: Señalización De Control

- Fase H.245 en esta fase se realiza la negociación para el intercambio de los mensajes (petición y respuesta), entre los dos terminales se establece quién será master y quién slave, las capacidades de los participantes y codecs de audio y video a utilizar. Como parte final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

Los principales mensajes H.245 que se utilizan en esta fase son:

• TerminalCapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

• *OpenLogicalChannel (OLC).* Mensaje para abrir el canal lógico de información que contiene los datos necesarios para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.

• *MasterSlaveDetermination (MSD).* Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Decide quién actuará de Master y quién de Slave.

Tercera Fase: Audio

Los terminales inician la comunicación y el intercambio de audio (o video) mediante el protocolo RTP/RTCP, con los parámetros establecidos en la fase H.245, previa apertura de los canales lógicos en los terminales. Estos canales lógicos son unidireccionales, por lo que para una comunicación bidireccional se requiere abrir uno en cada dirección de transmisión.

Cuarta Fase*:* Desconexión

En esta fase cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes

CloseLogicalChannel y ***EndSessionComand*** de H.245.

Posteriormente utilizando el protocolo H.225 se cierra la conexión con el mensaje ***RELEASE COMPLETE***. Finalmente se liberan los registros con el gatekeeper utilizando mensajes del protocolo RAS.

Establecimiento de llamada H.323 entre dos terminales [20]

Para la realización de la comunicación de voz entre dos terminales se efectúan las siguientes fases:

Primera fase: Inicio de llamada

En esta fase se utiliza el protocolo ***H.225.0*** para efectuar el intercambio de mensajes entre terminales para establecimiento y liberación de la llamada.

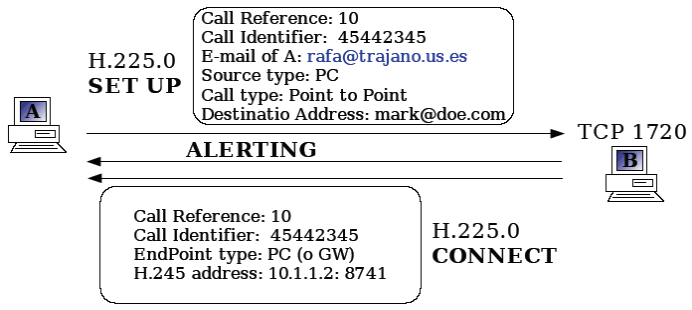


Figura 1.7: Inicio de Llamada [6]

Segunda fase: Establecimiento del canal de control

En esta fase se utiliza el protocolo ***H.245*** para la negociación de las capacidades de los terminales, codecs de audio y video; se determina que terminal realizará la función de maestro y cual de esclavo.

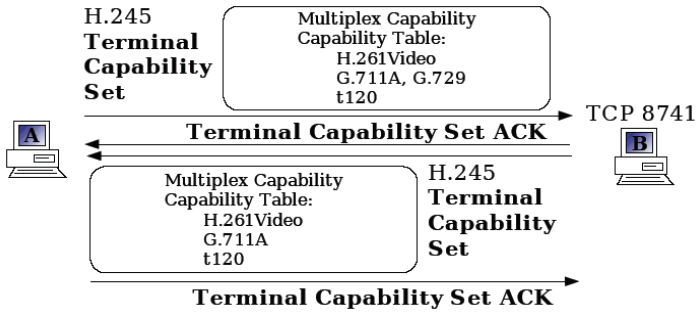


Figura 1.8: Establecimiento del Canal de Control [6]

Tercera fase: Comienzo de la llamada

En esta fase se da apertura a los canales lógicos unidireccionales para medios. Se establece los canales ***T.120*** para los datos bidireccionales.

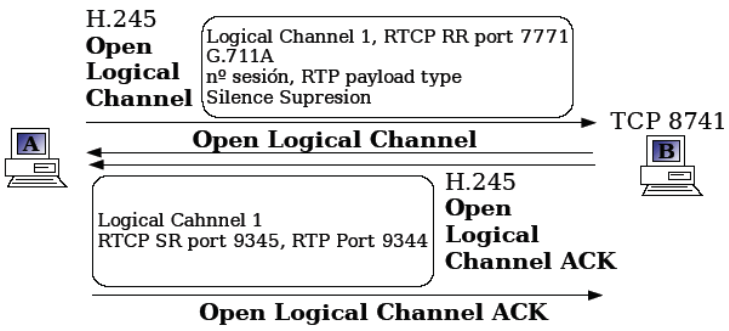


Figura 1.9: Comienzo de la Llamada [6]

Cuarta fase: Diálogo

En esta fase se mantienen los canales lógicos unidireccionales para medios. Con la posibilidad de que existan varios canales lógicos abiertos, sincronizados.

Mediante los paquetes *SR (Sender Report, Informe del transmisor)*[1], *RR (Receiver Report, Informe del receptor)*[2] se puede tener información acerca de la calidad de la transmisión.

Se mantienen las sesiones de intercambio de información (audio, video y datos).

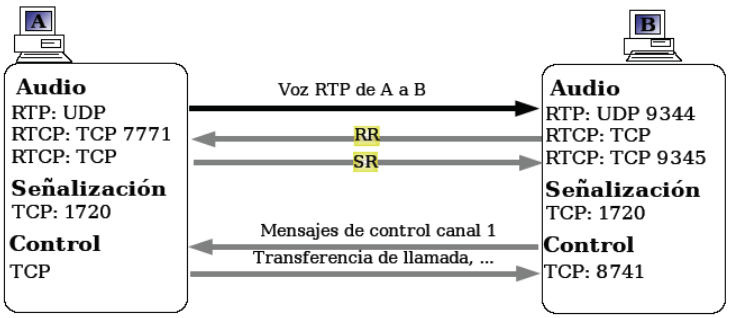


Figura 1.10: Diálogo [6]

Quinta fase: Finalización de la llamada

Esta es la última fase en la cual se sigue una secuencia lógica:

- Uno de los terminales envía el mensaje ***Close Logical Channel*** por cada canal abierto

---

[1] SR [Sender Report, Informe del transmisor]: Un tipo de paquete RTCP que adiciona información del emisor.

[2] RR [Receiver Report, Informe del receptor]: Tipo de paquete RTCP que incluye información del receptor.

- Se recibe un ACK
- Se envía un mensaje ***H.245 End Session Command***
- Se recibe un ACK para cerrar el canal H.245
- Finalmente se envía un mensaje ***H.225.0 Release Complete***

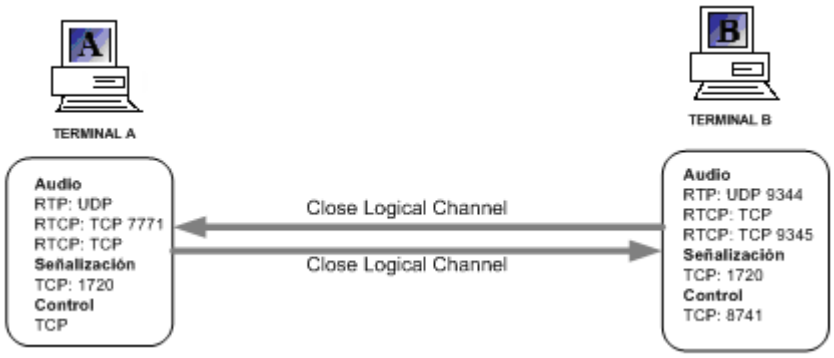


Figura 1.11: Finalización de la Llamada [6]

DIRECCIONAMIENTO

H.323 establece que para la comunicación con cualquier dispositivo de una red H.323 se necesita saber la dirección de red y un identificador *TSAP (Transport Service Access Point, Punto de acceso al servicio de transporte)*[3], este es un identificador de punto de acceso al servicio de transporte y direcciones.

Para el caso particular de las redes IP la dirección de red es una dirección IP, y el identificador TSAP es un número de puerto TCP o UDP.

De esta manera todas las entidades H.323 deben tener por lo menos una dirección de IP.

---

[3] TSAP (Transport Service Access Point, Punto de acceso al servicio de transporte): Definición utilizada en H.323 para designar al dispositivo que transmite los datos en una comunicación. Para iniciar un diálogo se necesita la dirección de red respectiva y el identificador del TSAP que generalmente es el número del puerto UDP o TCP.

H.323 otorga alias para identificar los puntos finales y conferencias multiparte, los mismos que pueden ser representados de las siguientes formas:

- Cadenas alfanuméricas: Bob, bob@host.com, host.com, cadenas arbitrarias.
- Direcciones E.164: +1-408-555-1212, 5551212, 4199.

Algunos ejemplos de identificadores TSAP utilizados para los distintos tipos de capas de las comunicaciones H.323 son:

- Descubrimiento del GK mediante mensajes GRQ (Gatekeeper Request, Solicitud de Gatekeeper)[4]: es configurado estáticamente, puerto UDP 1718.
- Comunicaciones gatekeeper RAS: es configurado estáticamente, puerto UDP 1719.
- Consultas a llamada H.225.0: puede resolverse el alias H.323, puerto TCP 1720.
- Canales de control de medios H.245: es un puerto TCP dinámico conocido a través de negociación H.225.0.
- Canales de medios RTP/RTCP: es un puerto UDP dinámico conocido a través de negociación H.245.

1.1.2.2 Protocolo Session Initiation Protocol (SIP)

"Session Initiation Protocol" (SIP) es un protocolo de señalización utilizado para establecer, enrutar, modificar y cerrar sesiones de comunicaciones a través de redes IP. Estas sesiones incluyen conferencias multimedia, llamadas telefónicas y distribución multimedia por Internet, etc. Las sesiones pueden realizarse en multicast o en unicast; los participantes pueden negociar los

[4] GRQ (Gatekeeper Request, Solicitud de Gatekeeper): Paquete que se envía a la red para descubrir los gatekeepers disponibles.

contenidos y capacidades que van a utilizar, adicionalmente soporta movilidad de los usuarios mediante la utilización de proxies.

Este protocolo fue desarrollado por el SIPWG (Session Initiation Protocol Working Group) del IETF (Internet Engineering Task Force) (RFC 2543, 2543bis) con sesiones multimedia RFC 3261.

Utiliza el modelo de Internet ocupando ciertas funcionalidades de protocolos de Internet existentes tales como HTTP (Hyper Text Transport Protocol) y SMTP (Simple Mail Transfer Protocol).

SIP se basa en el modelo cliente/servidor como HTTP. Para el direccionamiento utiliza el concepto “Uniform Resource Locutor “o “URL SIP” que es similar a una dirección E-mail. Usa estas direcciones de tipo correo electrónico para identificar a los usuarios en lugar de los dispositivos que los utilizan, de esta manera cada participante en una red SIP es reconocido por una dirección, es decir por medio de una URL SIP; logrando la independencia del dispositivo, y sin hacer distinción alguna entre voz y datos, teléfono u ordenador.

SIP soporta numerosos servicios tales como la mensajería instantánea (similar al servicio SMS en las redes móviles), la transferencia de llamada, la conferencia, los servicios complementarios de telefonía, etc.

Conforme al 3GPP (Third Generation Partnership Project), SIP es un protocolo utilizado en la arquitectura “IP Multimedia Subsystem” o “IMS” para el control de sesión y el control de servicio.

El protocolo SIP únicamente se utiliza para la señalización. Una vez que la sesión esté establecida, los participantes intercambian directamente su tráfico audio/video a través del protocolo Real-Time Transport Protocol (RTP). Además SIP no es un protocolo de reservación de recursos, y en consecuencia, no puede asegurar la calidad de servicio.

Algunos de los principales protocolos excluyendo QoS de esta arquitectura son:

- RTP y RTCP especificados en la RFC 1889, proporcionan una entrega en tiempo real de los medios.

- Real-Time Streaming Protocol (RTSP) especificado en la RFC 2327, es el protocolo que proporciona una entrega bajo demanda de datos en tiempo real.

- Session Description Protocol (SDP) es el protocolo de descripción de sesión que proporciona un formato de descripción estándar para el intercambio de capacidad de los medios (codecs de voz para VoIP).

- Session Description Protocol (SAP) es el protocolo de anuncio de sesión que proporciona un método de publicación destinado a las sesiones multidifusión.

1.1.2.2.1 Componentes del Sistema

SIP define los componentes que se muestra en la siguiente figura:

Figura 1.12: Cliente SIP y Componentes del Sistema del Servidor. [2]

El **Servidor Proxy (Proxy Server)**: este servidor recibe solicitudes de clientes que son resueltas por el mismo servidor o las enruta hacia otros servidores. Los servidores Proxy SIP pueden tener un reconocimiento local de los agentes de usuario desde un registrador SIP. Además pueden conocer varias alternativas para localizar a un agente de usuario, y pueden intentar cada una de ellas en un proceso de bifurcación que puede ser paralelo o secuencial.

El **Servidor de Redireccionamiento (Redirect Server)**: este servidor acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones de red y las devuelve al cliente. De manera contraria al ProxyServer, el Redirect Server no encamina las solicitudes SIP.

En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario recibido en el mensaje SIP, a un número de reenvió de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo número de reenvió al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.

El **Agente Usuario (UserAgent) o "UA"**: se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. Se materializa por un software instalado sobre un « UserEquipment » o UE (PC, teléfono IP).
Los Clientes de agentes del usuario (UAC) envían peticiones SIP a la parte llamante, y los Servidores de agentes del usuario (UAS) reciben las respuestas de la parte llamada. Cada usuario puede tener varios agentes del usuario y cada uno asociado a una dirección SIP.

El **Registrador (Registrar)**: se trata de un servidor quien acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al registrador, la dirección donde se lo puede localizar (dirección IP). El "registrador" actualiza la base de datos de localización. El registrador es una función asociada a un Proxy Server o a un Redirect Server. Un mismo usuario puede registrarse sobre distintas

UAs SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UAs.

1.1.2.2.2 Direccionamiento

Las direcciones SIP son otorgadas únicamente a los usuarios y los agentes de usuario. Los servidores SIP (Proxy, Redirección, Registradores) se identifican por direcciones IP y los puertos TCP/UDP. Generalmente los servidores SIP escuchan en los puertos TCP y UDP 5060, sin embargo pueden utilizar cualquier número de puerto.

Sintaxis de dirección SIP

El formato básico de un URL SIP se representa en el siguiente formato:
“sip:” [user [“:” password] “@”] ((hostname | IP-address) [::port]
A continuación se enumera algunos ejemplos de URL SIP:

sip:company.com
sip:pavila@company.com
sip:pavila@192.168.1.1
sip:pavila:inge@company.com
sip:pavila:inge@company.com:5060
sip:pavila@192.168.1.1:5060

Soporte SIP para direcciones E.164

SIP diferencia los puntos finales E.164 (teléfonos) de los puntos finales IP regulares, utilizando los parámetros del usuario en un URL SIP.

Los siguientes ejemplos muestran las direcciones SIP para los puntos finales E.164:

sip:+1-408-555-1212@voip-gw.company.com;user=phone
sip:+14085551212@492.168.1.1;user:phone
sip:4199@192.168.1.1:5060;user:phone

El parámetro user permite un soporte generalizado para los puntos finales E.164.

En los URL SIP la opción user=ip no se puede referir a un número E.164; además de que esta opción es predeterminada.

URL de teléfono para direcciones E.164

Existen tres alternativas para URL SIP: teléfono, fax y módem. Estos URL codifican los números básicos, adicionalmente pueden indicar las capacidades de los dispositivos asociados o las secuencias especiales de llamadas. Poniendo como ejemplo un módem, este puede indicar los protocolos que soporta, el número de bits de datos, paridad y bits de parada.

Los siguientes ejemplos muestran varias variaciones de un URL de teléfono:

tel:555-1212

Este ejemplo indica el número de teléfono local, el guión no tiene ningún significado funcional se lo coloca para mejorar la legibilidad del número de teléfono.

tel:+18005551212;postd=ppppp1p4085551212pp123456789#

Este ejemplo indica cuando un agente de conexión telefónica puede utilizar un servicio de tarjeta de llamada. Después de marcar los números toll-free del servicio de tarjeta de llamada, el agente hace una pausa de cinco segundos (indicada por ppppp). Al mismo tiempo, un asistente automatizado lee un menú de opciones y el agente de conexión telefónica introduce 1. Después de una pausa de un segundo, durante la cual el asistente automatizado pregunta el número de destino, el agente de conexión telefónica introduce 4085551212, y hace una pausa de dos segundos. Durante este tiempo, el asistente automatizado pregunta el número de la tarjeta de llamada y el PIN, que el agente de conexión telefónica proporciona como 123456789#. El teléfono suena otra vez en este momento, que es el tono de devolución procedente de la parte llamada (es decir, 4085551212). El usuario del teléfono URL escucha el tono de llamada del destino final después de que se hayan completado todos los pasos.

1.1.2.2.3 Estructura de Mensaje

Un mensaje SIP consta de las siguientes partes:

- Línea de inicio: indica el propósito del mensaje.
- Cabeceras: proporcionan los detalles del mensaje.
- Cuerpo: proporcionan detalles del mensaje.

Línea de inicio

Su formato depende si el mensaje se trata de una respuesta o una solicitud.

Solicitudes SIP

Las solicitudes SIP son enviadas por los clientes para comunicarse con los servidores.

El formato de línea de inicio de una solicitud es el siguiente:

<Método> <Solicitud-URI> <versión SIP>

<Método> Es uno de los tipos de solicitudes SIP que se identifican en la Tabla 1.4.

<Solicitud-URI> Es el URL SIP u otro tipo de URL de la entidad que debería recibir el mensaje.

<versión SIP> Es actualmente SIP/2.0

A continuación algunos ejemplos:

INVITE sip:jdoe@company.com SIP/2.0

ACK sip:+14085551212@192.168.1.1;user=phone SIP/2.0

BYE tel:+1-408-555-1212;postd=p4199 SIP/2.0

1.1.2.2.4 Métodos y Respuestas SIP

Métodos SIP

El RFC 2543 define seis solicitudes/requerimientos o métodos SIP.

INVITE usado para el establecimiento de una sesión entre UAs. Contiene información sobre el que genera la llamada y el destinatario así como sobre el tipo de flujo que será intercambiado (voz, video, etc).

ACK confirma la recepción de una respuesta SIP.

BYE permite la liberación de una sesión anteriormente establecida. Puede ser emitido por el que genera la llamada o el que la recibe.

REGISTER usado por una UA para indicar correspondencia entre su dirección SIP y su dirección de contacto al registrarla.

CANCEL utilizado para cancelar una solicitud pendiente.

OPTIONS utilizado para consultar las capacidades y el estado de un User Agent o de un servidor. La respuesta debe incluir los métodos SIP que soporta.

1.1.2.2.5 Extensiones del Protocolo SIP

SUBSCRIBE utilizado para requerir notificación de evento. Los clientes UA (User Agent) solicitan actualizaciones de presencia/disponibilidad de otros usuarios a partir de un registrador SIP, cuando el usuario cambia la información de registro.

NOTIFY utilizado para notificar un evento. Actualizaciones instantáneas desde un registrador a un cliente UA acerca de los usuarios que han cambiado la información del registro. Los clientes UA deben primero SUBSCRIBE para recibir las actualizaciones NOTIFY sobre un usuario determinado.

PUBLISH permite publicar el estado.

REFER utilizado para reenviar el receptor hacia un recurso identificado en este método, es decir una transferencia a otra URL.

MESSAGE permite la transferencia de mensajes instantáneos. La mensajería instantánea “Instant Messaging” o “IM” consiste en el intercambio de mensajes entre usuarios en seudo tiempo real.

INFO permite transferir informaciones de señalización durante la llamada (por ejemplo: ISUP).

PRACK definido para realizar una recepción confiable de las respuestas temporales de tipo 1XX.

UPDATE permite a un terminal SIP actualizar los parámetros de una sesión multimedia (flujo media y codecs). El método UPDATE puede ser enviado antes de que la sesión sea establecida.

1.1.2.2.6 Respuestas SIP

Después de haber recibido e interpretado un requerimiento SIP, el destinatario de este requerimiento devuelve una respuesta SIP.

El formato de línea de inicio de una respuesta es el siguiente:

<VersiónSIP> <Código de estado> <Frase razón>

<VersiónSIP> actualmente es SIP/2.0
<Código de estado> y ***<Frase razón>*** se establecen a uno de los pares que se muestran en la tabla1.7

A continuación algunos ejemplos:

SIP /2.0 404 Not Found
SIP /2.0 180 Ringing
SIP /2.0 200 OK

Las respuestas SIP estándar están codificadas con tres dígitos de respuesta y una descripción textual seguidos del formato de la versión HTTP1.1. Las respuestas se clasifican en seis categorías, identificadas por el primer dígito del código de respuesta como se muestra en la tabla 1.6

CÓDIGO	CATEGORÍA DE RESPUESTA SIP	DESCRIPCIÓN
1xx	Informational	Proporciona el estado, la información sobre la llamada en progreso.
2xx	Success	El requerimiento ha sido recibido, entendido y aceptado.
3xx	Redirection	La llamada requiere procesamientos adicionales para completar la solicitud.
4xx	Request Failure	El requerimiento no puede ser interpretado por el servidor (puede ser válido en otro servidor).
5xx	Server Failure	El servidor fracasa en el procesamiento de un requerimiento aparentemente válido.
6xx	Global Failures	El requerimiento no puede ser procesado por ningún servidor.

Tabla 1.6: Categorías de Respuesta SIP[2]

En la tabla 1.6 se muestra los códigos de respuesta SIP para la versión 2.0.

Los códigos de respuesta SIP de la categoría 1xx, son respuestas provisionales, razón por la cual el servidor adicionará respuestas a la solicitud del cliente. El resto de las respuestas del servidor son el final de una solicitud SIP.

1.1.2.2.7 Cabeceras SIP

La cabecera SIP representa un valor variable que es transportado a través de la red. Algunas cabeceras SIP son obligatorias en cada mensaje, y otras si utilizan dependiendo del tipo de solicitud o de respuesta.

El formato de las cabeceras SIP es el siguiente:

<Nombre cabecera>: <Valor cabecera>
<Continuación de valor de cabecera>

CÓDIGO	DESCRIPCIÓN DE LA RESPUESTA	CÓDIGO	DESCRIPCIÓN DE LA RESPUESTA
100	Intentando	411	Longitud requerida
180	Ringing	413	Entidad solicitada demasiado grande
181	La llamada está remitiéndose	414	Solicitud-URI demasiado grande
182	En cola	415	Tipo de medio no soportado
183	Progreso de la sesión*	420	Extensión errónea
200	OK	480	No disponible temporalmente
202	Accepted	481	Circuito de llamada o transacción no existe
300	Opciones múltiples	482	Detectado un bucle
301	Movido permanentemente	483	Demasiados saltos
302	Movido temporalmente	484	Dirección incompleta
303	Vero otro	485	Ambiguo
305	Utilizar Proxy	486	Ocupado aquí
380	Servicio alternativo	487	Solicitud terminada
400	Respuesta mala	488	No aceptable aquí
401	Sin autorización	500	Error interior del servidor
402	Pago requerido	501	No implementado
403	Prohibido	502	Gateway erróneo
404	No encontrado	503	Servicio no disponible
405	Método no permitido	504	Límite de tiempo del gateway
406	No aceptable	505	Versión de SIP no soportada
407	Se requiere autenticación de Proxy	600	Ocupado completamente
408	Se requiere límite de tiempo	603	Declinar
409	Conflicto	604	No existe en cualquier parte
410	Hecho	606	No aceptable

Tabla 1.7: Código de Respuesta SIP (*denota trabajo de la IEFT en progreso) [2]

<Nombre cabecera> se los enumera en la tabla 1.8

<Valor cabecera> una o más líneas de información.

<Continuación de valor de cabecera> continuación de la cabecera multilínea.

A continuación algunos ejemplos:

From: sip:102@2.0.0.1
User-Agent: Cisco VoIP Gateway / IOS12.x / SIP enable
Content-Type: application / sdp

La tabla 1.8 muestra las cabeceras SIP las mismas que se organizan en cuatro grupos lógicos, el orden en el que se presentan estos grupos representan como deberían aparecer en los mensajes SIP, es decir: cabeceras generales, cabeceras de solicitud, cabeceras de respuesta y cabeceras de entidad.

GENERAL	**SOLICITUD**	**RESPUESTA**	**ENTIDAD**
Accept	Accept-Contact*	Allow	Content-Encoding
Accept-Encoding	Authorization	Proxy-Authenticate	Content-Length
Accept-Language	Contact	Retry-After	Content-Type
Call-ID	Hide	Rseq*	
Contact	Max-Forwrds	Server	
CSeq	Organization	Unsupported	
Date	Priority	Warning	
Encryption	Proxy-Authorization	WWW-Authenticate	
Expires	Proxy-Require		
From	RAck*		
Record-Route	Reject-Contact*		
Session-Expires*	Request-Disposition*		
Supported*	Require		
Time Stamp	Response Key		
To	Route		
Via	Subject		
User-Agent			

Tabla 1.8: Elementos de la Cabecera SIP (* trabajo de la IEFT en progreso) [2]

Abreviaturas del nombre de cabecera

Algunos nombres de las cabeceras SIP puede ser abreviados para evitar la fragmentación y los servidores SIP deben tener la facultad de interpretar los nombres de cabecera normales y abreviados.

En la tabla 1.9 se muestra los nombres de cabeceras que pueden ser abreviados.

NOMBRE DE CABECERA COMPLETO	**NOMBRE DE CABECERA ABREVIADO**
Call-ID	i
Contact	m
Content-Encoding	e
Content-Length	l
Content-Type	c
From	f
Subject	s
To	t
Via	v

Tabla 1.9: Abreviaturas de Nombre de Cabecera [2]

1.1.2.2.8 Cuerpo de los Mensajes SIP

Protocolo de Descripción de la Sesión

SDP es el protocolo de descripción de la sesión diseñado para identificar los atributos de una sesión, incluyendo información administrativa, sobre el programa y sobre los medios.

SDP especifica un estricto orden de los atributos; este orden se basa en minimizar el tamaño y complejidad del analizador sintáctico del protocolo.

La tabla 1.10 especifica los atributos de SDP:

TIPO SDP	VALOR
Descripción de la sesión	
v=	Versión del protocolo.
o=	Propietario-creador e identificador de sesión
s=	Nombre de la sesión
i=	*Información de la sesión
u=	*URI de descripción
e=	*Dirección de e-mail
p=	*Número de teléfono
c=	*Información de la conexión (no es necesario si se incluye en todos los medios).
b=	*Información del ancho de banda
<TIME_DESCR>	Una o más descripciones horarias
z=	*Ajustes de zona horaria
k=	*Clave de encriptación
a=	*Ninguna o más líneas de atributos de sesión
<MEDIA_DESCR>	*Ninguna o más descripciones de los medios
Descripción del tiempo	
t=	Tiempo en que la sesión está activa
r=	*Cero o más repeticiones.
Descripción de los medios	
m=	Nombre de los medios y dirección del transporte.
i=	*Título de los medios.
c=	*Información de la conexión (opcional si incluye el nivel de la sesión)
b=	*Información del ancho de banda
k=	*Clave de encriptación
a=	*Ninguna o más líneas de atributo.

Tabla 1.10: Atributos de SDP [2]

1.1.2.2.9 Operación SIP

Llamada SIP directa entre puntos finales IP

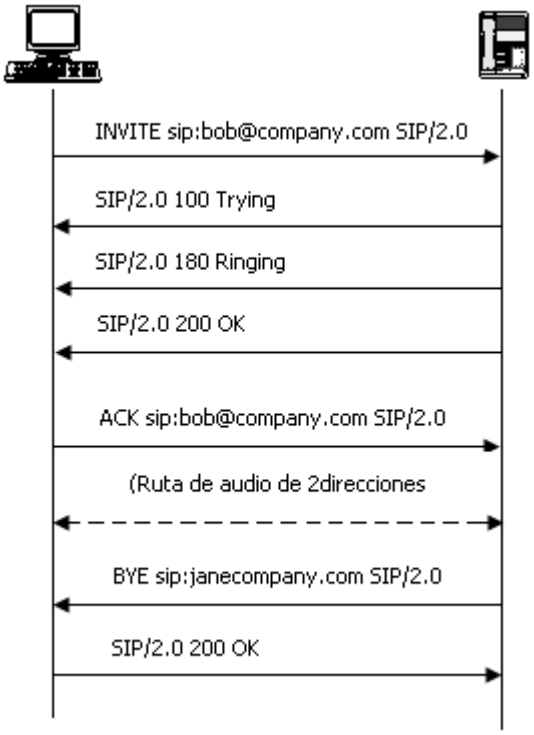


Figura 1.13: Llamada SIP directa entre puntos finales IP. [2]

Llamada SIP directa entre routers VoIP actuando como gateways SIP/RDSI

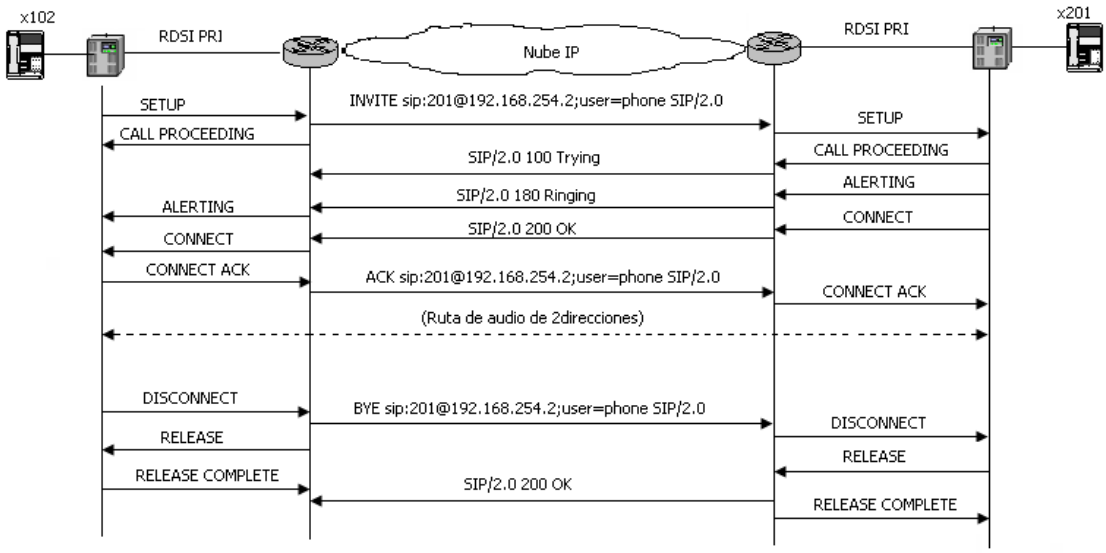


Figura 1.14: Llamada SIP directa entre gateways VoIP. [2]

Nuevo registro de un cliente SIP

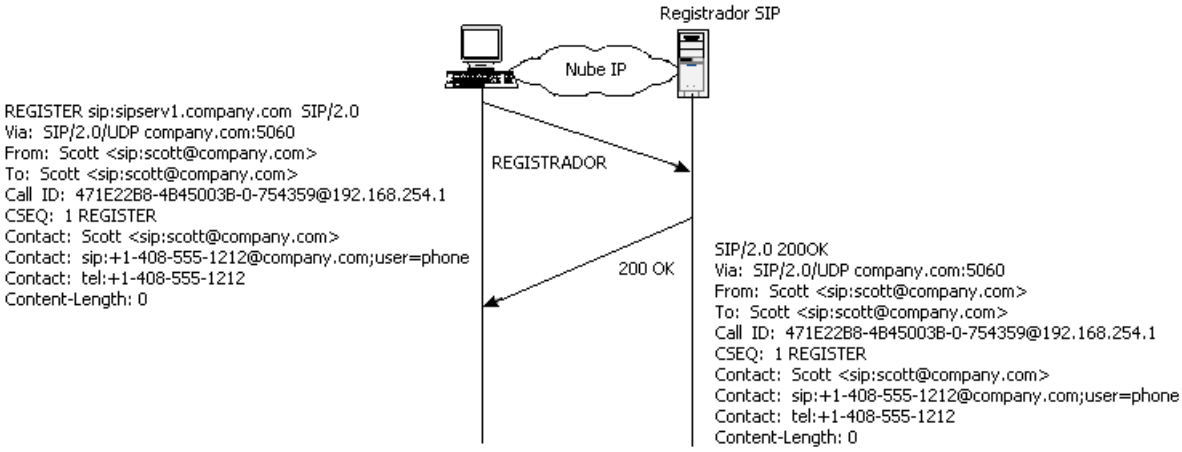


Figura 1.15: Registros de cliente con el registrador SIP por primera vez desde que está encendido [2]

Registro actualizado de un cliente SIP

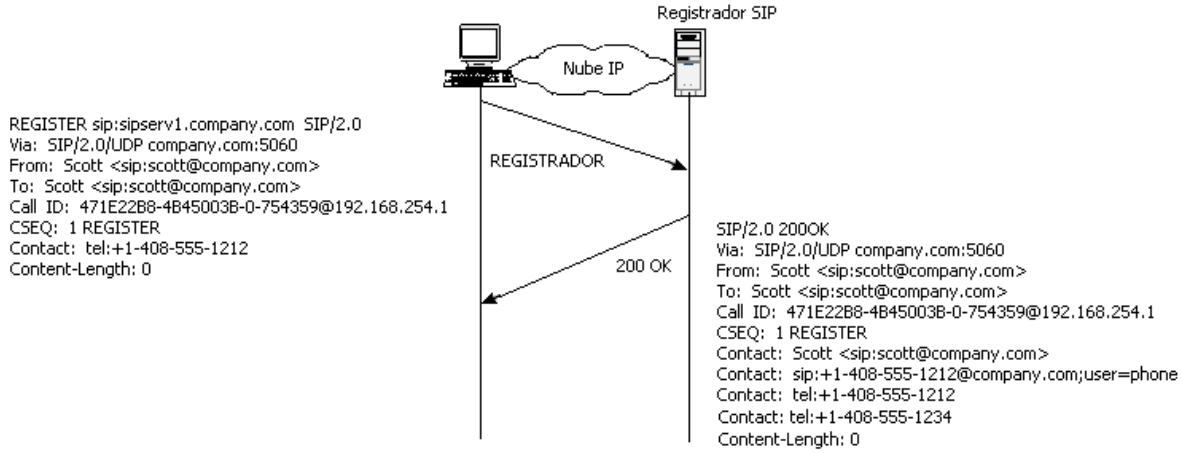


Figura 1.16: Información de contacto de las actualizaciones del cliente con el registrador SIP. [2]

Servidor Redirigido, servidor Proxy y gateway VoIP

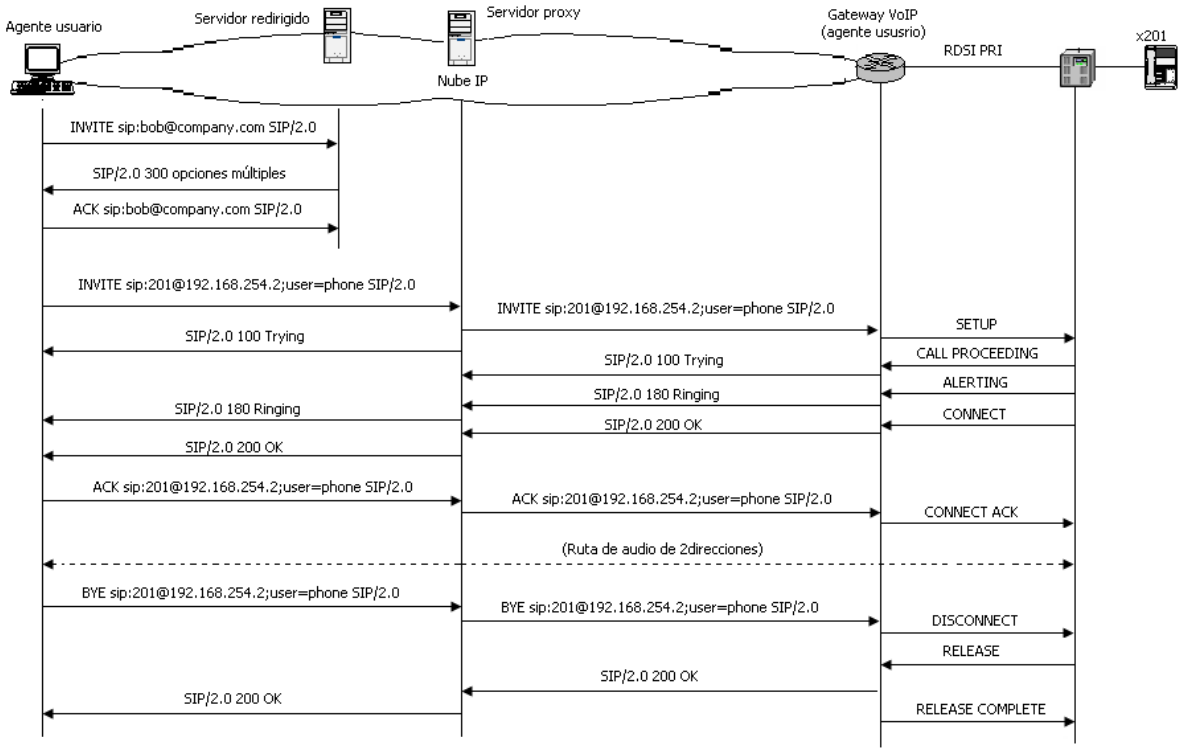


Figura 1.17: Cliente UA redirigido a un servidor Proxy. El router VoIP actúa cómo un gateway SIP/RDSI. [2]

SERVICIOS SIP

Entre los servicios que ofrece SIP se encuentran los siguientes:

Usuarios:

1. Localización.
2. Disponibilidad y capacidades (servicio de presencia y terminal asociado).
3. Perfil.

Llamadas

1. Establecimiento.
2. Mantenimiento.
3. Desvíos.
4. Traducción de direcciones.
5. Entrega de los números llamado y llamante.

6. Movilidad: direccionamiento único independiente de la ubicación del usuario.
7. Negociación del tipo de terminal
8. Negociación de las capacidades del terminal.
9. Autenticación de usuarios llamado y llamante.
10. Trasferencias ciegas y supervisadas.
11. Incorporación a conferencias multicast.

1.1.2.3 Protocolo H.248 (MEGACO)

Protocolo definido en la Recomendación H.248 de la ITU-T, y en el RFC 3525 por la IETF. Fue el resultado del trabajo conjunto entre la ITU y el IETF.

El protocolo H.248 o Megaco es utilizado para la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y la red IP o entre redes IP.

Este protocolo es la evolución del protocolo MGCP (Media Gateway Control Protocol, Protocolo de control de puerta de enlace al medio), el cual proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes IP.

Megaco es un protocolo de señalización utilizado entre los elementos de una arquitectura distribuida que incluye media gateway MGW (GW de VoIP, un DSLAM, un router MPLS, un teléfono IP, etc) y controladores de media gateway MGC (softswitches-SS, gatekeeper-GK o call agent).

Este protocolo que se basa en la arquitectura maestro/esclavo, en donde los MGW ejecutan los comandos enviados por el Gatekeeper o MGC. Este protocolo maneja comandos basados en texto para el establecimiento y control de dispositivos que intercambian flujos de información.

H.248 es un protocolo que trabaja conjuntamente con H.323 y SIP. Debido a que para la comunicación de MGC con los MG se utiliza el protocolo H.248 sin embargo para establecer la comunicación con otro MGC se debe utilizar el

protocolo H.323 o SIP. Además Megaco provee servicios básicos y necesita de un protocolo de mayor funcionalidad como SIP para ofrecer servicios más avanzados.

Componentes

Este protocolo busca hacer una separación de funciones de interconexión en tres capas independientes; separando la inteligencia y funciones de control de las de transporte para obtener un mayor número de servicios y conseguir aumentar la fiabilidad y la escalabilidad en la arquitectura de red. Por consiguiente se ha dividido a las pasarelas en tres entidades lógicas como son:

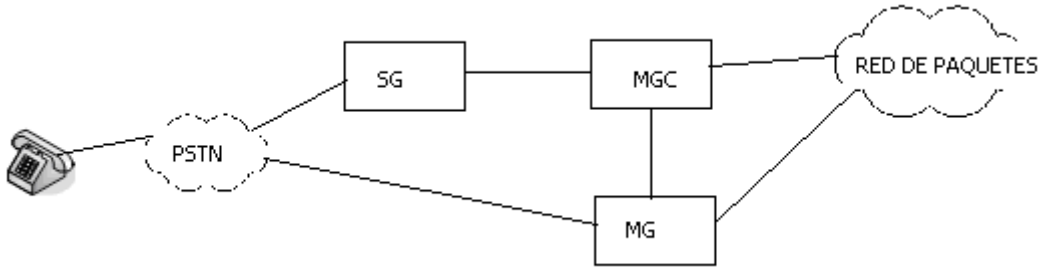


Figura 1.18: Componentes Protocolo H.248 [7]

Pasarela Física (Media Gateways – MG): Elementos funcionales que intervienen en la comunicación entre los puntos finales. Realizan la conversión de flujos de información entre una red de conmutación de circuitos (PSTN) y una red de conmutación de paquetes (IP).

Controlador de la Pasarela (Media Gateway Controller - MGC): Se lo puede llamar también *Call Agent*. Se encarga del control de los Media Gateways y del manejo de la señalización para la entrega de servicios además de realizar funciones de procesamiento y control de llamadas.

Pasarela de Señalización (Signalling Gateway – SG): Proporciona una interfaz bidireccional para la traducción de la señalización entre las redes SS7 y los elementos de control de las redes IP, estas redes utilizan los protocolos de

gestión de sesión H.323 y SIP. Esta entidad puede ser parte del softswitch o del MG o a su vez ser un elemento físico específico para esta función.

El proceso de llamada se describiría de manera general de la siguiente forma: Cuando el usuario marca desde su Terminal el número del Terminal de otro usuario, conectado a una central diferente, la central local del abonado llamante asignará a dicha llamada un canal vocal bidireccional y generará la señalización SS7 para la central destino.

En el extremo del abonado llamante el canal bidireccional asignado a la llamada se dirigirá hacia el MG que se encargará de procesar la señal PCM (conmutación de circuitos), transformándola a un formato digital para su transmisión en una red IP (conmutación de paquetes).

Paralelamente, desde la central local llamante se enviará el tráfico de señalización correspondiente a esa llamada al SG, el cual interpretará la señalización SS7. Esta información traducida se envía al ssw que establece sesiones SIP o H.323 con un SS destino, identificado por una dirección IP, pudiendo ser otro o el mismo SS. La sesión de control SIP/H.323 establece un flujo UDP entre el MG origen y el destino una vez identificadas sus direcciones IP por los SSs. En el envío de este flujo UDP se realiza la transmisión de los paquetes de voz.

En el MG destino se realizará el proceso inverso, convirtiendo la señal a formato PCM y transmitiéndola a una central local que utilizando la manera tradicional la encaminará hacia el Terminal del abonado llamado.

1.1.2.4 Internet Protocol (IP)

1.1.2.4.1 IPv6

Es la versión 6 del Protocolo IP creada para sustituir al protocolo IPv4 ya que debido al amplio desarrollo del Internet el número de direcciones que actualmente existen resultan insuficientes, mientras que IPV6 ofrece 2^{128}

direcciones, y nuevos servicios como movilidad, calidad de servicio, privacidad, clase de servicio, auto configuración (plug and play), etc.

Las direcciones IPv6, están conformadas por ocho grupos de cuatro dígitos hexadecimales. Por ejemplo,
2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Si un grupo de cuatro dígitos son ceros, puede ser comprimido. Así:

De 2001:0db8:85a3:0000:1319:8a2e:0370:7344
A 2001:0db8:85a3::1319:8a2e:0370:7344

Si la dirección es una dirección IPv4 , los últimos 32 bits pueden escribirse en base decimal; así,
::ffff:192.168.89.9 es lo mismo que
::ffff:c0a8:5909, pero no lo mismo que
::192.168.89.9 o
::c0a8:5909.

Tipos de Paquetes IP

Las direcciones IP son clasificadas en tres tipos de direcciones e identifican interfaces de la red ya sea grupal o individual:

- *Dirección Unicast.-* Usada para identificar a una sola interfaz, es equivalente a las direcciones IPv4.
- *Dirección Anycast.-* Identifica un conjunto de interfaces, el paquete enviado es entregado a la interfaz más cercana, permitiendo crear ámbitos de redundancia de manera que varios equipos pueden ocuparse de un tráfico de acuerdo a una secuencia determinada.
- *Dirección Multicast.-* Identifica a un grupo de interfaces, el paquete es entregado a todas las interfaces. Usado para mensajes broadcast, ya que este tipo de direcciones no existen en IP V6

Ejemplos de paquetes IP

Los tipos de direcciones IPv6 se identifican con los primeros bits de cada dirección:

- ::/128 – la dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.
- ::1/128 – la dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.
- ::ffff:0:0/96 – La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.
- fe80::/10 – Indica que se trata de una dirección válida solo en el enlace físico local.
- fec0::/10 –Específica que la dirección sólo es válida dentro de una organización local.
- ff00::/8 – El prefijo de multicast .

Paquete IP

En el paquete IpV6 con respecto a la versión 4 se han modificado algunos campos o se han convertido en opcionales y se han eliminado otros, como podemos observar en la figura 1.19. El formato de la cabecera sin las extensiones es el siguiente:

- Versión: Al igual que en la versión indica el número de versión del protocolo IP.
- Prioridad: Contiene el valor de la prioridad o importancia del paquete que se está enviando. Tamaño: 4 bit.
- Etiqueta de flujo: se utiliza el campo para indicar que el paquete requiere un tratamiento especial por parte de los *routers*. *Tamaño: 24 bit.*
- Longitud: Es la longitud de los datos en bytes. *Tamaño: 16 bit.*
- Siguiente cabecera: Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. *Tamaño: 8 bit.*

- Límite de existencia: Indica el tiempo de vida del paquete. *Tamaño:8 bit.*
- Dirección de origen: El número de dirección del *host* que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. *Tamaño: 128 bit.*
- Dirección de destino: Número de dirección de destino, aunque puede no coincidir con la dirección del *host* final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. *Tamaño: 128 bit.* " [1]

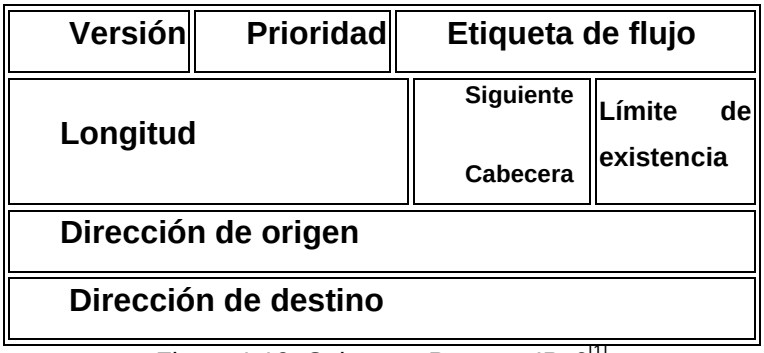


Figura 1.19: Cabecera Paquete IPv6[1]

En esta versión del protocolo IP la cabecera no tiene un tamaño fijo, posterior a la cabecera normal se colocan las extensiones o cabeceras opcionales, y son procesadas únicamente por el receptor del mensaje.

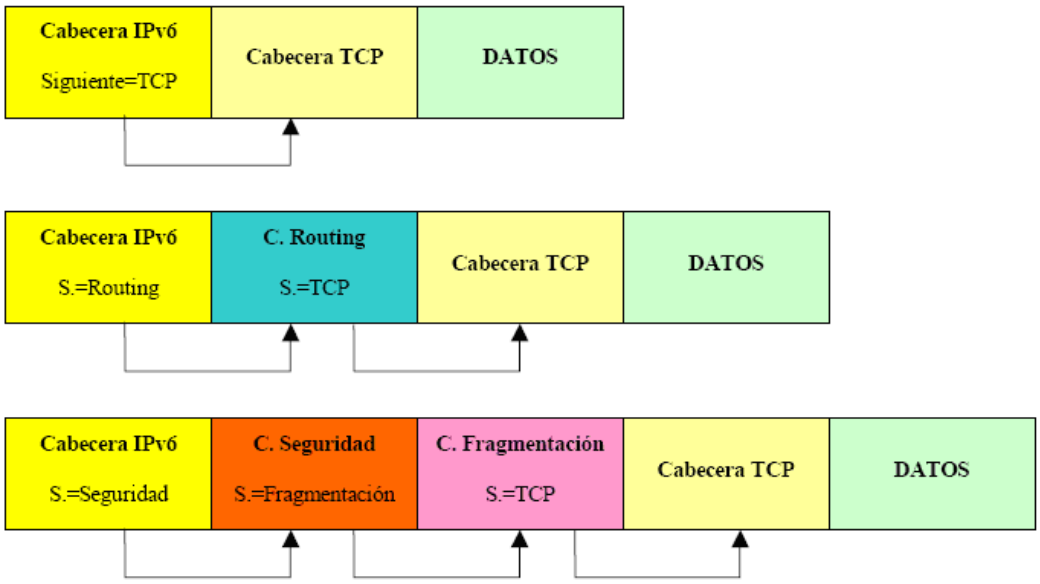


Figura 1.20: Paquete IPv6[1]

1.2 CALIDAD DE SERVICIO EN REDES

1.2.1 INTRODUCCIÓN

En la actualidad las redes son transporte de una gran variedad de servicios, cada uno tiene sus propias características, por esta razón deben ser tratados de forma diferente. El objetivo es evitar que la congestión que existe en la red afecte a las aplicaciones críticas que necesitan de un determinado caudal o retardo.

Para proporcionar un nivel de servicio adecuado para la transmisión de información se establece un conjunto de requerimientos que la red debe cumplir para asegurar calidad de servicio. Para ello se debe considerar aspectos que beneficien tanto al proveedor como al usuario.

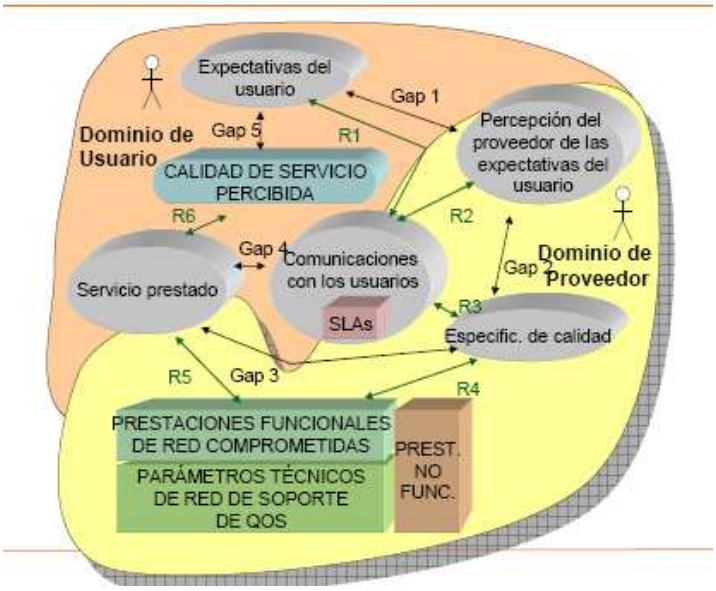


Figura 1.21: Provisión y Factores de QoS 8

La eficiencia debe ser independiente de los diferentes tipos de tecnología que interactúan ya sean inalámbricos o cableados, por lo que se debe tener en cuenta ciertos parámetros, como los que a continuación se muestran, para proporcionar un mejor servicio:

- ***Retardo de los paquetes (latencia):*** Es el tiempo que transcurre en la entrega de un paquete, si la demora es muy grande puede tener consecuencias en la calidad de la aplicación.

- ***Jitter (retardo medio de los paquetes):*** se refiere a las variaciones del retardo de los paquetes o latencia.
- ***Retardo máximo de los paquetes:*** Al enviar un paquete se le determina un tiempo de vida, cuando haya transcurrido este tiempo sin que el paquete llegue a su destino este será descartado.
- ***Tasa máxima de paquetes perdidos:*** porcentaje de paquetes descartados por diversas razones que puede tolerar la aplicación
- ***Tasa de error media en los bits de información****:* Se refiere a los bits errados que puede soportar una aplicación sin que esta pérdida le afecte.

Existen otras causas de deficiencia en la calidad de servicio como protocolos de enrutamiento inestables, en ocasiones los ruteadores pueden dar a los paquetes rutas divergentes aumentando la fluctuación.

En una red se puede proporcionar calidad de servicio mediante el uso de colas con preferencias, protocolos de reserva de recursos, mecanismos de control de congestión entre otros.

1.2.2 NORMAS DE ENCOLAMIENTO

El uso de colas a la salida de la información nos da control sobre la transmisión de paquetes permitiéndonos optimizar la comunicación.

Las normas de encolamiento se han desarrollado principalmente para proporcionar las solicitudes de QoS para aplicaciones identificadas y proporcionar una distribución equitativa de los recursos de ancho de banda, esto lo han enfocado desde dos perspectivas:

- Administrar la profundidad de la cola
- Programar el orden de envío de los paquetes

1.2.2.1 Cola FIFO

Es la técnica consiste en un simple búfer que retiene los paquetes salientes hasta que la interfaz de transmisión pueda enviarlos. Los paquetes son enviados en el mismo orden que llegaron al búfer, tal como muestra la figura 1.

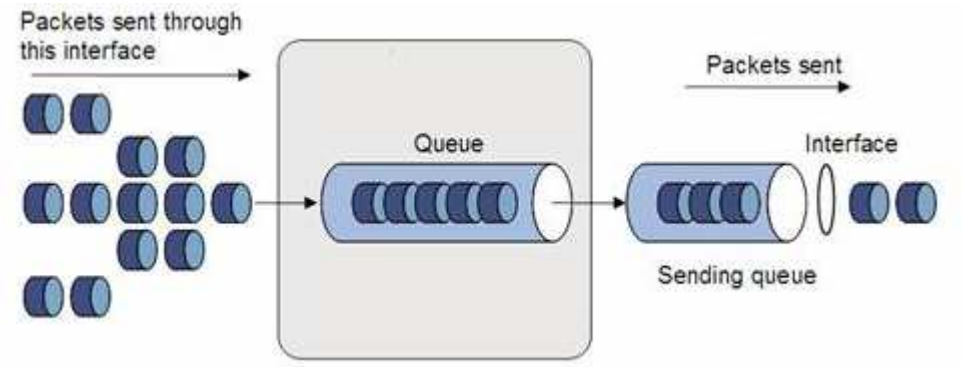


Figura 1.22: Cola FIFO [22]

Esta técnica de encolamiento no proporciona ningún tipo de QoS ni distribuye un ancho de banda equitativo entre flujos que comparten un enlace. Durante los periodos de congestión, se llena el búfer y los paquetes se descartan sin importar el tipo de paquete o la solicitud de la aplicación asociada, por los que no es muy recomendable para VoIP.

1.2.2.2 Cola de prioridad

Los paquetes que llegan son divididos en cuatro colas con prioridades: baja, normal, Media y alta, la salida de estas cuatro colas alimenta un búfer de transmisión como se muestra en la figura 1.23.

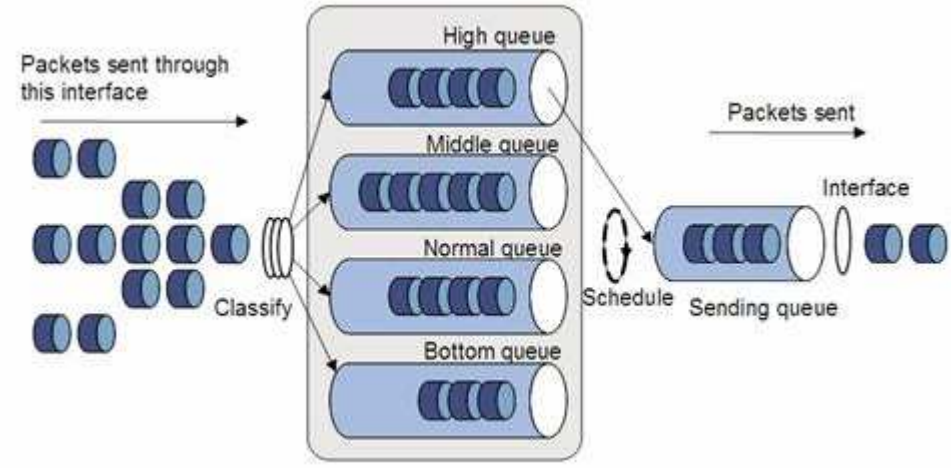


Figura 1.23: Cola de prioridad [22]

Los paquetes se envían primero desde las colas de alta, media, normal y baja prioridad, si los paquetes están esperando en dichas colas se los envía al búfer

de transmisión. La cola de prioridad consigue los requisitos de QoS de VoIP, pero dejan mucho que desear en cuanto a la distribución del ancho de banda equitativo para el resto de tráfico.

1.2.2.3 Cola personalizada

Es un algoritmo de encolamiento configurado equitativamente. El tráfico se clasifica en colas y se vacían todas por igual, tal como muestra la figura 1.24figura 1.2.

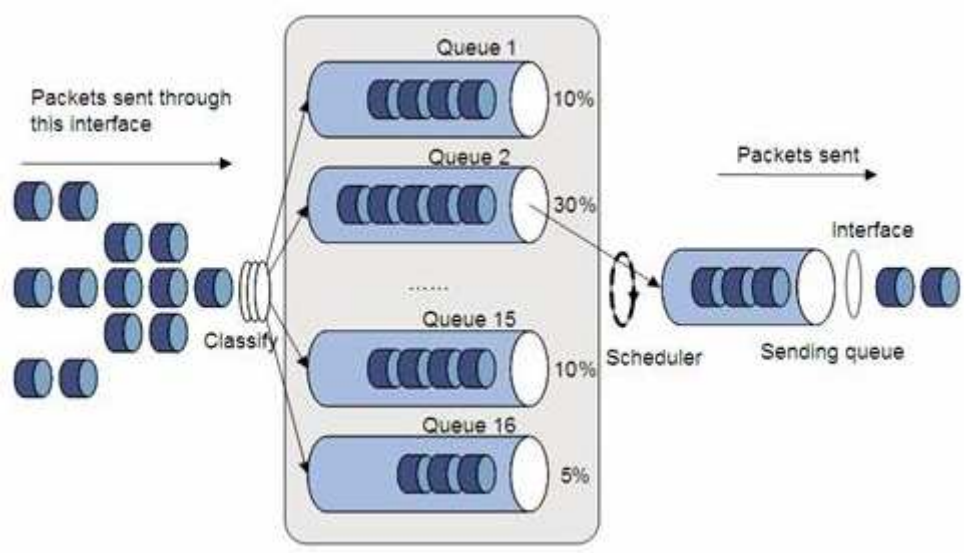


Figura 1.24: Cola Personalizada [22]

Se configura manualmente, el tráfico que se asocia a cada cola, cuántos paquetes pueden esperar en cada cola y qué cantidad de ancho de banda se destina a cada cola. Puede que la cola personalizada supla el tema de ancho de banda equitativo, pero no se ajusta para proporcionar QoS a flujos de tráfico específico, ya que todas las colas tienen la misma prioridad, por esta razón no es aconsejable utilizarla para VoIP.

1.2.2.4 Colas Basadas en Clases (CBQ *Class Based Queueing*)

Es un mecanismo basado en la clase de tráfico, se clasifica el tráfico por el tipo y de acuerdo a esta clasificación se le asigna una cola de salida. Previamente CBQ determina un conjunto de colas y la clase de tráfico que se dirigirá a cada una.

El objetivo es determinar un ancho de banda a cada clase de servicio de acuerdo al tráfico que genera. Si una cola no utiliza el ancho de banda asignado este será distribuido siguiendo determinadas reglas especificadas con anticipación.

1.2.2.5 Colas Equitativa Ponderadas (Weighted Fair Queueing, WFQ)

Es un mecanismo que reparte el ancho de banda disponible de acuerdo al comportamiento del tráfico. El tráfico de poco volumen recibe un trato preferencial, mientras que el tráfico de mayor volumen se reparte en el ancho de banda restante.

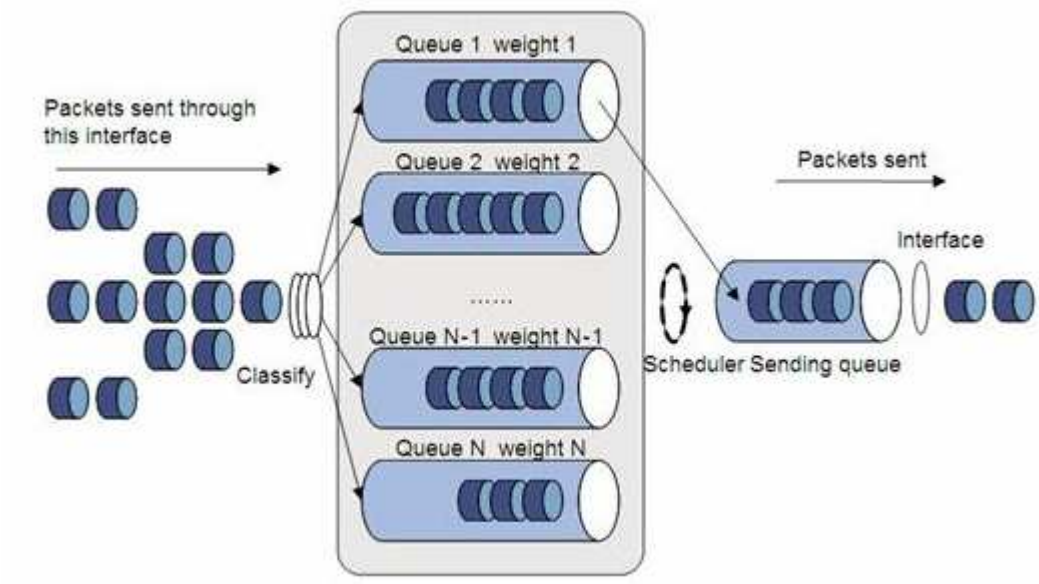


Figura 1.25: Cola Equitativa Ponderada [22]

Es muy similar a la cola personalizada, salvo que no necesita ninguna configuración.

1.2.3 ARQUITECTURA INTSERV (SERVICIOS INTEGRADOS) Y PROTOCOLO RSVP

1.2.3.1 Arquitectura Intserv

En Intserv la idea básica es definir una forma de reserva de recursos independiente de los protocolos utilizados para señalización y detalles de aplicación.

En la arquitectura IntServ se definen tres tipos de servicio:

Servicio Garantizado: Este servicio garantiza un caudal mínimo y un retardo máximo, asegurando a las aplicaciones un tiempo máximo de transmisión extremo a extremo evitando pérdidas por congestión. Sin embargo pueden existir variaciones en el retardo debido a paquetes que llegan antes del plazo establecido.

Servicio de Carga Controlada: este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada, es decir en general un buen tiempo de respuesta, pero sin garantías estrictas. Eventualmente se pueden producir retardos grandes.

Servicio Best Effort: este servicio no tiene ninguna garantía. No establece un límite máximo de retardo. Para conseguir sus objetivos IntServ dispone del protocolo RSVP.

1.2.3.2 RSVP (Resorce Reservation Protocol)[2]

RSVP es un protocolo de control que permite reservar recursos de la red entre el transmisor y el receptor, opera sobre el protocolo IP (IPv4 o IPv6) y está diseñado para tráfico multidifusión así como también para tráfico unidifusión. Generalmente las implementaciones de VoIP son tráfico de unidifusión, ya que casi todas las llamadas son de naturaleza punto a punto. Mientras que para la

distribución de flujos de audio y vídeo en tiempo real usualmente se realiza con tráfico multidifusión.

RSVP permite a los routers establecer dinámicamente anchos de banda para flujos específicos que requieren un servicio especial, cada receptor realiza las solicitudes de reserva de recursos para recibir determinado flujo lo que permite que varios receptores soliciten diferentes niveles de calidad de servicio del mismo remitente.

Cuando se realiza una reserva a través de RSVP es indispensable una fuente, la dirección IP destino y el puerto que define el flujo, por lo que en una llamada de VoIP no se puede establecer la reserva hasta después que se realice la conexión e identificar los números del puerto que interviene en la llamada.

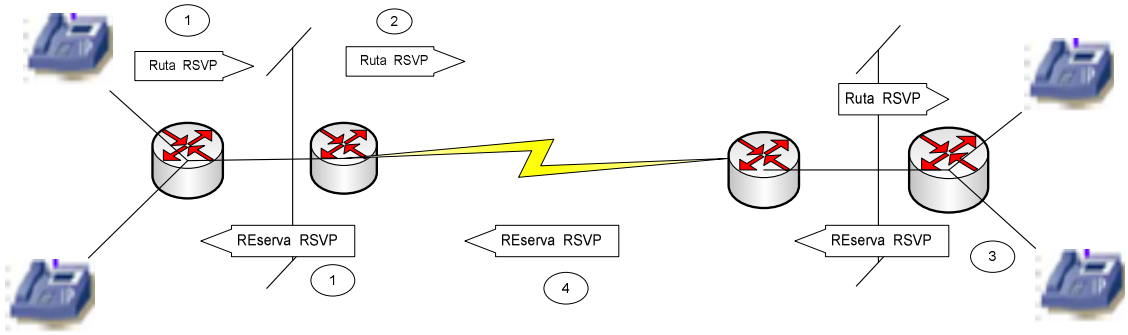


Figura 1.26: Proceso para establecer la Reserva RSVP[2]

1.2.3.2.1 Configuración de una Reserva RSVP

1. El emisor solicita una sesión RSVP, envía un mensaje ***PATH*** a todos los destinatarios. Este mensaje contiene la dirección IP destino que determinará la ruta que posteriormente recorrerán los paquetes de datos.

2. El mensaje PATH almacena su información en los routers RSVP y crea en cada nodo la información de estado de camino transportando en cada salto la dirección IP del nodo anterior.

3. El receptor al obtener el mensaje PATH responde con un mensaje ***RESV*** que viaja a través de los routers con capacidad RSVP. Este mensaje es la solicitud de los recursos de la red.

4. Los routers por los que recorre el mensaje RESV efectúa dos verificaciones; el ancho de banda que dispone para realizar la reserva y si el receptor está autorizado para hacerla. Si las verificaciones son satisfactorias, el router reserva los recursos de cola y pasa el mensaje RESV al siguiente router con capacidad RSVP. Cuando el emisor original recibe el mensaje RESV, la reserva se ha completado y ya puede empezar a emitir datos.

Las reservas que se establecen mediante RSVP tienen un tiempo de vida por lo que deben ser refrescadas periódicamente para que no sean suspendidas.

1.2.3.2.2 Mensajes

Además de los mensajes PATH y RESV se tiene los siguientes mensajes:

- **PATHTEAR** mensaje que borra la información de estado de camino explícitamente
- **RESVTEAR** borra la información de estado de reserva explícitamente
- **PATHERR** informa si ha ocurrido un error al procesar un mensaje PATH
- **RESVERR** informa si ha ocurrido un error con un mensaje RESV
- **RESVCONF** es un mensaje confirmando la reserva de recursos, se da en respuesta a una solicitud realizada a través del mensaje RESV.

1.2.3.2.3 Formato

Un mensaje RSVP consta de cabecera y un número variable de Objetos.

Cabecera
Objeto1
Objeto2
……
Objeto n

Formato de los Mensajes RSVP

Cabecera

32	28	24	16	0
Versión	Flag	Tipo Mensaje	Checksum RSVP	
Send_TTL		(Reservado)	Longitud RSVP	

Figura 1.27: Formato de la Cabecera de los Mensajes RSVP[9]

Versión del protocolo RSVP

Flags Valores no definidos en el estándar

Tipo de Mensaje: Indica el tipo de mensaje. Los posibles son:

- Mensaje de Ruta (Path)
- Mensaje de reserva
- Mensaje de error de ruta
- Mensaje de error de Reserva
- Mensaje de finalización de Estado de Ruta
- Mensaje de finalización de Estado de reserva
- Mensaje de confirmación de Reserva

Checksum RSVP

Send_TTL Es el tiempo de vida el paquete IP.

Longitud RSVP: Es la longitud total del mensaje RSVP en bytes

1.2.4 ARQUITECTURA DIFFSERV[2]

En la arquitectura DiffServ a diferencia de IntServ la información de calidad de servicio se escribe en los datagramas, no en los routers.

Para brindar calidad de servicio el tráfico se clasifica en clases, los que pertenecen a una determinada clase se marcan con un código específico

(DSCP – Diffserv CodePoint). Este código identifica la clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, a esto se conoce como PHB (Per Hop Behavior).

1.2.4.1 Elementos

DiffServ esta conformada básicamente por:

Dominio DS: un dominio Diffserv puede estar formado por más de una red, de manera que el administrador será responsable de repartir adecuadamente los recursos.

Nodo frontera DS: conjunto de funciones que posibilitan el acondicionamiento de tráfico entre los dominios Diffserv interconectados.

Nodo interno: conjunto de funciones necesarias en los nodos que están conectados únicamente a otros nodos DS.

Nodo de entrada: conjunto de funciones necesarias para manejar el tráfico entrante en un dominio DS.

Nodo de salida: conjunto de funciones necesarias para manejar el tráfico de salida en un dominio DS.

1.2.4.2 Comportamiento por Salto PHB

Los comportamientos PHB se implementan por operaciones o algoritmos específicos como por ejemplo disciplinas de colas.
Algunos PHB estandarizados son:

- PHB por defecto Similar al servicio best effort (mejor Esfuerzo), no tiene ninguna garantía. No establece un límite máximo de retardo.

- PHB Selector de Clase Este servicio clasifica el flujo en clases a los que proporciona una garantía de transmisión relativa. En caso de congestión el tráfico experimentará retardos de acuerdo a la prioridad, los de mayor prioridad tendrán menos retardos de colas que el tráfico de menor prioridad.

- PHB reenvío Expedito El objetivo de este servicio es proporcionar un ancho de banda garantizado y bajos valores de pérdidas, latencia y variación de retardo. Usada en aplicaciones de tiempo real como videoconferencia, voz sobre IP entre otras.

- PHB de Reenvío Asegurado Su objetivo es satisfacer la demanda en el reenvío de los paquetes IP en Internet e Intranets, el tráfico en este servicio no puede exceder la velocidad suscrita. Con este servicio un proveedor de un dominio DS puede ofrecer diferentes niveles de seguridad de reenvío a los paquetes IP recibidos por el cliente. Este servicio se debe asignar una capacidad (ancho de banda y buffers) configurable a cada clase de acuerdo a los SLA acordados y no se pueden reordenar los paquetes de un mismo flujo, cuando pertenecen a una misma clase independiente de su prioridad.

Generalmente un nodo frontera contiene todas las funciones antes mencionadas y los nodos internos pueden contener parte de las funciones de un nodo frontera.

1.2.5 DIFFSERV vs INTSERV

La tabla 1.11 corresponde a la comparación entre las arquitecturas Intserv y Difserv, el primero basa sus sevicios en el envío de datagramas extras mientras que el otro envía información de calidad de servicio en los propios datagramas IP.

	INTSERV	DIFFSERV
Forma de la diferenciación del servicio	Flujos individuales	Agregado de flujo
Base de la clasificación de tráfico	Algunos campos de cabecera	El campo DSCP
Control de admisión	Requerido	Requerido solo para diferenciación absoluta
Protocolo de señalización	Requerido (RSVP)	No requerido para esquemas relativos; esquemas absolutos necesitan reservaciones semi-estáticas o un agente broker
Coordinación para la diferenciación del servicio	Extremo a extremo	Local (por salto)
Alcance de diferenciación de servicio	Ruta unicast o multicast	Cualquier lugar de la red o rutas específicas
Escalabilidad	Limitada por el número de flujos	Limitado por el número de clases de servicio
Manejo de red	Similar a la de los circuitos conmutados	Similar ala existentes en redes IP

Tabla 1.11: Comparación arquitectura DifSer vs Intserv[21]

1.2.6 PROTOCOLOS DE TRANSPORTE [2]

El protocolo RTP fue desarrollado IETF, en el se definen dos protocolos:

- RTP (Real Time Transport Protocol)
- RTCP (Real Time Transport Control Protocol)

RTP está diseñado para proveer a una aplicación escalabilidad automáticamente sobre el tamaño de las sesiones, de manera que una aplicación puede tener pocos participantes o cientos.

RTP es el encargado del transporte de los datos, mientras el RTCP es utilizado para el control del flujo de datos enviando periódicamente información.

El protocolo de transporte utilizado por RTP es UDP.

RTP trabaja con una amplia variedad de aplicaciones multimedia y está diseñado para adicionarle más aplicaciones sin cambiar el protocolo. RTP define un perfil (*profile*) para cada aplicación y uno o más formatos (*formats*). El *profile* proporciona información para asegurar el entendimiento de los campos del *header* de RTP para la aplicación. El formato especifica cómo los datos que siguen al *header* deben ser interpretados.

1.2.6.1 Protocolo de Transporte Rápido (RTP)

Proporciona los siguientes servicios:

- Distingue los emisores múltiples en un flujo multidifusión RTP
- Conserva la relación de temporización entre los paquetes
- Posibilita la sincronización de temporización entre los flujos de medios
- No proporciona o asegura QoS

Trama RTP:

- Número de versión de RTP (V - versión number): 2 bits. La versión definida por la especificación actual es 2.
- Relleno (P - Padding): 1 bit. Si el bit del relleno está colocado, hay uno o más bytes al final del paquete que no es parte de la carga útil. El último byte del paquete indica el número de bytes de relleno. El relleno es usado por algunos algoritmos de cifrado.

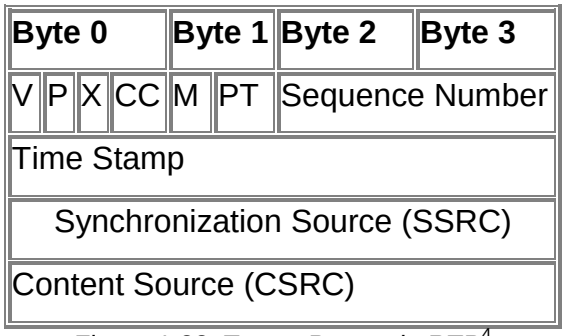


Figura 1.28: Trama Protocolo RTP[4]

- La extensión (X - Extensión): 1 bit. Si el bit de extensión está colocado, entonces el encabezado fijo es seguido por una extensión del

encabezado. Este mecanismo de la extensión posibilita implementaciones para añadir información al encabezado RTP.

- Conteo CSRC (CC): 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.
- El marcador (M - Marker): 1 bit. Un bit de marcador definido por el perfil particular de media.
- La carga útil Type (PT): 7 bits. Un índice en una tabla de perfiles de media que describe el formato de carga útil. Los mapeos de carga útil para audio y vídeo están especificados en el RFC 1890.
- El número de Secuencia: 16 bits. Un único número de paquete que identifica la posición de este en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.
- Sellado de tiempo: 32 bits. Refleja el instante de muestreo del primer byte en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo - por ejemplo, si son todo parte del mismo *frame* de vídeo.
- SSRC: 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, entonces el SSRC identifica el mixer (mezclador).
- CSRC: 32 bits cada uno. Identifica las fuentes contribuyentes para la carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; Allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.

Los paquetes RTP perdidos son detectados por el receptor mediante el número de secuencia, aunque no se utilice este para la retransmisión.

Cuando se utiliza RTP con VoIP la sobrecarga es 0.

1.2.6.2 Protocolo de Control Rápido RTCP[2]

Este protocolo se encarga de aspectos relacionados con los informes y la administración de una conferencia RTP multidifusión.

Este *stream* de control tiene tres funciones principales:

1. Retroalimenta información sobre el desempeño de la aplicación y de la red. Es muy útil para esquemas de compresión y diagnóstico de problemas en la red. Utilizado en aplicaciones de velocidad adaptiva.
2. Ofrece una forma de correlacionar y sincronizar diferentes *media streams* que provienen del mismo emisor
3. Proporciona una forma de transferir la identidad de un emisor para ser mostrada en la *interface* de un usuario

La segunda función parece estar ya cubierta con el identificador de fuente de sincronización de RTP (SSRC), pero en realidad no es así. Como se dijo antes, un nodo con varias cámaras pueden tener un SSRC diferente para cada cámara. Adicionalmente, no se requiere que un *stream* de audio y otro de video provenientes del mismo nodo utilicen el mismo SSRC. Ya que pueden darse colisiones de identificadores de SSRC es posible que se requiera cambiar el valor SSRC de un *stream*. Para poder manejar este problema, RTCP utiliza el concepto de Nombre Canónico (CNAME) que es asignado al emisor, este nombre canónico es luego asociado a varios valores SSRC que pueden ser utilizados por dicho emisor utilizando RTCP.

La correlación simple de dos *streams* es sólo parte del problema de sincronización intermedia. Como, además, diferentes *streams* pueden tener también relojes diferentes (con diferentes grados de inexactitud) existe la necesidad de definir una forma de sincronizar *streams* exactamente entre ellos. RTCP maneja este problema.

En trasmisiones multicast la información de control puede consumir un ancho de banda considerable (2 o 3 personas en audioconferencia consumen cierta

cantidad de ancho de banda para información de control). Para manejar este problema RTCP ha establecido un mecanismo para reducir la transmisión de información de control a medida que ingresan más nodos a la conferencia. El mecanismo es complejo para contarlo en este documento, pero la meta básica es limitar la cantidad de tráfico de RTCP a un pequeño porcentaje del tráfico de datos en RTP (normalmente el 5%). También es recomendado asignar más ancho de banda RTCP a los emisores activos, bajo el supuesto que la mayoría de los participantes desean ver los reportes enviados por ellos, como por ejemplo saber "quién habla".

1.3 SEGURIDAD EN REDES[10] [11] [13]

En la actualidad se debe proporcionar protección al transmitir información para reflejar la confianza que se tiene en el mundo tradicional al mundo electrónico.

La seguridad debe estar basada en la prevención, detección y respuesta ante ataques. La importancia de la prevención radica en que nos permite evitar ataques. Mientras que la detección es un proceso importante ya que si se conoce a tiempo que la red esta siendo atacada se puede evitar un daño irreparable con graves consecuencias.

Una vez detectado el ataque el siguiente paso sería implementar un plan de respuesta que permita contra restar el ataque.

Para proporcionar seguridad en la información se debe tomar en cuenta aspectos como:

Confidencialidad se trata de mantener la privacidad de la información, de forma que los datos transmitidos no puedan ser leídos por terceros. Para lograrlo generalmente se utiliza encriptación.

Integridad al hablar de integridad nos referimos a la protección de la información garantizando que no sea alterada por terceros, ya que esto podría traer graves consecuencias para el propietario legítimo de los datos.

Disponibilidad se entiende que los elementos de una red, tanto software como hardware puedan recuperarse rápida y completamente ante eventos de interrupción.

Autenticación es comprobar que un usuario identificado es quien dice ser, garantizando que solo los usuarios autorizados puedan acceder a la información.

Se debe tomar en cuenta que éstos son los aspectos fundamentales, sin embargo implementar la seguridad en una red abarca más características.

La seguridad también implica el establecimiento de políticas y procedimientos para la protección ante malos manejos, accidentes, etc. La seguridad siempre se puede ir mejorando y actualizando considerando un balance entre el costo de la seguridad contra el costo de lo que será protegido.

A continuación se realiza una descripción de los ítems que se consideraron de mayor trascendencia en el tema de la seguridad en redes informáticas, tales como son: ataques, cortafuegos (firewall), sistema de detección de intrusos, redes virtuales privadas (VPN), IPSec.

1.3.1 ATAQUES

"Un ataque es una técnica específica usada para explotar una vulnerabilidad" [10]

Virus: Es un programa o fragmento de código capaz de reproducirse a sí mismo (programa parásito). Un virus necesita de un programa host (programa al cual el virus se pega) para su funcionamiento, e infecta cualquier tipo de archivo ejecutable propagándose al ser ejecutado.

Gusanos: es un programa independiente diseñado para propagarse o reproducirse por si mismo dentro de sistemas infectados, buscando mecanismos para atacar otros sistemas.

Caballo de Troya: es un programa o fragmento de código que se oculta dentro de otro programa para evitar ser detectado e identificarse a sí mismo como un programa legítimo, lo cual lo logra mediante la modificación o el reemplazo de un programa existente. Tiene la capacidad de capturar información confidencial, generalmente contraseñas para enviarlas hacia otro sitio.

La Puerta Trasera (trap-door): son fragmentos de código en un programa que provee una forma de acceso a un sistema. Dicho acceso puede ser proporcionado a los mismos diseñadores o a su vez a alguien más, o a un sistema o proceso.

Port Scanning: es un programa encargado de "escuchar" puertos para determinar los servicios que ofrece un sistema, obtener información acerca de que sistema operativo está instalado en los hosts o ciertas características de la arquitectura de la red. Y de esta manera poder ingresar en el sistema.

Spoofs (engaños): se trata de una falsificación o el enmascaramiento de la identidad de alguien con otra y de esta manera poder tener acceso a una red o sistema.

- ***Spoofing de la dirección IP:*** es efectuado cuando en los sistemas se usan la dirección IP para autenticación de acceso válidos; el intruso detecta esas direcciones y la suplanta obteniendo acceso a los sistemas o recursos.

- ***Spoofing del número de secuencia:*** para conexiones TCP/IP es común el uso de números de secuencia. Estos números están presentes en cada transmisión y se intercambian en cada transacción. Dichos números son predecibles en base a algoritmos por lo tanto si el intruso los detecta puede insertarse en el intercambio de información y robarla o suplantarla. Por lo general se inserta en una conexión cliente-servidor a través de un dispositivo de red como un router.

- ***Ataque del hombre en la mitad (Man in the Midle Attack-MIM):*** es un ataque basado en la manipulación de DNSs, permite al intruso modificar y visualizar cualquier página web que el usuario solicite a través del navegador de modo que se redirecciona la conexión hacia el intruso para registrar cualquier evento generado por el usuario. El intruso se coloca entre el browser y el Web Server por lo que también se llama *Web spoofing.*

- ***DNS Spoofing:*** es un ataque en donde se suplanta la dirección IP al alterar la tabla de conversión de url a dirección IP, se puede hacer que el usuario vaya directamente a una página del intruso e ingrese información confidencial. Otras acciones que se podría realizar serían alterar la tabla DNS para redireccionar algunas direcciones hacia otros sitios o incluso haciendo que un servidor infecte la caché de otro (DNS Poisoning).

Sniffing: es ataque de interceptación, consiste en filtrar todos los paquetes que pasan por la red para obtener información útil para un ataque, tal como usuarios, contraseñas, direcciones IP, información confidencial.

Denegación de Servicio (Denial of Service, DoS)

Estos ataques consisten en evitar que usuarios legítimos puedan acceder a la información mediante la apropiación exclusiva de un recurso o servicio. Pudiendo también realizar los ataques con el fin de colapsar un recurso o sistema para inhabilitar el servicio o recurso.

- ***IP Flooding:*** es la generación de tráfico espurio con el fin de degradar el servicio de la red. De esta manera el intruso logra el consumo del ancho de banda disponible saturando el resto de las comunicaciones en la red. Este tipo de ataques por lo general se realizan en redes locales en donde el control del consumo de AB es mínimo o nulo, o en conexiones con un gran ancho de banda disponible.

Como ejemplos de este tipo de ataque tenemos los siguientes:

- *Definido o dirigido*: en este ataque la dirección de origen o destino (o ambas) es la de la máquina que recibe el ataque. Este ataque tiene dos objetivos: el primero es degradar el servicio de red dónde el atacante genera los paquetes IP y el segundo es colapsar un ordenador destino mediante la reducción del ancho de banda disponible para el servicio que ofrece, o a su vez saturarlo con una gran cantidad de peticiones de manera que no será capaz de procesarlas.

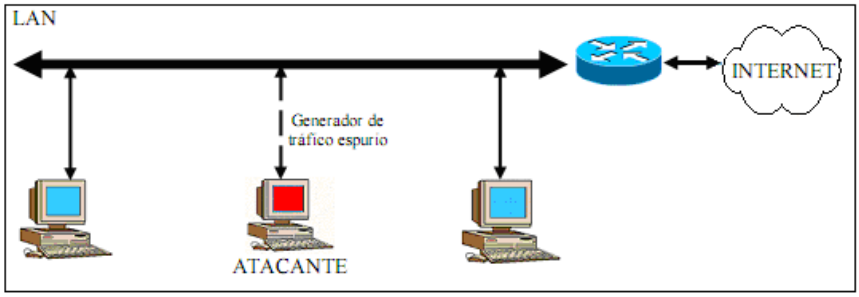


Figura 1.29: Ataque IP Flooding [11]

- *TCP:* en este ataque se genera peticiones de conexión con el objetivo de saturar los recursos de red de la máquina atacada. Este protocolo (orientado a conexión) consume recursos de memoria y CPU por cada conexión, por lo tanto con el ataque se saturan los recursos de red disponibles de los ordenadores que reciben las peticiones de conexión disminuyendo la calidad del servicio.

Broadcast: este ataque utiliza la dirección de identificación de la red IP (broadcast address) como dirección de destino del paquete IP. Razón por la cual el router envía el paquete a todos los ordenadores pertenecientes a la red, lo que ocasiona consumo de ancho de banda y baja el nivel de rendimiento del servicio.

Otra manera de realizar el ataque es enviando peticiones PING a varios ordenadores falsificando la dirección IP de origen y sustituyéndola por la dirección de broadcast de la red a la cual se le va a atacar. De modo que todas

las respuestas individuales son enviadas a los ordenadores pertenecientes a la red.

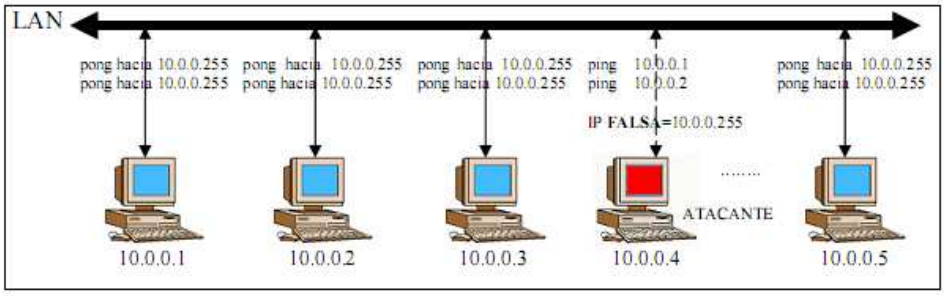


Figura 1.30: Ataque Broadcast [11]

Smurf: este ataque falsifica las direcciones de origen y destino de una petición ICMP de ECHO (PING). En la dirección de origen se coloca la IP de la máquina que va a ser atacada y en la dirección destino se coloca la dirección de broadcast de la red local o red que se utilizará para realizar el ataque.

Como consecuencia se obtiene que todas las máquinas de la red respondan al mismo tiempo a una misma máquina causando la saturación de la máquina atacada además del consumo del ancho de banda disponible.

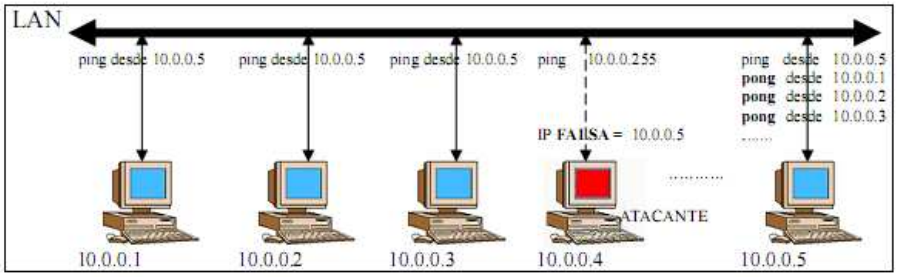


Figura 1.31: Ataque Smurf [11]

Ping de la muerte: este ataque utiliza las definiciones de la longitud máxima del paquete IP (65 535 Bytes) y la fragmentación de los datagramas, que se realiza cuando el paquete es superior a esta longitud máxima y será reconstruido en el destino.

En este tipo de ataque se envía a la máquina que se desea atacar numerosos paquetes ICMP (ping) de longitud mayor a los 65535 bytes, por lo cual debe ser

fragmentado para su envío, cuando la máquina de destino, la atacada, vuelve a reensamblar el paquete puede ocurrir una saturación del buffer (overflow) que causa un fallo del sistema.

1.3.2 CORTAFUEGOS (FIREWALLS)

1.3.2.1 Introducción

Un firewall o cortafuego es un sistema que se encarga del cumplimiento de una política de control de acceso entre dos redes. Permite aplicar filtros para el tráfico de entrada como para el de salida. Un firewall oculta la configuración de la red interna.

Este sistema se utiliza para la protección de una máquina o una subred (perímetro de seguridad) de servicios y protocolos que provienen de una red externa no confiable (zona de riesgo) y suponen una amenaza a la seguridad.

Un firewall no constituye toda la seguridad de la red, se necesita sistemas complementarios a este para implementar la seguridad de manera más eficiente. Debido a que este dispositivo sea router o máquina constituye un punto centralizado si su funcionamiento se ve afectado toda la red quedaría vulnerable. Además se debe tomar en cuenta que para un correcto funcionamiento de los equipos hay que mantener los sistemas actualizados y configurados adecuadamente y con el monitoreo respectivo.

Finalmente un firewall protege a la red únicamente de los ataques llevados acabo a través de él; los sistemas complementarios se utilizarían para los ataques internos o para detectar tipos de ataques más sofisticados (DOS).

1.3.2.2 Componentes de Firewall

Un firewall está compuesto básicamente de los siguientes elementos: filtrado de paquetes, el proxy de aplicación y la monitorización y detección de actividades anómalas.

1.3.2.3 Filtrado de Paquetes

Se utiliza para la implementación de las políticas de seguridad reflejadas en las reglas de acceso a la red.

Su funcionamiento radica en el análisis de la cabecera de cada paquete para bloquearlo o permitir su acceso. Se analizan campos como por ejemplo el de protocolo utilizado (tcp, udp, icmp), direcciones fuente y destino, puerto origen y destino (tcp y udp), tipo de mensaje (icmp). Este tipo de análisis involucra que un firewall tiene la capacidad de trabajar a nivel red (discriminación por direcciones origen y destino) y a nivel de transporte (discriminación por puertos).

Además se puede realizar el filtrado basado en reglas que involucran el interfaz de entrada y salida de la trama en el router. Para la toma de decisiones basadas en reglas se utiliza una tabla de condiciones y acciones que se consulta en forma ordenada hasta encontrar una regla que permita tomar una decisión ya sea para el bloqueo o el reenvío de la trama.

1.3.2.4 Proxy Servers

El firewall provee un servicio de Proxy que es utilizado para reenviar o bloquear conexiones a servicios como por ejemplo finger, telnet, ftp o http.

Un Proxy oculta la estructura de la red, es el equipo disponible hacia el exterior (por ejemplo: NAT para la navegación en Internet). Facilita la autenticación, el monitoreo y el análisis de tráfico antes de llegar al destino.

Proxy Server a nivel de aplicación

Un Proxy de Aplicación únicamente permitirá la utilización de servicios habilitados en éste, con las respectivas restricciones de ser el caso. El Proxy controla el establecimiento de conexiones, autentica al usuario, a la dirección de origen/destino y al protocolo.

Proxy Server a nivel de circuitos

Este tipo de Proxy una vez autenticado el usuario (la conexión) establece un circuito virtual entre un cliente y un servidor sin interpretar la naturaleza de la

aplicación. Además es necesario que en el cliente corra una aplicación especial, el software más conocido para este fin es Socks.

1.3.2.5 Monitorización de la Actividad

Método utilizado para obtener información acerca de los intentos de ataque a nuestra red (origen, hora, duración, tipos de acceso, etc), además de la existencia de tramas sospechosas.

Adicionalmente se debe controlar la información de la conexión: origen y destino, nombre de usuario, intentos de uso de protocolos denegados, intentos de falsificación de dirección de un equipo interno en paquetes cuyo origen es la red externa y tramas recibidas desde routers desconocidos.

Estos registros deben ser examinados con frecuencia y tomar las medidas necesarias si se detectan actividades sospechosas.

1.3.2.6 Zona Desmilitarizada (DMZ)

La De-Militarized Zone (DMZ) consiste en la creación de una subred (DMZ) que tiene acceso al exterior (Internet) para de esta manera aislar el resto de la red y minimizar el riesgo de ataques a la información protegida de la organización o a su vez reducir los efectos de estos ataques.

1.3.3 REDES VIRTUALES PRIVADAS VPN

Virtual Private Network (VPN) es una implementación o sistema que simula una red privada sobre una red pública (Internet). Es una red de comunicación segura entre dos puntos de manera que la información sea conocida únicamente por el emisor y el receptor.

Esta comunicación se realiza estableciendo túneles virtuales entre dos puntos, para los cuales se negocian esquemas de encriptación y autentificación asegurando así la confidencialidad e integridad de los datos transmitidos sobre la red pública.

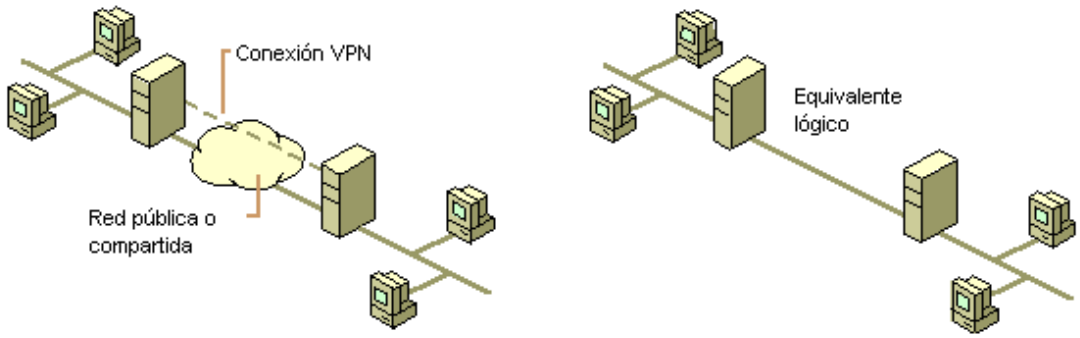


Figura 1.32: Redes Virtuales Privadas [12]

Las redes virtuales privadas se pueden implementar formando los siguientes tipos:

1. Redes separadas y seguras en Intranets (VPN Interna).
2. Interconexión por Internet:
    a) Conexión permanente entre oficinas (VPN sitio-a-sitio).
    b) Conexiones aleatorias de los agentes móviles con su oficina (VPN de acceso remoto).
3. Conexiones entre equipos mediante Wireless (VPN Interna).
4. Acceso remoto Dial-Up a Intranets o Extranets.

1.3.3.1 Implementación de las Redes Privadas Virtuales

El proceso de encriptación y desencriptación de la información se debe realizar en las capas equivalentes.

Para la seguridad las VPNs deben cumplir requerimiento como:

- Privacidad mediante:

    Encripción: se encripta únicamente los datos. Se utiliza protocolos como: DES, 3DES, RSA, IDEA.

    Encapsulamiento (túnel): se encripta el header y los datos, además se añade un nuevo header. Se utiliza protocolos como IPSec y L2TP.

- Integridad: se utiliza algoritmos de hashing como: SHA, MD4, MD5.

- Autenticación: se utiliza esquemas como user/password, token cards, smartcards, certificados X.509.

- Autorización: se utiliza perfiles de usuario con niveles de autorización y acceso.

- Accounting: se mantiene un registro de actividad del usuario.

1.3.3.2 Alternativa de Encripción

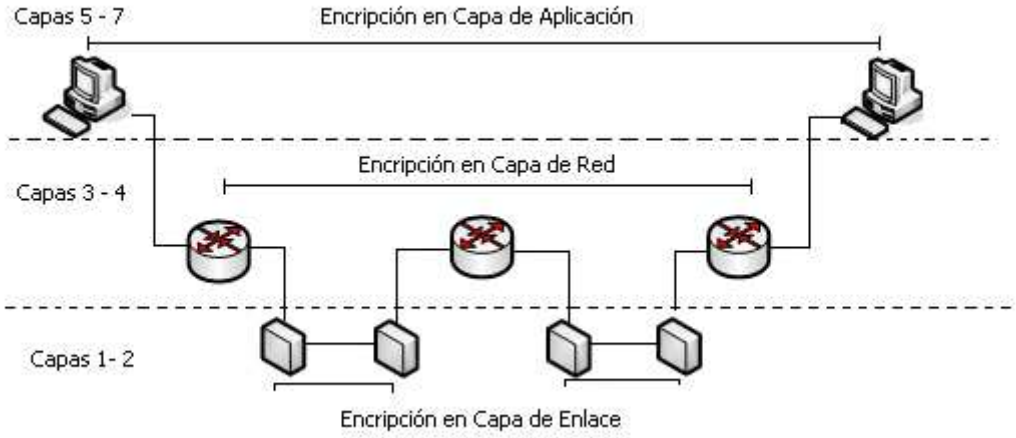


Figura 1.33: Encripción VPNs [10]

1.3.3.3 Tecnologías para Formación VPNs

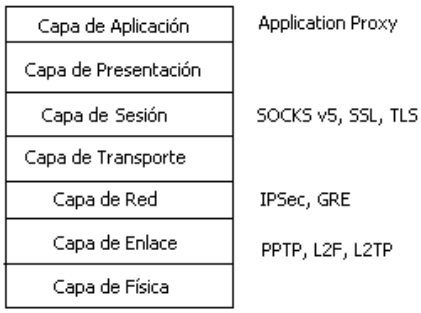


Figura 1.34: Tecnologías VPNs [10]

A continuación se muestra algunos protocolos utilizados para la formación de VPN, para mayores detalles ver Anexo B.

SSL Secure Socket Layer

TLS Transport Layer Security

IPSec IP security extensions
GRE Generic Routing Encapsulation
PPTP Point to Point Tunneling Protocol
L2F Layer 2 Forwarding
L2TP Layer 2 Tunneling Protocol

1.3.4 SISTEMAS DE DETECCIÓN DE INTRUSOS[10]

Un sistema de detección de intrusos es aquel sistema que permite detectar acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso. Puede estar basado en hardware o software que inspeccione todo tráfico entrante o saliente en busca de un comportamiento malicioso que comprometa la red o el sistema para proveer alertas en tiempo real.

1.3.4.1 Clasificación de los Sistemas de Detección de Intrusos

- En función del origen de los datos

  – *IDSs basados en máquina*.- Protege un sistema, puede trabajar en background buscando patrones que puedan denotar intrusos.
  – *IDSs basados en red (NIDS).*- Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque, puede situarse en cualquier elemento de la red que analice todo el tráfico. Opera sobre un dominio de colisión.

- En función de la técnica de análisis utilizada

  – *Detección de anomalías*.- Estos IDS consideran un comportamiento anormal como una intrusión, para ello estos sistemas deben ser capaces de establecer un perfil de comportamiento habitual.
  – *Detección de usos indebidos.*- A diferencia de IDS de detección de anomalías estos sistemas buscan establecer patrones de ataques y algunas variaciones de estos para poder detectarlos. Utiliza firmas y solo detecta ataques conocidos.

- Otras Clasificaciones

  Existen otras clasificaciones entre los que encontramos a los IDS que trabajan periódicamente llamados pasivos y aquellos que trabajan en tiempo real llamados activos.

1.3.4.2 Características de un IDS

- Un IDS debe ejecutarse sin interacción humana de forma transparente, independiente de que al detectar un problema se informe a un operador o se lance una respuesta automática.
- No debe introducir sobrecarga al sistema, o generar una cantidad elevada de falsos positivos.
- Debe ser adaptable a cambios en el entorno de trabajo.
- Deben presentar cierta tolerancia a fallos o tener la capacidad de respuesta ante situaciones inesperadas. Por ejemplo un reinicio inesperado de varias máquina.

Al ser detectado un intruso se debe generar una respuesta automática o manual, con acciones inmediatas o a corto plazo. Es recomendable contar con un equipo de respuesta ante incidentes de seguridad, este podría evaluar si los supuestos ataques son reales o no.

1.3.5 IPSEC [13]

IPSec proporciona autenticación, integridad, y confidencialidad empleando: protocolos de seguridad (AH Authentication Header y ESP Encapsulating Security Payload), algoritmos de autenticación, manejo de llaves y asociaciones de seguridad. Puede proteger el datagrama IP completo a lo que se denomina modo túnel o proteger protocolos de capas superiores a lo que se denomina modo transporte.

En el modelo túnel el datagrama IP es encapsulado completamente dentro de un nuevo datagrama, en el modo transporte se inserta la cabecera IPSec entre la cabecera de la capa IP y la cabecera del protocolo de capa superior.

Cabecera de autenticación IP (AH, Authentication Header).- provee una conexión con integridad y autenticación del origen de los paquetes de datos.

Encapsulante de Seguridad (ESP, Encapsulating Security Payload).- Proporcionar confidencialidad (encriptación), y limitación del tráfico circulante, además adicionalmente podemos obtener autenticación y protección de integridad.

1.3.5.1 Authentication Header (AH)

Opcionalmente puede proteger contra ataques de repetición utilizando ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los que pueden ser alterados en el tránsito.

0 - 7 bit	**8 - 15 bit**	**16 - 23 bit**	**24 - 31 bit**
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

Figura 1.35: Authentication Header[13]

Significado de los campos:

Next header	Identifica el protocolo de los datos transferidos
Payload length	Tamaño del paquete AH
RESERVED	Reservado para uso futuro (hasta entonces todo ceros)
Security parameters index (SPI)	Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
Sequence number	Un número siempre creciente, utilizado para evitar ataques de repetición
Authentication data	Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno

Tabla 1.12: Campos Authentication Header[13]

1.3.5.2 Encapsulating Security Payload (ESP)

ESP no protege la cabecera del paquete IP, excepto en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno.

Un diagrama de paquete ESP:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
	Padding (0-255 bytes)		
		Pad Length	Next Header
Authentication Data (variable)			

Figura 1.36: Encapsulating Security Payload (ESP)[13]

Significado de los campos

Security parameters index (SPI)	Identifica los parámetros de seguridad en combinación con la dirección IP
Sequence number	Un número siempre creciente, utilizado para evitar ataques de repetición
Payload data	Los datos a transferir
Padding	Usado por algunos algoritmos criptográficos para rellenar por completo los bloques
Pad length	Tamaño del relleno en bytes
Next header	Identifica el protocolo de los datos transferidos
Authentication data	Contiene los datos utilizados para autenticar el paquete

Tabla 1.13: Campos Encapsulating Security Payload (ESP)[13]

1.3.5.3 Asociaciones de Seguridad

Las Asociaciones de Seguridad (SAs) proveen un método seguro para que dos dispositivos que soportan IPSec que requieran establecer una sesión, puedan negociar los parámetros de seguridad. Las SAs trabajan de modo unidireccional, para tráfico bidireccional se específica dos SAs. La SA IPSec especifica los siguientes parámetros:

- Modo de autenticación AH (Algoritmo y Claves)
- Algoritmo de cifrado ESP
- Forma de intercambiar claves
- Cada que tiempo se cambian las claves
- Vida útil de la SA
- Dirección IP origen

1.3.5.4 Gestión de Claves

Para el intercambio de claves comúnmente se usa la codificación manual, apropiada para un número pequeño de sitios, o un protocolo definido.

1.3.5.4.1 Intercambio Manual de Claves

En este método los extremos del túnel IPSec deben configurarse manualmente con las claves correspondientes. Pero la codificación manual tiene desventajas entre ellas tenemos:

- La actualización o cambio de claves se realizan manualmente, por lo que no se lo realiza con frecuencia proporcionando al atacante más tiempo para descifrarlas y descodificar datos.

- Hay una probabilidad de error en la configuración, dado que la misma clave debe configurarse en los dos extremos distintos del túnel IPSec.

1.3.5.4.2 ISAKMP (Internet Security Association and Key Management)

Este protocolo define procedimientos para la creación y manejo de asociaciones de seguridad, técnicas de generación de llaves y mitigación ante

ataques. Para ello establece dos estados, el primero establece la asociación de seguridad entre dos entidades y el segundo establece el uso de AH y ESP.

1.3.5.4.3 OAKLEY

Establece la forma en que dos entidades realizan el intercambio de las llaves. Informa el ID de las entidades, el nombre de la llave, un componente secreto de la llave, y el tipo de algoritmo de encripción, autenticación e integridad. Es compatible con ISAKMP.

1.3.5.4.4 IKE (Internet Key Exchange protocol)

IKE es un protocolo para establecimiento de comunicaciones seguras, para ello proporciona la autenticación de los participantes y el intercambio de claves simétricas. Funciona en dos fases, la primera crea un ISAKMP SA (basándose en claves compartidas con anterioridad, claves RSA y certificados X.509), en la segunda fase usa el ISAKMP para negociar y establecer las SAs de IPSec.

1.3.5.5 Reglas IPSec

Una directiva de IPSec es invocada por reglas, estas proporcionan la capacidad para iniciar y controlar una comunicación segura en función del origen, el destino y el tipo de tráfico IP. Una directiva IPSec puede contener una o varias reglas y una o más pueden ser activadas simultáneamente.

1.3.5.5.1 Componentes de una Regla

Lista de filtros IP.- Define el tráfico que protegerá esta regla.

Acciones de filtrado.- Indica las funciones que se seguirán cuando el tráfico cumple los criterios del filtro. Las acciones pueden ser bloquear, permitir el tráfico o negociar la seguridad de la conexión.

Métodos de seguridad.- Específica la forma en que los equipos protegen el intercambio de datos. Puede utilizar los métodos definidos medio y alto, o definir métodos de seguridad personalizados.

Métodos de autenticación.- Específica el método utilizado por un usuario para comprobar que quién se encuentra al otro lado de la comunicación es quién dice ser. Cada regla puede configurarse con uno o varios métodos de autenticación.

Tipos de conexión.- Permite al administrador elegir si la regla se aplica a todas las conexiones, a la de área local, o a las conexiones de acceso remoto.

1.4 REDES DE NUEVA GENERACIÓN[14] [17] [18]

1.4.1 INTRODUCCIÓN

La evolución de las redes clásicas se fue concretando debido a que éstas redes estaban limitadas a características tales como: que el ancho de banda era insuficiente para las aplicaciones que día a día se iban incrementando, los servicios dependían de la infraestructura de red lo que dificultaba el mejoramiento de los mismos.

El Internet originó que los operadores de redes incursionen en el transporte de información tal como voz y datos no solo a nivel local. Con el crecimiento del tráfico de Internet comenzaron a detectarse problemas en los diseños existentes, ya que los usuarios tenían acceso a más servicios por la tanto necesitaban redes cuya infraestructura soporte toda aplicación a la que tenían disponibilidad. Razón por la cual apareció una solución basada en las redes IP, conocida como All-IP (All Internet Protocol).

Sin embargo, las primeras soluciones IP aún estaban basadas en equipos con limitaciones en cuanto a capacidad, calidad de servicio y la seguridad aun estaba pobremente definida.

En este momento nace la idea de desarrollar el concepto NGN como la solución All-IP, en la cual se basa la convergencia de las redes que poseen interfaces de alta velocidad, con seguridad y calidad de servicio garantizadas, facilitando la interacción con los servicios tanto actuales como futuros.

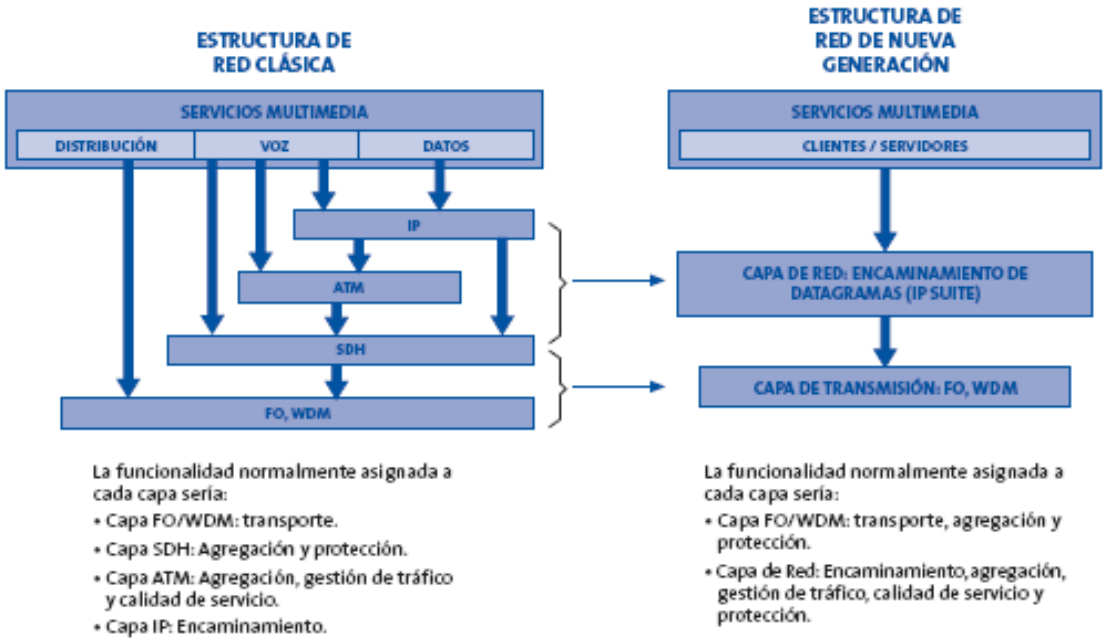


Figura 1.37: Evolución de la Red Clásica a la NGN – Simplificiación de la torre de Protocolos[14]

Por el crecimiento tecnológico de los medios de transmisión, el uso del Internet y la necesidad de compartir infraestructuras entre distintas unidades de negocio nace la propuesta de una nueva infraestructura de red.

Una red de nueva generación permite ofrecer numerosas aplicaciones (voz, datos, vídeo) integrando las diversas tecnologías que existen actualmente en el mercado, sean fijas o móviles, satisfaciendo las necesidades de los usuarios de forma transparente.

1.4.2 CARACTERÍSTICAS

- Una NGN debe operar con flexibilidad, ofreciendo una amplia gama de servicios ya sea requerida la transmisión en tiempo real o no, con una calidad de servicio de acuerdo a las necesidades de la aplicación.

- La arquitectura de red la conforman interfaces abiertas que permitan la operación de nuevos servicios.

- Los servicios son independientes de la red por la que se transmiten, lo que proporciona escalabilidad a la infraestructura de red y permite la interoperabilidad con las redes tradicionales.

- Una red de nueva Generación debe permitir movilidad del usuario.

1.4.3 ARQUITECTURA

Una red NGN consta de cuatro niveles que dan flexibilidad y escalabilidad a la red, cada nivel se conecta mediante interfaces abiertas que permiten la interconexión e integración de nuevos servicios. Estos cuatro niveles son los siguientes:

- **Servicios:** Esta interfaz es la encargada de la conexión “lógica” con los usuarios.
- **Control:** Interfaz intermedia que permite la comunicación entre los niveles de servicio y de transporte.
- **Transporte:** ofrece la conectividad y de calidad de servicio requeridos por los servicios.
- **Acceso:** Cualquier acceso de banda ancha para hacer llegar al usuario las aplicaciones solicitadas. La tecnología usada puede ser en cable (fibra o cobre) o inalámbrica.

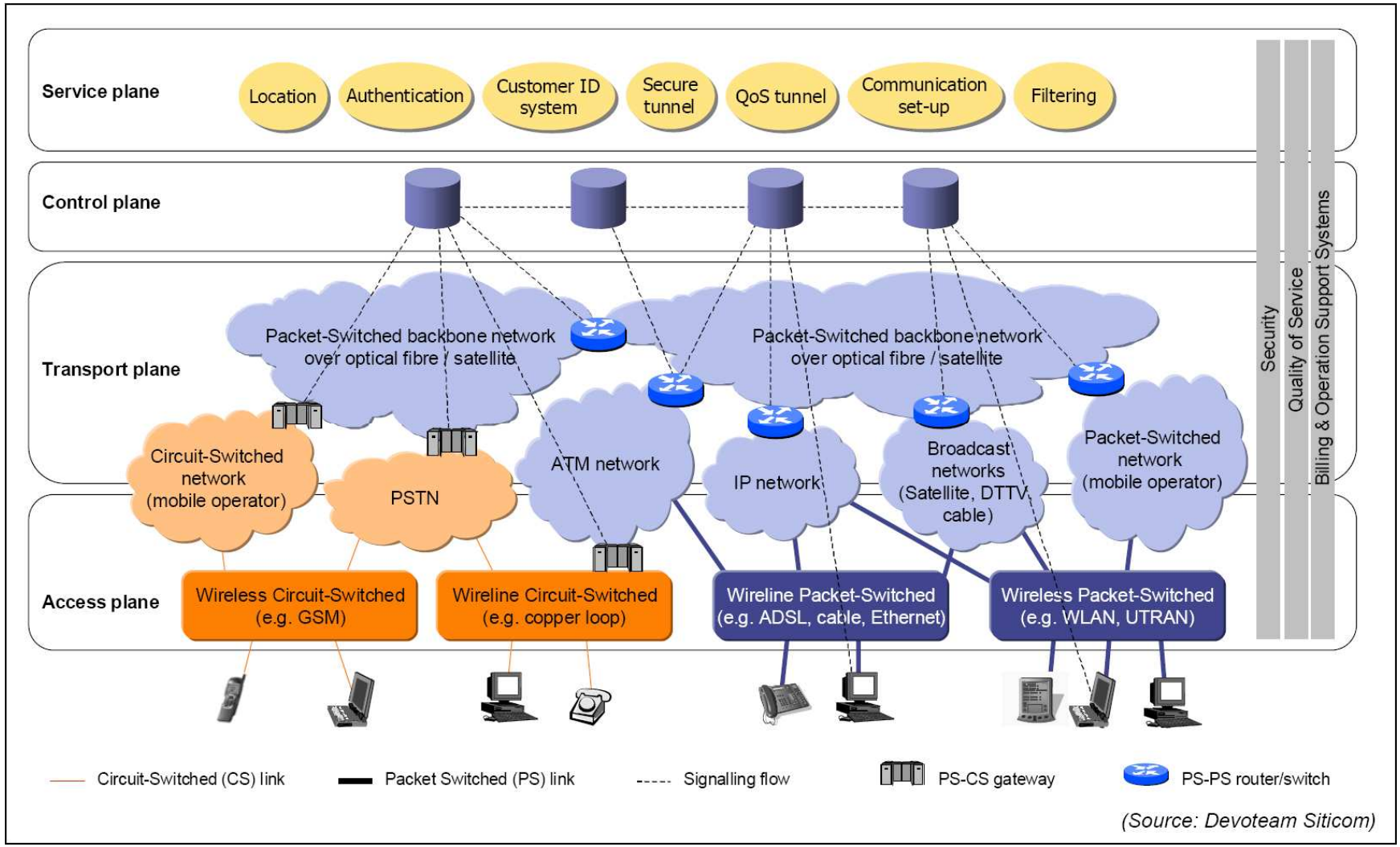


Figura 1.38: Arquitectura habitual de una Red de Nueva Generación[15]

1.5 REDES IMS (IP Multimedia Subsystem)[14] [17] [18]

1.5.1 INTRODUCCIÓN

Todo proveedor de servicios busca la convergencia de éstos para ser cada vez más ágil en el manejo de la información. Se puede enumerar tres pilares en los cuales se fundamenta dicha convergencia: trasformación de los servicios, transformación de la red y transformación de las expectativas del usuario.

Figura 1.39: Transformaciones[16]

Transformación de la red: Tanto la capa de red y la capa de control se deben consolidar en una arquitectura extremo a extremo que soporte servicios multimedia móviles y fijos, los mismos que deben estar basados en SIP (Session Initiation Protocol).

Transformación del Servicio: Los servicios se han constituido independientes; lo que se necesita es unificar las capacidades comunes de estos y lograr integrarlos. Como por ejemplo se comparten bases de datos, tarificación común para distintos servicios, etc.

Transformación del negocio o de las expectativas del usuario: Los usuarios finales (jóvenes, usuarios residenciales, corporaciones, etc) demandan un entorno multi-aplicación que permitan la comunicación en tiempo real utilizando combinaciones de voz, imagen, mensajería, vídeo, etc. Adicionalmente se tiene

la necesidad de continuidad, tener acceso desde cualquier lugar. Y la prestación de estos servicios debe ser a un costo reducido y de interfaz amigable para el usuario.

IMS es una arquitectura para ofrecer servicios multimedia sobre infraestructura IP. Con IMS el usuario es accesible mediante una única dirección, similar a la del correo electrónico, independientemente del dispositivo (teléfono móvil o fijo, PC, PDA (Personal Digital Assistant), televisor, etc.) y tipo de red de acceso ya que soporta múltiples tipos de tecnologías de acceso, como GSM (Global System Mobil Communication), GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunictions System), DSL (Digital Subscriber Line), Wi-fi (Wireless Fidelity), Wi-MAX (*Worldwide Interoperability for Microwave Access*), Bluetooth, etc. Lo que permitirá pasar de un sistema a otro sin interrumpir la conexión y utilizar varios medios a la vez.

1.5.2 ORGANISMOS DE ESTANDARIZACIÓN

Esta arquitectura de red nace sustentada por el 3GPP/3GPP2 (*Third Generation Partnership Project/ Third Generation Partnership Project2)*, con el apoyo de importantes organismos de estandarización (ITU / ANSI / ETSI /OMA / IETF).

Inicialmente desarrollado para aplicaciones en redes móviles 3G, fue definida en la Release 5 y 6 del 3GGP (Third Generation Partnership Project), conjuntamente con el IETF (Internet Engineering Task Force) y posteriormente nace el interés de las redes fijas en esta arquitectura. Otro organismo de estandarización que está contribuyendo a la definición es el ETSI (*European Telecommunication Standards Institute)* dentro del proyecto NGN, apoyando la convergencia de redes y servicios tanto en escenarios fijos como móviles.

Entre las ramas de estandarización de la ETSI tenemos a TISPAN (*Telecommunications and Internet converged Services and Protocols for Advanced Networkíng*) encargado de la estandarización de redes combinadas, para lo cual considera aspectos de: servicios, arquitectura, protocolo, QoS,

estudios relacionados con la seguridad, movilidad, tecnologías existentes y emergentes. Los estándares IMS/TISPAN incluyen los estándar definidos por 3GPP y añaden el acceso desde el entorno fijo.

TISPAN trabaja en la convergencia de redes e Internet con el objetivo de que usuarios de redes basadas en IP puedan comunicarse con los usuarios de las redes tradicionales como PSTN, ISDN, GSM, etc. Se enfoca en que servicios IP y NGN proporcionen el mismo nivel de calidad y conectividad que el que se recibe hoy.

TISPAN está estructurado como un comité técnico, constituido por Grupos de Trabajo (Working Groups) y Equipos de Proyectos (Project Teams) tal como indica en la figura. Los grupos de trabajo son: WG1 (Servicios), WG2 (Arquitectura), WG3 (Protocolo), WG4 (Numeración, Direccionamiento y Encaminamiento), WG5 (Calidad de Servicio), WG6 (Testing), WG7 (Seguridad) y WG8 (Gestión de red).

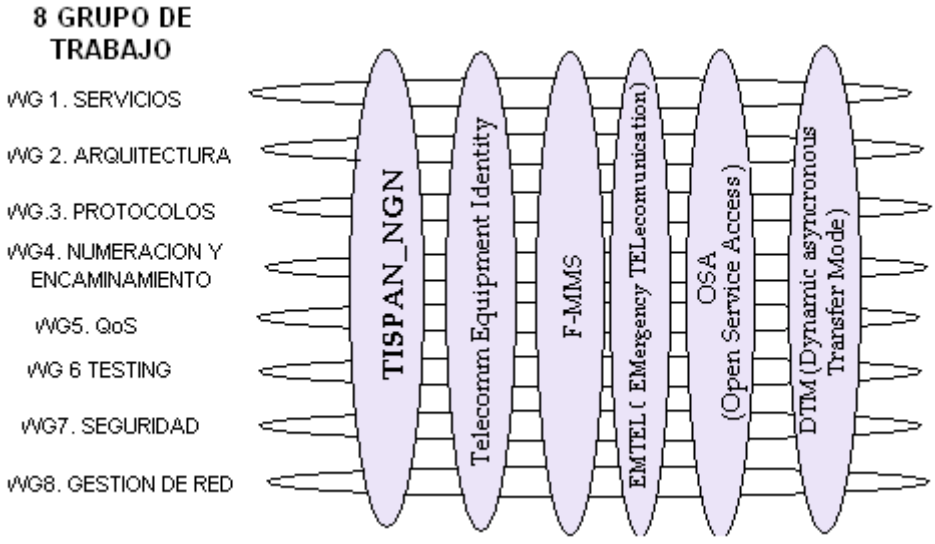


Figura 1.40: Estructura TISPAN[17]

Otro cuerpo de estandarización es OMA (Open Mobile Alliance) que como base para la estandarización se tiene al protocolo SIP para señalización al igual que lo hizo en su momento 3GPP Release 6 de IMS. Además considera el acceso IP desde diferentes dominios (residencial, móvil y corporativo). Igualmente se

tiene en cuenta la interconexión entre los sistemas tradicionales de telefonía (Subsistema PTSN/ISDN). Los proveedores de servicios, a través de la arquitectura NGN, ofrecen diferentes servicios de comunicaciones con configuraciones peer-to-peer y cliente-servidor.

1.5.3 CARACTERÍSTICAS

Entre las características de los servicios IP multimedia que IMS proporciona se tienen las siguientes:

- La comunicación establecida es orientada a sesión de un usuario a otro(s) usuario(s), o de un usuario a un servicio.
- La transmisión puede ser en tiempo real o diferido.
- Las sesiones IP multimedia se establecen con un nivel adecuado de Calidad de Servicio para vídeo, audio y sonido, texto, imagen, datos de aplicación, etc.
- Los usuarios, servicios y nodos se identifican mediante URIs (Universal Resource Identifier), es decir, maneja nombres como el correo electrónico.
- IMS admite una gran gama de servicios integrados en un subsistema, conservando las características propias de estos.

1. IMS soporta la itinerancia (roaming) de tipo nativo, es decir que puede obtener y dar servicio a los abonados de otros operadores con la misma tecnología.
2. IMS permite la interconexión con redes y servicios de forma que los abonados IMS podrían comunicarse con usuarios no IMS.
3. Integra Seguridad mediante la aplicación lógica llamada ISIM (IMS SIM) que ejecuta funciones de autenticación de abonado durante su registro en IMS.

1.5.3.1 El Transporte de Red

El direccionamiento de IMS se fundamenta en IPv6, como previsión de su futuro uso en Internet, ya que Ipv6 tiene ventajas como: la QoS y la seguridad integradas, así como la autoconfiguración y un mayor espacio de

direccionamiento. Sin embargo, IMS da compatibilidad con la versión anterior simplemente parte de una situación más avanzada técnicamente, por lo que el terminal IMS debe soportar Ipv6 e IPv4.

Además de SIP e IPv6 se emplean otros protocolos para proveer servicios IP multimedia, como son:

1. Los protocolos RTP (Real Time Protocol) y RTCP (Real Time Control Protocol), que se utilizan para el transporte de flujos IP multimedia del plano de usuario.
2. El protocolo Diameter, para aquellas acciones relacionadas con la autorización, autenticación y tarificación.
3. Los protocolos RSVP (Resource Reservation Protocol) y DiffServ, para proporcionar QoS extremo a extremo.
4. El protocolo Megaco, para el control remoto de los Media Gateways.

IMS se centraliza en las aplicaciones buscando la integración de éstas en la red y los sistemas de gestión y negocio.

DIAMETER

Desarrollado por la IETF. Es un protocolo de red utilizado para la autenticación de los usuarios que se conectan remotamente a la Internet.

Provee servicios de autorización y auditoria para aplicaciones tales como acceso de red o movilidad IP. El concepto básico del protocolo DIAMETER es de proporcionar servicios de autenticación, autorización y auditoria, (AAA) a nuevas tecnologías de acceso.

Diameter proporciona los siguientes servicios:

- Administración de sesiones y conexiones.

- Autenticación de usuario y capacidades de negociación.
- Entrega confiable del valor de atributo pares AVPs[5] (Attribute Value Pair).
- Agente de soporte para proxy, redireccionamiento, y relay de servidores.
- Servicios básicos de contabilidad.

El organismo de normalización 3GPP ha adoptado a Diameter como el principal protocolo de señalización para la AAA y la gestión de la movilidad en el Subsistema Multimedia IP (IMS).

Adicionalmente posee dos elementos fundamentales que son:

- Soft Switch (SS), con importante función de control
- Protocolo SIP, protocolo utilizado para la comunicación entre los principales elementos de la red.

1.5.4 ARQUITECTURA IMS

La arquitectura IMS se propone ciertas ventajas frente a las arquitecturas existentes como las siguientes:

Movilidad y roaming.- IMS provee a los usuarios específicos acceso a servicios independiente de la localización y servicios del operador.

Arquitectua Modular.- Permite integrar diferentes componentes de diferentes proveedores dentro del mismo sistema.

AAA (Autenticación, Autorización y Cuentas) y discriminación de usuarios.- permite la administración de perfiles, para administrar servicios por usuario, por grupos de usuarios y comunidades.

---

[5] AVP: El protocolo Diameter consta de una cabecera seguida de uno o más pares de valor de atributo (AVPs). Un AVP incluye una cabecera y se utiliza para encapsular el protocolo de datos específicos (por ejemplo, información de enrutamiento), así como la autenticación, autorización, o información contable.

Los servidores proveen flexibilidad para construir nuevos servicios sobre una infraestructura de señalización común.

Por otro lado IMS presenta las limitaciones como:

Baja Interacción entre plataformas de servicios. Servicios creados en diferentes plataformas no combinan dos o más capacidades de la red. Un servicio que utilice simultáneamente la información de localización y disponibilidad del usuario en una plataforma y no permite simultáneamente una conversación o intercambio de archivos.

Baja eficiencia en la administración de bases de datos. A menudo se crea cada servicio con su propia base de datos disminuyendo la eficiencia.

1.5.5 ELEMENTOS IMS (IP MULTIMEDIA SUBSYSTEM)

IMS se basa en *sesiones*. La sesión se efectúa entre el terminal y una aplicación o un cliente directamente. Además esta arquitectura se define en tres capas: la capa de acceso, la capa de control y la capa de aplicación como se muestra en la figura 1.41

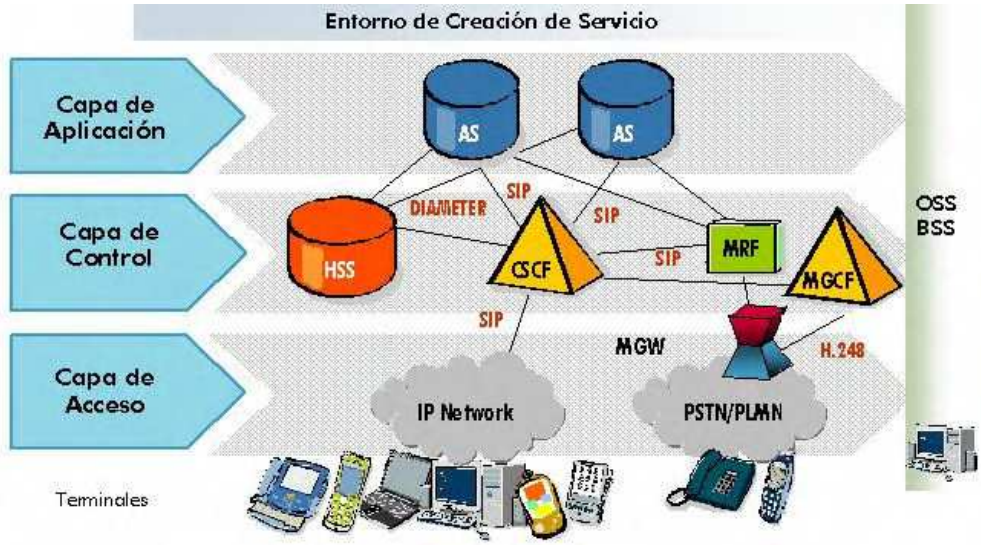


Figura 1.41: Representación simplificada de la Arquitectura IMS [16]

1.5.5.1 Definición General de los Componentes

La arquitectura IMS se divide básicamente en tres capas:
La capa de Aplicación: formada por Servidores de Aplicaciones. Estas aplicaciones pueden ser utilizadas por otras aplicaciones o directamente por los terminales.

La capa de Control: se encarga de la señalización para el establecimiento de la sesión entre las entidades correspondientes, los protocolos entre los elementos y las funciones de cada uno de ellos.
El Soft Switch es el elemento principal de esta capa.

La capa de Acceso en esta capa se establece la conexión de voz o datos con la calidad de servicio que se define en la capa de Control.

El Soft Switch (SS) posee las funciones de servidor IMS. Es el encargado del control de la llamada/sesión establecida por el IMS en la red de origen del suscriptor (Home Network), administra las sesiones IP, provee los servicios, y aloja recursos de “media”.

Las funciones de un servidor IMS pueden ser implementadas en un único Soft Switch, ya que los elementos que lo conforman representan entidades lógicas; sin embargo pueden ser implementadas en SS diferentes.

Red IMS

A continuación (Figura 1.42) se presenta en forma más detallada a la arquitectura IMS, sus elementos e interfaces:

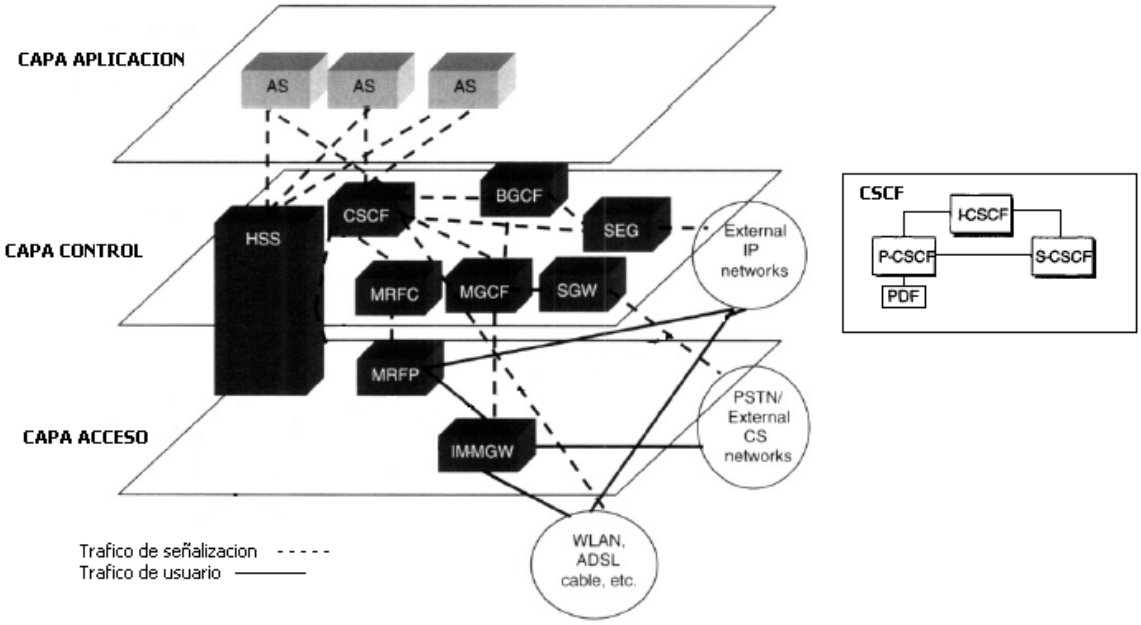


Figura 1.42: Componentes de la Red IMS.[18]

1.5.5.1.1 Call Session Control Function (CSCF)

El CSCF (Call/Session Control Function) es un servidor SIP, el cual procesa la señalización SIP en IMS. El CSCF se puede clasificar en tres tipos dependiendo de la funcionalidad que provea:

Serving-CSCF (S-CSCF): Este elemento administra las sesiones SIP y coordina con otros elementos de la red el control de las llamadas/sesiones. Adicionalmente es responsable por las siguientes funciones:

- Registro SIP: procesa solicitudes de registro SIP (SIP REG) de datos y condición de suscriptores en el transcurso de la sesión de registro.
- Control de la Sesión: efectúa el establecimiento de la llamada/sesión, modificación y terminación.
- Control de Servicio: interactúa con los Servidores de Aplicación (Application Server) para proporcionar soporte de servicios y aplicaciones.
- Monitoreo de la llamada y generación de registros de tarifación
- Provee seguridad para la sesión.

Proxy-CSCF (P-CSCF): Es el elemento que interactúa directamente con el Terminal de usuario permitiendo el acceso a la red IMS a partir de una red orientada a paquetes. El elemento P-CSCF:

- Provee el ruteamiento SIP entre el equipo de usuario y la red IMS.
- Ejecuta la política de control definida para la red.
- Autoriza el control de recursos y calidad (QoS) de las llamadas/sesiones según los parámetros negociados con la red acceso.

Interrogating-CSCF (I-CSCF): es el enlace entre la red de un operador y las conexiones destinadas a un suscriptor de la red de este operador, o para un suscriptor que pertenece a otra red. Pueden existir múltiples I-CSCF en una red. Las funciones del I-CSCF son:

- Mediante un registro SIP designa un S-CSCF para un usuario.
- Rutea un requerimiento SIP recibido de otra red en dirección al S-CSCF.
- Obtener del HSS (Home Subscriber Subsystem) la dirección del S-CSCF.
- Encaminar el requerimiento SIP o respuesta al S-CSCF determinado en el HSS.
- Encamina el requerimiento SIP o respuesta a la designación de la mejor opción de MGW.
- Envía requerimientos/respuestas SIP al I-CSCF en otra red para designación óptima de un Media Gateway (MGW), para terminación de una llamada en la red pública conmutada (PSTN).

El I-CSCF sirve para ocultar la configuración, capacidad y topología de su propia red, del exterior; pudiendo enviar requerimientos/respuestas SIP para otro I-CSCF permitiendo la independencia de configuración entre redes.

1.5.5.1.2 Breakout Gateway Control Function (BGCF)

El BGCF selecciona la red de acceso a la red pública conmutada. Si la red de acceso es la misma red en donde el BGCF está localizado, éste selecciona un

MGCF que se encargará del interfuncionamiento con la red PSTN. Si el punto de acceso está en otra red, enviará la señalización de esta sesión a un BGCF o MGCF en la otra red, optimizando el recorrido de la llamada/sesión.

1.5.5.1.3 Media Gateway Control Function (MGCF)

El MGCF es el responsable del interfuncionamiento de señalización entre los elementos de la red IMS y la PSTN. Adicionalmente controla un conjunto de MGWs a través de la señalización H.248.

1.5.5.1.4 Multimedia Resource Function Controller (MRFC)

El MFRC controla los recursos de media del elemento MultiMedia Resource Function Processor (MRFP), tales como conferencia, anuncios al usuario.
El MRFC interpreta la señalización SIP recibida del S-CSCF y usa instrucciones MEGACO para el control del MRFP.

1.5.5.1.5 Multimedia Resource Function Processor (MRFP)

El MRFP provee recursos que son solicitados por el MRFC.
El MRFP desarrolla las siguientes funciones:

- Combinar los media streams
- Fuente de recursos media
- Procesamiento del Media stream.

1.5.5.1.6 Signaling Gateway

Provee la conversión de señalización en ambas direcciones en la capa de transporte entre SS7 y señalización basada en IP (por ejemplo ISUP/SS7 e ISUP/SCTP/IP).

1.5.5.1.7 Policy Decision Function (PDF)

PDF es la función lógica responsable de implementar la política de decisión basada en la información de sesión y medios de comunicación relacionados, obtenida del P-CSCF. Adicionalmente hace uso de mecanismos de QoS en la capa de conectividad IP. Almacena la información de sesión y medios de comunicación relacionados (dirección IP, número de puertos, ancho de banda, etc.).

También genera un testigo (token) de autorización para identificar el PDF y la sesión.

1.5.5.1.8 Home Subscriber Server (HSS)

El HSS contiene la principal base de datos con información de todos los usuarios (incluyendo servicios autorizados); al cual las entidades lógicas de control (CSCF) acceden al momento de administrar los suscriptores. Estos datos son pasados al S-CSCF mientras que el HSS almacena temporalmente la información con la localización del S-CSCF donde el usuario está registrado en un determinado momento.

1.5.6 APLICACIONES IMS

La arquitectura IMS busca aumentar las prestaciones de las aplicaciones con capacidades multimedia para crear servicios nuevos con un mayor número de funcionalidades que permiten al usuario tener comunicaciones más fáciles y más atractivas; de modo que el usuario pueda utilizar cualquier terminal o cualquier acceso a Internet para concretar su comunicación.

Entre algunas aplicaciones que se puede enumerar para IMS se tienen las siguientes:

- Servicios de Accesibilidad
- Servicios para Entornos Empresariales
- Servicios de Comunidades
- Servicios de Estilo de vida (Lyfestyle)
- Servicios de Publicidad

1.5.6.1 Servicios de Accesibilidad

Servicio "Botón Rojo" y Teleasistencia: consiste en realizar una lista de contactos del usuario para su localización en caso de emergencia. Al presionar el botón rojo se realiza una llamada al usuario que se encuentre más cercano.

De forma semejante se realiza el servicio de Asistencia remota para personas ancianas, discapacitadas o con algún tipo de dependencia, en donde se utilizan dispositivos de localización y seguimiento para el monitoreo.

Servicio "Sígueme": este servicio consiste en utilizar los datos de presencia o localización de un usuario registrado en la red para enrutar la llamada hacia el terminal más cercano. O a su vez establecer un diálogo a través de mensajes instantáneos.

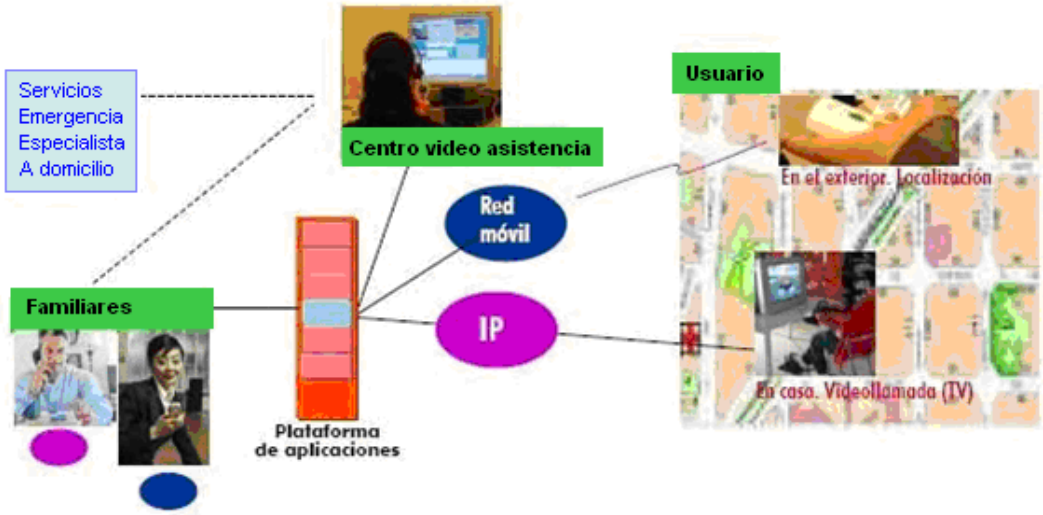


Figura 1.43: Servicio de Teleasistencia [16]

Servicio "IMR" o Teléfono Único: consiste de un teléfono único dual que proporciona un servicio convergente permitiendo al usuario cambiarse entre la red fija de banda ancha y la red móvil, enganchándose de forma automática a la mejor conexión, y manteniendo el mismo número. Pudiendo realizar y recibir llamadas a fijos y móviles evitando poseer más de un teléfono de contacto.

Además, al ser un servicio convergente, de forma automática el terminal se engancha a la mejor conexión: la red fija a través de WLAN (Wireless LAN (802.11x)) utilizando protocolo SIP/WIFI (Wireless Fidelity) o UMA (Unlicensed Mobile Access) o a la red móvil a través de GSM.

Servicio "Envío Inteligente de Mensajes": al enviar un mensaje urgente a un usuario se utiliza la información de registro y presencia de dicho usuario para enviar el mensaje al primer Terminal de su lista de preferencias de conexión (presencia).

1.5.6.2 Servicios para Entornos Empresariales

Para un entorno empresarial se busca aplicaciones situadas en la red del operador que sean accesibles independientemente del tipo de empresa o localización sin que se tenga que realizar una inversión significativa.

Otro tema de importancia es la convergencia, por la facilidad que presta para la utilización de distintos servicios sin la necesitar que el usuario use diferentes dispositivos.

Algunos modelos de aplicaciones a nivel empresarial se pueden nombrar ejemplos como:

- *Modelo Servidor(es) de aplicaciones localizados en la empresa*: algunas empresas mantendrán la gestión de sus servicios.

- *Modelo Aplicaciones en red:* en este modelo las aplicaciones de telecomunicaciones se encuentran en la red del operador. Este modelo es aplicable a empresas con un personal que necesita un gran nivel de movilidad.

- *Modelo Mixto:* este modelo agrupa las aplicaciones en la localización de la empresa con las aplicaciones repartidas en la red para proporcionar los mismos servicios a todos sus empleados sin importar su ubicación.

Se pueden nombrar algunas de las aplicaciones requeridas por las empresas tales como:

- *Global Voice/Multimedia VPN (Virtual Private Network, Redes Privadas Virtuales)*: esta aplicación de voz consiste en poder realizar las comunicaciones integrando líneas fijas, terminales móviles y usuario IP conectados a través de estructuras IMS, independientemente de ubicación, tipo de redes y dispositivos de acceso.

- *Central Virtual o Virtual PBX*: mediante el servicio de IP Centrex en red se puede realizar control de llamada a los usuarios finales independientemente del tipo de terminal y red de acceso.

- *Servicio IMR, Intelligent Mobile Redirect:* se realiza una convergencia fijo-móvil con la utilización de terminales duales. WiFi/GSM

- *Multiconferencia y Colaboración:* esta aplicación presta servicios de conferencias de audio / vídeo, conferencias en la Red y compartición de datos y aplicaciones.

  - Conferencias de Audio / vídeo: se necesita marcar el número telefónico del servicio, con el respectivo código de conferencia y contraseña, para una conferencia audio y vídeo o sólo audio.
  - Multiconferencias: son conferencias en red con capacidades de audio, video y datos que por medio de la utilización de un interfaz gráfico el usuario configura su perfil y gestiona sus conferencias.

- *Colaboración instantánea*: un usuario puede crear su lista de contactos y comprobar en tiempo real cual de ellos está en línea y disponible. Pudiendo establecer comunicación mediante IM (Instan Messaging, Mensajería Instantánea), realizar llamadas, compartición de documentos o envío de videos.

1.5.6.3 Servicios de Comunidades de Usuarios

- *Amigo TV:* es una aplicación en la cual los televidentes puede establecer comunicación (Chat) con su lista de contactos que esté viendo la televisión.

- My Own TV: aplicación mediante la cual se puede compartir fotos, películas, etc, a través de la televisión. El acceso a estos contenidos está definida por el propietario de los contenidos mediante una lista de contactos.

- *"Llamadas a ciegas":* son llamadas anónimas a otro usuario con gustos o preferencias similares a los del abonado.

- *Mensajería instantánea en 3D:* mensajería en espacios virtuales con avatares en representación del usuario.

- *"Push To Talk":* mediante la utilización de VoIP los usuarios finales pueden unirse a una conversación half-duplex.

- *Push To Show"*: se puede establecer una comunicación en grupo, además de la posibilidad de difundir un vídeo en vivo o pregrabado a uno o varios receptores simultáneamente.

- *"Push To Share/Share File"*: es un servicio para la comunicación en grupo que proporciona a los usuarios finales una manera de compartir fotos/ficheros durante una sesión de IMS (por ejemplo Push To Talk, Mensajería Instantánea) a uno o varios contactos al mismo tiempo.

1.5.6.4 Emulación de Servicios PSTN/ISDN (PES) [20]

El término emulación de la PSTN/ISDN es usado para referirse a una NGN que implementa los mismos servicios de la PSTN e ISDN. El objetivo de la implementación de la emulación es sustituir el núcleo de la red PSTN/ISDN sin reemplazar los terminales. Los usuarios conectados a una NGN que provee emulación PSTN/ISDN tendrán exactamente los mismos servicios de la PSTN/ISDN sin notar que es la NGN la prestadora del servicio.

El Sistema de Emulación de PSTN/ISDN (PES) implementa el concepto de emulación de PSTN/ISDN. PES permite a los usuarios recibir los mismos servicios que ellos actualmente reciben en las redes PSTN/ISDN con la existencia de terminales PSTN/ISDN. PES puede ser implementada tanto como un Softswitch o como una red distribuida IMS.

PES es un subsistema que proporciona las capacidades de servicio e interfaces de RTC[6] utilizando una adaptación a una infraestructura IP.

1.5.6.5 Simulación de Servicios PSTN/ISDN (PSS)[20]

El término simulación de PSTN/ISDN es usado para hacer referencia a una NGN que provee servicios de telecomunicaciones compatibles con

[6] RTC: Red Telefónica Conmutada

PSTN/ISDN, pero no necesariamente son lo mismo. El concepto también indica no solo una sustitución de PSTN/ISDN, sino también un reemplazo de los terminales, que además soporta comparación de capacidades con un teléfono convencional PSTN/ISDN.

Los terminales convencionales con un adaptador pueden utilizar estos servicios de simulación.

PSS proporciona capacidades de servicio similares a RTC utilizando control de sesión e infraestructura IP, sea a terminales de voz o a terminales avanzados.

PES representa un modelo de arquitectura de red más centralizada en el que la inteligencia se concentra en el plano de control, siendo los gateways los controladores de eventos. PSS, en cambio, es un modelo más colaborativo en el que los servidores de aplicaciones mantienen el control de los servicios, pero exigiendo a los gateways una mayor inteligencia y colaboración en la ejecución de los mismos.

Índice	REFERENCIA BIBLIOGRÁFICA, CAPÍTULO 1
[1]	CASTAÑEDA, Rodolfo. Dirección de Telemática CICESE www.cudi.edu.mx/primavera_2005/presentaciones/rodolfo_castaneda.pdf
[2]	KEAGY, Scott, Integración de redes de voz y datos, tercera edición, Cisco Publication, Madrid, 2001
[3]	http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones2.shtml Protocolos de Señalización
[4]	http://es.wikipedia.org/wiki/Real-time_Transport_Protocol#column-one Wikimedia Foundation, Inc, 13 dic 2007
[5]	http://www.voipforo.com http://www.voipforo.com/SIP/SIParquitectura.php SIP http://www.voipforo.com/H323/H323objetivo.php H.323 http://www.voipforo.com/codec/codecs.php Codecs
[6]	UNIVERSIDAD DE OVIEDO, ÁREA DE INGENIERÍA TELEMÁTICA. Fundamentos de transmisión de datos, www.it.uniovi.es/material/cursos/InternetNG_EU_072005/voipcursoV3.pdf
[7]	http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/telecomunicacionesng/capitulos/07_la_capa_de_control.pdf Las Telecomunicaciones de Nueva Generación La capa de control
[8]	Departamento de Ingeniería de Sistemas Telemáticos ETS, Universidad Politécnica de Madrid Aplicación y Servicios Avanzados Internet http://greco.dit.upm.es/~encarna/doctorado/0708/0apd-indice.pdf
[9]	García Tomás, Jesús, “Alta Velocidad y Calidad se Servicio en Redes IP”, Febrero 2002, Editorial Ra-ma
[10]	Folleto Seguridades. Ing. Nelson Ávila, 2007
[11]	VERDEJO, Gabriel, Seguridad en Redes IP, Barcelona, Septiembre 2003

[12]	HEVIA, Mariano, “Virtual Private Networks”, Agosto 2001. http://www.monografias.com/trabajos12/monvpn/monvpn.shtml
[13]	STALLINGS, William, “Cryptography and network security”, segunda edición, Pentice hall, 1999
[14]	http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_11.pdf *Las Telecomunicaciones y la Movilidad en la Sociedad de la Información* Telefónica Investigación, Desarrollo y la Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET)
[15]	http://pruebas.wikitel.info/wiki/Redes_de_nueva_generaci%C3%B3nCullen Internacional – Devoteam Siticom (2003). Regulatory implications of the introduction of next generation networks and other new developments in electronic communications. Informe para la Comisión Europea.
[16]	http://telecomid.webs.upv.es/anteriores/2006/trabajosdefinitivos2006/Programa_archivos/pdf/132.pdf Aplicaciones innovadoras en el entorno IMS/TISPAN Raquel Pérez Leal, Pilar Cid Fernández, Alcatel, Madrid
[17]	http://w3.iec.csic.es/URSI/articulos_gandia_2005/articulos/CMo2/621.pdf GONZÁLEZ-MIRANDA, Sergio, Departamento de Ingeniería Telemática, Universidad Politécnica de Madrid ROBLES, Tomás , Departamento de Ingeniería Telemática, Universidad Politécnica de Madrid GALINDO, Luis Angel , Telefónica Móviles de España S. A GALÁN MÁRQUEZ, Fermín, Ágora Systems, S. A
[18]	POIKSELKA Miikka, MAYER Georg, KHARTABIL Hisham and NIEMI Aki, “The IMS IP Multimedia Concepts and Services in the Mobile Domain”, John wiley & Sons Ltd, Inglaterra 2004
[19]	CEVALLOS Gabriel, TASINTUÑA Luis, “Diseño de una red integrada de voz y datos para el campus e.p.n. Basado en un análisis comparativo de las soluciones existentes en el mercado nacional”, EPN. Quito, Mayo 2007
[20]	LUNA AIZAGA, Elena Paola, “Estudio de factibilidad y diseño de una red que brinde servicios Triple Play en el sector de Pueblo Blanco mediante la implementación de un Access Media Gateway (AMG), que se conectará al softswitch de ANDINATEL S.A”. EPN,Quito Octubre 2007

[21]	ROJAS, Franklin; VASQUEZ Carlos “Diseño de un Proveedor de Servicio de Internet (ISP) con Tecnología Frame Relay, Integrando el Servicio de Voz Sobre Ip Y Análisis de Factibilidad Para su Posible Implementación”.EPN, Quito Abril 2008
[22]	http://www.h3c.com/portal/Products___Solutions/Technology/QoS/QoS/200701/195599_57_0.htm Introducción a QoS

CAPÍTULO 2 ANÁLISIS DE LA RED

2.1 ANÁLISIS DE LA INFRAESTRUCTURA

2.1.1 DESCRIPCIÓN GENERAL

ReadyNet es una empresa privada dedicada a la prestación de servicios de valor agregado (SVA), nace como Proveedor de Servicios de Internet (ISP) el 5 de Octubre del 2000 según la resolución No. 466 otorgada por el Consejo Nacional de Telecomunicaciones (CONATEL). El principal objetivo de la empresa es ofrecer excelentes servicios de valor agregado a usuarios de Internet, ya sean individuales y corporativos.

Opera y explota los servicios de Valor Agregado, desde sus oficinas ubicadas en Quito, en la calle Obispo Díaz de la Madrid 445 en donde se encuentra también la infraestructura de comunicación de la empresa.

ReadyNet lleva 8 años prestando servicios, nace en la ciudad de Quito y actualmente proporciona sus servicios a nivel nacional, en especial a ciudades que dispongan de las posibilidades de transmisión a través de ANDINATEL, PACIFICTEL y ETAPA. Para ello se ha diseñado un nodo de acceso principal, ubicado en la ciudad de Quito, el cual se conecta con ciudades como Ambato, Ibarra, Latacunga, Otavalo, Riobamba.

ReadyNet ofrece a sus clientes servicios de conexión Dial-Up (telefónico), Dial-Net (telefónico en red), dedicados banda ancha (Clear Channel, Frame Relay, ADSL, SDSL y Clear channel con radio). También se ofrece Web Hosting (Almacenamiento de páginas web), diseño de páginas web, diseño de aplicaciones para uso de web, registro de dominio, navegación en Internet, correo electrónico, transferencia de archivos, cableado de red y en general todos los servicios que en la actualidad el Internet o las telecomunicaciones ofrece.

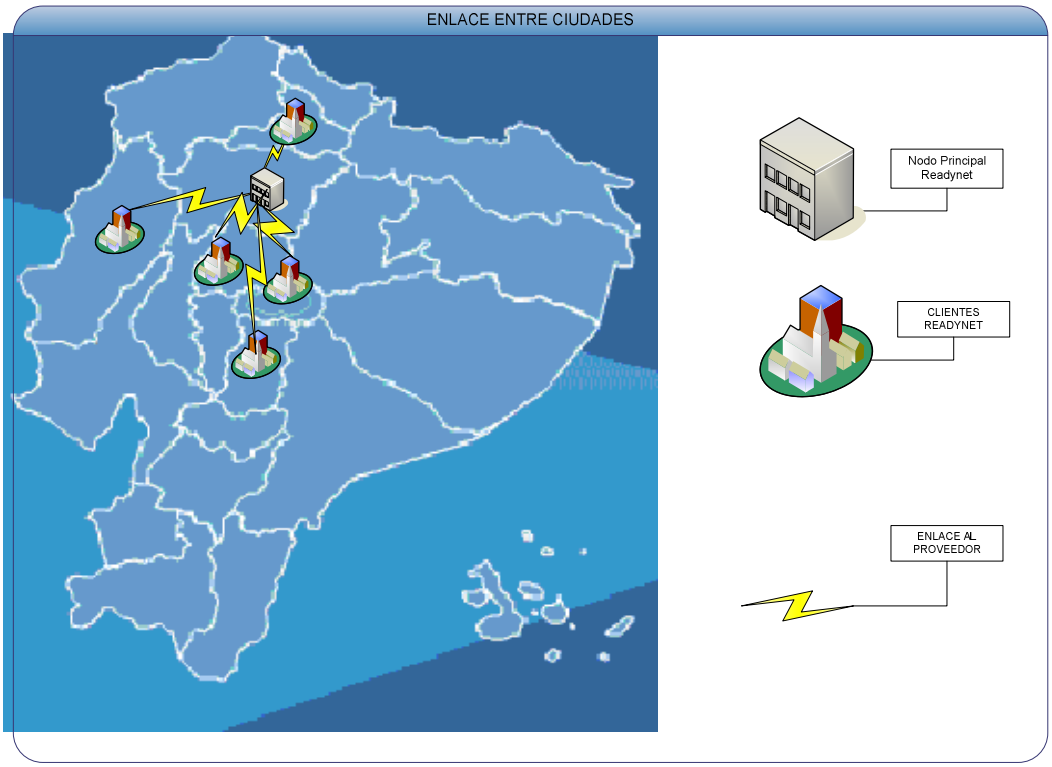


Figura 2.1: Diagrama ReadyNet

2.1.2 SERVICIOS

2.1.2.1 Conexión Dial - Up

El cliente se conecta al Internet mediante una llamada telefónica realizada a ReadyNet para ello utiliza un módem alcanzando una velocidad máxima de 56 Kbps. Debido a que el acceso Dial-Up utiliza líneas telefónicas convencionales, la calidad de la conexión no siempre es óptima y la tasa de transferencia de los datos es limitada por la misma.

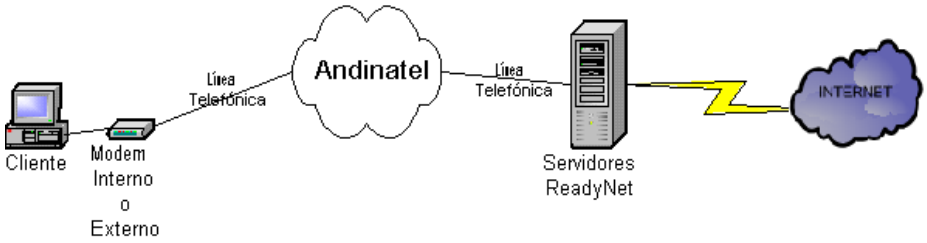


Figura 2.2: Conexión Dial Up

2.1.2.1.1 Requerimientos Técnicos para el Uso del Servicio Dial-Up

El usuario que desee utilizar estos servicios debe contar con los siguientes dispositivos y software:

- Computador
- Módem
- Línea telefónica

2.1.2.2 Conexión Dial – Net

Es la conexión de una red LAN (dos o más computadores personales en red) que a través de un servidor que posea un módem y por medio de una llamada telefónica hacia ReadyNet ingresa al Internet, permitiendo el uso simultáneo del acceso a Internet a todas las máquinas conectadas a la red por medio del proxy.

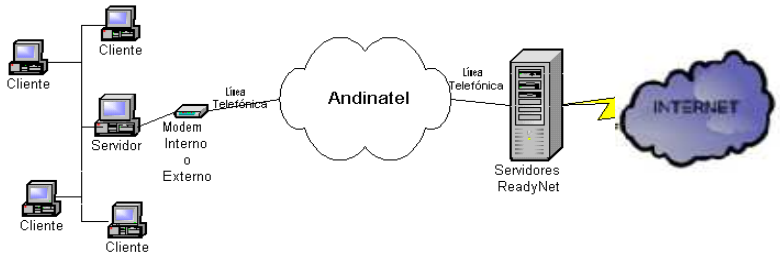


Figura 2.3: Conexión Dial Up - LAN

El Acceso Dial-Net es una conexión telefónica que debido a que utiliza líneas telefónicas convencionales, la calidad de la conexión no siempre es óptima y la tasa de transferencia de los datos es limitada por la misma. Obteniendo una tasa de transferencia máxima de 56 Kbps.

2.1.2.2.1 Requerimientos Técnicos para el Uso del Servicio Dial-Net

El usuario debe contar con lo siguiente:

- Red
- Computadoras conectadas en red
- Servidor conectado a la red
- Módem
- Línea telefónica
- Proxy

2.1.2.3 Conexión Dedicada a la Red Internet

Es una conexión siempre disponible, permite al usuario a través de un puerto dedicado mantener la posibilidad de enviar, recibir correo electrónico, navegación en páginas Web y presentar su propio sitio Web al mundo entero.

2.1.2.3.1 Tipos de Enlaces Dedicados

Entre los enlaces dedicados que ReadyNet ofrece tenemos:

- Clear Channel
- Frame Relay
- Radio (Clear Channel)
- ADSL
- SDSL

Enlace Clear Channel

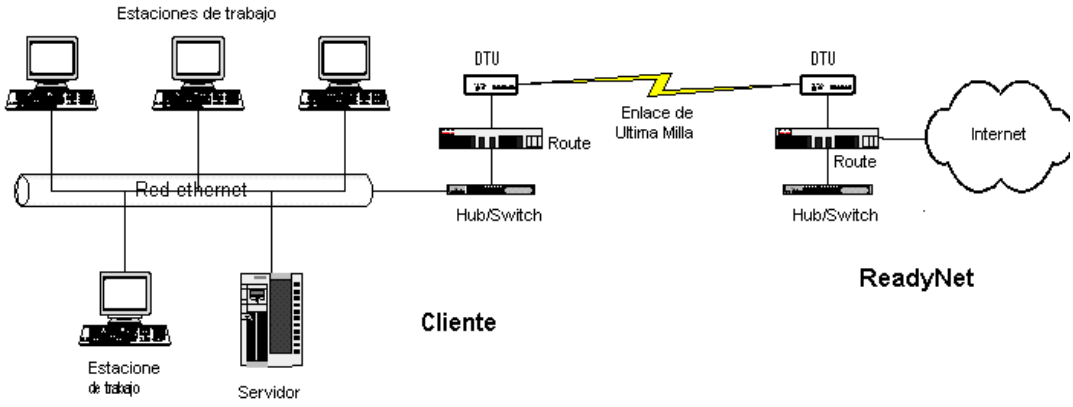


Figura 2.4: Clear Channel [1]

Enlace Frame Relay

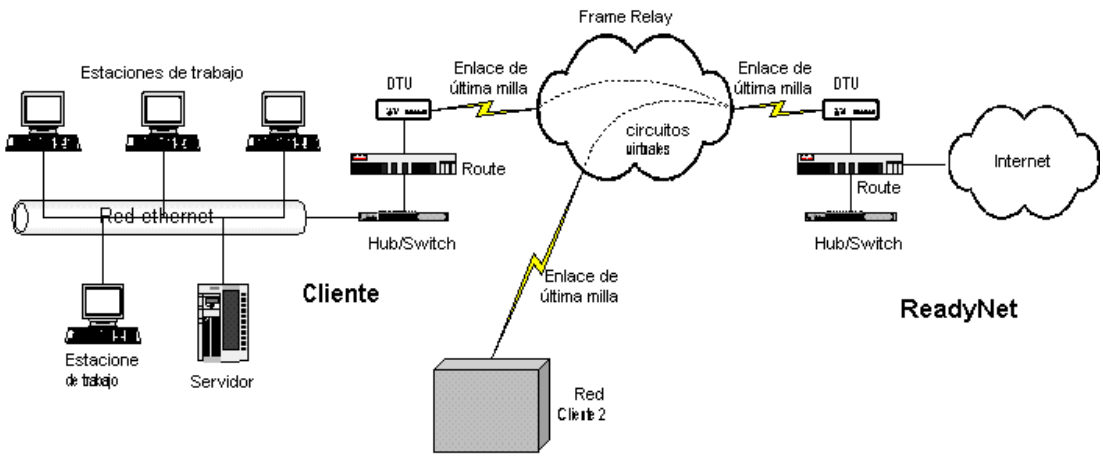


Figura 2.5: Frame Relay [1]

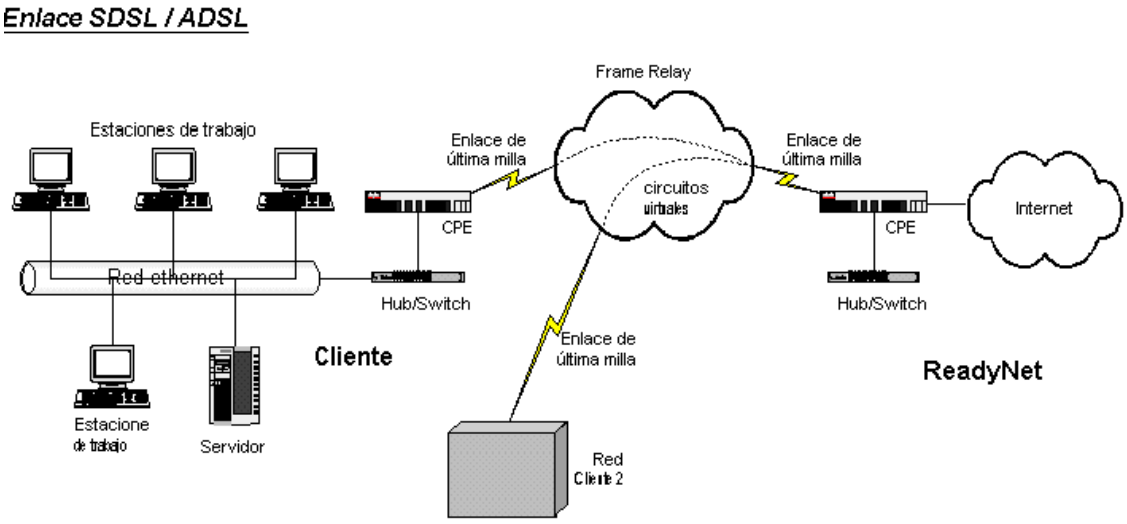


Figura 2.6: Enlace SDSL/ADSL[1]

2.1.2.3.2 Características Técnicas Mínimas de Hardware y Software para una Conexión Dedicada:

El usuario debe contar con lo siguiente:

- Red
- Computadoras conectadas en red
- Servidor conectado a la red
- Software proxy
- Enlace de última milla

2.1.3 INFRAESTRUCTURA DEL NODO PRINCIPAL

Para la prestación de servicio ReadyNet dispone de dos enlaces dedicados directos con operadoras autorizadas como son Global Crossing y ANDINATEL.

El primer enlace se lo realiza con Global Crossing como proveedor de la salida al backbone. Este enlace conecta a ReadyNet con Internet con capacidad de 1792 Kbps. La conexión hacia la red es a través de un router Cisco conectado directamente hacia el switch de core.

El segundo enlace se lo realiza con ANDINADATOS como proveedor de la salida a Internet mediante fibra óptica. Este enlace conecta a ReadyNet con Internet en USA y permitirá incrementar el ancho de banda gradualmente de acuerdo a las necesidades de tráfico existentes. La conexión hacia la red es a través de un router Cisco conectado directamente hacia el switch de core. Conjuntamente esta empresa es el proveedor de última milla para los clientes dedicados.

En el ámbito de red los servidores y equipos de acceso se encuentran conectados al switch de core, Cisco Catalyst 2950-24 10BaseT/100BaseTx. Entre los servidores podemos mencionar: el servidor de facturación, que dispone del software necesario para realizar los servicios de gestión, administración y tarifación entre otras aplicaciones que corren en él; los servidores de correo, DNS, FTP, etc, algunos de los cuales tienen redundancia para precautelar la continuidad de estos servicios.

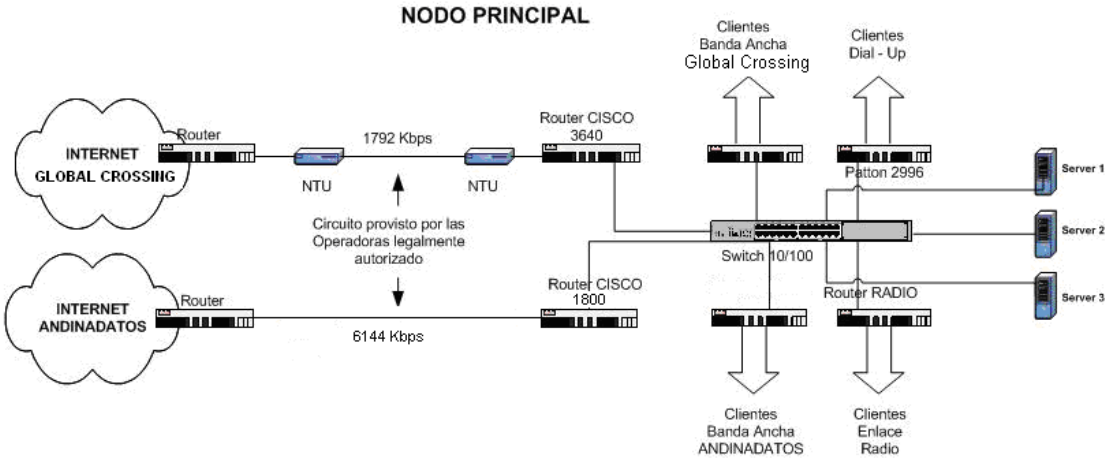


Figura 2.7: Nodo Principal

2.1.3.1 Conectividad al Nodo Principal

El Nodo principal situado en Quito da servicio a todos los usuarios de ReadyNet. El acceso a este nodo es por medio de las diferentes empresas que proveen el servicio de última milla.

2.1.3.1.1 Acceso de los Usuarios al Nodo Principal

Los clientes de Readynet acceden al nodo principal de dos formas, cada forma representará un tipo de usuario:

- A través de la red telefónica conmutada (Dial up).
- A través de líneas o enlaces dedicados, provistos por las portadoras que se encuentren legalmente autorizadas.

2.1.3.1.2 Acceso de Usuarios por la Red Pública Telefónica

Los usuarios se conectarán al nodo principal de ReadyNet. a través de la red telefónica llamando a un número colectivo PBX para conectarse a un access server Patton modelo 2996 con 2 líneas E1 y módems digitales V.92, V.90, K56Flex, V.34+, ISDN B-channel incorporados, a fin de proveer la conexión a Internet a través del router de salida correspondiente.

2.1.3.1.3 Acceso de los Usuarios por Conexión Dedicada

Los usuarios de una conexión dedicada tendrán un acceso permanente al nodo principal a través de enlaces dedicados de radio, cobre, etc., provistos por las portadoras legalmente autorizadas, hasta conectarse a los respectivos servidores de acceso remoto en el nodo principal.

2.2 TOPOLOGÍA DE LA RED

Se denomina topología física de una red a la forma física y geométrica que se le dará a la instalación de la red, tanto a los terminales como a los cables.

Con la topología se intenta obtener una instalación ordenada de terminales y cables de enlace.

Se denomina topología lógica de una red a la forma en que los hosts se comunican a través del medio.

Topología Física

La red posee una topología física en estrella que es la configuración dominante en la industria. Todos los equipos se conectan a un switch (Cisco Catalyst 2950), el cual tiene un modo de funcionamiento de nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacenará en el nodo y se retransmitirá sobre un enlace de salida hacia el destino.

Topología Lógica

La red utiliza una topología lógica en estrella, debido a que el switch principal es el encargado de dirigir el tráfico,

Medio Físico

- Cable UTP cat 5
- Conectores RJ45
- Jacks y Plugs cat 5
- Canaleta para interiores y exteriores

Conectividad de equipos

- Router
- Switchs
- Rack de comunicaciones
- Patch Panel
- Módems
- CSU-DTU

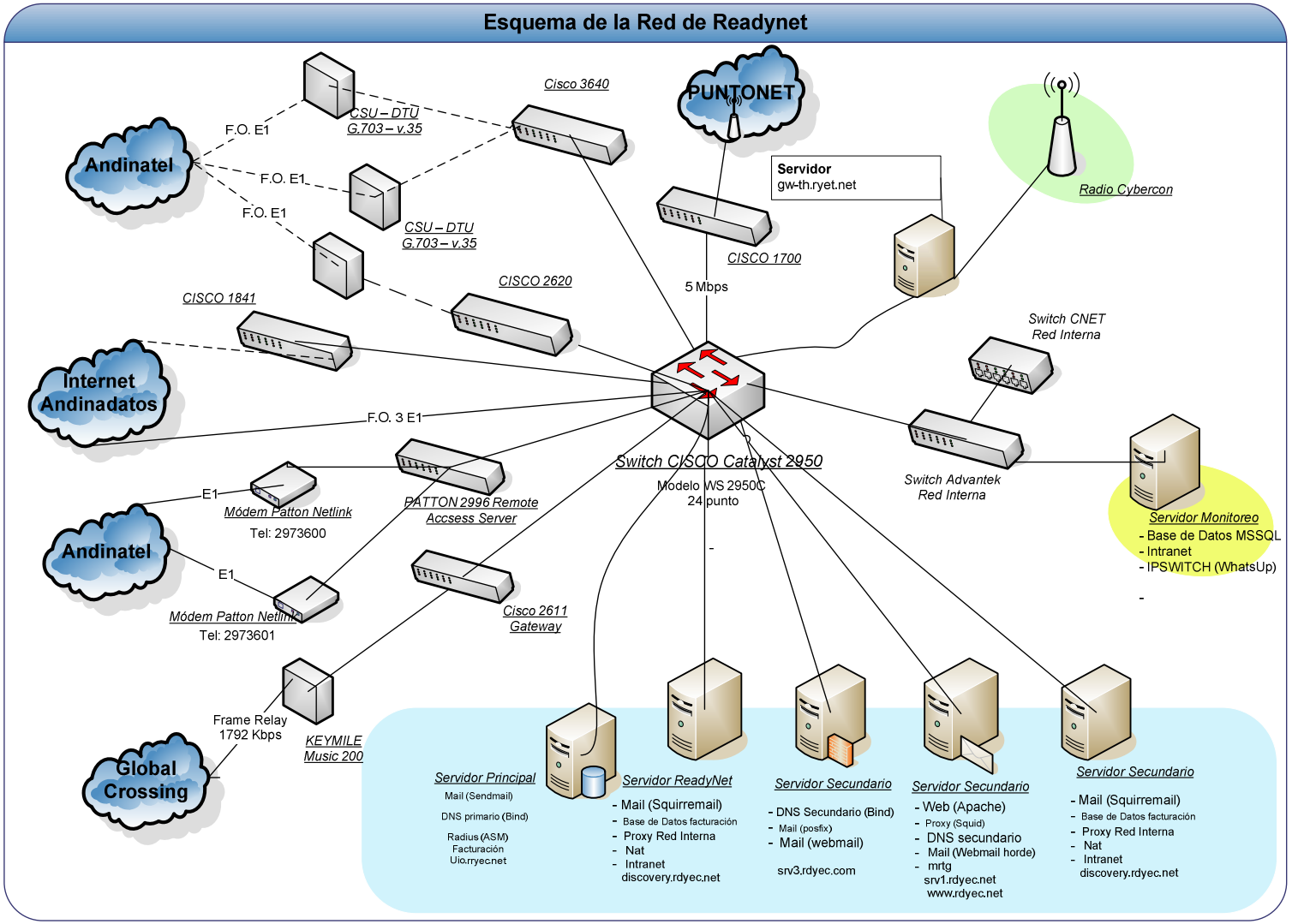


Figura2.8: Topología de ReadyNet

2.3 ENLACES

ReadyNet hasta Mayo del 2008 cuenta con 7 enlaces que se dividen en tres partes:

- Enlaces de Internet
- Enlaces de última milla radio
- Enlaces de última milla

2.3.1 ENLACES DE INTERNET

- La empresa cuenta con un enlace a Andinadatos a través de fibra óptica conectado al router Cisco 1800 con una capacidad igual a 3 E1 (6144 Kbps).

- La empresa cuenta con un segundo enlace de salida de Internet o backbone a Global Crossing a través de Frame Relay conectado al router Cisco 2600 con una capacidad de 1729 kbps.

2.3.1.1 Enlaces de Última Milla Radio

Para los clientes que no tienen acceso ADSL tienen la opción de conexión de última milla inalámbrica, para ello la empresa cuenta con enlaces de radio que son proveídos por Puntonet y Stealth Telecom.

- El enlace proporcionada por Stealth Telecom cuenta con un ancho de banda de 7 Mbps, se conecta mediante una antena de radio Cybercom la que se encuentra enlazada a un servidor de acceso.

- El enlace de última milla a través de PuntoNet posee un ancho de banda de 5 Mbps, se conecta con un router Cisco 1700.

2.3.1.2 Enlaces de Última Milla

Para los clientes Dial-Up y ADSL sin conexión por radio los enlaces de última milla se realizan mediante enlaces a Andinatel:

- Un enlace con una capacidad de 2 E1 (4.096 Mbps), para los usuarios con servicio Dial-Up, que se conecta con un RAS (Remote Acces Server) a través de una PBX Panasonic cuyos números de ingreso son 2973600 y 2973601.

- Dos enlaces: el primero con un ancho de banda de 2.048 Mbps (E1) para los clientes con servicio ADSL que se conectan al router Cisco 2600; y el segundo con un ancho de banda de 6144 Mbps (2 E1) para los usuarios conectados al router Cisco 3640.

2.3.2 CARACTERÍSTICAS DE LOS ENLACES

2.3.2.1 GLOBAL CROSSING

Global Crossing proporciona a ReadyNet asistencia en horario hábil de trabajo por medio del CAC (Centro de Atención al cliente) además cuenta con el NOC (Centro de operaciones de la Red), centro encargado de proveer asistencia ininterrumpida los 365 días al año de 19:00 a 7:59 y las veinticuatro horas los fines de semana y feriados.

Disponibilidad del Servicio: Se mide a partir de la información histórica de la solicitud de servicio técnico generada por una llamada al NOC o al CAC para reportar un problema.

2.3.2.2 STEALTH

Stealth está comprometido a proveer una operación del sistema en un 97% los 365 días las 24 horas al día y de ocurrir cualquier problema el cliente deberá informar al soporte técnico; en caso de necesitarlo fuera de horario este será facturado.

2.3.2.3 ANDINATEL

Andinatel proporciona enlaces conmutados desde una conexión de 2.048 Mbps tipo E1; en caso de existir falla se deberá comunicar a Andinatel para que proceda a solucionarlo. Para el caso de daño en última milla, se estima un periodo de 4 a 48 horas, dependiendo del tipo de daño reportado, para Servicio Home y de 4 horas para Servicio Plus. En caso de que la reparación requiera de mayor tiempo (generalmente daños con alguna línea o mantenimiento de nodos), se debe notificar por escrito al ISP explicando las razones.

Además es responsabilidad de esta empresa la calidad del servicio telefónico que ellos mismo proveen.

2.4 DIRECCIONAMIENTO IP

Para el direccionamiento IP ReadyNet cuenta con direcciones públicas, tanto para usuarios dedicadas o conmutados y únicamente se hará referencia a la IP administrativa, que será con la que se maneje el monitoreo del tráfico.

Estas direcciones se manejan con VLSM[7] (Variable Length Subnet Mask) y se expondrá solamente los pools (tabla 2.1, 2.2, 2.3) con los que cuentan ya que el subneteo de las direcciones es realizado según los requerimientos de los clientes.

Los clientes ADSL hacen uso de los siguientes rangos de direcciones IP públicas:

Desde	Hasta
201.219.16.17	201.219.16.254
201.219.21.1	201.219.21.254
201.219.38.33	201.219.38.254
64.76.195.1	64.76.195.254
64.76.222.1	64.76.222.254
190.152.70.1	190.152.70.254

Tabla 2.1: Direcciones IP ADSL

Los clientes del servicio de Dial-Up comparten el siguiente pull de direcciones IP públicas.

Desde	Hasta
64.76.194.33	64.76.194.254

Tabla 2.2: Direcciones IP Dial- Up

[7] VLSM (Variable Length Subnet Mask): Máscaras de subred de tamaño variable, es presentada como solución para el agotamiento de direcciones ip. Se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de la red.

Para la ubicación de los servidores de aplicaciones de ReadyNet se utilizan las direcciones IP públicas:

Desde	Hasta
64.76.194.1	64.76.194.30

Tabla 2.3: Direcciones Servidores

La red interna de ReadyNet pertenece a la red privada 10.10.10.0, dentro de la cual la dirección IP administrativa del servidor de monitoreo es la 10.10.10.2, en el cual se encuentra instalada la aplicación de monitoreo de tráfico de la cual se obtuvo las gráficas presentadas en los Anexos B y C.

2.5 EQUIPOS DE INTERCONECTIVIDAD

Físicamente la red de ReadyNet en su totalidad se encuentra ubicada en un solo cuarto de equipos.

A mayo 2008 la red está constituida por los siguientes equipos de conectividad con sus respectivas características:

2.5.1 SWITCH PRINCIPAL

El núcleo de la red es un switch Cisco Catalyst 2950.

Este switch es utilizado para centralizar las conexiones de todos los equipos de la red, acceso a los servidores, conexiones de últimas millas hacia el backbone de Internet. Adicionalmente se encarga de la conexión de la red interna y el acceso a Internet de la misma.

Mediante este switch se puede monitorear la red, para obtener información de enlaces, clientes y equipos de la red interna.

2.5.1.1 Características Técnicas

Nivel de conmutación	2.
Velocidad de conmutación de paquetes	6 Mpps
Velocidad de backplane	4.8 Gbits/s.
MAC soportadas	8K
ACLs de nivel	2.
Maneja hasta 1000 VLANs	(Protocolo 802.1q)
Manejo de enlaces	*Trunking*.
Monitoreable	(SNMP V1,V2, V3, RMON (4 grupos Alarmas, Eventos, Estadísticas, e Historia), MIB II)
Spanning Tree Protocol	(802.1D)
Protocolo 802.1X	
QoS	(802.1p), 2 colas por puerto físico
MTBF (*Middle Time between fail*)	200000 horas
Número de puertos habilitados:	24 puertos 10/100
	2 puertos GBIC-SX
Software Asistente de Redes Cisco	Cisco AVVID (Architecture for Voice, Video and Integrated Data) manejo de diferentes tipos de tráfico: voz, video, multicast, datos de alta prioridad.
DRAM	16MB
Flash memory	8MB

Tabla 2.4: Características Técnicas Switch Cisco Catalyst 2950[2]

2.5.2 BACKBONE DE INTERNET

2.5.2.1 Ruteador Backbone Andinadatos

El acceso a Internet por el enlace provisto para Andinadatos se realiza a través de un ruteador Cisco 1800. Este ruteador se encuentra conectado a un multiplexor de fibra óptica utilizado para la conversión de interfaces.

2.5.2.2 Características Técnicas

Puertos habilitados	2 PUERTOS WAN (T1/E1)
	2 puertos Fast Ethernet
Multiservicio	voz, datos y video
Protocolos	IPv6 DES, 3DES, AES.
VLAN	802.1q
QoS	802.1p
Monitoreable	SNMP, Telnet, TFTP, VTP
DRAM	Default: 128 MB Máximo: 384 MB
Flash memory	Default: 32 MB Máximo: 128 MB

Tabla 2.5: Características Técnicas Router Cisco 1841[2]

2.5.3 RUTEADOR BACKBONE GLOBAL CROSSING

La salida a Internet por Global Crossing se realiza a través de un ruteador Cisco 2611. Que a su vez se conecta a un DTU para la conexión con un enlace Frame Relay.

2.5.3.1 Características Técnicas

Puertos habilitados	2 Ethernet/IEEE 802.3
	WAN ATM, ISDN BRI/PRI, T1/E1
	2 Serial network
Multiservicio	voz, datos y video
Protocolos	DES, 3DES, AES, GRE, IPSec
QoS	Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ)
Soporte VLANs	Protocolo 802.1q y Cisco Inter-Switch Link (ISL)
DRAM	Default: 128 MB Maximum: 256 MB
Flash memory	Default: 32 MB Maximum: 48 MB

Tabla 2.6: Características Técnicas Router Cisco 2611[2]

El equipo utilizado como DTU es un Keymile Music 200.

2.5.3.2 Características Técnicas

INTERFACES	G.703/G.704; X.21/V.11; V.35; V.36 10BASE-T ETHERNET; ISDN-PRA
Código de línea	PAM16 / CAP / 2B1Q

Tabla 2.7: Características Técnicas Keymile Music 200[5]

2.5.4 ÚLTIMA MILLA

2.5.4.1 Ruteador para Acceso ADSL

Este acceso se realiza a través de dos ruteadores: un Cisco 3640 conectado a dos conversores G.703 a v.35 los cuales están conectados a dos enlaces de fibra óptica con Andinatel; y un Cisco 2620, el mismo que se encuentra conectado a un conversor G.703 a v.35 de la misma forma que el equipo anterior.

2.5.4.1.1 Características Técnicas

Puertos habilitados	1 Ethernet/IEEE 802.3
	WAN ATM, ISDN BRI/PRI, T1/E1
	2 Serial network
Multiservicio	voz, datos, video
Seguridad	encriptación de datos, túneles, y Radius, Tacacs, y AAA
QoS	802.1p
DRAM	Default: 32 MB Maximum: 128 MB
Flash memory	Default: 8 MB Maximum: 32 MB

Tabla 2.8: Características Técnicas Cisco 3640[2]

2.5.4.1.2 Características Técnicas

Puertos habilitados	1 Fastethernet/IEEE 802.3
	WAN ATM, ISDN BRI/PRI, T1/E1
	1 Serial network
Multiservicio	voz, datos y video
QoS	802.1p
Protocolo	DES, 3DES, AES, GRE, IPSec, RSVP
DRAM	Default: 128 MB Máximo: 256 MB
Flash memory	Default: 32 MB Máximo: 48 MB

Tabla 2.9: Características Técnicas Cisco 2620[2]

2.5.4.2 Enlace Radio Stealth

La última milla con servicio de radio se realiza con la infraestructura de la empresa Stealth Telecom.

La conexión se realiza mediante un servidor Linux que posee funciones de enrutamiento. Este servidor tiene dos tarjetas de red: la primera para la conexión interna hacia ReadyNet y la segunda se encuentra conectada a una antena de radio Cybercom para el acceso de los usuarios.

2.5.4.3 Enlace PuntoNet

La última milla inalámbrica además se realiza por medio de otro proveedor como es PuntoNet. Este enlace es provisto por un ruteador Cisco 1700.

2.5.4.3.1 Características Técnicas

Puertos habilitados	1 Fastethernet (10/100BASETX)
	ISDN BRI, DSU/CSU, FT1/T1 DSU/CSU
	Serial y dual-serial.
Soporte VLANs	Protocolo 802.1q
Protocolos	IP, IPX, OSPF, RSVP
QoS	802.3p
Monitoreable	SNMP, Telnet
DRAM	64 MB
Flash memory	16 MB

Tabla 2.10: Características Técnicas Cisco 1700[2]

2.5.5 DIAL UP

2.5.5.1 Servidor de Acceso Remoto

El RAS (Remote Access Server) es un equipo Patton 2996. Este equipo se encarga de la autenticación y autorización de los usuarios de la red mediante conexiones de tipo dial-up.

El RAS se encuentra conectado a dos enlaces de última milla mediante dos equipos Módem Patton Netlink.

Para el acceso de conexiones Dial-Up se lo realiza mediante las PBX 2973600 y 2973601.

2.5.5.1.1 Características Técnicas

Número de conexiones	96 llamadas – 4 T1 o 3 E1
Abastecimiento de energía	Redundancia dual AC
Puertos Ethernet	1 (auto-sensing/full-duplex10Base-T o 100Base-T)
Puertos WAN	4 (conexiones E1, T1 o PR1)
Modulación de módems	V.90, V.92, V.34, V32bis
Administración	HTTP, SNMP
Autenticación	Radius, PAP/CHAP, Username/Password.
FLASH memory	4 MB
EDO DRAM	32 Mbytes

Tabla 2.11: Características Técnicas Patton 2996[3]

2.5.6 RED INTERNA

Los equipos principales de conectividad de la red interna son:

2.5.6.1 Switch Principal Red Interna

Este es un switch Advantek que se encuentra conectado al núcleo de la red interna de Readynet. A este equipo se encuentran conectados los equipos que constituyen propiamente la intranet.

2.5.6.1.1 Características Técnicas

Puertos	16
Standard	802.3 (10BaseT), 802.3u (100BaseTX)
Velocidad	10/100Mbps
Interfase	Puerto RJ45
Packet Buffer Memory	256KBytes
Tipo de procesador	Store and Forward, Full/Half Duplex, Non-Blocking Flow Control

Tabla 2.12: Características Técnicas Switch Advantek[3]

2.5.6.2 Switch Secundario

Es un equipo CNET, al cual están conectadas la mayoría de las PCs que conforman la red interna. Este equipo se encuentra conectado al switch principal de la red interna Readynet.

2.5.6.2.1 Características Técnicas

PUERTOS	24
Standard	802.3 (10BaseT), 802.3u (100BaseTX)
Velocidad	10/100Mbps
Interfase	Puerto RJ45
MAC Address	8K
Tipo de procesador	Store-and-Forward
Medios compatibles	10BASE-T Cat. 3,4 o 5 TP y 100BASE-TX Cat. 5 TP
Cada puerto puede crear un segmento de red diferente	
Todos los puertos soportan Auto-MDI/MDI-X	

Tabla 2.13: Características Técnicas Switch CNET[6]

2.5.7 SERVIDORES

2.5.7.1 Aplicaciones para Servicios

Las aplicaciones que ReadyNet posee son orientadas a los servicios que se provee a sus clientes tales como:

DNS (Domain Name System): servidor que resuelve un nombre de dominio en una dirección IP de manera que nos permite trabajar con nombres de dominio en lugar de IPs para facilitar el trabajo al usuario de la web. Para implementación de este servicio se utilizó BIND (*Berkeley Internet Name Domain)*, el cual es el más común entre las plataformas UNIX por ser estable.

Correo Electrónico: ReadyNet mantiene las cuentas de correo en 3 servidores: uio.rdyec.net, srv3.rdyec.com, smtp.rdyec.net. Se configuran cuentas de tipo POP. El software que utilizan estos servidores para implementar el correo son:

SendMail: es el agente de transporte de correo (MTA - Mail Transport Agent) más común en Internet, corre sobre sistemas Unix, sin embargo es de compleja configuración.

Postfix es un Agente de Transporte de Correo (MTA) que constituye una alternativa más rápida, fácil de administrar y segura en comparación con Sendmail.

Squirrelmail: es una aplicación webmail que está diseñada para trabajar con plugins, permitiendo incrementar nuevas características a la aplicación para ser más funcional, y extensible. Presenta funcionalidades como el filtrado de mails, característica que es utilizada por ReadyNet para brindar un mejor servicio al eliminar spam.

Webmail**:** es un servicio que permite acceder a tu cuenta de correo electrónico a través de una página web utilizando un navegador con cualquier conexión a Internet. Se puede leer, enviar y organizar los correos sin descargarlos en el ordenador. En donde la privacidad de los usuarios se realiza mediante nombres de usuario y contraseña, los mismos que serán únicos para cada cliente.

Hosting: se provee el alojamiento de páginas Web en un servidor de ReadyNet para su publicación en el Internet. El propietario de la página podrá almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web. Para dicho servicio se utiliza el software libre Apache (HTTPD) para plataformas Unix.

Transferencia de archivos FTP: servicio utilizado para que el cliente pueda conectarse remotamente al servidor de ReadyNet e intercambiar información, como por ejemplo para realizar la actualización de su página web alojada en dicho servidor.

Proxy: este servicio se utiliza para mejorar la velocidad de acceso a la Web y ahorrar ancho de banda en la conexión a Internet. Se utiliza el programa *Squid,* el cual hace caché de las consultas DNS, para que en la próxima consulta a la misma página simplemente se transfiere la copia almacenada en memoria acelerando la transferencia de información.

Los servicios que ofrece ReadyNet se encuentran disponibles en cinco servidores para el acceso de los clientes.

2.5.7.2 Servidor Principal

Este servidor implementado en la plataforma Linux, es utilizado para la autenticación de los usuarios dial-up y para realizar la facturación.

Se encuentran levantados los servicios de DNS primario y Correo Electrónico. Además este servidor es utilizado para Hosting, como servidor FTP y realiza el monitoreo de virus y spam en correo de los usuarios.

DIRECCIÓN IP	64.76.194.10
Nombre y dominio	uio.rdyec.net
Mail	SendMail
DNS	DNS Primario mediante Bind
Radius	ASM (autenticación usuarios dial-up)

Tabla 2.14: Características Servidor Principal

Especificaciones Técnicas

Procesador	INTEL PENTIUM III A 1GHZ
Memoria RAM	256 MB
Disco duro	Samsung de 10GB y Quantum de 40GB
Unidad óptica	CD-ROM Samsung
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.15: Especificaciones Técnicas Servidor Principal

2.5.7.3 Servidor Correo Cliente

Servidor implementado en la plataforma Linux se utiliza conjuntamente con el servidor principal para proveer el acceso a los usuarios Dial-up y realiza el proceso de NAT (Network Address Translation) para los mismos.

DIRECCIÓN IP	64.76.194.21
Nombre y dominio	discovery.rdyec.net
Mail	Squirrelmail
Proxy	Squid en Linux Para los equipos de escritorio de las oficinas de ReadyNet
NAT	FireStarter Sirve para uso de los clientes Dial-up
Base de datos para facturación de los clientes de la empresa	

Tabla 2.16: Características Servidor

Especificaciones Técnicas

Procesador	INTEL PENTIUM IV A 1.8GHZ
Memoria RAM	256 MB
Disco duro	Maxtor de 60GB
Unidad óptica	CD-ROM Samsung
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.17: Especificaciones Técnicas Servidor

2.5.7.4 Servidor Secundario 1

Servidor implementado en la plataforma Linux. Se lo utiliza para agregar servicios y respaldos de aplicaciones del servidor principal y también como servidor principal de transferencia de archivos FTP.

DIRECCIÓN IP	64.76.194.11 Y 64.76.194.12
Nombre y dominio	srv1.rdyec.net o www.rdyec.net
Mail	Webmail y HORDE
Proxy	Squid
DNS	DNS secundario mediante Bind
WEB	Apache (HTTPD) Servicio de Hosting a los clientes.
Tráfico: Permite realizar el monitoreo de tráfico tanto interno como de cada uno de los clientes ADSL mediante el MRTG.	

Tabla 2.18: Características Servidor

Especificaciones Técnicas

Procesador	INTEL XEON A 2.4GHZ (QUAD CORE)
Memoria RAM	512MB
Disco duro	SCSI de 60GB
Unidad óptica	CD-ROM Samsung
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.19: Especificaciones Técnicas Servidor

2.5.7.5 Servidor Secundario 2

Servidor implementado en la plataforma Linux. Utilizado para realizar respaldos de aplicaciones del servidor principal.

DIRECCIÓN IP	201.219.16.10
Nombre y dominio	srv3.rdyec.com
Mail	PostFix y Webmail
DNS	DNS secundario mediante Bind

Tabla 2.20: Características Servidor

Especificaciones Técnicas

Procesador	INTEL XEON 3.0 GHZ (DUAL CORE)
Memoria RAM	512MB
Disco duro	Samsung de 120GB SATA
Unidad óptica	CD-RW Samsung
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.21: Especificaciones Técnicas Servidor

2.5.7.6 Servidor de Correo

Servidor implementado en la plataforma Linux, se lo utiliza como servidor de respaldo del servicio de correo electrónico.

DIRECCIÓN IP	64.76.194.23
Nombre y dominio	smtp.rdyec.com
Mail	SMTP con Postfix y un servidor de Webmail utilizando Squirrelmail.

Tabla 2.22: Características Servidor

Especificaciones Técnicas

Procesador	PIV XEON 3GHZ
Memoria RAM	1 GB
Disco duro	Seagate de 500GB SATA
Unidad óptica	CD-RW Samsung
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.23: Especificaciones Técnicas Servidor

2.5.7.7 Servidor de Monitoreo

Servidor con sistema operativo WinXP Sevice Pack 2; en el cual se encuentra levantada la herramienta de administración WhatsUp, con la cual se realizar el seguimiento del comportamiento de los equipos de conectividad de ReadyNet y de los enlaces de los usuarios, pudiendo monitorear módems y servidores de ser el caso.

DIRECCIÓN IP	10.10.10.2
Administración de red	Mediante IP Switch WhatsUp
Base de datos: A través de Microsoft SQL Server	

Tabla 2.24: Características Servidor

Especificaciones Técnicas

Procesador	CELARON 2.4 GHZ
Memoria RAM	512 MB
Disco duro	SAMSUNG 40 GB PATA
Unidad óptica	DVD-ROM LG
Velocidad de la tarjeta de red [Mbits/s]	100\10

Tabla 2.25: Especificaciones Técnicas Servidor

2.6 DESCRIPCIÓN Y ANÁLISIS DE TRÁFICO

2.6.1 TRÁFICO

Para las lecturas de tráfico de los diferentes enlaces y dispositivos de la red se utilizaron herramientas que mediante el servicio de SNMP (*Simple Network Management Protocol*) levantado en estos dispositivos y con información tal como la dirección de administración del dispositivo y la comunidad SNMP a la que pertenecen, dichos elementos de red pueden ser monitoreados y obtener los reportes del tráfico.

Las herramientas que se utilizaron fueron: MRTG (Multi Router Traffic Grapher), la cual ya la disponían en la empresa para lecturas de tráfico tanto para los enlaces principales tales como: Internet, Servidores, Últimas Millas; como para los enlaces individuales de los clientes que son monitoreables y PRTG (*Paessler Router Traffic Grapher*), software que se utilizó para monitorear los interfaces del switch principal en la semana del 26 de mayo al 1 de junio 2008 para obtener un informe más detallado.

Las mediciones de niveles de tráfico de entrada, salida y total se realizaron en los puertos conectados a los enlaces para Servidores, acceso a Internet, últimas millas, cuentas Dial Up y red interna.

En el Anexo C y D se muestran los resultados totales del análisis de tráfico.

2.6.1.1 Tráfico de Servidores

En la tabla 2.26 se muestra el resumen del tráfico promedio para los servidores. El ancho de banda ocupado para los servidores no tiene ningún tipo de restricción, su utilización es bajo demanda, es decir va de acuerdo a lo requerido por los usuarios.

Servidor	Tráfico de salida [Kbits/s]	Tráfico de entrada [Kbits/s]	Tráfico total [Kbits/s]
uio.rdyec.net	91,432	260,593	352,025
srv1.rdyec.net	281,407	88,541	369,948
www.rdyec.net	8,628	0,025	8,653
discovery.rdyec.net	1,788	2,134	3,922
srv3.rdyec.net	44,625	52,402	97,027

Tabla 2.26: Tráfico promedio en los enlaces de los Servidores.

En la figura 2.9 se puede apreciar que el servidor con mayor tráfico de entrada es el uio.rdyec.net y el de mayor tráfico de salida es el srv1.rdyec.net. Esto se debe a que se mantienen constantes respaldos del servidor uio, los mismos que son almacenados en el servidor srv1. Dichos respaldos son efectuados a horas de la madrugada para no disminuir la disponibilidad de los recursos hacia los clientes.

Adicionalmente el servidor con mayor flujo de información es el srv3, ya que de este servidor no se obtienen respaldos, y la cantidad de información que maneja es propia de las cuentas de correo de clientes, y tráfico DNS, que son las principales aplicaciones que corren en este servidor.

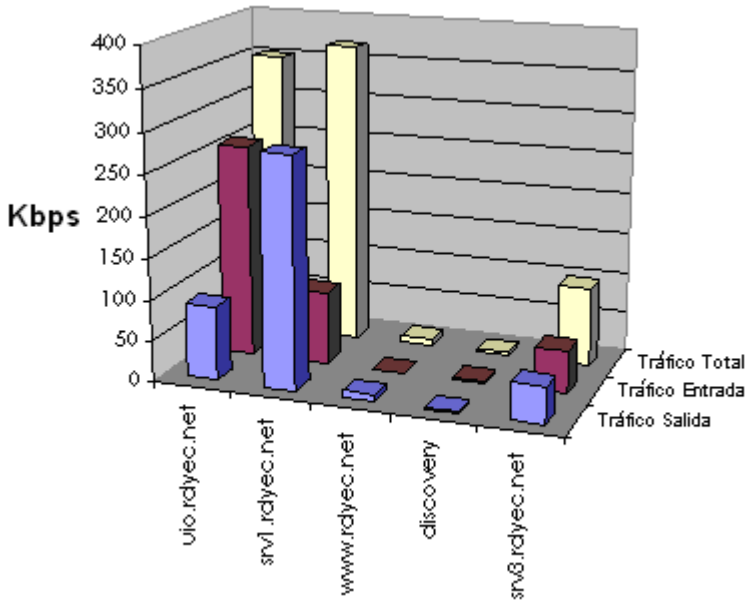


Figura 2.9: Esquema de los niveles de tráfico de los servidores.

2.6.1.2 Tráfico Acceso a Internet

La tabla 2.27 se muestra el tráfico promedio de los enlaces hacia la salida a Internet por medio de los dos proveedores Andinadatos y Global Crossing.

Enlace Internet	Tráfico de salida [Kbits/s]	Tráfico de entrada [Kbits/s]	Tráfico total [Kbits/s]
Enlace Andinadatos Cisco 1800	921,580	3.203,164	4.124,743
Enlace Global Crossing Cisco 2600	438,355	614,841	1.053,196

Tabla 2.27: Tráfico Promedio en los enlaces de los Servidores.

Como se puede apreciar en la figura 2.10, el enlace con mayor nivel de tráfico es el de Andinadatos, lo cual ratifica que la mayoría de los clientes tienen salida por este enlace ya que la capacidad que ofrece este backbone es mayor que la del otro proveedor.

En el Anexo C y D se muestra la gráfica obtenida de los niveles de tráfico que se manejan en estos dos enlaces. Para el enlace de Andinadatos se llega a picos de tráfico total entre 8.000 y 9.000 Kbps; lo cual supera la capacidad de este enlace.

En el enlace de Global Crossing se obtiene un tráfico total con picos entre 2.200 y 2.600 Kbps, en donde de igual manera se supera la capacidad prevista para dicho enlace.

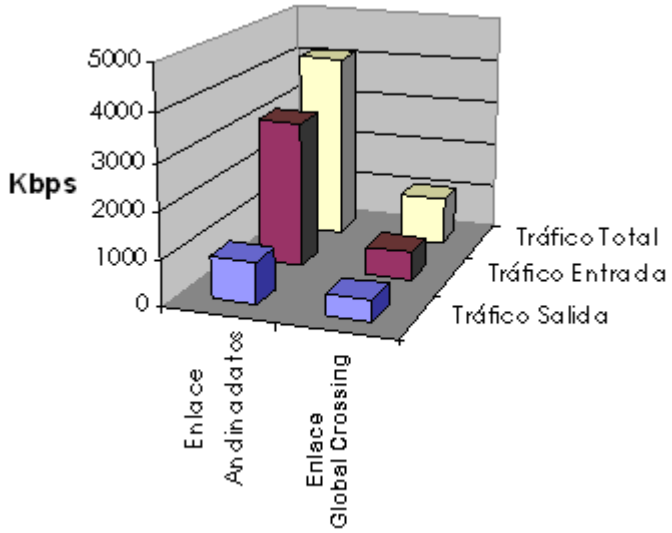


Figura 2.10: Esquema de los niveles de tráfico de los enlaces para Internet.

2.6.1.3 Tráfico Última Milla

En la tabla 2.28 se presenta los niveles promedios del tráfico de los distintos enlaces utilizados para proveer la última milla.

Ultima Milla	Tráfico de salida [Kbits/s]	Tráfico de entrada [Kbits/s]	Tráfico total [Kbits/s]
CORE: Cisco 3640	1.494,795	538,544	2.033,338
CORE2: Cisco 2600	698,402	147,117	845,518
Stealth	882,585	339,949	1.222,534
PuntoNet	106,4	*367,2*	473,6
MetroEthernet	15,125	*1,25*	16,375

Tabla 2.28: Tráfico promedio en los enlaces de última milla.

En la figura 2.11 se puede observar que el mayor número de usuarios están dirigidos al enlace denominado Core ya que éste es el que tiene mayor nivel de tráfico. Core2 es un enlace en el cual se está incrementando el número de usuarios; y finalmente se tiene un tráfico bajo por la MetroEthernet.

Se puede apreciar que el enlace Core tiene picos de tráfico total entre 4.000 y 4.500 Kbps, superando la capacidad para este enlace.

En el enlace Core2 se tiene picos de tráfico total entre 1.800 y 2.000 Kbps, lo cual se aproxima a la capacidad total del enlace.

En cuanto a última milla inalámbrica se tiene que el mayor flujo de tráfico se da por el enlace de Stealth, sin embargo incluyendo los picos de tráfico no llega a ocupar la totalidad de la capacidad del enlace.

El enlace con PuntoNet de igual manera mantiene un tráfico menor al de la capacidad total del enlace.

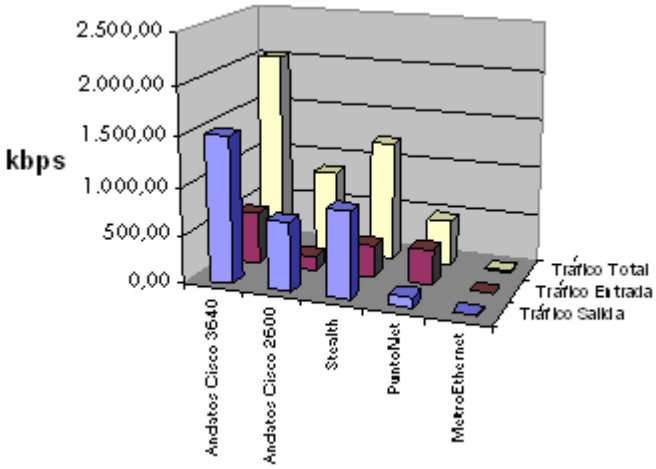


Figura 2.11: Esquema de los niveles de tráfico de los enlaces de última milla

2.6.1.4 Tráfico Usuarios Dial-Up

La tabla 2.29 muestra el tráfico originado por los usuarios dial-up.

Usuarios Dial-Up	Tráfico de salida [Kbits/s]	Tráfico de entrada [Kbits/s]	Tráfico total [Kbits/s]
Patton 2996 RAS	86,739	29,082	115,821

Tabla 2. 29: Trafico promedio en los enlaces de última milla.

En la figura 2.12 se puede apreciar que este enlace no tiene gran nivel de tráfico, se mantiene un menor número de usuarios, ya que la mayoría buscan una conexión a Internet de mayor capacidad razón por la cual migran hacia conexiones ADSL.

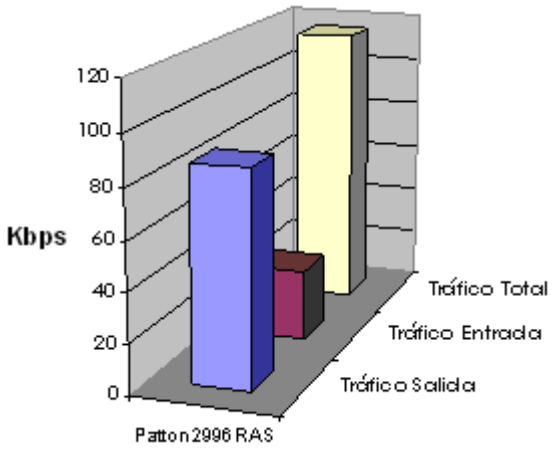


Figura 2.12: Esquema de los niveles de tráfico de los enlaces de última milla

2.6.1.5 Tráfico Red Interna

La tabla 2.30 contiene la información acerca del tráfico que se maneja de manera interna en ReadyNet.

Red Interna	Tráfico de salida [Kbits/s]	Tráfico de entrada [Kbits/s]	Tráfico total [Kbits/s]
Switch CNET	435,2	164	599,2

Tabla 2.30: Tráfico promedio en los enlaces de última milla.

En la figura 2.13 se muestra los niveles de tráfico de la red interna. Para el tráfico manejado internamente en ReadyNet no existe ningún tipo de restricción de ancho de banda, la salida a Internet lo realiza mediante el enlace de Global Crossing.

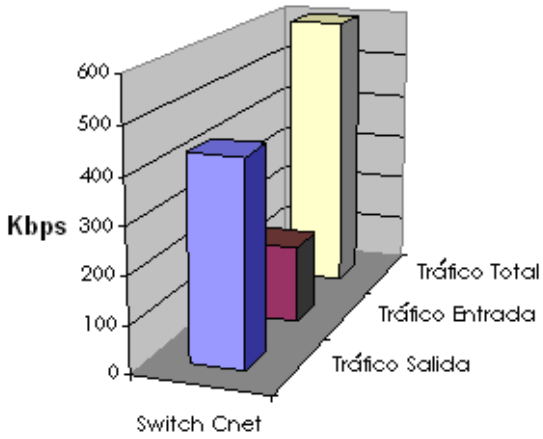


Figura 2.13: Esquema de los niveles de tráfico de la Red Interna

2.7 EVALUACIÓN DEL RENDIMIENTO DE LA RED ACTUAL

Para realizar un análisis de la red se muestra en la tabla 2.31 el cálculo del rendimiento de cada enlace que posee una capacidad limitada.

Se debe tomar en cuenta que este análisis es efectuado con el tráfico total promedio, por lo tanto no se refleja con exactitud aquellos instantes de tiempo en el cual se produce picos de tráfico que sobrepasan la capacidad del enlace.

Se puede apreciar que los dos enlaces de Internet tienen un alto porcentaje de utilización del canal, lo cual llevaría a la necesidad de incrementar la capacidad de dichos enlaces ya que el incremento de clientes ADSL es constante y en un período de tiempo corto.

Siguiendo con los enlaces de última milla se observa que en la salida por Andinadatos, de igual manera que en los enlaces de Internet se incrementa el uso de estos canales, razón por la cual se debe tomar en cuenta una ampliación de la capacidad para soportar niveles de tráfico acorde al número de usuarios.

Sin embargo tanto en las últimas millas inalámbricas (Stealth y PuntoNet) como en el enlace de usuarios Dial Up (RAS) la capacidad de los enlaces es suficiente para el tráfico que se maneja por ellos, sin necesidad de incrementos.

Enlace	Tráfico total promedio (kbits/s)	Capacidad Total (Kbits/s)	η %
Enlace Andinadatos Cisco 1800	4.124,743	6144	67.13
Enlace Global Crossing Cisco 2600	1.053,196	1792	58.77
CORE: Cisco 3640	2.033,338	4096	49.64
CORE2: Cisco 2600	845,518	2048	41.29
Stealth	1.222,534	7168	17.1
PuntoNet	473,6	5120	9.25
Patton 2996 RAS	115,821	4096	2.83

Tabla 2.31: Rendimiento Enlaces

$$\eta = \frac{trafico\_total}{capacidad\_total} * 100$$

$$\eta = \frac{4124.743}{6144} * 100$$
$$\eta = 67.13$$

La tabla 2.32 presenta el cálculo del porcentaje de utilización de los canales con el tráfico pico referencial obtenido de los anexos B y C.

Enlace	Tráfico Pico (kbits/s)	Capacidad Total (Kbits/s)	η %
Enlace Andinadatos Cisco 1800	9000	6144	146.48
Enlace Global Crossing Cisco 2600	2600	1792	145.08
CORE: Cisco 3640	4500	4096	109.86
CORE2: Cisco 2600	2000	2048	97.65
Stealth	2800	7168	39.06
PuntoNet	2010	5120	39.25
Patton 2996 RAS	300	4096	7.32

Tabla 2.32: Rendimiento Enlaces

Estos datos indican que en los enlaces de salida al Internet (Andinadatos y Global Crossing) y uno de los enlaces de última milla (Core) la utilización del canal sobrepasa la capacidad asociada a éstos. Lo que comprueba que el incremento de capacidad es necesario para estos instantes en los cuales el tráfico se eleva. Si no se cuenta con la capacidad adecuada decrece la calidad del servicio, ocasionando saturación que se refleja en el bajo desempeño del servicio contratado por cada cliente o a su vez en la posible falta de servicio.

En el segundo enlace de última milla (Core2) la ocupación del canal redondea la capacidad completa, en este enlace se debe considerar también el incremento de la capacidad.

En lo que respecta a los dos enlaces de radio (Stealth y PuntoNet) y el enlace de las cuentas Dial-Up (Patton 2996 RAS) la capacidad de los enlaces es suficiente con respecto a la utilización de éstos canales.

Para tener una apreciación de la utilización de los servidores se realizó un monitoreo con ayuda de herramientas del sistema, en este caso se usó el comando ***top*** para obtener mediciones de la utilización de CPU y memoria de cada servidor tomando en cuenta que la utilización varía según el servicio que preste en ese momento el servidor; realizando un promedio de las medidas obtenidas se elabora la tabla 2.33 con los resultados.
El porcentaje de uso de la memoria se obtuvo de la comparación de la memoria utilizada con la capacidad total mostrada en la tabla de características técnicas correspondiente a cada servidor.

Se obtiene como resultado que en promedio el porcentaje de CPU que es utilizado en los servidores no es muy elevado; caso contrario ocurre con la memoria, que aun sin saturar la utilización se tiene un porcentaje elevado.

DISPOSITIVO	UTILIZACIÓN CPU (%)	UTILIZACIÓN MEMORIA (KBITS/S)	η MEMORIA (%)
uio	13.55	177168	67.58
srv1	10.9	424696	81
srv3	18.53	362894	69.21
discovery	15.75	235555	89.85

Tabla 2.33: Rendimiento Servidores

$$\eta = \frac{memoria\_utilizada}{memoria\_total} * 100$$

$$\eta = \frac{173.0156MB}{256MB} * 100$$

$$\eta = 67.58$$

ReadyNet se basa en los servicios prestados al usuario, se debe considerar que para un óptimo desempeño de la red se debe contar con enlaces cuya capacidad sea la necesaria para soportar la sobrecarga ocasional de tráfico, poniendo principal atención en los enlaces de salida a Internet que son los cuellos de botella que presenta esta red.

Los servidores deben ser capaces de procesar de forma inmediata la mayoría de las solicitudes de los clientes.

En cuanto a mantenimiento de los equipos se debería tomar en cuenta el tiempo de vida útil de los dispositivos para migrar a mejores tecnologías y de mayores capacidades manteniendo un nivel de escalabilidad acorde al número de usuarios y servicios.

Se debe mejorar el cableado estructurado ya que la red no cuenta con el debido etiquetado de los puntos para la ubicación de dispositivos y facilitar la administración de conexiones.

Se cuenta con un sistema de administración y gestión como es la herramienta What’s Up, sin embargo se debería incluir otro tipo de herramienta que presente un mayor número de funcionalidades como la obtención de logs y reportes detallados ante cualquier tipo de falla de la red para poder realizar una acción correctiva inmediata y evitar problemas mayores.

En cuanto a políticas de seguridad ReadyNet no posee ningún tipo de documentación sin embargo se tiene un método de seguridad basado en listas de acceso en los ruteadores de borde y acceso.

Las listas de acceso (ACL) se usan para el filtrado de paquetes, entre los ejemplos que podemos mencionar de su utilización se encuentra la protección del puerto 25.

La protección del puerto 25 consiste en permitir a los clientes el envío de correos únicamente por el servidor de salida asignado para dicho cliente por personal técnico de ReadyNet.

Con esto se evita que si clientes envían correo basura toda la red de ReadyNet sea considerada generadora de spam, ya que esto provocaría que los correos de

todos los clientes fuesen clasificados y tratados como spam por otros operadores, llegando incluso a eliminarlos e impedir que lleguen a su destino.

Los clientes cuentan con la opción de la utilización del webmail en caso de que el cliente use las cuentas de correo de ReadyNet fuera de su red asignada.

Ésta medida controla el spam que sale de la red pero no evita que puedan instalarse virus en las PCs; para ello se cuenta las instalaciones de antivirus y se recomienda la revisión de los equipos y de ser necesario dicha revisión la efectúa un técnico de ReadyNet.

Otro método de seguridad empleado por ReadyNet es el control de acceso a equipos de configuración y servicio. El cual es asignado solamente a personal técnico, con su respectiva autenticación por medio de usuario y contraseña. Contraseña que cuenta con dígitos combinados de letras, números y caracteres especiales.

Para el acceso remoto puede realizarse a través de SSH o Telnet desde una conexión de Internet de ReadyNet o desde IPs clasificadas como seguras.

Tomando en cuenta que éstas son medidas que necesita un respaldo se debe considerar la adquisición de un equipo exclusivo para la seguridad, considerando también que el número de usuarios que deben tener acceso a la red es considerable y los protocolos manejados son variados y el tiempo de recuperación en cualquier tipo de falla debe ser casi inmediato.

Por seguridad y para mantener el servicio constante ofrecido por la empresa, ésta cuenta con un sistema UPS (Uninterrumpible Power Supply, Fuente de Poder Ininterrumpido) como una opción de energía en caso de alguna interrupción de la energía eléctrica.

Se cuenta con 10 UPS Prestige 6 KVA. Suministran la energía inmediatamente suspendida la alimentación de la empresa eléctrica con una duración entre 3 a 5 horas, entregada a toda la red de ReadyNet.

Índice	REFERENCIA BIBLIOGRÁFICA CAPÍTULO 2
[1]	Manual Técnico de ReadyNet
[2]	www.Cisco.com - Data Sheet 1992–2001 Cisco Systems, Inc http://www.cisco.com/warp/public/cc/pd/si/casi/ca2950/prodlit/2955s_ds.pdf *Cisco Catalyst 2950* http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1710s_ds.pdf *Router Cisco 1700* http://www.cisco.com/en/US/prod/collateral/routers/ps5853/product_data_sheet0900aecd8016a59b.pdf *Router Cisco 1800* http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd800fa5be.pdf *Router Cisco 2600* http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/34dcm_ds.pdf *Router Cisco 3640*
[3]	http://www.data-connect.com/Patton_2996.htm RAS Patton 2996
[4]	http://www.massivepc.com/switch-advantek-ans08p-puertos-10100mbps-1326-p-1326.html?manufacturers_id=92 SWITCH ADVANTEK ANS-08P 8 PUERTOS 10/100MBPS -1326
[5]	http://www.rflcomms.co.uk/downloads/products/MUSIC%20200.pdf KEYMILE MUSIC 200
[6]	http://tampico.pcdomino.com/page/PROD/CSH-2400.html Switch de 24 puertos Ethernet CNet CSH-2400

CAPÍTULO 3 DISEÑO DE LA RED

Este capítulo presenta el diseño de una Red de Nueva Generación basada en la Arquitectura IMS para la empresa privada ReadyNet, con el cual se busca presentar una solución que mejore los servicios que actualmente brinda la empresa y que pueda tener la opción de incrementarlos a medida que la tecnología presente nuevas prestaciones.

Se ha elegido IMS ya que es una arquitectura acorde a las necesidades tecnológicas de desarrollo en el campo de las redes; ya que en la actualidad se necesita de una red compatible con todo tipo de redes o sistemas ya existentes además de manejar el concepto de convergencia, permitiéndonos tener una red escalable sin necesidad de inversiones futuras excesivas.

3.1 ANÁLISIS DE REQUERIMIENTOS FÍSICOS LÓGICOS Y DE CAPACIDAD

El análisis de requerimientos es una parte fundamental para el diseño de una red, ya que se necesita conocer las características y necesidades de los usuarios para dimensionar una red cuyas especificaciones técnicas permitan cubrir todos los requerimientos de servicios y aplicaciones en niveles altos de calidad de servicio.

3.1.1 SERVICIOS

Una de las principales características de las redes NGN es que facilitan la integración de aplicaciones a la red ofreciendo la posibilidad de acceso a información difícilmente imaginable hace unos años. Permiten la integración efectiva de los servicios, aplicaciones e información de la red en un marco de uso unificado.

A continuación se realizará una breve descripción de los servicios existentes y de aquellos que podrían adicionarse en ReadyNet:

3.1.1.1 Internet

Debido a la naturaleza de la empresa el servicio primordial que ofrece es el Internet, la mayor parte de su tráfico se enfoca a este servicio el cual se proporciona las 24 horas del día, los siete días de la semana.

3.1.1.2 Video Conferencia

El servicio de videoconferencia se ofrece bajo pedido previo del cliente, generalmente se realizan dos video conferencias por mes. Con la nueva red IMS se buscará incrementar este servicio a un número mayor de clientes, los cuales se podrán comunicar en cualquier momento ya que la red tiene la capacidad de soporte de audio, video y datos. Una variante de este servicio es la multi conferencia, es decir entre tres o más protagonistas. En las conferencias se puede realizar presentaciones, compartir aplicaciones, distribuir documentos a los participantes. Todos los medios de audio, datos y video pueden mezclarse dinámicamente según sea necesario durante las conferencias.

El ancho de banda requerido depende del tipo de Videoconferencia si es grupal o sala a sala generalmente se trabaja a velocidades de 64 Kbps (E0) hasta 2048 Mbps (E1), si es videotelefonía, trabaja a 64 Kbps y 128 Kbps, la misma se usa para la comunicación personal o videoconferencia escritorio a escritorio. Este servicio solo será accesible para clientes que contraten un ancho de banda adecuado para proporcionarlo con una calidad aceptable.

3.1.1.3 Correo Electrónico

El servicio de correo permite a los clientes de ReadyNet recibir mensajes desde cualquier dirección e-mail, a través de los protocolos Simple Mail Transfer Protocolo[8] y POP3[9]

---

[8] Simple Mail Transfer Protocol: Protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

[9] POP: Protocolo utilizado en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto

3.1.1.4 Telefonía IP

La telefonía IP es la transmisión de voz previamente convertida a paquete, utilizando la red de datos para efectuar las llamadas telefónicas, lo cual resulta beneficioso para cualquier operador que ofrezca ambos servicios. Debido a que la telefonía es un servicio en tiempo real, se debe proporcionar QoS de manera que la voz no se recorte por pérdida de paquetes o retardo, y que no exista eco.

Para proporcionar un servicio de calidad se debe dimensionar la red tomando en cuenta aspectos como:

- Equipo de usuario
- Llamadas simultáneas
- Verificar que en los equipos elegidos no se produce congestión cuando el número de usuarios incremente, es decir deben ser elegidos pensando en el crecimiento de clientes.
- Determinar el ancho de banda necesario y los retardos
- Que CODECs[10] se usarían

Entre los equipos que el cliente necesita para realizar llamadas a través de una red IP tenemos terminales IP o no IP. Entre los primeros está el teléfono IP, un ordenador multimedia, un fax IP, que entregan y reciben paquetes IP, y entre los segundos está un teléfono convencional, un fax convencional, que necesitan de un dispositivo intermedio que transforma la señal analógica que manejan estos equipos en paquetes IP antes de conectarlos a la red IP de transporte.

Codecs

La elección de un codec es importante en una red integrada de voz y datos ya que proporciona la cancelación del eco y comprime la secuencia de datos, lo que permite un ahorro de ancho de banda. La compresión puede ser parte del

[10] CODEC: describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones.

esquema de codificación (algoritmo) y no necesita compresión digital adicional de las capas superiores o se puede suprimir los silencios, que es el proceso de no enviar los paquetes de voz cuando se detectan silencios en conversaciones humanas.

El codec es un parámetro de alta influencia en la calidad que se presenta al usuario final ya que la VoIP es un servicio en tiempo real por lo que no debe tener retardos significativos, y al estar integrado en un ambiente el ahorro de ancho de banda es primordial.

Entre los parámetros utilizados para la elección de un codec se tiene los siguientes:

- Tasa de bits codificados.- Es la velocidad de muestreo y codificación, la ocupación del ancho de banda del enlace depende de este, mientras mayor sea el valor de la tasa de bits codificados mayor será el ancho de banda.

- Retraso de Algoritmo.- Es la latencia que se produce por la lectura y procesamiento de las cabeceras de las tramas enviadas.

- Complejidad de procesamiento.- Son los recursos requeridos del CPU[11] al procesar las tramas. Los recursos generalmente son el tiempo y el espacio necesarios para el procesamiento.

- Calidad de Conversación.- Depende de aspectos como: la pérdida de paquetes, ruido en la señal y errores en la red de datos.

- Rendimiento de señales que no son de conversación.- Busca fiabilidad en la transmisión/recepción de señales que no son de voz pero se relacionan con la comunicación como tonos DTMF[12], señales de fax y módems, etc.

---

[11] CPU: Unidad Central de Procesamiento. es el componente en una computadora digital que interpreta las instrucciones y procesa los datos contenidos en los programas.

[12] DTMF: Dual-Tone Multi-Frequency. Sistema de marcación por tonos.

Se ha seleccionado el codec G.729 que es usado en la mayoría de aplicaciones de VoIP por que como se observa en la tabla 3.1, opera a una tasa de bits de 8 kbit/s, pero existen variaciones, las cuales suministran también tasas de 6.4 kbit/s y de 11.8 kbit/s que aumenta o disminuye la calidad de la conversación respectivamente.

También es muy común G.729a el cual es compatible con G.729, pero requiere menos procesamiento lo cual afecta en la calidad de la conversación.

El tamaño de la trama está relacionado con la complejidad del procesamiento, afectando directamente al retraso del algoritmo, el codec G.729 usa tramas de tamaño moderado por lo que presenta un procesamiento medio, un consumo de ancho de banda razonable y una calidad de voz aceptable

La tabla muestra algunos de los estándares de codificación utilizados:

Codec	Capacidad	Periodo de Muestreo	Tamaño de Trama	Tramas/ Paquetes	Capacidad Ethernet
G.711	64 kbps	20 ms	160	1	95.2 kbps
G.723.1A (ACELP)	5.3 kbps	30 ms	20	1	26.1 kbps
G.723.1A (MP-MLQ)	6.4 kbps	30 ms	24	1	27.2 kbps
G.726 (ADPCM)	32 kbps	20 ms	80	1	63.2 kbps
G.728 (LD-CELP)	16 kbps	2.5 ms	5	4	78.4 kbps
G.729 *(CS-CELP)	8 kbps	10 ms	10	2	39.2 kbps
G.722.2 (ACELP)	6.6 kbps	20 ms	17	1	38.0 kbps

*G729: es el codec original

G729A o anexo A: es una simplificación de G729 y es compatible con G729. Es menos complejo pero tiene algo menos de calidad.

G729B o anexo B: Es G729 pero con supresión de silencios y no es compatible con las anteriores.

G729AB: Es G729A con supresión de silencios y sería compatible solo con G729B. Aparte de esto G729 (todas las versiones) en general tienen un bit rate de 8Kbps pero existen versiones de 6.4 kbps (anexo D) y 11.4 Kbps (anexo E).

Tabla 3.1: Características de Codecs

3.1.1.5 TELEVISIÓN IP (IPTV)

IPTV (Internet Protocol Television), describe un servicio a través del cual se puede recibir la señal de televisión o vídeo a través de la conexión de banda ancha a Internet.

IPTV al tratarse de imágenes en tiempo real necesita un gran ancho de banda para su correcto funcionamiento (valor que varía entre 1.5 y 6 Mbps) debido a que las imágenes deben llegar sin retraso al usuario.

La solicitud de estos contenidos es personalizada para cada cliente; es decir el usuario seleccionará y recibirá los contenidos solo cuando los solicite pudiendo verlos o descargarlos para almacenarlos en el receptor y de esta manera poder visualizarlos las veces que desee, dando lugar al denominado *pay per view* o el video bajo demanda.

Este es un servicio que amplía las opciones de entretenimiento para los usuarios, además de generar mayores ingresos para los operadores que brinden este servicio aprovechando las infraestructuras existentes.

La convergencia de servicios de datos, voz y video optimiza el rendimiento de la infraestructura del operador y mantiene la atención del cliente en el mismo proveedor, ya que no necesitaría adquirir los distintos servicios por separado.

Figura 3.1: Esquema IPTV[6]

VoD

El Video bajo Demanda (VoD *Video on Demand*) es un servicio que permite a los clientes recibir y reproducir contenidos audiovisuales solicitados explícitamente.

Esta reproducción de contenidos puede ser controlada por los clientes mediante opciones del tipo reproducir, pausa, rebobinado, avance rápido y parada.

Estos contenidos deben ser emitidos desde un servidor de vídeo únicamente hacia el dispositivo que cursó la petición.

Este servicio es interactivo, es decir para las peticiones de servicio y el envío de las órdenes de reproducción es necesario establecer un diálogo entre el cliente y el servidor, para lo cual se utiliza el protocolo RTSP; mediante los mensajes de este protocolo los clientes pueden solicitar un contenido y controlar la reproducción del mismo.

Descripción técnica

La televisión IP ha basado su desarrollado en el *video-streaming* [13]teniendo como requisito primordial para un correcto funcionamiento una conexión a Internet de gran ancho de banda.

En el *video-streaming* se diferencian dos tipos de canal: el de definición estándar SDTV[14] (Standard Definition Televisión) o el de alta definición HDTV[15] (High Definition Televisión).

---

[13] Streaming es un término que se refiere a ver u oír un archivo directamente en una página web sin necesidad de descargarlo antes al ordenador, es la distribución de contenido multimedia a través del Internet.

[14] SDTV señales de televisión (analógicas de 480 líneas) que no se pueden considerar señales de alta definición (HDTV).

[15] HDTV señales televisivas en una calidad digital superior a los demás sistemas (NTSC, SECAM, PAL).

El primer tipo de canal ocupa una conexión de 1.5Mbps y para el segundo canal se necesita 8Mbps.

La tecnología de compresión y codificación de video que se utiliza es MPEG4. Este es un estándar con mayor nivel de compresión que MPEG2, estándar empleado en video-streaming, lo cual favorece cuando el ancho de banda no es de gran capacidad. Por ejemplo con MPEG2[16] (Moving Picture Experts Group 2) el ancho de banda necesario oscila entre 4 y 6 Mbps para un canal SDTV en cambio con MPEG4 únicamente se necesitan los 1.5Mbps.

La tecnología ADSL realiza la transmisión de datos de video, sin embargo tiene limitaciones en lo que respecta a la distancia; trabajando sobre un alcance máximo de 5 Km sobre la cual no se puede ofrecer servicios de televisión. Como solución a este inconveniente los proveedores han considerado la tecnología ADSL 2+, la cual permite una transmisión de información comprimida a mayor distancia y de forma más eficiente y rápida.

Requerimientos Técnicos

A continuación se enumerará los dispositivos necesarios para la implementación del servicio de IPTV:

Servidores de Video: Son la parte fundamental del servicio. En estos equipos se almacenan los contenidos de video (películas, noticias, series, documentales, etc.) en formato digital. Desde el servidor se transmiten los flujos de video hacia los clientes a medida que los solicitan. Cada flujo está conformado por dos tipos de comunicaciones: la primera es la transmisión del video, es de carácter unidireccional (del servidor al cliente) y ocupa gran ancho de banda. El segundo es un diálogo de control mediante el cual el cliente envía sus órdenes al servidor

[16] MPEG es un grupo de trabajo del ISO/IEC encargado de desarrollar estándares de codificación de audio y vídeo.

(*play*, pausa, *stop*, rw, fw, etc.), siendo de carácter bidireccional (los mensajes van en ambos sentidos) para lo cual no se necesita de un gran ancho de banda.

Especificaciones técnicas de los servidores:
Estos servidores deben ser capaces de atender a un gran número de clientes simultáneos. Estos equipos requieren de una gran potencia y de interfaces de red de elevada velocidad de transmisión. Además como los contenidos se codifican con alta calidad de imagen se necesita que los servidores de vídeo dispongan de gran capacidad de almacenamiento. Y equipos basados en arquitecturas multiprocesador para mayor eficiencia.

Filtro de audio *Splitter:* Filtro utilizado para separar la señal vocal de la transmisión de video e Internet.

Módem – router ADSL: Dispositivo que se conecta a la línea telefónica, teniendo un interfaz para la conexión del decodificador. Además se podrá conectar a él un ordenador para el uso del Internet. El tipo de tráfico que cursa por el equipo es IP.

Decodificador digital *STB (set top box):* En IPTV los canales se difunden uno a uno donde el cliente. El usuario requiere del decodificador para el envío de solicitudes al servidor del contenido que desea ver. El decodificador descomprime y decodifica la señal de video para presentarla al usuario.

El servicio de IPTV además puede ser transmitido a los usuarios por medio de su computador, el cual deberá disponer de un programa para la reproducción como *Windows Media.* De este modo el usuario no ocupará el STB para interactuar con el receptor TV debido a que el módem tendrá la misma funcionalidad que este equipo para la PC.

Middleware: Sistema en el cual corre una aplicación utilizada para la administración de los servicios IPTV. Define y coordina la interacción entre los servidores de contenido y los usuarios. El Middleware otorga a los usuarios un

menú gráfico que constituye un portal para el acceso del abonado a los contenidos disponibles (mediante una aplicación cliente que se ejecuta en el STB); este menú está basado en Web.

3.2 PROYECCIONES DE CRECIMIENTO

3.2.1 USUARIOS

Para el análisis en el incremento de usuarios de ReadyNet se contemplarán los años desde 2004 hasta 2007; además de que por usuario se considerará a la cuenta Dial – Up o ADSL y no al número de Terminales que utilizan el servicio con la misma cuenta, como se puede observar en la siguiente tabla:

Año	Dial Up	Dedicados	Totales
2004	452	56	508
2005	418	76	494
2006	369	114	483
2007	295	165	460

Tabla 3.2: Cuentas Usuarios ReadyNet

Como muestra la tabla 3.2, las cuentas Dial – Up van decreciendo. El acceso a Internet por cuenta Dial Up es una tecnología que pierde mercado debido a las nuevas propuestas que el cliente encuentra en la actualidad, por lo que estos usuarios se redireccionan hacia el servicio banda ancha ya que las aplicaciones actuales y futuras demandan un mayor nivel de velocidad. Sin embargo como las cuentas Dial Up aún son utilizadas por clientes que no pueden acceder a otra tecnología o a su vez no tienen interés en la utilización de servicios de banda ancha, para el análisis se mantendrá el número de cuentas existentes en el año 2007.

3.2.1.1 Tasa de Crecimiento

Para determinar el incremento de las cuentas dedicadas se obtiene la tasa de crecimiento correspondiente a los años considerados para el análisis.

La taba 3.3 contiene los porcentajes de crecimiento de los usuarios dedicados correspondientes a cada año. Tomando la información de la tabla 3.5, que corresponde a la tasa de crecimiento por velocidades se realiza un promedio por año para obtener el crecimiento anual, en donde por ejemplo se tiene:

Para el año 2004 – 2005 la tasa de crecimiento tomada de la tabla 3.5 es la siguiente:

AÑO	*64-128 [Kbps]*	*128-256 [Kbps]*	*256-512 [Kbps]*	*1024 [Kbps]*
2004-2005	25,8	50	50	0

De donde se calcula el promedio anual:

$$tasa.de.crecimiento.anual = \frac{25.8 + 50 + 50 + 0}{4} * 100$$

$$tasa.de.crecimiento.anual = 31.5\%$$

Años	*Tasa %*
2004-2005	31,5
2005-2006	49,21
2006-2007	40
Promedio	**40,24**

Tabla 3.3: Crecimiento de Usuarios Dedicados

3.2.1.2 Tasa de Crecimiento por Velocidades

Debido a que no todas las velocidades representan los mismos ingresos, además de la influencia que tiene en los recursos de la red, es importante conocer el crecimiento por cada una de ellas.

La tabla 3.4[17] muestra el número de usuarios agrupados de acuerdo a la capacidad de su servicio.

Capacidad [kbps]	2004	2005	2006	2007
64-128	49	66	90	126
128-256	6	16	19	31
256-512	1	2	3	5
1024	0	0	1	3

Tabla 3.4: Usuarios Dedicados por Capacidad del Canal

Utilizando la información de la tabla 3.4, se tiene que 66 es el número de usuarios en el año 2005 y 49 corresponde al número de usuarios del 2004.

Ejemplo de cálculo:

$$Tasa\_de\_crecimiento = \frac{Usuarios \quad año2 - Usuarios \quad año1}{Usuarios \quad año2} * 100$$

Ecuación 3.1: Crecimiento

El procedimiento que se desarrolló fue la resta de usuarios del año 2005 (66) de los usuarios del año 2004 (49) dividido para los usuarios del año 2005, multiplicado por 100, lo cual dio como resultado la tasa de crecimiento que es igual a 25.75%, el mismo procedimiento se realizó con el resto de años a considerarse. Completando de ésta manera la información de la tabla 3.5.

$$Tasa\_de\_crecimiento = \frac{66 - 49}{66} * 100$$

Tasa de crecimiento anual por velocidad= 25.75%

[17] Esta información se obtuvo de los archivos de ReadyNet, misma que se maneja con alto nivel de confidencialidad por ser datos de gran importancia de la empresa.

AÑO	*64-128 [Kbps]*	*128-256 [Kbps]*	*256-512 [Kbps]*	*1024 [Kbps]*
2004-2005	25,8	50	50	0
2005-2006	27	36,84	33	100
2006-2007	29	24	40	67
Promedio	***27,27***	***36,95***	***41,00***	***55,67***

Tabla 3.5: Tasa de Crecimiento por Velocidades

Esta información como antes se mencionó es utilizada para completar la tabla 3.3 que expone la tasa de crecimiento de los usuarios anualmente.

Las gráficas a continuación muestran el crecimiento de la empresa en los últimos cuatro años. En la figura 3.2 cada barra representa el número de usuarios por ancho de banda contratado en un determinado año, mientras que las gráficas a continuación son una representación del crecimiento por velocidad en el período establecido.

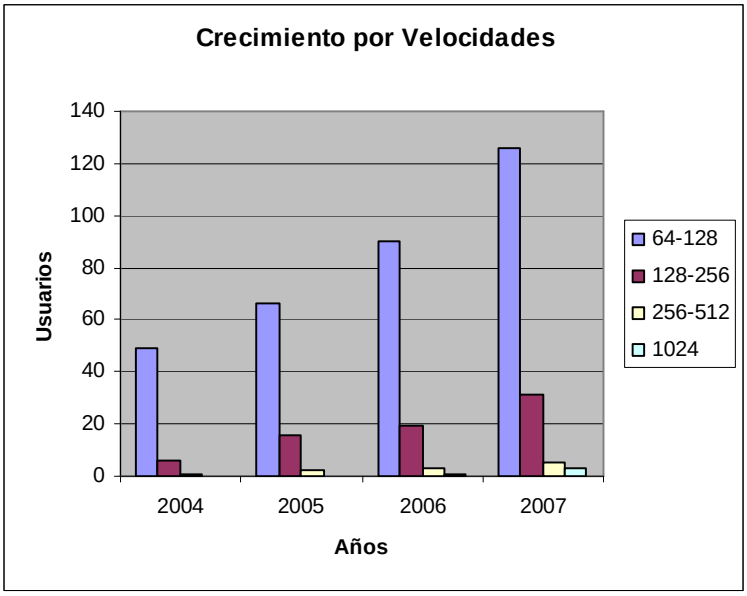


Figura 3.2: Esquema de Crecimiento de Usuarios

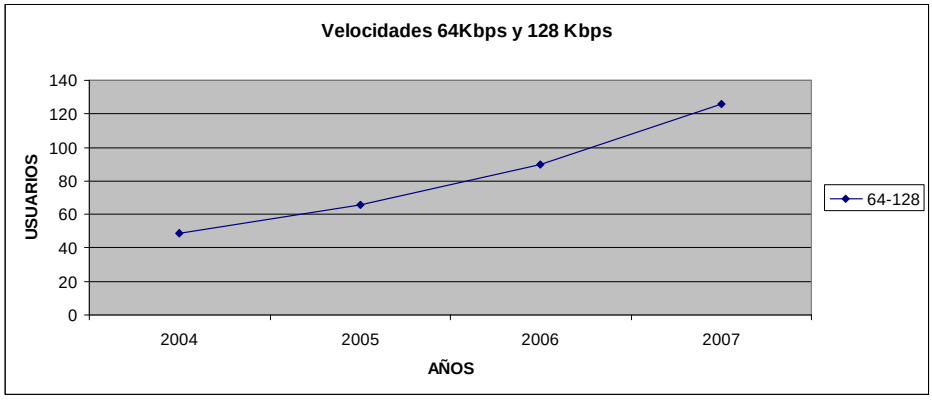


Figura 3. 3: Esquema de Crecimiento Usuarios con Capacidad de Canal 64 -128 Kbps

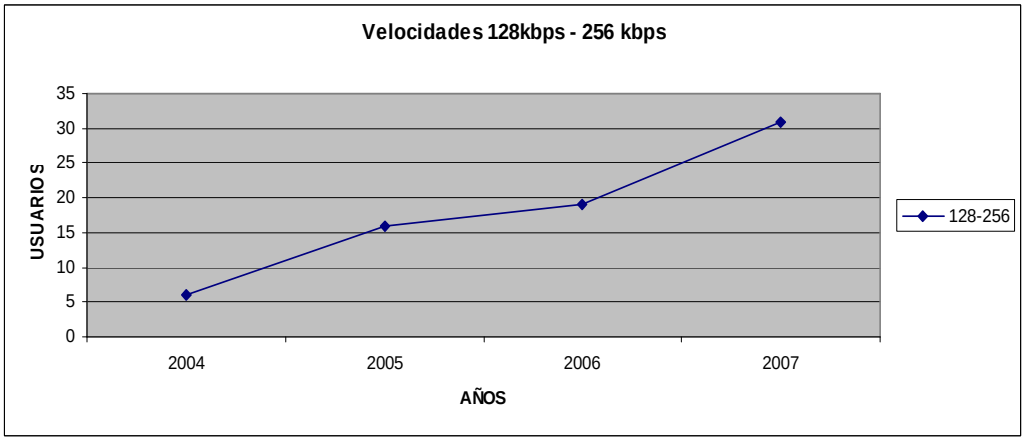


Figura 3.4: Esquema de Crecimiento Usuarios con Capacidad de Canal 128-256 Kbps

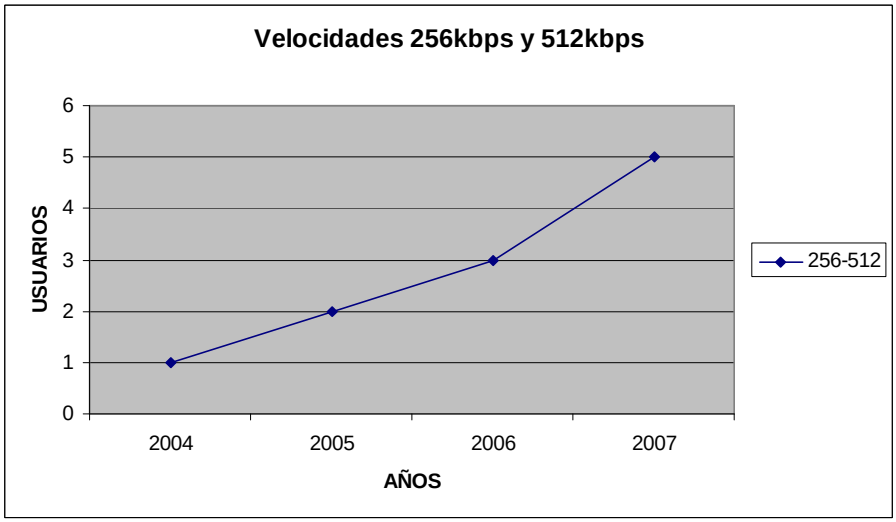


Figura 3.5: Esquema de Crecimiento Usuarios con Capacidad de Canal 256-512 Kbps

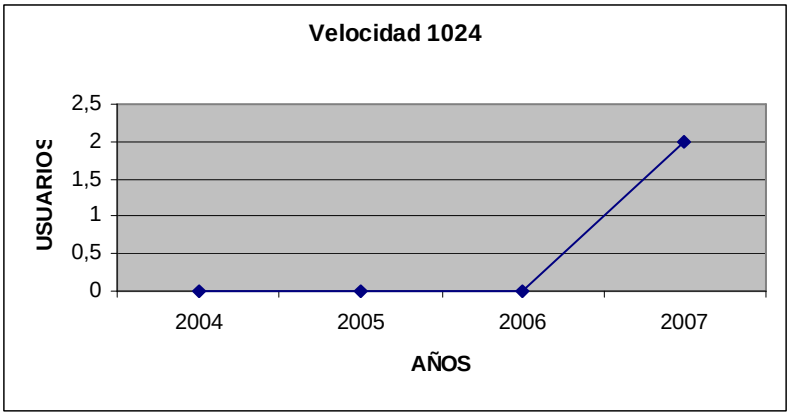


Figura 3.6: Esquema de Crecimiento Usuarios con Capacidad de Canal 1024 Kbps

La tabla 3.6 indica el número posible de clientes que ReadyNet tendría en caso de que la empresa siga con el nivel de crecimiento que mantiene hasta ahora.

Para esta tabla se utiliza la información de las tablas 3.4 y 3.5. En donde se tomó los datos del número de usuarios del año 2007 y la tasa de crecimiento respectiva para cada velocidad.

Por ejemplo el número de usuarios de la velocidad 64-128 Kbps en el año 2007 es de 126 y la tasa de crecimiento promedio respectiva es de 27.27%.

Años	Usuarios 64-128 Kbps	Usuarios 128-256 Kbps	Usuarios 256-512 Kbps	Usuarios 1024 Kbps	Usuarios Totales
2008	160	43	8	5	216
2009	205	59	12	8	284
2010	262	81	17	13	373
2011	334	111	24	21	490
2012	425	152	34	33	644

Tabla 3.6: Número de Usuarios Proyección de Crecimiento por Velocidades

Para lo cual se tiene:

$$Usuarios = 126 * (1 + 0.272)$$
$$usuarios = 160.3$$
$$usuarios.2008 \approx 160$$

3.3 DIMENSIONAMIENTO Y DISEÑO DE LA RED

3.3.1 ANCHO DE BANDA

Previo a este cálculo cabe mencionar que para el manejo de usuarios conmutados, ReadyNet cuenta con un equipo RAS que procesa las llamadas recibidas mediante 2 puertos por los cuales soporta una línea telefónica en cada uno donde se direccionan las llamadas recibidas por la PBX, cada uno de estos puertos está provisto con una capacidad de canal equivalente a un E1 (2048 Kbps) trabajando con tecnología PCM (30 canales de voz y 2 de señalización), capacidad suficiente para el número de usuarios actuales; dicha capacidad se mantendrá ya que como se mencionó el número de usuarios conmutados permanecerá constante para el análisis.

Usuarios Conmutados	Ancho de Banda (Kbps)
295	4096

Tabla 3.7: Ancho de Banda Cuentas Conmutadas

Para el caso de las cuentas dedicadas se toma en cuenta el número estimado de crecimiento de usuarios y se procede a calcular el ancho de banda requerido.

Considerando una simultaneidad del 50% debido a la estimación que se obtiene del tráfico promedio monitoreado (Anexo C y D) en los enlaces de salida a Internet en este ISP.

Se tiene por ejemplo para el año 2008 según el número de usuarios y la respectiva capacidad de subida y bajada lo siguiente:

Tráfico salida = (160*64) + (43*128) +(8*256) + (5*1024) = 22912 Kbps

Tráfico entrada = (160*128) + (43*256) + (8*512) + (5*1024) = 40704 Kbps

AB Total = 22912 + 40704 = 63616 Kbps

AB Simultáneo = 63616*0.5 = 31808 Kbps

Años	Usuarios 64-128 Kbps	Usuarios 128-256 Kbps	Usuarios 256-512 Kbps	Usuarios 1024 Kbps	Tráfico de salida (UL) [Kbps]	Tráfico de entrada (DL) [Kbps]	*AB Total* [Kbps]	*AB Simultáneo* [Kbps]
2008	160	43	8	5	22912	40704	63616	31808
2009	205	59	12	8	31936	55680	87616	43808
2010	262	81	17	13	44800	76288	121088	60544
2011	334	111	24	21	63232	104960	168192	84096
2012	425	152	34	33	89152	144512	233664	116832

Tabla 3.8: Ancho de Banda Cuentas Dedicadas

Llamadas Simultáneas

Para este cálculo se asumirá que solo los clientes dedicados de velocidades mayores a 64/128 accederán a este servicio ya que si se toma parte del ancho de banda contratado para telefonía el Internet se verá afectado. En base a la tabla 3.6 se tiene lo siguiente:

Usuarios telefonía 2008= 43 + 8 + 5 = 56

Años	Potenciales Usuarios de telefonía
2008	56
2009	79
2010	111
2011	156
2012	219

Tabla 3.9: Potenciales usuarios de telefonía

Existen empresas pequeñas, medianas y grandes, " con objetivo de adoptar una terminología común y evitar que cada país realice interpretaciones distintas, la UE ha definido las empresas, atendiendo a su dimensión[18]" , de la siguiente forma:

- 0 empleados (autoempleo)
- 1 a 9 empleados (microempresa)
- 10 a 49 empleados (empresa pequeñas)
- 50 a 249 empleados (empresa mediana)
- 250 a 499 empleados (empresa grande)
- 500 o más empleados (empresa muy grande)

Se considera que los clientes de RedyNet que accedan a telefonía serán en su mayoría pequeñas empresas. "En promedio una pequeña empresa tiene un promedio de 250 llamadas de salida al mes[19]" .

Para determinar el número de llamadas por hora se considera que una empresa trabaja 20 días al mes, ocho horas diarias. Por lo que el número de llamadas por hora será:

$$Tm = \frac{250 llamadas}{mes} * \frac{1 mes}{20} * \frac{1 dia}{8 horas}$$
$$Tm = 1{,}57 \cong 2 \quad llamadas / hora$$

Capacidad de Abonados 2008 POTS Totales= 56
Tiempo Medio de Ocupación (***Tm***) = 120 seg.= 2 min.
Probabilidad de Pérdida de tráfico (B) = 0.1%

---

[18] http://www.lukor.com/not-neg/empresas/0709/21142507.htm ; Clasificación de las empresas

[19] http://www.reseller.com.mx/extras/reseller_13.pdf; **RESELLER** Comunicación Magazine número trece mayo de 2008, Nuevos Planes de Llamadas Locales pág 20.

Aplicando la fórmula de duración media (tiempo medio) ***Tm*** se tiene que:

V: volumen de tráfico.
c: número de comunicaciones
c= 2 (por abonado)
***Tm*=** 120 seg.= 2 min

[*Ecuación 3.2*] $V = Tm * c$

Aplicando la fórmula de intensidad de tráfico (***I***) se obtiene:

[Ecuación 3.3] $I = (Tm * c)/T$

I= (2min*2)/60min = 0.06 Erlang

El tráfico se obtiene multiplicando la intensidad por el número de usuarios.

[Ecuación 3.4] I=56*0.06

I= 3.4 Erlangs

Con el número de erlangs y la probabilidad de tráfico igual a 0.1% se puede determinar la cantidad de circuitos telefónicos necesarios.

Por ejemplo para 56 potenciales usuarios de telefonía que se calcula con 3.4 erlangs de intensidad de tráfico; ubicamos los 3.4 erlangs aproximadamente en el eje horizontal inferior de la tabla y conjuntamente con la probabilidad de tráfico del 0.1% ubicada en el eje vertical de la tabla se observa que aproximadamente se obtiene un total de 11 circuitos telefónicos necesarios para dichos usuarios, cifra situada en el eje horizontal superior. Dichos datos se pueden comprobar en la tabla numérica de ealangs que es más precisa y se muestra en el Anexo H.

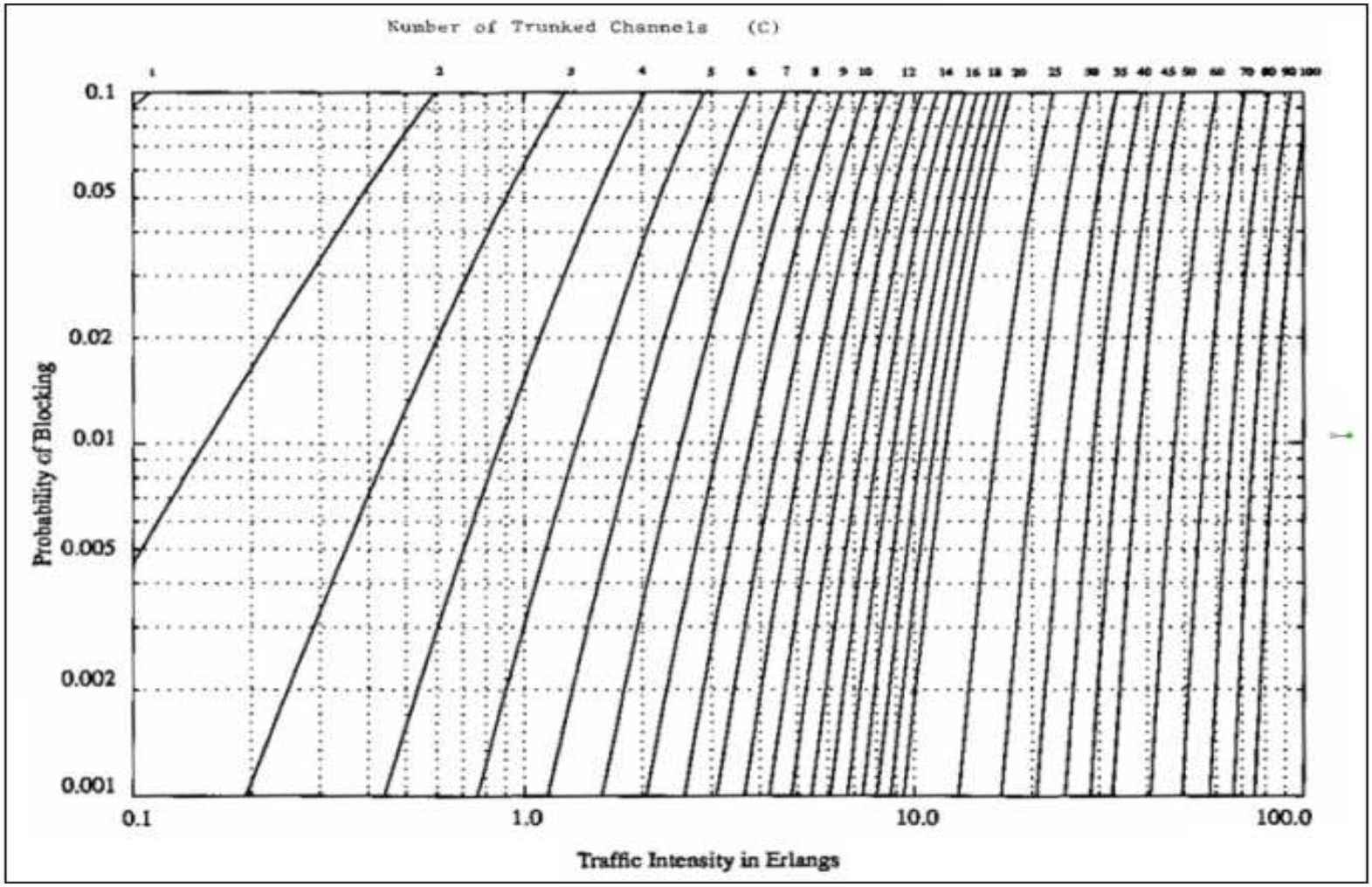


Figura 3.7: Tabla de Erlangs

Por ejemplo para

Años	Potenciales Usuarios de telefonía	Erlangs	Canales
2008	56	3.4	11
2009	79	4.7	14
2010	111	6.7	17
2011	156	9.4	21
2012	219	13.14	25

Tabla 3.10: Canales Telefónicos

3.3.2 TOPOLOGÍA

El diseño realizado conservará la misma topología que posee actualmente Readynet. Ya que posee una topología en estrella, actualmente la topología en anillo es poco usada y la topología en bus no es utiliza por sus limitaciones.

La topología en estrella permite establecer una distribución jerarquizada, en este caso se establecen capas, las cuales tienen bien definidas su función dentro de la red o sistema de comunicación. Las capas principalmente se agrupan en tres tipos: Capa “Core” o núcleo, capa de distribución y capa de acceso.

La capa núcleo agrupa todas las conexiones de la capa de distribución, la capa núcleo suele formarse de equipos de grandes capacidades, gestionables y con manejo de un gran número de protocolos, la capa de acceso es la que permite el contacto con el usuario.

3.3.2.1 Red de Acceso

IMS es una arquitectura que puede comunicarse con diferentes tipos de redes para ello necesita gateways ubicados en las últimas millas, para conexiones XDSL como es el caso de Readynet se requiere en la capa de acceso BAS (Broadband Access Server, Servido de Acceso de Banda Ancha)[20]. Al tratarse de

[20] BAS (Broadband Access Server, Servido de Acceso de Banda Ancha): es un equipo que registra las rutas de tráfico hacia y desde el multiplexor digital de acceso de la línea de abonado (DSLAM) en la red de un proveedor de servicios de Internet (ISP). Tiene funcionalidades de enrutamiento, autenticación y control de tráfico.

una empresa pequeña que no tiene su propia estructura de transporte no debe encontrarse dentro de su red sino en la del Carrier.

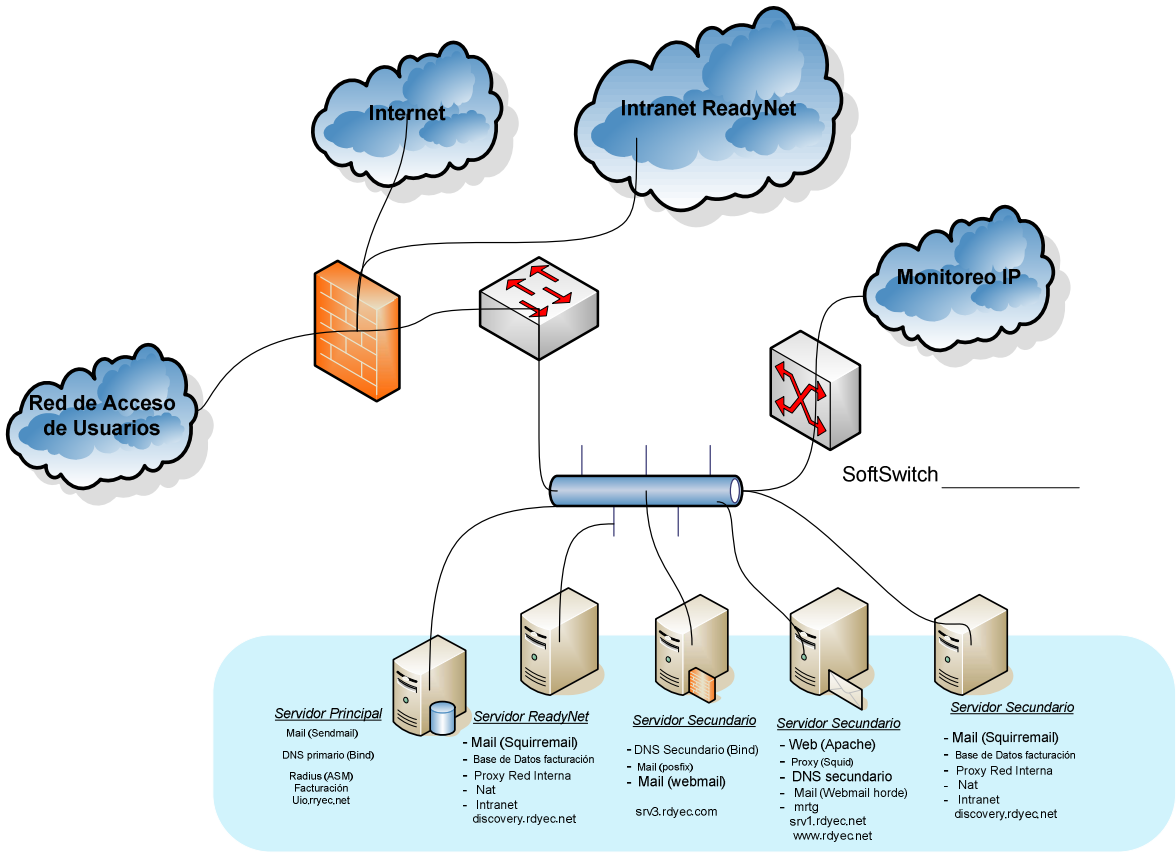


Figura 3.8: Esquema Red ReadyNet

Para otras tecnologías tenemos:

- PDSN (Packet Data Serving Node) [21] para CDMA (Code Division Multiple Access)[22]
- PDG (Packet Data Gateway) [23] para WLAN

---

[21] PDSN (Packet Data Serving Node): interfaz entre la red inalámbrica y la red de datos (IP) que provee el acceso a Internet a los usuarios del sistema CDMA.

[22] CDMA (Code Division Multiple Access): Acceso múltiple por división en código. Métodos de multiplexión o control de acceso al medio basados en la tecnología de espectro difuso o espectro disperso *(spread spectrum)*.

[23] PDG (Packet Data Gateway): realiza la transferencia y enrutamiento de los datos de usuario hacia y desde las redes IP.

- CMTS (Cable Modem Termination System) [24] para Cable
- El caso de EDGE (Enhanced Data rates for GSM Evolution) [25] y UMTS (Universal Mobile Telecommunications System) [26] se requiere de un GGSN (Gateway GPRS Support Node) [27]

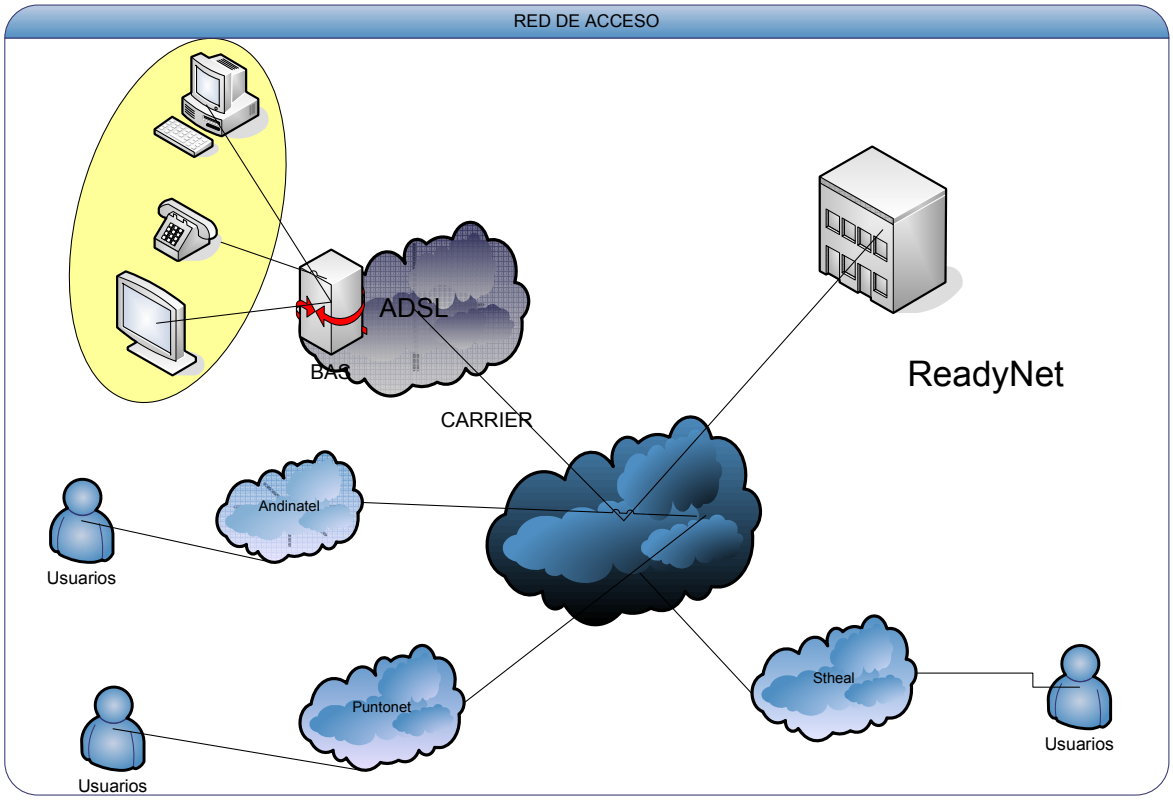


Figura 3.9: Esquema de la Red de Acceso

[24] CMTS (Cable Modem Termination System): equipo encargado de la comunicación con los cablemódems de los abonados. Se utiliza para proporcionar servicios de datos de alta velocidad, como Internet por cable o Voz sobre IP, a los abonados.

[25] EDGE (Enhanced Data rates for GSM Evolution): tecnología que mejora el estándar GSM mediante el uso de codificaciones más avanzadas.

[26] UMTS (Universal Mobile Telecommunications System): sistema de telecomunicaciones móviles universales de tercera generación.

[27] GGSN (Gateway GPRS Support Node): interfaz de GPRS entre la red inalámbrica de datos, Internet o redes privadas.

3.3.2.2 Cableado

Actualmente en su red interna la empresa cuenta con una estructura de cableado categoría 5, este permite en condiciones normales sin mayores problemas tener aplicaciones Fast-Ethernet, telefonía analógica, digital, incluida telefonía IP e incluso con restricciones se puede manejar aplicaciones Gigabit-Ethernet por lo que se podría conservar el cableado. Pero, la nueva Red manejará aplicaciones de mayor ancho de banda que las actuales y debido a que Readynet es una empresa que debe garantizar la calidad de sus aplicaciones y que la tecnología aumenta a pasos agigantados, aumentando el tráfico de datos y la capacidad de transmisión se aconseja tener una red categoría 6A, para contar con un prolongado tiempo de uso y para poder realizar aplicaciones Gigabit Ethernet sin restricciones ya que esta categoría soporta hasta 10 Gigabit.

En el nuevo cableado se debe mantener ciertas consideraciones como:

- Un mínimo radio de curvatura de por lo menos cuatro veces el diámetro del cable
- Evitar el estiramiento excesivo el momento de tender el cable
- Utilizar métodos de apoyo adecuados de acuerdo a la necesidad del punto, como canaleta si recorre por pared o de piso, bandejas o escalerillas sobre sueldo falso,
- Utilizar patch cords adecuado, de acuerdo a las especificaciones del cableado utilizado y la categoría en caso de utilizar cableado categoría 6A el pacth coros deberá corresponder a la misma categoría.
- Evitar que se produzcan anillos en el recorrido, entre otros.

Otro aspecto importante en el cableado es el cuarto de telecomunicaciones, es decir el área de equipos de telecomunicaciones por lo que se recomienda mejorar la ventilación e incorporar un sistema de extinción de incendios y la protección para el equipo.

3.3.3 ANCHO DE BANDA IPTV

Anteriormente se mencionó que el ancho de banda mínimo requerido por contenido en IPTV en un canal de definición estándar SDTV con compresión MPEG 4 es de 1.5 Mbps, siguiendo esta consideración de un solo canal SDTV y tomando un 7% del total de los usuarios como posibles clientes del servicio de IPTV, se calculará una estimación de la capacidad de canal necesario para brindar el servicio. Éste porcentaje fue considerado haciendo un análisis de los clientes con mayor capacidad de canal para el servicio de Internet, velocidades entre 256/128 y 512/256 Kbps, obteniendo el 23% de clientes; adicionalmente a esto se consideró que dentro de este porcentaje la mayoría son clientes empresariales de los cuales sería poco factible que se decidieran por un plan de IPTV razón por la cual se tomó una estimación de entre los usuarios residenciales como posibles clientes correspondiente al mencionado 7%.

Tomando la información de la tabla 3.6, se toma el número total de usuarios del año 2008 que es igual a 216 y obteniendo el 7% de usuarios se obtiene alrededor de 15 potenciales usuarios de IPTV. Obteniendo de esta manera los resultados expuestos en la tabla 3.11.

Adicionalmente para obtener la capacidad se multiplica el número de posibles usuarios por la capacidad requerida, en este caso 1.5Mbps. Por ejemplo 15 usuarios por 1.5 Mbps da como resultado 22.5 Mbps.

Usuarios Totales	Usuarios IPTV	Capacidad [Mbps]
216	15	22.5
284	20	30
373	26	39
490	34	51
644	45	67.5

Tabla 3.11: Capacidad del canal potenciales usuarios IPTV

ReadyNet es un ISP de mediana escala para el cual lo más conveniente sería contratar a un proveedor de video, es decir necesitaría de un operador que suministre el contenido (con la infraestructura que esto implica) y el ISP presta la estructura de acceso a los abonados para la entrega del servicio (*Modelo 'Carrier' de servicios de video).* De esta forma, ReadyNet no realizaría la inversión de equipos que involucra ser el proveedor de video.

Como referencia se presentará el presupuesto para un proveedor de video, para tener una apreciación de lo significativa que es ese tipo de inversión en el Anexo I.

3.4 POLÍTICAS Y SEGURIDAD

Las políticas de seguridad son reglas enfocadas en la realidad de cada empresa, que permiten un control y administración de la información y tecnología con el objetivo de mantener un nivel de seguridad aceptable de la organización. Dichas políticas tienen el carácter de prevención, detección y recuperación frente a los riesgos que amenazan la seguridad empresarial.

Hay que destacar que la realización de las Políticas de Seguridad involucra a varios participantes, tales como: el administrador de la seguridad, gerentes administrativos, jefes departamentales, entre otros. Una vez establecidas las políticas y los procedimientos (manual de procedimientos de seguridad), se necesitarán de nuevos participantes como son: el equipo de respuesta a incidentes de seguridad, quienes serán los encargados de llevar a cabo las tareas correspondientes a cada política; también encontramos a los usuarios, quiénes serán las personas a las cuales deba instruirse para la ejecución, comprensión, la responsabilidad del cumplimiento, y las consecuencia de incumplimiento de las políticas.

Debido a estos aspectos las políticas aquí presentadas servirán únicamente como un lineamiento para la implementación de un Manual de Políticas de Seguridad propio del ISP.

Para la realización de las políticas de seguridad se considerarán como problemas para la seguridad de la organización los siguientes: acceso no autorizado, ataques a los servidores (negación de servicio, suplantación de identidad, etc), virus, spam, entre otros.

La infraestructura se la puede segmentar en cuatro áreas: Red de acceso a Internet, Red de acceso por clientes (últimas millas), Servidores y Servicios, Intranet ReadyNet.

3.4.1 RED DE ACCESO A INTERNET

Políticas

- El acceso a los equipos de conectividad debe ser permitido únicamente a personal técnico del ISP, previa autorización del administrador de red.
- Se debe realizar respaldos periódicos de la información de estos dispositivos en caso de falla del equipo.
- El equipo de conectividad debe contar con normas de seguridad, tanto en configuración como actualizaciones de software, de ser necesario.
- Se debe realizar un control de tráfico que fluye por estos dispositivos.

Propósito

Mantener el acceso restringido a personal autorizado para evitar la intromisión de intrusos hacia la red del ISP. Cuidar los dispositivos para un buen rendimiento de la red. Controlar el tráfico hacia y desde el Internet.

Cobertura

Se aplica al administrador de red y personal del Departamento Técnico, quienes son los únicos autorizados para el ingreso a los equipos de conectividad del backbone de Internet.

Procedimiento

- El administrador de red será el único en emitir la autorización para que el personal técnico pueda ingresar a los routers; el acceso se debe realizar mediante mecanismos seguros y con procedimiento de autenticación

usuario-contraseña, en donde la contraseña debe ser robusta (mínimo 8 caracteres alfa-numéricos).

- El administrador de red es el encargado de mantener los equipos actualizados, control de configuraciones (tener cuidado con las configuraciones por defecto) y sacar los respaldos pertinentes, evaluar si hay necesidad de migración de equipos.
- El administrador de red debe realizar la configuración de ACLs, para poder limitar el tráfico entrante y saliente.

Penalidad

Se realizará evaluaciones periódicas, si se encuentra el incumplimiento de alguna política se realizará una amonestación verbal, posteriormente el pago de una multa previamente establecida.

3.4.2 RED DE ACCESO POR CLIENTES

Políticas

- El ingreso a la red de acceso debe ser permitido únicamente a los clientes del ISP, previa autenticación.
- El tráfico de entrada y de salida deberá ser controlado.
- Los usuarios que acceden a la red serán autenticados, mediante usuario y contraseña.

Propósito

Proporcionar seguridad evitando el acceso no autorizado desde el exterior para evitar la penetración de intrusos que representen una potencial amenaza hacia la red del ISP.

Cobertura

Se aplica a los clientes del ISP, quienes son los únicos autorizados para el ingreso a la red de acceso de los clientes.

Procedimiento

- La autorización de acceso a la red desde el exterior será otorgada por el administrador de red con el mecanismo de seguridad usuario-contraseña.
- En caso de requerir el acceso remoto por parte del personal técnico, deberá ser autorizado por el administrador de la red.
- El tráfico de la red entrante y saliente será monitoreado y controlado por el personal técnico para asegurar que no ingrese tráfico que amenace la seguridad de la red de ReadyNet.
- Debe existir monitoreo constante, para obtener información sobre las posibles violaciones del sistema.

Penalidad

Se realizará evaluaciones y en caso de encontrar el incumplimiento de alguna política se realizará una amonestación verbal.

3.4.3 SERVIDORES Y SERVICIOS

Políticas

- Los servidores deben contar con las actualizaciones de software necesarias para un buen desempeño de los servicios, tener un nivel de seguridad aceptable y una correcta configuración.
- El número de servicios levantados en un mismo servidor debe limitarse lo suficiente para no ocasionar degradación en ninguna prestación.
- Se debe realizar el control de acceso para administración y configuración de los servidores.
- Asignar una DMZ para ubicar a los servidores que necesitan el acceso desde el exterior.
- Monitorear los equipos con el fin de evitar o detectar violaciones de seguridad (spoofing, negación de servicio, etc).
- Realizar respaldos periódicos del sistema para salvaguardar información tanto de la empresa como de los clientes.

Propósito

Tener servidores óptimos para el desempeño de los servicios ofrecidos para el cliente, con un alto nivel de seguridad. Presentar consideraciones necesarias para el acceso a los servidores.

Cobertura

Se aplica al administrador de red y personal del Departamento Técnico, que serán los encargados del mantenimiento de los servidores y demás elementos necesarios para proveer los servicios.

Procedimiento

- La configuración y levantamiento de servicios deben ser efectuados por el administrador de red o a su vez por un técnico calificado para esta función, se debe considerar las capacidades de la máquina para el levantamiento del servicio y evaluar si es posible el levantamiento de más de uno en el mismo equipo, tomar en cuenta la instalación de herramientas adicionales (antivirus, antispam) para la seguridad e integridad de la información.
- La autorización de acceso a los equipos será otorgada por el administrador de red con el mecanismo de seguridad usuario-contraseña (robusta) en sesión segura.
- Los respaldos de los servidores deberán ser almacenados en medios seguros, quizás asignando un equipo específico para este fin.
- La seguridad debe ser respaldada por un equipo tal como un UTM (Unified Threat Management), en donde se pueda designar la zona desmilitarizada (DMZ), además de funcionalidades de analizador de contenido, antispam y antivirus entre otras principalmente para el correo.

Penalidad

Se realizará evaluaciones periódicas, si se encuentra el incumplimiento de alguna política se realizará una amonestación verbal, posteriormente el pago de una multa previamente establecida.

3.4.4 INTRANET READYNET

Políticas

- Existirá monitoreo sobre los sitios Web que el administrador estime relacionado a las necesidades del negocio.
- Se restringirá el uso del Internet de manera que no amenace las actividades de los empleados.
- Se restringirá el acceso a los servidores, de manera que los servicios y aplicaciones que estos proveen se encuentren protegidos de intrusos o personal no autorizado ni calificado.
- Los usuarios no deberán transmitir ningún tipo de información que revele el funcionamiento de la empresa.
- Se deberán cumplir normas de correo electrónico que estipule el grupo de seguridad de la empresa. Como:
    - La prohibición del envío de archivos con extensión .exe que puedan representar una amenaza a la red.
    - Los correos no deberán sobrepasar los 2 MBs salvo excepciones de caso extremo.
    - Se debe actualizar las listas blancas y negras del correo para el control de spam.
    - Mantener un esquema de contraseña seguro se aconseja el uso de letras mayúsculas y minúsculas combinadas con números y símbolos.
    - Se deberá mantener actualizados los correos de la empresa de manera que un ex empleado no pueda dar mal uso de este.

Propósito

Determinar el acceso a los elementos de la red para prestar los diferentes servicios, garantizando el acceso y la confidencialidad de la información.

Cobertura

Se aplicará a todos los empleados de las diferentes áreas de la organización, es decir área técnica, administrativa y ventas.

Procedimiento

- El área técnica será la encargada del monitoreo del tráfico interno de Readynet para que éste no genere amenazas a la red.
- Solo personal autorizado podrá ingresar al cuarto de equipos de la organización.
- El acceso a plataformas de servicio serán mediante aplicaciones que permitan la administración usando protocolos seguros.
- Solo el administrador de la red o usuarios del área técnica con autorización podrán ingresar a la configuración de los equipos.

Penalidad

Se realizará evaluaciones y en caso de encontrar el incumplimiento de alguna política se realizará una amonestación verbal anterior a una multa, si la acción que amenaza la seguridad es realizada con conocimiento de causa podrá ser penada con el despido del cargo.

3.5 ANÁLISIS TÉCNICO DE LOS EQUIPOS

3.5.1 SERVIDORES

Los servidores deben tener las características necesarias para proveer un servicio eficiente y brindar la disponibilidad que los usuarios demandan.

Características Técnicas Servidores

Los servidores deben cumplir con ciertas características técnicas mínimas para un buen desempeño y funcionamiento:

PROCESADOR	Intel Dual Core 3.0 GHz
Memoria RAM	1 GB
Disco duro	SAS , capacidad de acuerdo al servicio mínimo 80 GB
Unidad óptica	CD-ROM 24x o superior
Tarjeta de red [Mbits/s]	2 puertos Ethernet 10/100 Base TX, RJ45
Puertos	Más de un puerto USB 2.0 Puerto para teclado monitor y ratón

Tabla 3.12: Características Técnicas Servidor

Cada servidor tendrá su análisis de criterios para el cálculo de las capacidades de disco duro, ya que de acuerdo a la utilización del servicio que prestan se determina los requerimientos.

Sistema operativo

El sistema operativo de los servidores debe presentar características robustas en cuanto a seguridad, estabilidad, escalabilidad de aplicaciones, rendimiento, entre las más importantes.

La plataforma LINUX es un sistema operativo estable de gran utilización en lo que corresponde al levantamiento de servidores de aplicación. Es un sistema operativo de gran acogida debido a características tales como: es un sistema operativo de código abierto "Open Source" (software distribuido desarrollado libremente) y de licencia libre; es más robusto en cuanto a seguridad, es menos propenso a infecciones de virus ya que estos no se pueden ejecutar debido a que se necesitan los permisos correspondientes para la ejecución de cualquier aplicación.

Los servidores de ReadyNet configurados recientemente trabajan bajo el sistema operativo CentOS (V4.6, Kernel 2.6.9), que ha mostrado características de disponibilidad y confiabilidad permitiendo que los servicios ofrecidos por los servidores de ReadyNet tengan un desempeño óptimo.

Otro factor importante para el buen funcionamiento de un servidor es el hardware; para CentOS las recomendaciones de hardware son: Memoria RAM con un mínimo de 256MB, capacidad de Disco Duro como mínimo de 8 GB.

Correo Electrónico

Para un servidor de correo electrónico, es necesario estimar la capacidad del disco duro en base al número de cuentas de correo y a la capacidad del buzón que se le dará a cada una de ellas.

Se considerará una capacidad de buzón de 50 MB por cuenta de correo ya que RedyNet ofrece dicha capacidad a sus clientes, además se estima que el 50% de los clientes maneja una cuenta de correo administrada en los servidores de ReadyNet ya que no todos los usuarios residenciales adquieren una cuenta y los usuarios corporativos poseen servidores propios.

Tomando en cuenta 8 GB como valor básico para el disco duro, espacio que será utilizado para el sistema operativo, se realiza el cálculo para obtener los requerimientos de disco duro.

Si el buzón de cada usuario es de 50 MB y el 50% de los 216 usuarios totales del año 2008 es de 108 se tiene:
108*50 MB = 5.3 GB.

Adicional a esto se incrementa la capacidad mínima del disco duro se tiene:
8 GB (S.O) + 5.3 GB = 13.3 GB

Año	Usuarios Totales	Usuarios	Capacidad en disco [GB]
2008	216	108	13.3
2009	284	142	14.9
2010	373	187	17.1
2011	490	245	19.9
2012	644	322	21.72

Tabla 3.13: Capacidad en disco del Servidor de Correo Electrónico

Software

Como agente de transporte de correo electrónico se utiliza el software Postfix (MTA, Mail Transfer Agent). Ya que es un software seguro, eficiente, de fácil administración y configuración, compatible con Sendmail, que es otro MTA utilizado en los servidores de ReadyNet.

Adicionalmente brinda soporte para: LDAP[28], Bases de datos (MySQL)[29], autentificación mediante SASL[30], LMTP[31], etc.

Es de fácil integración con antivirus, uso sencillo de listas negras, realiza filtrado de cabeceras y cuerpos de mensajes por expresiones regulares y finalmente gestiona las colas de mensajes.

Además se debe tomar en cuenta herramientas para la seguridad de la información:

Se debe realizar el escaneo de correo entrante y saliente tanto por "asunto", "cuerpo" y "adjunto" con un mínimo de utilización de recursos del sistema.
Tener un filtro de contenido, para tomar acciones frente a mensajes con virus y protección antispam contra envíos masivos.

Tener un Filtro AntiSpam para el bloqueo de correo indeseado basado en direcciones predefinidas, consultas en tiempo real de listas de direcciones

---

[28] LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio.

[29] MySQL: es un sistema de gestión de base de datos relacional multiusuario.

[30] SASL (Simple Authentication and Security Layer): es un framework para autenticación y autorización en protocolos de Internet.

[31] LMTP (Local Mail Transfer Protocol): es un MTA (Mail Delivery Agent) derivado de SMTP utilizado en situaciones donde el lado receptor no dispone de cola de correo.

consideradas como Spam y el análisis de cabecera, asunto y cuerpo para determinar contenido considerado como Spam.

Servidor web

Servidor utilizado para proveer a los usuarios de Internet un sistema de almacenamiento de información, imágenes, vídeo, o cualquier contenido accesible vía Web.

Se realizará una estimación de la capacidad del disco para brindar el alojamiento web, se considerará una capacidad de 125 MB que es lo que ofrece ReadyNet para los clientes que soliciten este servicio, además tomando en cuenta que no todos los clientes solicitan este servicio se considera un porcentaje del 50%, valor estimado de entre clientes de empresas pequeñas que ocupan el hosting, para el cálculo:

Teniendo como base de la capacidad del servidor 8 GB para sistema operativo se efectúa el cálculo de la capacidad del servidor:

El 50% de 216 que es el total de los clientes del año 2008 es igual a 108 usuarios para los cuales se estima una capacidad de 125 MB con un total de 13 GB.

Y sumando la capacidad mínima del S.O. se tiene:
8 GB (S.O) + 13 GB = 21 GB

Año	Usuarios Totales	Usuarios	Capacidad en disco [GB]
2008	216	108	21
2009	284	142	25.2
2010	373	187	30.8
2011	490	245	37.9
2012	644	322	47.3

Tabla 3.14: Capacidad en disco del Servidor Web

Software

El software que se utiliza es Apache 2.2 con PHP 5.1.6 por ventajas que presenta tales como que es un software libre de código abierto para plataformas Unix que constituye un servidor web potente y flexible, posee mensajes de error configurables, bases de datos de autenticación y negociado de contenido, es multi-plataforma.

Servidor FTP

El servidor FTP debe poseer un disco de gran capacidad y poseer gran velocidad. La capacidad empleada para este servidor va acorde con el servidor Web, ya que como este, el servidor FTP es utilizado para el almacenamiento de los programas que ofrece ReadyNet para que los usuarios puedan descargarlos.

Software

El software que se utiliza es **Very Secure FTP Daemon (VSFTPD)** debido a que es un software caracterizado por la seguridad que brinda, es de sencilla configuración y de buen desempeño.

Servidor Cache

El servidor Cache es utilizado para disminuir el tiempo en proveer la información de páginas web (www World Wide Web) a los usuarios mediante el almacenamiento de las páginas visitadas.

Este servidor elimina las páginas no solicitadas cada cierto período de tiempo, y almacena las nuevas peticiones.

Para el cálculo estimado de la capacidad del servidor se considerará un período de 8 horas (horas laborables) con un 70%[3] de tráfico web y un 50%[3] de porcentaje de repetición de peticiones.

Considerando los datos de la tabla 3.8 con la capacidad simultánea total se tiene por ejemplo para el año 2008 una capacidad de canal de 31808 Kbps, en donde da como resultado 3976 KBps.

La cantidad de información transmitida[3] es igual a:
AB [KB/s] * 8[h/día] * [3600s/1h]

Capacidad de disco[3] ≈ Cantidad de información transmitida *0.7*0.5

Ejemplo de cálculo:

$$Inf\_tx = 3976KB * 8 * 3600 = 114508800KB$$
$$Capacidad\_disco = 109.20GB * 0.35 = 38.22GB$$

Se suma adicionalmente la capacidad de disco asumida para el S.O.
8 GB (S.O) + 38.22 GB = 46.22 GB

Año	AB [KBps]	Capacidad en disco [GB]
2008	3976	46.22
2009	5476	60.64
2010	7568	80.75
2011	10512	109.05
2012	14604	148.38

Tabla 3.15: Capacidad en disco del Servidor Cache

Software

El software que se utilizará para la implementación del servidor será *Squid*, ya que es un software de libre distribución (RPM), soporta HTTP y FTP, además de poseer un mecanismo avanzado de autenticación y control de acceso.

Servidor DNS

El servidor DNS es utilizado para resolver peticiones de nombres de dominio, es decir traduce un nombre de dominio en una dirección IP permitiéndonos trabajar con nombres de dominio en lugar de IPs.

La capacidad mínima en disco para un servidor DNS aparte del espacio utilizado para el Sistema Operativo es de un aproximado de 9 GB[3] para almacenamiento de archivos DNS.

Software

Se utilizará una implementación del protocolo DNS como es el software BIND 9.4.1 (Berkeley Internet Name Domain), provee mejores componentes del sistema DNS tales como: un Sistema de Dominio de Nombres, una librería de resolución de nombres y herramientas para verificar la correcta operación del servidor DNS. Además incorporar DNSSEC (DNS Security Extensions), IPv6, entre otras características. Finalmente es una arquitectura estable y robusta.

3.5.2 DISPOSITIVOS DE CONECTIVIDAD

CORE

ReadyNet posee un conmutador como núcleo de red para la interacción entre todos los dispositivos de la red interna.

Este dispositivo debe presentar características de acuerdo al tráfico que se va a manejar en la red, es decir debe estar acorde a la convergencia de servicios que se quiere ofrecer en ReadyNet.

- 48 puertos 10/100/1000 base TX autosensing[32], RJ45
- Al menos 1 Puerto UpLink 1000
- Nivel de conmutación: 2 y 3
- DRAM de 16 MB Memoria
- Flash de 8 MB
- 1 Puerto de consola RJ-45 Asincrónico EIA 232
- 1 puerto auxiliar
- Soporte VLANs y direcciones MAC sobre 8K
- Telnet, SNMP, TFTP, VTP
- STP (Spanning-Tree Protocol, IEEE 802.1D)
- DiffServ (Servicios Diferenciados)
- Puertos half/full duplex
- Manejo de enlaces Trunking
- IPv6

[32] Autosensing: Detección automática de la velocidad de transmisión.

- ACLs L2-L3
- IEEE 802.1x
- Alimentación de energía 120/230V AC (50/60 Hz)
- Soporte VoIP
- Multiservicio (voz, datos y video)

3.5.2.1 SoftSwitch

Figura 3.10 Equipos de Telefonía IP

Introducción

El Softswitch es el componente primordial en la arquitectura de Redes de Próxima Generación (NGN), en la Capa de Control. Es un dispositivo que sirve como plataforma de integración para aplicaciones e intercambio de servicios para redes de conmutación de paquetes y circuitos. Este equipo utiliza estándares abiertos para crear redes integradas capaces de transportar voz, vídeo y datos además de futuros nuevos servicios con gran eficiencia.

La ubicación de un softswitch en la red puede ser de forma distribuida o centralizada. Por ejemplo si la red es amplia se puede distribuir varios softswitches para administrar los diferentes dominios o zonas, además de poder acceder a servicios de manera local o desde otras regiones. En el caso contrario, si la red es pequeña se puede utilizar únicamente dos softswitches (para redundancia). Tomando en cuenta que si se adiciona otro equipo, será útil para mantener baja la latencia cuando la demanda de los clientes aumente.

Arquitectura de Servicios del softswitch

Arquitectura Funcional

Un softswitch está formado por uno o más componentes, en donde sus funciones pueden establecerse en un sistema o distribuirse en varios sistemas. Los componentes más comunes de un softswitch son:

The Gateway Controller (MGC)

Se lo llama también Call Agent. Es la unidad funcional del softswitch, se comunica con los otros elementos del Softswitch y componentes externos usando diferentes protocolos.

Es utilizado como puente entre redes heterogéneas, incluyendo la PSTN (SS7) y redes IP. Este elemento es responsable del manejo del tráfico de voz y datos a través de varias redes.

Requerimientos Funcionales

Algunas de las funciones que el Gateway Controller debe soportar son las siguientes:

- Control de llamada
- Protocolos de establecimiento de llamadas: H.323, SIP
- Protocolos de Control de Media: MGCP, MEGACO H.248
- Control sobre la Calidad y Clase de Servicio.
- Protocolo de Control SS7: SIGTRAN (SS7 sobre IP) y procesamiento SS7 cuando usa SIGTRAN.
- En el enrutamiento soporte para IP, FR, ATM y otras redes.
- Control de manejo del Ancho de Banda.
- Provee para la transmisión de Voz: codificación, compresión y paquetización (Media Gateway)

The Signalling Gateway

Este componente es utilizado como enlace entre la red de señalización SS7 y los nodos manejados por el Softswitch en la red IP bajo el control de MGC.

Adicionalmente es el responsable para ejecutar el establecimiento y desconexión de la llamada. Un Signaling Gateway establece el protocolo, tiempo y requerimiento de las redes SS7, así como las equivalentes funcionalidades de la red IP.

Requerimientos Funcionales

Entre las funciones que este elemento debe soportar tenemos las siguientes:

- Proveer conectividad física para la red SS7 vía T1/E1 o T1/V.35.
- Capaz de transportar información SS7 entre el Gateway Controller y el Signaling Gateway vía red IP.
- Proveer una ruta de transmisión para la voz y opcionalmente para los datos.
- Proveer alta disponibilidad de operación para servicios de telecomunicaciones.

The Media Gateway

Este elemento proporciona el transporte de paquetes de voz, datos y video entre la red IP y la red PSTN. Además es utilizado para las aplicaciones de codificación, decodificación y compresión de voz, así como la interacción con las interfaces PSTN y los protocolos CAS e ISDN.

El Media Gateway consta de un componente denominado DSP (digital signal processors) el cual permite llevar a cabo las funciones de conversión de analógico a digital, los códigos de compresión de audio/video, cancelación del eco, detección del silencio, la señal de salida de DTMF, y la translación de la voz en paquetes para ser tratados por la red IP.

Requerimientos funcionales

Entre las funciones de un Media Gateway se encuentra:

- Realiza la transmisión de los paquetes de voz utilizando como protocolo de transmisión a RTP.
- El Gateway controller administra los recursos del DSP.

- Debe tener la capacidad de escalabilidad tanto en puertos, tarjetas, nodos externos y otros componentes del softswitch.

The Media Server

Este componente mejora las características funcionales del Softswitch. Posee las aplicaciones de procesamiento del medio, esto implica que soporta el funcionamiento del hardware del Digital Signal Processing (DSP).

Requerimientos funcionales

El media Server posee algunos requerimientos funcionales como por ejemplo:

- Funcionalidad básica de voicemail.
- Integrar fax y mail box, dando notificaciones por e-mail o pregrabación de los mensajes.
- Capacidad de videoconferencia por medio de los protocolos H.323 o SIP.
- Unificación de los mensajes de lectura para voice, fax y e-mail por una interface Ethernet.

The Feature Server

Este elemento realiza el control de los datos para la generación de la facturación. Utiliza los recursos y los servicios localizados en los componentes del softswitch.

Es una aplicación a nivel de servidor que incorpora un conjunto de servicios de valor agregado que pueden ser parte de CALL AGENT.

Los protocolos de comunicación entre las aplicaciones y el CALL AGENT son SIP, H.323 y otros.

Entre los servicios que se implementan están:

- H.323 GateKeeper: se encarga del enrutamiento de llamada para cada punto final, puede proveer facturación y control del ancho de banda para el Softswitch.

- VPN: puede establecer redes privadas de voz, en las cuales se puede proveer: ancho de banda dedicado, garantía de Calidad de servicio, plan de marcado privado, transmisión encriptada.

Arquitectura de servicio

Services Targeted.

Este servicio se encarga de la traslación de direcciones, enrutamiento, IVR, llamadas en espera (en el caso de telefonía).

Service Interface.

Esta prestación proporciona soporte para servicios suplementarios y clases de servicios. Es una arquitectura independiente de la señalización ya que soporta protocolos como SIP, H.323, SS7, ISDN, R2.

En resumen un softswitch involucra varios componentes y se deben tomar varias consideraciones como: escalabilidad, confiabilidad del Hardware, disponibilidad, requerimientos de funcionamiento, soporte de múltiples protocolos y el retorno de la Inversión.

A continuación se resume los requerimientos para los cinco componentes del softswitch.

COMPONENTE	**CARACTERÍSTICAS**
GATEWAY CONTROLLER	Capacidades de procesamiento elevadas, escalabilidad y soporte de un amplio rango de protocolos.
MEDIA GATEWAY	Tiempo real de respuesta y disponibilidad remota.
SIGNALING GATEWAY	Escalabilidad IP, T1/E1,SS7. Acceso remoto
MEDIA SERVER	Alto tráfico IP, tiempo real de respuesta, alta disponibilidad, escalable según la demanda.
FEATURE SERVER	Capacidad alta de procesamiento en su mayoría de tráfico IP

Tabla 3.16: Resumen de Requerimientos para los Componentes del Softswitch

Requerimientos técnicos Softswitch

- Al menos un puerto ethernet 10/100/1000 autonegociable
- En preferencia una unidad rackeable

Protocolos

- SIP - H.323
- BGP, etc
- Protocolo de encolamiento y calidad de servicio, protocolo de priorización, 802.1p, 802.1q,

Codecs

- G.723 (LAN), G 729 (WIRELESS), G.726
- robustez del equipo
- Acceso remoto: VPN: PPP, IpSec
- SNMP

Unified Threat Management (UTM)

El UTM describe a un firewall que trabaja a nivel de capa aplicación, y que reúne múltiples funcionalidades en un mismo dispositivo. Entre las funcionalidades que se debe incluir se tiene las siguientes:

- Antispam
- Antiphishing
- Filtro de contenidos
- Antivirus
- Detección/Prevención de Intrusos (IDS/IPS)

El UTM es un dispositivo que ayudará a controlar las comunicaciones entre nuestra red y el exterior, permitiéndolas o prohibiéndolas según las políticas de red.

Se debe tomar en cuenta que los servidores (DNS, Correo, FTP, etc) de la organización que deben permanecer accesibles desde la red exterior deben colocarse en la Zona desmilitarizada o DMZ.

Protección de tráfico:

Capacidad de manejo de redes privadas virtuales (VPNs) del tipo IPSec, SSL, PPTP.

Disponibilidad de algoritmos de encripción 3DES, AES

Debe incluir una licencia para soportar al menos 10 usuarios VPN del tipo SSL

Traslación de direcciones:

Capacidad de conversión de las direcciones de red con NAT en dos vías, estática y dinámicamente.

Conexiones simultáneas por segundo:

Al menos 1.000 conexiones simultáneas por segundo considerando que por cada cliente se tiene al menos 5 peticiones por usuario (pág. Web, descarga de archivos, telefonía, entre otros).

VLANs:

Soporte de al menos 50 VLANs ya que son principalmente utilizadas para priorizar tráfico, por lo que son requeridas en la telefonía.

Puertos o interfaces físicas de cada unidad:

Al menos cuatro (4) puertos 10 / 100 /1000 RJ-45

Un puerto para administración independiente 10 / 100 /1000.

Memoria del sistema:

Al menos 1GB de memoria RAM por cada unidad que conforme el sistema de firewall

Administración:

Soporte de interfaz en línea de comandos (CLI) segura SSH v1 y v2,
Administración por interfaz segura de Web HTTPS

Capacidad de envío de alertas a sistema de consola central

Voltaje:

110 o 220 voltios AC

Equipo montable en rack:

Requerido (no indispensable)

Otras

Funcionalidad de AntiVirus, AntiSpware, File Blocking, AntiSpam, AntiPhising, URL blocking/filtering.

3.5.3 RED DE ACCESO AL CLIENTE

3.5.3.1 Evolución hacia el Nuevo Concepto de NGN.

La red de acceso al cliente se realiza mediante la tecnología xDSL, en la cual se quiere implementar el servicio de telefonía e IpTv además de los servicios de valor agregado que ya ofrece el ISP.

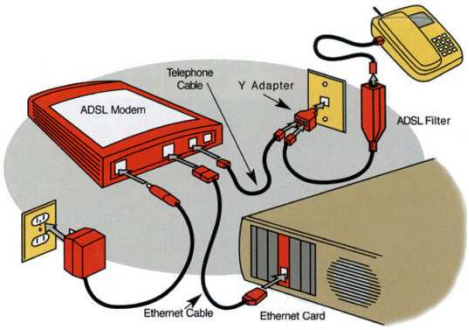


Figura 3.11: Conexión ADSL

El concepto de Redes de Nueva Generación es la convergencia de voz, datos y videos que serán implementados utilizando tecnología IP basada en Packet Switch.

Una de las representaciones de esta generación es la tecnología Softswitch, utilizada para la telefonía, en este modelo la información útil y la señalización se transporta a través del mismo paquete. Los mensajes de SS7 son transmitidos a la red IP y son transportados usando el protocolo TCP, mientras que la voz, datos y video son transportados por la red IP usando el protocolo UDP.

Se puede observar en las figuras 3.12 y 3.13 la evolución que han tenido las redes. Al desarrollarse en una Red de Nueva Generación convergen los tipos de información como son telefonía, datos, video. Se puede observar que la telefonía

convencional está inmersa en esta transformación gracias a Gateways que son la puerta de enlace para la conmutación de la información como paquetes. Las típicas centrales son cambiadas por los ya mencionados Gateways que forman parte fundamental de la arquitectura para poder converger la información pudiendo acceder al Internet sin mayor enrutamiento. A breves rasgos el fin de estas representaciones gráficas es mostrar que tanto voz (IP y convencional), datos, video y el Internet viajan por los equipos de conmutación como paquetes simplificando la infraestructura necesaria para su transporte, mostrando que sin importar el equipo final la información viaja por un mismo tipo de red.

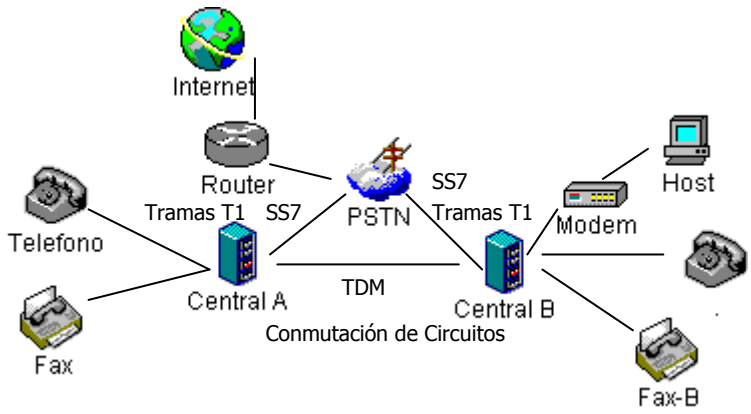


Figura 3.12: Conmutación de Circuitos

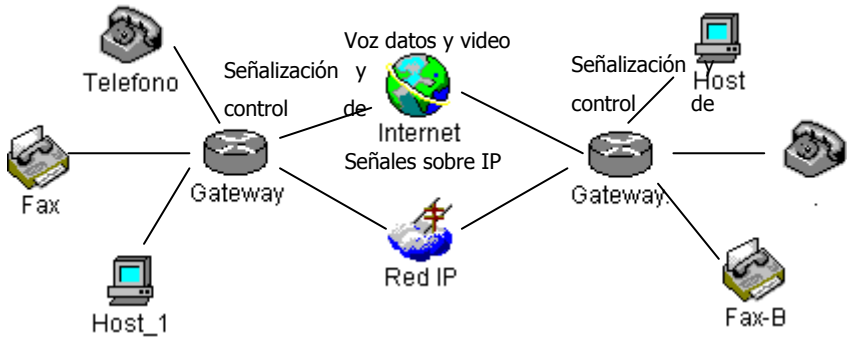


Figura 3.13: Conmutación Paquetes – Próxima Generación

Para la parte de video, el funcionamiento consiste en que la línea de teléfono recibe el canal de voz convencional, un canal de datos ADSL y la señal de televisión IP. El módem establece la conexión ADSL del PC del usuario y envía la señal de TV al decodificador. Pudiendo funcionar ambos servicios independientes,

el usuario puede navegar por el Internet, mientras interactúa con el decodificador para solicitar los contenidos a través de los menús interactivos.

3.6 SELECCIÓN DE EQUIPO

3.6.1 EQUIPOS DE RED REUTILIZABLES

ACCESO A INTERNET

El acceso a Internet, como ya se mencionó anteriormente, se provee mediante dos empresas.

Los routers utilizados para la conexión cuenta con las características básicas y necesarias para soportar la convergencia de servicios, las mismas se detalla en el Anexo. Los equipos mencionados son:

- *Enlace Andinadatos: Cisco 1841*

Entre las más relevantes se puede mencionar:

- Arquitectura Modular: posee gran variedad de opciones para módulos WAN/LAN
- Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, T3/E3, Serial Asíncrono)
- Puertos Ethernet 10/100/ baseTX
- IPv6
- Soporte para protocolos: DES, 3DES, AES.
- QoS
- Multiservicio (voz, datos y video)
- Soporte para VoIP

- Enlace Global Crossing: Cisco 2611

Entre las características que resaltaremos encontramos:

- Arquitectura Modular
- Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, Serial Asíncrono)
- Puertos Ethernet (1o2) 10/100/ baseTX
- Soporte para protocolos: DES, 3DES, AES, GRE, IPSec, RSVP.
- QoS
- Multiservicio (voz, datos y video)
- Soporte para VoIP

ACCESO A ÚLTIMA MILLA

ADSL

Los routers utilizados para la conexión con la última milla poseen las características básicas necesarias para el tratamiento del tráfico generado por la unión de los servicios que se desea implementar (voz, datos, video).

Alguna de las características que se desea detallar de cada equipo se enumeran a continuación.

- *CORE: Cisco 3640*

- Arquitectura Modular
- Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, Serial Asíncrono)
- Multiservicio (voz, datos y video)
- Puerto Ethernet 10/100Base-TX

- ATM, PPP, HDLC, Ethernet, VPN
- Seguridad: encriptación de datos, túneles, y Radius, Tacacs, y AAA.
- QoS
- Soporte VoIP.

- CORE2: Cisco 2620

- Arquitectura Modular
- Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, Serial Asíncrono)
- Puertos Ethernet (1o2) 10/100/ baseTX
- Soporte para protocolos: DES, 3DES, AES, GRE, IPSec, RSVP.
- QoS
- Multiservicio (voz, datos y video)
- Soporte para VoIP

ÚLTIMA MILLA INALÁMBRICA

Lo que respecta a equipos para acceso de última milla inalámbrica, ReadyNet no tiene gestión para el cambio de equipos (router Cisco 1700 y Servidor-router).

Por tanto si se desea que dichos equipos tengan características específicas que no las contengan se debe realizar la solicitud a los proveedores.

DIAL – UP

Servidor de Acceso Remoto (RAS)

El RAS (Remote Access Server) que conforma la red es el equipo Patton 2996. Se mantendrá el equipo ya que su desempeño es muy bueno y suficiente para los usuarios conmutados considerados.

Este servidor de acceso remoto tiene soporte para protocolos específicos para conexiones de entrada y salida (dial-in/dial-out), enrutamiento y seguridad tales como: PPP (Point to Point Protocol, Protocolo Punto a Punto), SLIP, TCP/IP, IPX, NetBEUI, PAP/CHAP, entre otros, además de características especiales. Tienen la funcionalidad de router dado que decide la realización de la conexión remota. El RAS tiene la capacidad de soportar varios tipos de configuraciones de usuario.

Tiene compatibilidad con diferentes tipos de interfaz (RS-232, V.35, RDSI, etc.), en función del tipo de conexiones que tiene la capacidad de establecer.

Realiza la gestión de los enlaces como: llamada automática, rellamada ("dial-back") automática, desconexión del enlace (time-out, por tipo de tráfico, inactividad, etc.), tiempo de conexión, ancho de banda bajo demanda.

Su administración es mediante el protocolo SNMP, cuenta con utilidades de gestión y configuración.

3.6.2 EQUIPOS NUEVOS

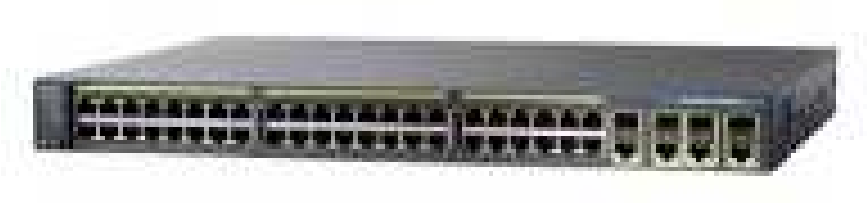
CORE

3Com® Switch 4200G 48-Port

Especificaciones del equipo:

- **Puertos:**
  44 Ethernet 10/100/1000; detección automática, auto-MDI/MDIX; RJ-45 4 pares de puertos Gigabit de uso dual; configurables como 1000BASE-T o SFP
- **Rendimiento:**
  Capacidad de conmutación de hasta 136 Gbps
  Velocidad de transmisión de hasta 101,2 Mpps
- **Conmutación de Nivel 2:** 8.196 direcciones MAC; VLANs basadas en puerto, LACP; protocolo Spanning Tree (STP) y protocolo Rapid Spanning Tree (RSTP); snooping IGMP y filtrado multicast
- **Conmutación de Nivel 3:** routing basado en hardware con 32 rutas estáticas
- **Convergencia:** Ocho colas hardware por puerto; CoS/QoS IEEE 802.1p; asignación automática de VLAN de voz
- **Seguridad:** IEEE 802.1X, ACLs, RADA
- **Administración de 3Com:** 3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite
- **Otro tipo de administración:** CLI mediante consola o Telnet, interfaz de administración web integrada, administración SNMP
- **Alimentador de energía:** 90-240 VAC, 50/60 Hz; 2.0A

CISCO CATALYST 2960G-48TC



- **Puertos:**
  44 Ethernet 10Base-T/100Base-TX/1000Base-T detección automática, auto-MDI/MDIX; RJ-45 half y full duplex.

4x10/100/1000 de uso dual; configurables Base-T/SFP

- **Rendimiento:**
  Capacidad de conmutación de hasta: 32 Gbps
  Velocidad de transmisión de hasta: 39 Mpps
  MTBF: 167.605 horas
  DRAM 64MB
  Flash 32MB

- **Conmutación de Nivel 2:** 8K de entradas direcciones MAC; IEEE 802.3ad (LACP); protocolo Spanning Tree (STP), IEEE 802.1w Rapid Spanning Tree Protocol, Per-VLAN Spanning Tree Plus (PVST+); snooping IGMP
- **Conmutación de Nivel 3:** routing basado en políticas.
- **Convergencia:** CoS/QoS IEEE 802.1p; IEEE 802.1q soporte VLAN
- **Seguridad:** IEEE 802.1X, ACLs
- **Otro tipo de administración:** CLI mediante consola, SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, web browser.
- **Alimentador de energía:** CA 120/230 V (50/60 Hz)
- Dynamic Trunking Protocol (DTP)
- **Cumplimiento de normas:** IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1s, IEEE 802.3ah
- **IPv6**

Ambos dispositivos presentan características similares, el equipo que integrará la red es el Catalyst 2960, ya que se acoplará de mejor forma a la infraestructura por tratarse de una red en su mayoría compuesta de dispositivos Cisco.

Adicionalmente se consideró un switch con características tales como 48 puertos 10/100/1000, ya que se necesita la conexión para los dispositivos de los nuevos servicios que manejan mayor velocidad, además de que se considera ir migrando paulatinamente a una red que maneje completamente interfaces gigabit.

EQUIPO	3COM® SWITCH 4200G 48-PORT	CISCO CATALYST 2960G-48TC
Puertos	44 Ethernet RJ-45 10/100/1000 detección automática 4 pares de puertos Gigabit de uso dual (1000BASE-T o SFP)	44 Ethernet RJ-45 half y full duplex 10Base-T/100Base-TX/1000Base-T detección automática 4x10/100/1000 de uso dual (Base-T/SFP)
Rendimiento	Capacidad de conmutación: 136 Gbps Velocidad de transmisión: 101,2 Mpps	Capacidad de conmutación: 32 Gbps Velocidad de transmisión: 39 Mpps MTBF: 167.605 horas
Conmutación Nivel 2	8.196 direcciones MAC VLANs basadas en puerto protocolo Spanning Tree (STP) protocolo Rapid Spanning Tree (RSTP) snooping IGMP	8K de entradas direcciones MAC Protocolo Spanning Tree (STP) IEEE 802.1w Rapid Spanning Tree Protocol Per-VLAN Spanning Tree Plus (PVST+)snooping IGMP
Conmutación Nivel 3	routing basado en hardware con 32 rutas estáticas	routing basado en políticas
Convergencia	CoS/QoS IEEE 802.1p asignación automática de VLAN de voz	CoS/QoS IEEE 802.1p; IEEE 802.1q soporte VLAN
Seguridad	IEEE 802.1X, ACLs, RADA	IEEE 802.1X, ACLs
Administración	CLI mediante consola o Telnet, interfaz de administración web integrada, administración SNMP	CLI mediante consola, SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, web browser.
IPv6	no especifica	si
Normas		IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1s, IEEE 802.3ah
Características		Dynamic Trunking Protocol (DTP)
Precio ($)	4.354,15	3165

Tabla 3.17: Cuadro Comparativo de Características de Switch

3.6.3 SERVICIO DE VOZ

Cisco PGW 2200 Softswitch

- SIP, H.323, SS7, MGCP.
- G 729, G.726
- SSH, Radius
- SNMP, MIBs
- Administrable CLI, GUI.

CenIP VirtualServer

- Administración de gateways
- Estadísticas de cada gateways
- Administración de destinos vía web o CVS
- Administración de costos vía web o CVS
- Administración de precios vía web o CVS
- LCR (Ruteo inteligente de llamadas)
- Tablas de ruteo estático
- Administración de revendedores
- Gestión de numeración geográfica
- Reportes por gateway
- Reportes por destinos
- Reportes por canal
- Administración de usuarios y seguridad
- Administración de clientes.
- Definición de productos
- Definición de promociones
- Facturación

Protocolos

- SIP - H323 - IAX

Codecs

- G711a/u G729 a/b G726 GSM iLBC

Interfaces

- Interfaz E1/T1 ISDN Pri (opcional)
- Interfaz xFXO (opcional)
- Ethernet 1000 Gbps

EQUIPO	CISCO PGW 2200	CENIP VIRTUALSERVER
Puertos	No especifica en datasheet	Interfaz E1/T1 ISDN Pri (opcional) Interfaz xFXO (opcional) Ethernet 1000 Gbps
Protocolos	SIP, H.323, SS7, MGCP.	SIP, H323, IAX, SS7
Codecs	G 729, G.726	G711a/u G729 a/b G726 GSM iLBC
seguridad	SSH, Radius	No especifica
Administración	CLI, GUI. SNMP, MIBs	GUI
Precio $	80000	15000

Tabla 3.17: Cuadro Comparativo de Características de Softswitch

El dispositivo que se escoge es CenIPVirtualClient ya que esta solución de Telefonía IP está basada en estándares, con arquitectura distribuida y multiprotocolo; se implementan políticas inteligentes de ruteo hasta la administración del cliente final y los servicios de valor agregado del mismo. Tiene una interfaz web amigable y fácil de operar.

Permite la interconexión con las redes actuales y los sistemas de señalización estándares, facilitando la migración ordenada hacia nuevas tecnologías y servicios de valor agregado, basándose en AllIP e Internet.

Presenta soluciones de transporte de voz sobre IP con servicios suplementarios similares a los disponibles en las centrales telefónicas tradicionales.

Incluye soluciones de telefonía residencial y corporativa basadas en diversas tecnologías de acceso IP de última milla.

Tiene una plataforma modular para el procesamiento de voz, siendo escalable, lo que permite satisfacer los requerimientos iniciales y poder ampliar posteriormente su capacidad para adecuarlos a alta densidad de tráfico y servicios.

Adicionalmente posee la Herramienta CenIp Billing, la cual entrega herramientas administrativas de facturación y gestión sin necesidad de hardware o software adicional.

3.6.4 SEGURIDAD

Juniper Networks SSG 520M Series

Capacidad

RAM 1024

Disco duro 80 GB

Número máximo de sesiones simultáneas 128,000

Nuevas sesiones/segundo 10,000

Número máximo de políticas de seguridad 4,000

Interfaces

Interfaces ethernet 4x10/100/1000

Dos puertos USB, un puerto de consola y un puerto Auxiliar

6 Slots para expansión de interfaces modular Serial, T1, E1, DS3, E3, DSL/ADSL2/ADSL2+, G.SHDSL

Interfaces LAN opcionales: 10/100, 10/100/1000, y SFP

Firewall

Detección de ataque de Red

Protección DoS y DDoS

Unified Threat Management

IPS (Deep Inspection firewall)

Detección de Protocolos anómalos

Antivirus, Anti-spyware, Anti-adware, Anti-spam, Filtrado URL

Protocolos escaneados: POP3, HTTP, SMTP, IMAP, FTP, IM

Voice over IP (VoIP) Security

H.323, SIP, MGCP, NAT para protocolos VoIP.

IPSec VPN

VPN simultáneas 500

DES, 3DES, AES, MD-5, SHA-1

IKE, IKEv2 con EAP, PKI (X.509)

Acceso remotoVPN

L2TP incluido IPSec

IPSec NAT traversal

Auto-Connect VPN

Authentication and Control de Acceso

Autenticación: RADIUS, LDAP

802.1X

Routing

BGP, OSPF, RIP v1/v2, Rutas estáticas, enrutamiento basado en políticas, Multicast

IGMP (v1, v2), Multicast incluido en túnel IPSec.

IPv6

Dual stack IPv4/IPv6 firewall y VPN

Traslación y encapsulamiento IPv4 desde/hacia IPv6

Translación de Direcciones

Network Address Translation (NAT)

Port Address Translation (PAT)

Quality of Service (QoS)

Ancho de banda garantizado (políticas)

Máximo ancho de banda (políticas)

Prioridad de utilización de ancho de banda.

DiffServ

Administración del Sistema

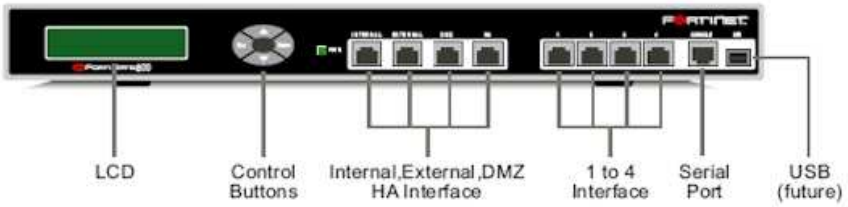
WebUI (HTTP and HTTPS)

CLI (consola), (telnet), (SSH)

NetScreen-Security Manager

Administración vía VPN

***FortiGate*-800**



Capacidad

RAM 1024

Disco duro 80 GB

Firewall Throughput 1Gbps

Número máximo de sesiones simultáneas 400,000

Nuevas sesiones/segundo 10K

Número máximo de políticas de seguridad 20,000

Interfaces

Interfaces Ethernet 4x10/100/1000, configurables.

Interfaces Ethernet 4x10/100/1000 para DMZ

Un puerto de consola, un puerto serial, un puerto USB

Firewall

Detección de ataque de Red

Protección DoS y DDoS

Unified Threat Management

IPS (Deep Inspection firewall)

Detección de Protocolos anómalos

Antivirus, Anti-spyware, Anti-adware, Anti-spam, Filtrado URL

Protocolos escaneados: POP3, HTTP, SMTP, IMAP, FTP, IM y túneles VPN encriptados.

Voice over IP (VoIP) Security

H.323, SIP, NAT para protocolos VoIP.

IPSec VPN

ICSA Labs Certified (IPSec & SSL)

PPTP, IPSec, and SSL

Túneles dedicados

DES, 3DES, AES

Autenticación SHA-1/MD5

PPTP, L2TP,

Certificados de autenticación IKE

IPSec NAT Transversal

Dead Peer Detection

RSA SecurID Support

Authentication and Control de Acceso

Autenticación: RADIUS, LDAP, Active Directory

Routing

BGP, OSPF, RIP v1/v2, IGMP, Multicast, enrutamiento basado en políticas, enrutamiento entre LANs virtuales (VDOMS).

IPv6 n/a

Traslación de Direcciones

Network Address Translation (NAT)

Port Address Translation (PAT)

Quality of Service (QoS)

Ancho de banda garantizado (políticas)

Máximo ancho de banda (políticas)

Prioridad de utilización de ancho de banda.

DiffServ

Administración del Sistema

WebUI (HTTP and HTTPS)

CLI (consola), (telnet), (SSH)

Administración vía VPN

Soporte multi-lenguaje

Central Management vía FortiManager (opcional)

EQUIPO	JUNIPER NETWORKS SSG 520M SERIES	FORTIGATE 800
Capacidad	RAM 1024 Disco duro 80 GB Número máximo de sesiones simultáneas 128,000 Nuevas sesiones/segundo 10K Número máximo de políticas de seguridad 4,000	RAM 1024 Disco duro 80 GB Número máximo de sesiones simultáneas 400,000 Nuevas sesiones/segundo 10K Número máximo de políticas de seguridad 20,000 Firewall Throughput 1Gbps
Interfaces	Interfaces ethernet 4x10/100/1000 Dos puertos USB Puerto de consola y un puerto Auxiliar 6 Slots para expansión de interfaces modular Serial, T1, E1, DS3, E3, DSL/ADSL2/ADSL2+, G.SHDSL Interfaces LAN opcionales: 10/100, 10/100/1000, y SFP	Interfaces ethernet 4x10/100/1000, configurables. Interfaces Ethernet 4x10/100/1000 para DMZ Un puerto de consola, un puerto serial
Firewall	Detección de ataque de Red Protección DoS y DDoS	Detección de ataque de Red Protección DoS y DDoS
Unified Threat Management	IPS (Deep Inspection firewall) Detección de Protocolos anómalos Antivirus, Anti-spyware, Anti-adware, Anti-spam, Filtrado URL Protocolos escaneados: POP3, HTTP, SMTP, IMAP, FTP, IM	IPS (Deep Inspection firewall) Detección de Protocolos anómalos Antivirus, Anti-spyware, Anti-adware, Anti-spam, Filtrado URL Protocolos escaneados: POP3, HTTP, SMTP, IMAP, FTP, IM y túneles VPN .
Voice over IP (VoIP) Security	H.323, SIP, MGCP, NAT para protocolos VoIP	H.323, SIP, NAT para protocolos VoIP.

IPSec VPN	VPN simultáneas 500 DES, 3DES, AES, MD-5, SHA-1 IKE, IKEv2 con EAP, PKI (X.509) Acceso remotoVPN L2TP incluido IPSec IPSec NAT traversal Auto-Connect VPN	ICSA Labs Certified (IPSec & SSL), PPTP, IPSec, and SSL Túneles dedicados DES, 3DES, AES Autenticación SHA-1/MD5 PPTP, L2TP, Certificados de autenticación IPSec NAT Transversal Dead Peer Detection RSA SecurID Support
Authentication and Control de Acceso	Autenticación: RADIUS, LDAP, 802.1X	Autenticación: RADIUS, LDAP, Active Directory
Routing	BGP, OSPF, RIP v1/v2, Rutas estáticas, enrutamiento basado en políticas, Multicast IGMP (v1, v2), Multicast incluido en túnel IPSec	BGP, OSPF, RIP v1/v2, IGMP, Multicast, enrutamiento basado en políticas, enrutamiento entre LANs virtuales (VDOMS).
IPv6	Traslación y encapsulamiento IPv4 desde/hacia IPv6	N/A
Translación de Direcciones	Network Address Translation (NAT) Port Address Translation (PAT)	Network Address Translation (NAT) Port Address Translation (PAT)
Quality of Service (QoS)	Ancho de banda garantizado (políticas) Máximo ancho de banda (políticas) Prioridad de utilización de ancho de banda. DiffServ	Ancho de banda garantizado (políticas) Máximo ancho de banda (políticas) Prioridad de utilización de ancho de banda. DiffServ
Administración del Sistema	WebUI (HTTP and HTTPS) CLI (consola), (telnet), (SSH) NetScreen-Security Manager Administración vía VPN	WebUI (HTTP and HTTPS) CLI (consola), (telnet), (SSH) Administración vía VPN Soporte multi-lenguaje Central Management vía FortiManager (opcional)
Precio	22750	15594

Tabla 3.18: Cuadro Comparativo de Características de UTM

El dispositivo que se utilizará como UTM es Fortigate 800. Se puede apreciar que las características de ambos equipos son bastante similares, sin embargo Foritgate posee un mayor número de sesiones simultáneas, y se puede manejar una mayor cantidad de políticas de seguridad. Presenta puertos exclusivos para el manejo de DMZ, que es una característica bastante útil. Además es un dispositivo que interactúa con plataforma Cisco.

3.6.5 SERVIDORES

Para el número actual de usuarios en ReadyNet, los servidores con los que cuentan se abastecen para las funcionalidades requeridas por los clientes. Así que en cada servidor hay más de un servicio levantado para poder repartir los requerimientos de los abonados así como las aplicaciones complementarias de los servicios (autenticación, facturación, etc):

Correo Electrónico

Para el correo electrónico se cuenta con los siguientes servidores:

- uio.rdyec.net
- srv3.rdyec.com
- smtp.rdyec.net

En donde los dos últimos se encargan de la mayoría de las cuentas de correo de los clientes dedicados, y el primero aloja las cuentas propias del personal de ReadyNet, usuarios conmutados que poseen cuenta, y muy pocos usuarios dedicados (antiguos).

DNS

Como servidores DNS se cuenta con:

- uio.rdyec.net (principal)
- srv1.rdyec.net (secundario)
- srv3.rdyec.com (secundario)

WEB

Para el alojamiento de las páginas web de los clientes se utiliza el servidor:

- srv1.rdyec.net o www.rdyec.net

FTP

Para la transferencia de archivos se puede acceder a los servidores:

- srv1.rdyec.net (principal)
- uio.rdyec.net (secundario)

CACHE

Para servidor caché se tienen los servidores:

- srv1.rdyec.net
- discovery.rdyec.net

En cuanto a las características de hardware los dos últimos servidores que se levantaron: srv3.rdyec.com y smpt.rdyec.net cumplen con las características sugeridas. El resto de servidores varían en algunas de ellas, sin embargo tienen un buen funcionamiento. Dichas características fueron presentadas en el Capítulo 2.

Las características sugeridas serán empleadas en los nuevos servidores que se vayan incrementando o suplantando, de ser necesario, cuando se estime oportuno.

Para realizar la granja de servidores utilizaremos el switch Catalyst 2950, equipo que era utilizado como switch de core, el mismo que tiene características recomendables para un buen manejo del tráfico:

Switch Catalyst 2950

- 24 puertos FastEthernet RJ4510/100base TX autosensing
- Puertos half/full duplex
- 1 Puerto UL 1000base TX fijo
- Nivel de conmutación: 2 y 3
- Backplane sobre 4.8 Gbps., Full Duplex
- Velocidad de conmutación de paquetes de 3.6 Mpps
- Soporte VLANs
- Telnet, SNMP, TFTP, VTP
- STP (Spanning-Tree Protocol, IEEE 802.1D)
- Protocolo IGMP
- IPv6
- IEEE 802.1x
- QoS
- MTBF: 300000 horas, para asegurar gran disponibilidad

A continuación se presenta el diagrama total de la red. Con los equipos adicionales que permitirán a la red utilizar la arquitectura IMS.

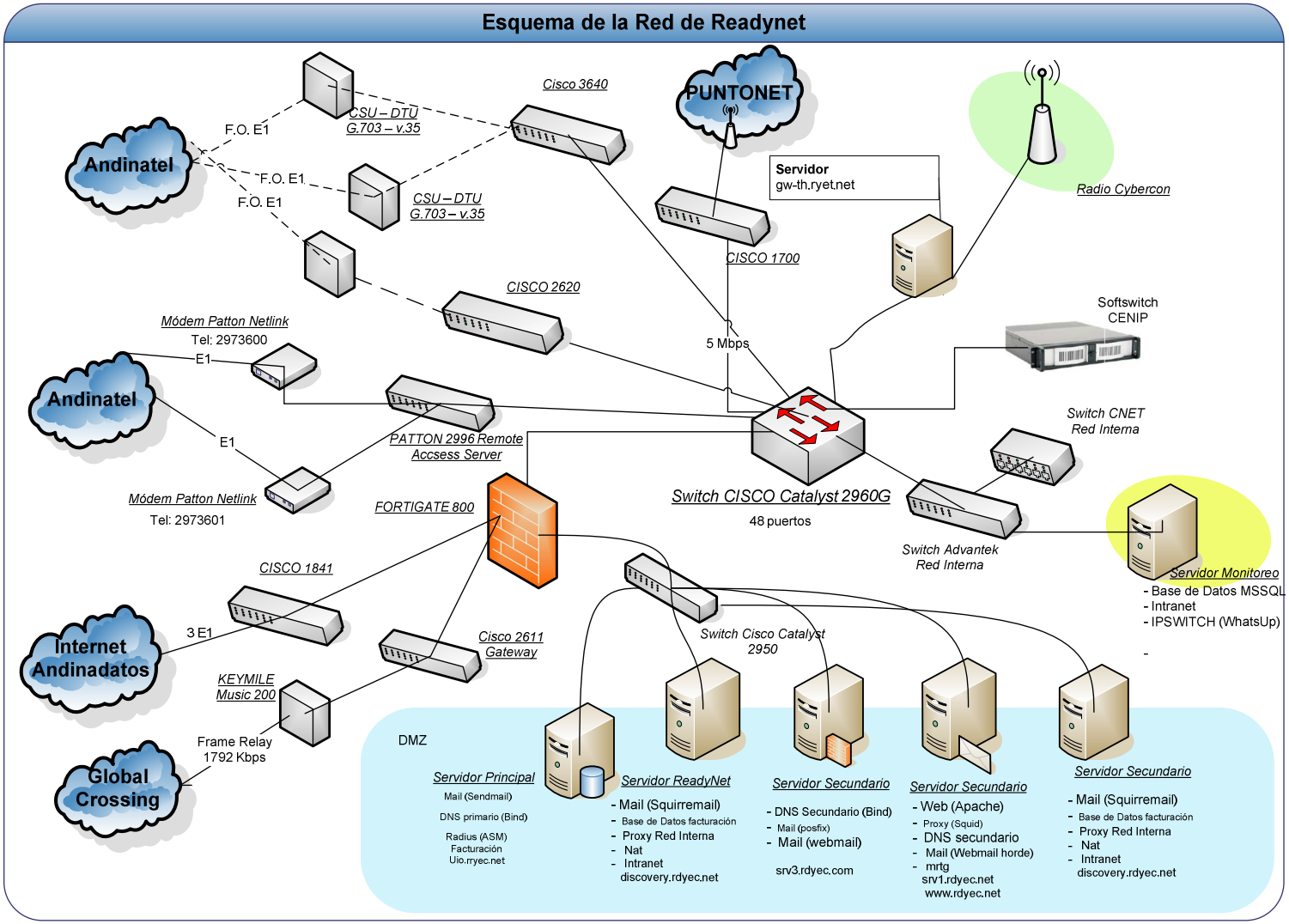


Figura 3.14: Esquema Red ReadyNet

Índice	REFERENCIA BIBLIOGRÁFICA, CAPÍTULO 3
[1]	CEVALLOS Gabriel, TASINTUÑA Luis, “Diseño de una red integrada de voz y datos para el campus e.p.n. Basado en un análisis comparativo de las soluciones existentes en el mercado nacional”, EPN. Quito, Mayo 2007
[2]	www.Cisco.com 1992–2001 Cisco Systems, Inc http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2027/product_data_sheet09186a0080091b59.pdf Cisco PGW 2200 Softswitch http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf Cisco Catalyst 2960
[3]	ROJAS, Franklin; VASQUEZ Carlos “Diseño de un Proveedor de Servicio de Internet (ISP) con Tecnología Frame Relay, Integrando el Servicio de Voz Sobre Ip Y Análisis de Factibilidad para su Posible Implementación”.EPN, Quito Abril 2008
[4]	LALANGUI, Diana; “Diseño en una red para proveer el servicio de video bajo demanda VOD sobre IP”; EPN, Quito Marzo 2008
[5]	LUNA AIZAGA, Elena Paola, “Estudio de factibilidad y diseño de una red que brinde servicios Triple Play en el sector de Pueblo Blanco mediante la implementación de un Access Media Gateway (AMG), que se conectará al softswitch de ANDINATEL S.A”. EPN, Quito 2007
[6]	http://www.3com.com/other/pdfs/products/en_US/3com_400998.pdf 3Com® Switch 4200G Gigabit Family
[7]	http://www.net-alliance.net.ar/prestadores.htm CenIPVirtualServer
[8]	http://www.juniper.net/products/integrated/dsheet/100143.pdf Juniper Networks SSG 500 Series
[9]	http://www.fortinet.com/doc/FGT200_800DS.pdf FortiGate®-200-800 Series

CAPÍTULO 4 ANÁLISIS DE COSTOS

El presente capítulo se presentará un análisis del proyecto en lo que a la inversión se refiere ya que en un proyecto no solo es importante la parte técnica sino también la viabilidad económica que este puede representar por ello se presentará los costos de equipos y elementos para la red, los costos de operación al igual que los ingresos y la inversión que representa.

La empresa tiene ingresos de los diferentes planes que ofrece a sus clientes además ofrece servicios como: levantamiento de servidores y hosting, hora técnica, actualización de páginas web y venta de equipos.

El personal de ReadyNet está constituido por 6 técnicos, 2 vendedores, un contador, 1 mensajeros, 2 guardias, 1 diseñador, 1 recepcionista y el gerente.

Se considera que el impuesto a la renta y a las ganancias extraordinarias es del 25%, la participación a los trabajadores del 15%. Con estos datos se realizará la evaluación financiera.

4.1 INGRESOS Y EGRESOS

4.1.1 INGRESOS

La empresa tiene planes de acuerdo a la tecnología empleada y a la velocidad solicitada a continuación se muestran las tablas de los planes para ADSL y Radio y los respectivos precios, la primera columna indica el plan, la segunda el costo mensual sin IVA y la tercera el costo anual incluido el IVA.

Ejemplo:

El plan 128/164 ADSL cuesta 29.9 mensual para obtener el valor mensual se multiplica por 12 meses que tiene un año y por el 1.12 por el 12 % de IVA.

Plan 128/64 anual con IVA = 29.9*12*1.12 = 401.856

Valor Planes		
Plan	*Costo Mensual Sin IVA (dólares)*	*Costo Anual con IVA (dólares)*
128/64	29,9	401,856
256/128	75	1008
512/256	160	2150,4
1024	400	5376

Tabla 4.1: Planes ADSL

Valor Planes Radio		
Plan	*Costo Mensual sin IVA (dólares)*	*Costo Anual con IVA (dólares)*
64	100	1344
128	160	2150,4
256	220	2956,8
512	380	5107,2

Tabla 4.2: Planes Radio

Las siguientes tablas contienen los usuarios que se proyecta Readynet tendrá en los años indicados en la primero columna. Se ha llenado basado en la información obtenida en el capítulo 2 en el análisis de crecimiento de usuarios.

La tabla 4.3 contiene todos los usuarios dedicados, la tabla 4.4 contiene los usuarios dedicados ADSL y la tabla 4.5 contiene los usuarios dedicados radio. Las tablas especifican los usuarios vs los años, por ejemplo en el año 2009 se estiman 205 usuarios de 64-128 Kbps. En la última columna se puede

observar el número de usuarios de todos los planes para el año que indica la primera columna.

Años	Usuarios 64-128 Kbps	Usuarios 128-256 Kbps	Usuarios 256-512 Kbps	Usuarios 1024 Kbps	Usuarios Totales
2008	160	43	8	5	216
2009	205	59	12	8	284
2010	262	81	17	13	373
2011	334	111	24	21	490
2012	425	152	34	33	644

Tabla 4.3: Clientes por años

usuarios ADSL					
Años	Usuarios 64-128 Kbps	Usuarios 128-256 Kbps	Usuarios 256-512 Kbps	Usuarios 1024 Kbps	Usuarios Totales
2008	128	34	7	4	173
2009	164	47	10	6	227
2010	210	65	14	10	298
2011	267	89	19	17	392
2012	340	122	27	26	515

Tabla 4.4: Usuarios ADSL por año

usuarios radio					
Años	Usuarios 64-128 Kbps	Usuarios 128-256 Kbps	Usuarios 256-512 Kbps	Usuarios 1024 Kbps	Usuarios Totales
2008	32	9	1	1	43
2009	41	12	2	2	57
2010	52	16	3	3	75
2011	67	22	5	4	98
2012	85	30	7	7	129

Tabla 4.5: Usuarios Radio por año

Readynet tiene ingresos por instalación, que es pagado únicamente por los clientes nuevos dedicados, los clientes Dial Up no pagan valor de la instalación, el valor que Readynet cobra por instalación a cualquier plan es de 55 dólares. La tabla 4.6 en la parte superior especifica los años, la primera columna indica las velocidades y las otras columnas los usuarios por velocidad y por año que pagarán instalación.

Ejemplo de cálculo:

En la Tabla 4.3 se tiene para el plan 128/64 en el año 2008, 128 usuarios y en el año 2009 se tendrá 164 es decir 164 – 128 se tendrá 36 usuarios nuevos que pagan instalación en el año 2009.
Si se realiza el cálculo para el resto de planes y se suman tendremos que en el año 2009 se realizarán 52 instalaciones.

instalaciones 2009 = 36+13+3 = 52 instalaciones

Se multiplica por el costo de instalación:

Ingreso x Instalaciones (año 2009) = 52*55 = 2860 dólares

Ingresos por Instalación				
	2009	2010	2011	2012
128/64	36	46	57	73
256/128	13	18	24	33
512/256	3	4	5	8
1024	0	0	0	0
Total Instalaciones	52	68	86	114
Total Ingreso x Ins.(dólares)	**2860**	**3740**	**4730**	**6270**

Tabla 4.6: Ingresos de instalación por año

En base al valor de los planes (tablas 4.1 y 4.2) y a los usuarios (tabla 4.4 y 4.5) se han obtenido los ingresos por año y por plan como se muestra a continuación.

Ejemplo de cálculo:

En el año 2008 se tiene 160 usuarios de 128/64 para el servicio ADSL como se indica en la tabla 4.1 el valor anual con IVA para este plan es de 401.86 dólares, para obtener el ingreso por plan multiplicamos los usuarios por el valor del plan.

Ejemplo:

Ingreso por año (128/64) = 128 usu. * 401,856 dólares/usu.

Ingreso por año (128/64) = 51437,568 dólares

INGRESOS ANUALES POR PLANES					
Plan \ Año	2008 (dólares)	2009 (dólares)	2010 (dólares)	2011 (dólares)	2012 (dólares)
128/64	51437,568	65904,384	84389,76	107295,552	136631,04
256/128	34272	47376	65520	89712	122976
512/256	15052,8	21504	30105,6	40857,6	58060,8
1024	21504	32256	53760	145152	139776
Total por Año	124274,368	169049,384	235785,36	385028,152	459455,84

Tabla 4.7: Ingreso de Servicio ADSL

Para los ingresos por planes de radio se realizó la misma operación:

Ingreso por año (128/64) = 32 usuar. * 1344 dólares/usuar. = 43008 dólares

Ingresos Anuales por Planes de Radio					
Plan \ Año	2008 (dólares)	2009 (dólares)	2010 (dólares)	2011 (dólares)	2012 (dólares)
64	43008	55104	69888	90048	114240
128	19353,6	25804,8	34406,4	47308,8	64512
256	2956,8	5913,6	8870,4	14784	20697,6
520	5107,2	10214,4	15321,6	20428,8	35750,4
Total por Año	72433,6	99045,8	130496,4	174580,6	237212

Tabla 4.8: Ingreso Servicio Radio

Como ya se mencionó antes se mantendrá el número de usuarios Dial Up que es de 460 el costo mensual depende del plan que posea el cliente.

Según datos que actualmente maneja Readynet el 85% de usuarios dial up son ilimitados el 10 % de 15 a 30 horas mensuales y el 5 por ciento restante 15 horas mensuales. El plan ilimitado tiene un costo de 15 dólares el plan de 20 a 30 horas un costo de 10 y de 15 horas un costo de 5 dólares.

Ejemplo:

391 usuarios * 15 dólares*12 = 70380

Dial-Up	Usuarios	Ingreso Anuales (dólares)
85% ilimitado	391	70380
10% 20 - 30horas	46	5520
5% restantes	23	1380
		83720

Tabla 4.9: Ingreso Servicio Dial up

Adicionalmente, la empresa ofrece a sus clientes la venta de equipos como routers módems, switch, no tiene un número aproximado de venta por tipo de equipo pero anualmente obtiene alrededor de 1400 dólares y 6400 dólares por servicio técnico que proporciona a diferentes empresas principalmente a sus clientes.

venta de equipos(dólares)	1400
servicio técnico(dólares)	6400

Tabla 4.10: Ingresos Adicionales

El resultado de sumar todos los ingresos anteriormente obtenidos son los ingresos anuales de la empresa.

Ejemplo para el año 2009 (Año 2)

Instalaciones (tabla 4.15)= 3740 dólares

Usuarios ADSL (tabla 4.16)= 169049,384 dólares

Usuarios Radio (tabla 4.17)= 99045,8 dólares

Usuarios Dial Up (tabla 4.18)= 77280 dólares

Venta de equipos + Serv. técnico (tabla 4.19)= $1400+ $6400= 7800 dólares

Ingreso Año2 = 3740+169049.38+99045.8+77280+7800

Ingreso Año2 = 356915.2

	Año 0	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**
ingresos	0	283438	356915,2	455102	649419	788017,84

Tabla 4.11: Ingresos Anuales

4.1.2 EGRESOS

4.1.2.1 Equipos

Muchos de los equipos que actualmente posee ReadyNet serán reutilizados a continuación se muestran los equipos necesarios para la red IMS que no posee Readynet.

Entre los equipos que esencialmente deben ser obtenidos están el softswich, el UTM para brindar seguridad a la red, un switch.

EQUIPO	**MARCA**	**COSTO (dólares)**
SoftSwith	CISCO	15000
UTM	Fortines	15594
Switch	Cisco	3165
Total		33759

Tabla 4.12: Equipos

4.1.2.2 Costos de Operación

Entre los costos de operación están los egresos por sueldos, en la tabla 4.13 se muestra el número de personas, el cargo que poseen, el sueldo mensual que perciben por su trabajo y el total anual que este representa.

Número	personal	sueldo mensual	total anual
2	vendedores	400	9600
1	Recepcionista	400	4800
1	Gerente General	900	10800
1	Contadora	500	6000
2	Guardias	300	7200
1	Mensajeros	250	3000
6	técnicos	600	43200
1	diseñador	600	7200
	Total	**3950**	**91800**

Tabla 4.13: Personal ReadyNet

Para realizar sus operaciones el personal técnico requiere de ciertas herramientas y materiales que representan gastos para la empresa, en la tabla 4.14 se explica, las diferentes columnas detallan la cantidad anual, el costo unitario y el costo total.

Actualmente el costo por un enlace E1 es de 1100 pero por el tiempo que la empresa trabaja con Anditatel paga un valor de 900, se estima que en el futuro sea menor, pero también bajarán el precio de los planes proporcional a la reducción del costo de un E1. Por ello se realiza los cálculos con este valor.

Basado en la información de la tabla 3.8 en la columna de ancho de banda simultánea se obtiene el número de E1s considerando que un 60% de clientes acepta compartición de canal de 2 a 1.

COSTOS POR HERRAMIENTAS Y MATERIALES			
Nº Item	**HERRAMIENTAS Y MATERIALES**	**COSTO UNITARIO**	**COSTO TOTAL**
4	Juego de herramientas	100	400
12	Cable UTP	110	1320
10	Cable Telefónico	70	700
1000	Conectores RJ45	0,4	400
1000	Conectores RJ11	0,15	150
150	Splitters (Cajetín, Disyuntor, Filtro)	3	450
	TOTAL (USD)		**3370**

Tabla 4.14: Costos herramientas y materiales

Ejemplo :

$$E1 \quad 2008 \quad = \left[\frac{31808Kbps * 0.6}{2} + (31808Kbps * 0.4) \right] \quad \div \quad \frac{2048Kbps}{1E1}$$

$$E1 \quad 2008 \quad = 10.87 \quad \cong 11 \quad E1$$

Costo E1 para el año 2009 = 14E1 * $900 \frac{dólares}{E1 * mes}$ * 12meses = 151200 dólares

Año	2008	2009	2010	2011	2012
Cantidad E1	11 E1	14 E1	19 E1	28 E1	39 E1
Costo (dólares)	118800	151200	205200	302400	421200

Tabla 4.15: Costos de E1

Para dar el servicio y debido a que la mayoría de los clientes tienen la conexión ADSL a través de Andinatel se debe pagar un precio por el uso del

puerto para la transmisión de datos, en la tabla se han calculado este valor de acuerdo a los clientes anuales que ReadyNet tendrá.

Ya que la empresa también proporcionará telefonía se ha calculado el valor del equipo que el cliente requerirá para este servicio

Años	2008	2009	2010	2011	2012
última millas(dólares)	41520	54480	71760	96480	123600
atas(dólares)	1500	2250	3375	4500	12600

Tabla 4.16: Costos de últimas millas, equipos

Con los datos proporcionados por la empresa se realizará un estimado de los gastos de operación de está. Entre estos se tiene la capacitación que la empresa proporciona a sus técnicos, gastos de transporte, servicios básicos como luz, agua y teléfono.

La empresa no realiza a menudo publicidad sus clientes los obtiene a través de sus vendedores, y en ocasiones se da a conocer a través de la radio por lo que el presupuesto asignado para esta actividad es bajo.

Costo de Operación	Costo Mensual (dólares)	Costo Anual (dólares)
Capacitación	100,00	1.200,00
Costos Herramientas y Materiales	280,83	3369,96
Transporte	180	2160
Publicidad	50	600
Personal Planta	7650	91800
Teléfono	1800,00	21600,00
Servicios Básicos	170,00	2040,00
Mantenimiento CC	60,00	720
Personal Planta	7650	91800
Totales	10290,83	123489,96

Tabla 4.17: Costos de Operación

Para su funcionamiento la empresa debe adquirir una licencia la cual tiene un valor de 500 dólares y tiene una duración de 10 años.

Activos nominales	Costo	Tiempo de duración (años)	Costo Anual
LICENCIAS DE FUNCIONAMIENTO	500	10	50

Tabla 4.18: Activos Nominales

Tanto los equipos obtenidos para el proyecto como los que actualmente posee la empresa son considerados activos fijos por lo que se distribuirá su costo a lo largo de su vida útil.

Un equipo de interconectividad tiene una vida útil de 5 años, como los equipos existentes fueron adquiridos hace dos años se consideran que ya han sido depreciados este tiempo por lo que tendrán una vida útil restante de tres años.

Activos fijos	Costo del equipo ($)	tiempo vida (años)	Dep/año
Softswitch	15000	5	3000
UTM	15594	5	3118,8
switch	3165	5	633
Instalaciones complementarias	4260	10	426
Equipos existentes	10000	3	3333,33

Tabla 4.19: Activos Fijos

A continuación se puede observar la depreciación de los equipos en el período considerado.

Para obtener la depreciación del equipo se divide el valor del equipo para el tiempo de vida de este. Por ejemplo el valor del softswitch se divide para 5:

Deprec. Softsw. = $15000/5 = $5000 anuales

Equipo	Año 0 ($)	Año 1 ($)	Año2 ($)	Año3 ($)	Año4 ($)	Año5 ($)
Softswitch		3000	3000	3000	3000	3000
UTM		3119	3119	3119	3119	3119
switch		633	633	633	633	633
Instalaciones complementarias		852	852	852	852	852
Equipos existentes		3333,33	3333,33	3333,33	0	0
Softswitch		0	0	0	0	0
depreciación	0	10937,133	10937,13333	10937,133	7603,8	7603,8

Tabla 4.20: Depreciación

4.1.2.3 Equipamiento e instalaciones complementarias

Como se explico en el capítulo 3 se debería adquirir un sistema de aire para los equipos, además se debería considerar el cambio del cableado estructurado. La tabla 4.21 muestra el costo que significaría estos cambios.

INSTALACIONES COMPLEMENTARIAS			
COMPONENTE	**DESCRIPCION**	**CANTIDAD**	**PRECIO**
Instalaciones cableado estructurado.	Completa	**30 puntos de cableado**	**$ 2160**
Sistema de aire	Equipo para control de humedad y temperatura	**1**	**$ 1200**
Total			**$ 3 360**

Tabla 4.21: Instalaciones

Una vez detallados los gastos del proyecto podemos obtener los costos por año que este representaría la operación de la empresa.

Ejemplo :

Año 1 = Costos de Operación + costos de enlaces+costos de última milla y quipo de usuario

Año1 = $123489.96+$118800+$43020 = 285309.96 dólares

Año 0	Año 1	Año2	Año3	Año4	Año5
116040,00	116040,00	285309,96	331419,96	403824,96	526869,96

Tabla 4.22: Egresos anuales

4.2 ANÁLISIS DE RIESGO E INCERTIDUMBRE

Existen varios métodos o modelos de valoración de inversiones se usará los tres métodos indicados a continuación:

- El método de Flujo Neto
- El valor Actual Neto (V.A.N.)
- La Tasa de Rentabilidad Interna (T.I.R)

Estos métodos son complementarios, ya visualizan aspectos diferentes y al usarlos conjuntamente, contemplan una visión más amplia de la posibilidad de inversión.

El proyecto requiere del costo de los equipos nuevos ya que actualmente la empresa ya se encuentra en funcionamiento, para ello se cuenta con un capital del 20% del total, por lo que el 80% deberá ser financiado por una institución bancaria, por lo que previo al flujo de fondos se realizará el análisis del financiamiento, calculando la tabla de amortización de acuerdo a los parámetros actuales indicados en la siguiente tabla.

Costo del Proyecto	$ 38.519
Financiamiento	80%
Monto del préstamo	$ 30.815
Número de pagos	5
tasa nominal	14%
# capitalizaciones	12
tasa efectiva	14,934%
n periodos	5
Inversión	$ 7.704

Tabla 4.23: Parámetros de inversión

Periodo	Saldo inicial	Pago de capital	Pago de interés	Pago total	Saldo final
1	$ 30.815	$ 4.576,33	$ 4.602,00	$ 9.178,34	$ 26.238,87
2	$ 26.238,87	$ 5.259,77	$ 3.918,57	$ 9.178,34	$ 20.979,10
3	$ 20.979,10	$ 6.045,28	$ 3.133,06	$ 9.178,34	$ 14.933,82
4	$ 14.933,82	$ 6.948,09	$ 2.230,25	$ 9.178,34	$ 7.985,73
5	$ 7.985,73	$ 7.985,73	$ 1.192,61	$ 9.178,34	$ 0,00

Tabla 4.24: Tabla de amortización

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Pago interés	0	$ 4.602,00	$ 3.918,57	$ 3.133,06	$ 2.230,25	$ 1.192,61
Pago Capital	0	$ 4.576,33	$ 5.259,77	$ 6.045,28	$ 6.948,09	$ 7.985,73

Tabla 4.25: Interés y capital anual

4.2.1 FLUJO DE FONDOS

A continuación en la tabla 4.26 se observa todos los flujos netos de cajas del proyecto, como son los ingresos de operación, los costos de operación, los activos fijos, la inversión, los créditos entre otros.

La primera columna indica la operación (suma o resta) que se realizará con los datos para obtener el flujo de fondos, en la primera fila se tiene los ingresos anuales (tabla 4.11), la segunda fila son los egresos (tabla 4.22) y las filas de depreciación se refiere al valor que los equipos tendrán en la los diferentes periodos (tabla 4.20).

El pago de interés por los créditos recibidos y el pago del capital se pueden visualizar en la tabla 4.25.

La utilidad antes de la participación de impuestos es los ingresos de operación, menos los costos de operación, menos la depreciación y reduciendo el pago de interés por los créditos recibidos.

La participación a trabajadores es el 15% de las utilidades por ejemplo en el año2 se tiene una utilidad de 10639,52 el 15% sería 1595,93, esta será igual a cero en caso que la utilidad antes de la participación a trabajadores sea menor a cero por ejemplo el año uno.

La utilidad antes de los impuestos se obtiene de los dos campos previos, por ejemplo para el año 2 se tiene:

$10639.52- $1595.93 = $9043.60

Al igual que la participación a trabajadores si la utilidad antes de la participación e impuestos es menor a cero el impuesto a la renta será igual a cero. Por ejemplo el año 1, mientras que para el año 2 el impuesto a la renta es el 25 % de la utilidad antes de la participación e impuestos, al restar estos dos valores, según el signo de la primera columna, se obtiene la utilidad neta.

Por ejemplo para el año 2 :

$9043.6-$2260.9 = $6782.7

El capital de trabajo y la recuperación del capital de trabajo es el monto con el que contaba la empresa para la inversión, en el primero se ubica en el año cero con signo negativo mientras que el segundo solo en el último período con signo positivo, en este caso es igual al 20% de lo requerido 7703,80.

Después de obtener la utilidad neta se realiza las operaciones indicadas en la primera columna de las siguientes filas para obtener el flujo neto.

Por ejemplo para el año dos se tiene:

Flujo neto año2 = $6782,70 + $10937,13 - $ 5.259,77 = $**12460,06**

Signo		año 0	año1	año 2	año3	año4	año5
+	Ingresos de operación	0,00	283437,97	356915,18	455101,76	649418,75	788017,84
-	costos de operación	116040,00	285309,96	331419,96	403824,96	526869,96	680889,96
-	Depreciación	0,00	10937,13	10937,13	10937,13	7603,80	7603,80
-	Amortización de activos diferidos	0,00	0,00	0,00	0,00	0,00	0,00
-	**Pago de interés por los créditos recibidos**	0,00	4602,00	3918,57	3133,06	2230,25	1192,61
	Utilidad Antes de participación e impuestos	-116040,00	-17411,13	10639,52	37206,61	112714,74	98331,47
-	Participación a trabajadores (15% de la utilidad)	0,00	0,00	1595,93	5580,99	16907,21	14749,72
	Utilidad antes de impuestos	-116040,00	-17411,13	9043,60	31625,61	95807,53	83581,75
-	Impuesto a la circulación de capitales (% de los impuestos totales)	0,00	0,00	0,00	0,00	0,00	0,00
	Utilidad antes del impuesto a la renta	-116040,00	-17411,13	9043,60	31625,61	95807,53	83581,75
-	Impuesto a la renta (25%)	0,00	0,00	2260,90	7906,40	23951,88	20895,44
	Utilidad Neta	-116040,00	-17411,13	6782,70	23719,21	71855,65	62686,32
+	Utilidad en venta de activos (Valor de Venta - valor en libros				0,00		0,00
-	Impuesto a la utilidad en venta de libros				0,00	0	0,00
+	Ingresos no gravables						
-	Costo de operación no deducibles						
+	valor en libros de los activos vendidos						
+	depreciación	0,00	10937,13	10937,13	10937,13	7603,80	7603,80
+	amortización de activos diferidos	0,00	0,00	0,00	0,00	0,00	0,00
-	Costo de inversión		0,00	0,00	0,00	0,00	0,00
-	Capital del trabajo	7703,80					
+	recuperación del capital de trabajo						7703,80
+	**Crédito recibido**	30815,20					
-	**Pago de capita(amortización)**	0	$ 4.576,33	$ 5.259,77	$ 6.045,28	$ 6.948,09	$ 7.985,73
	FLUJO DE FONDOS PURO	**-92928,60**	**-11050,33**	**12460,06**	**28611,07**	**72511,36**	**70008,18**

Tabla 4.26: Flujo de Fondos

4.2.2 VALOR ACTUAL NETO

El Valor Actual Neto representa un equivalente de los ingresos netos futuros y presentes del proyecto para realizar el análisis del resultado existen tres alternativas:

- Si el VAN > 0 el proyecto debe ser aceptado
- Si el VAN = 0 para la empresa es igual si se realiza o no el proyecto
- Si el VAN < 0 el proyecto no vale la pena debe ser rechazado, resulta mejor invertir en otro.

Para realizar el cálculo se utiliza la siguiente fórmula:

$$VAN = -Io + \sum_{i=1}^{4}\left[\frac{FlujoNeto_i}{(1+r)^i}\right]$$

$$VAN = -35862{,}3 + \sum_{i=1}^{4}\left[\frac{FN_i}{(1+0{,}10)^i}\right]$$

Donde:

Io = Inversión inicial.

FN = Flujo Neto

I = Vida útil

r = Tasa de interés

4.2.3 TASA INTERNA DE RETORNO

Es te método devuelve la tasa interna de retorno de los flujos de caja ocurridos anualmente.

Lo definen como la tasa de interés que hace que el Valor actual de retorno sea igual a cero, su resultado depende del flujo de fondos y para el análisis de su resultado también depende de tres aspectos:

- TIR > d Rentable
- TIR < d no rentable
- TIR = d indiferente

d representa el costo de oportunidad del dinero si no se invierte en el proyecto.

$$0 = -Io + \sum_{i=1}^{4}\left[\frac{FlujoNeto_i}{(1+r)^i}\right]$$

$$0 = -35862{,}3 + \sum_{i=1}^{4}\left[\frac{FN_i}{(1+0{,}10)^i}\right]$$

Donde:

Io = Inversión inicial

FN= Flujo Neto

I = vida útil.

Se consideró una tasa de interés actual del 14% para calcular los indicadores:

Con el flujo de fondos puro y con ayuda del Excel (funciones TIR, VNA) se obtiene el valor del VAN y el TIR:

TIR	16%
VAN	5.570,00
tasa de oportunidad top	14%

Tabla 4.27: Resumen

Como se indicó un proyecto es viable con un van mayor a 1 que es este caso pero si observamos los valores del TIR y de la tasa de oportunidad que para este caso es la tasa interés, la diferencia es del 2 % no es mucho, lo que significa que en caso de realizarse el proyecto los beneficios serán mínimos.

Índice	REFERENCIA BIBLIOGRÁFICA, CAPÍTULO 4
[1]	SANCHEZ, Tarquino; “Folleto de Gestión y Evaluación de Proyectos”; EPN, Quito 2007
[2]	www.bce.fin.ec Banco Central del Ecuador Tasa de Interés

CAPÍTULO 5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

* Las diferencias existentes entre el tráfico de voz y datos, han dado lugar a que tradicionalmente sean manejados por redes diferentes sin que ninguna de éstas puedan aprovechar al máximo la infraestructura. Con las Redes IMS se busca manejar diferentes tipos de tráfico como voz, datos y video en una única red conservando las características que cada uno requiere. IMS nace para redes inalámbricas y en la actualidad varios organismos de estandarización han normando la arquitectura para redes fijas.

* En el mercado de las telecomunicaciones es de suma importancia la rapidez, seguridad y disponibilidad con la que los usuarios puedan manejar su información. Debido a esto la arquitectura NGN ofrece la capacidad de convergencia, característica importante para los proveedores de servicios que buscan la satisfacción de sus usuarios con una mínima inversión.

* ReadyNet como empresa proveedora de servicios debe buscar el mejoramiento tecnológico para poder ofrecer a sus clientes servicios multimedia que en la actualidad son de gran demanda. NGN es una opción para este mejoramiento ya que al tratarse de una arquitectura IP los elementos de conectividad de la red de esta empresa pueden acoplarse eficazmente y la inversión disminuiría.

* Del análisis de la infraestructura de ReadyNet se obtuvieron los siguientes resultados:

    - Los enlaces para salida a Internet no son suficientes para el número de usuarios que posee la empresa. En horas pico el tráfico se eleva hasta saturar la capacidad del canal.

Para poder proporcionar un servicio con calidad para los usuarios se debe contratar enlaces de mayor capacidad.

- El tráfico de última milla de igual forma es elevado, ocasionando en algunos instantes el consumo total de la capacidad asociada a estos enlaces.

- En las últimas millas inalámbricas la capacidad del enlace correspondiente a cada empresa es suficiente para el número de usuarios que ocupan esta tecnología. Sin embargo por el alto costo que ésta tiene, únicamente los clientes a los cuales no se tiene acceso con ADSL contratan este servicio, razón por la cual no se puede migrar a otros clientes a estos enlaces para aprovechar la capacidad del canal.

- Los servidores de ReadyNet son levantados en Linux, sistema operativo que es estable, seguro y de licencia libre lo cual hace posible la instalación de paquetes complementarios a los servicios sin costo, además de la fácil actualización del software.

- Los servidores brindan un buen nivel de disponibilidad, sin embargo la utilización de los recursos es alta al igual que el número de usuarios, por estos motivos se necesita más de un equipo para ofrecer los distintos servicios.

* ReadyNet es una empresa con limitaciones, debido a que depende de otras empresas para proveer el servicio de Internet. Estas empresas proveen la última milla lo cual ocasiona que ReadyNet no pueda tener un total control sobre los enlaces de sus clientes.

- En Readynet no se puede aprovechar todas las ventajas que IMS representa como red de nueva generación ya que al ser un ISP que no tiene red de transmisión propia podrá conectarse solo con la

tecnología contratada para el acceso a los clientes siendo en la actualidad ADSL y radio.

- En la actualidad la mayoría de Carriers y empresas con infraestructura de acceso propio se proyectan a una posible migración a redes IP, por lo que se busca que Readynet avance conjuntamente con las nuevas tecnologías que el mercado plantea.

* Cuando se da servicios de convergencia no se necesita convenios con otras empresas, pero se debe considerar que la interacción con la PSTN como lo demanda la comunicación con la telefonía tradicional se dificultaría debido a que la conexión es mediante Andinatel, por lo tanto se necesitaría de la colaboración de esta empresa para poder tener un servicio de telefonía IP completo.

* La mejor opción a considerarse por ReadyNet en cuanto al servicio de IPTV es buscar un proveedor de video, ya que la inversión de una infraestructura para este servicio además de los costos por contenidos son muy elevados y no compensaría al menos en un plazo mediano dicha inversión.

- Para poder proporcionar IPTV la empresa requerirá contratar mayor capacidad de ancho de banda, lo que se debe realizar de manera paulatina, acorde a los usuarios que se incorporen a este servicio.

* El equipo central de la arquitectura NGN es el softswitch, aquí se encuentra la mayoría de elementos funcionales del plano de control. Al invertir en este equipo se considera un gran avance a la migración a NGN.

- La solución de equipos que incorpora el softswitch Cisco no es una opción adecuada para Readynet, porque a pesar que presenta mejores características su uso representaría un

sobredimensionando para una empresa pequeña con pocos usuarios, además que su costo es muy elevado para la empresa.

- En la actualidad varios fabricantes realizan estudios sobre IMS y ofrecen ya una variada gama de equipos para esta arquitectura, entre los fabricantes tenemos a Lucent (Alcatel), Siemens, Nokia, Cisco, Nortel, Microtrol, entre otros, por lo que una empresa ya puede escoger la marca y el modelo que se ajuste a sus necesidades.

* El inicio de la migración de ReadyNet a servicios de nueva generación se puede dar con la adición del softswitch y con una red que en su mayoría soporte velocidad de gigabits y calidad de servicio ya que la multimedia y la voz demandan priorización en la transmisión de la información así como velocidad.

* IMS como solución para ReadyNet es técnicamente factible como parte de una solución mayor de convergencia de las telecomunicaciones, ya que actualmente se busca que un Proveedor de Servicios pueda interactuar con los diferentes tipos de redes.

* Debido al tamaño de la empresa, al número de usuarios que posee y a los ingresos que percibe, IMS económicamente no es una solución viable, ya que generalmente los inversionistas esperan recibir más ganancia con una inversión de la magnitud que representaría la compra de los equipos.

5.2 RECOMENDACIONES

* Un factor de importancia en una red es el cableado, dependiendo de la velocidad de transmisión empleada por los distintos dispositivos éste no debería causar pérdidas ni degradación. Razón por la cual debería mejorarse y etiquetarse debidamente.

* ReadyNet debe buscar métodos para introducirse en el mercado con nuevos servicios, al ser una mediana empresa debe buscar la manera de competir con aquellos proveedores mayoritarios.

* Se debería realizar un estudio de mercado para tener una apreciación más clara acerca de los posibles usuarios de los servicios que una red NGN puede ofrecer.

* El presente proyecto no analiza por completo el proporcionar IPTV por las limitaciones que presenta la empresa, pero en un futuro se pueden realizar nuevos proyectos con las pautas entregadas.

* Establecer convenios con Andinatel para la implementación de Telefonía IP. Ya que es el proveedor de última milla podría brindar un servicio complementario y ayudar a ReadyNet en nuevos proyectos.

* Toda empresa que quiera incursionar en nuevos servicios de valor agregados debe realizar un profundo estudio de mercado y análisis de factibilidad económica para poder competir con las empresas existentes.

* Se recomienda la consideración de la utilización de un equipo UTM para complementar la seguridad de la red, ya que es un dispositivo que a más de prestar servicios de seguridad como IDS/IPS, presenta características de antivirus, antispam, antiphishing y filtro de contenidos.